FORTRA

beSECURE
21.41 (rev: 11.4.6)
User Guide

202302070915

Table of Contents

Welcome

beSECURE performs a security mapping of an organization's network and simulates attacks originating from an internal or external network. Upon completing the security mapping, beSECURE generates a detailed vulnerability report that lists security breaches, as well as practical and easy-to-apply solutions for addressing the vulnerabilities. beSECURE is regularly updated to account for the most recent security vulnerabilities discovered by Beyond Security's R&D team and other organizations.

Customers who implement this service will gain a real-time view of their entire network security topographies, and demonstrate compliance with emerging global IT security standards and integrity legislation.

Contacting Fortra

Please do the following before contacting Fortra for technical support:

- Check this guide's table of contents or search for information that addresses your concern.
- Gather and organize as much information as possible about the problem.

Telephone
Sales/Technical Support: 888-273-1412 X 2 **General**: 952-736-5800 **Fax**: 952-736-5801
Email
Technical Support: support@beyondsecurity.com **Sales**: info@fortra.com
Website
Company: www.fortra.com **Technical Support**: https://beyondsecurity.freshdesk.com/support/home
Available business days: 9:00 AM to 7:00 PM Central Time

System Requirements

Virtual Instance

The minimum resource requirements for a virtual instance of beSECURE, IS/LSS or beSECUREII:

Hardware Component	Minimum Requirements
Processor	8 vCPUs
Memory	16 GB RAM (increase for better performance)
Hard Drive	32 GB available hard disk space

Virtual Machine Software

- VMWare Workstation 12 and above
- VMware ESXi 6 and above
- Azure Compute
- AWS EC2
- Hyper-V (Windows Server 2012 R2 and above)

Web Browser

- Chrome (recommended)
- Microsoft Edge
- Safari
- Firefox
- Opera

> **NOTE:** beSECURE does not support Internet Explorer.

Accessing beSECURE

beSECURE is accessible by way of a supported web browser and a valid username and password (supplied to you by your account manager).

To log into beSECURE:

1. Choose one of the following beSECURE servers, based on your geographical location:
   - US server: https://cloud2.beyondsecurity.com
   - European server: https://cloud3.beyondsecurity.com

   > **NOTE:** If you are unsure of which server address to use, contact Beyond Security Technical Support at support@beyondsecurity.com, or your account manager for login credentials.

2. On the Welcome page, enter your **username** and **password**, and then click **Login**.

IMPORTANT: If three failed log in attempts occur with your username, your account becomes locked and no additional log in attempts can be made for 30 minutes (default). For information on modifying this timer, see ***Creating a Security Profile* on page 68** for information on the **Password Failure Location Duration** parameter.

To log out of beSECURE

To end your beSECURE session and securely log out, click on your username in the top-right corner of the screen, and then select **Logout**.

Home page

The Home page provides an overview of scan results in a dashboard format by way of widgets, and is displayed by default upon logging into beSECURE. To access the Home page from anywhere in beSECURE, click **Home** in the navigation bar.

Managing widgets

beSECURE has several built-in widgets that provide information regarding your beSECURE account. Each widget can display organization, scan, or asset group information in real-time by way of the **Real-time** tab at the top of the Home page, refreshing every 60 seconds. Click the **Fixed** tab to view a snapshot of the last update to the results received for each widget, indicated by the Last Updated date stamp. Once added to the Home page, widgets can be arranged in any order, individually exported as a PNG or CSV file, expanded/compressed, and removed.

To add a widget to the Home page

1. In the bottom-right corner of the Home page, click the Add Widget button .
2. Select a **Category**.
3. If you chose **Organization**, **Scan**, or **Asset Group**, select the desired widget from the available **Charts** or **Informational** widget options, and then click the **Organization** and/or **Scan Name**, or **Asset Group** box(es) to make those corresponding selection (s).
4. Click **Add**.

To move a widget to a different position on the Home page

1. In the upper-right corner of the desired widget window, click the gear icon .
2. Select **Move Left** or **Move Right** to move the widget window in the corresponding direction.
3. Repeat step 2 as needed to achieve the desired position.

To export widget information to PNG or CSV file format

1. In the upper-right corner of the desired widget window, click the gear icon .
2. Select **Save as PNG** to export the scan results as a PNG file, or **Save as CSV** to

export the scan results as a comma-separated values (CSV) formatted file.

3. You can find your exported file in your web browser's current save location.

NOTE: Not all widgets support the PNG or CSV export option.

To remove a widget from the Home page

1. In the upper-right corner of the desired widget window, click the gear icon .
2. Select **Remove**.

Available widgets

The following widgets are available in beSECURE:

Category	Widget name	Widget type	Description
Quick Add	Quick Add	Scanner	Provides the ability to perform a quick scan, based on a cloud provider, IP address, URL, or IP address that requires an SSH connection. For more information on how to configure each tab, see Configuring the Quick Add Widget.

Category	Widget name	Widget type	Description
Organization - Charts	Affected Hosts vs Vulnerabilities	Bubble chart	Displays the Affected Hosts against their respective CVSS (Common Vulnerability Scoring System) Score of the vulnerabilities detected in the selected organization. The CVSS Score is displayed vertically ranging from 1 to 10, with 10 being the most severe. Affected Hosts are displayed horizontally, ranging from 0 to the total number of hosts in the organization. Hover the pointer over each bubble for more information.
	Lowest Score Host(s)	Bar chart	Displays up to five hosts with the lowest scores in the selected organization. The IP address of each host is displayed vertically, and the score of each host is displayed horizontally, ranging from 0 to 100. Hover the pointer over each bar for more information.
	Most Frequent Vulnerabilities	Pie chart	Displays a distribution of the most frequent vulnerabilities in the selected organization. Hover the pointer over each section of the chart for more information.

Category	Widget name	Widget type	Description
	Most Frequent Vulnerability Type	Pie chart	Displays a distribution of the most frequent vulnerability types in the selected organization. Hover the pointer over each section of the chart for more information.
	Most Vulnerable Host (s)	Bar chart	Displays up to four of the most vulnerable hosts in the selected organization. The Medium and High risk vulnerabilities are displayed vertically, ranging 0 to 10, with 10 being the most severe, and the IP address of each host is displayed horizontally. Hover the pointer over each bar for more information.
	Organization Monthly Trend	Line chart	Displays the number of hosts affected per month by Medium and High risk vulnerabilities for the selected organization. The number of Medium or High risk vulnerabilities is displayed vertically, ranging from 0 to the maximum found, and each month reported is displayed horizontally. Hover the pointer over each dot for more information.

Category	Widget name	Widget type	Description
	Organization Quarterly Trend	Bar chart	Displays the number of hosts affected per quarter by Medium and High risk vulnerabilities for the selected organization. The number of Medium or High risk vulnerabilities is displayed vertically, ranging from 0 to the maximum found, and each quarter reported is displayed horizontally. Hover the pointer over each dot for more information.
	Persistent / New / Remediated Vulnerabilities	Bar chart	Displays the Persistent (i.e., vulnerabilities that were remediated but came back or need remediation), New, and Remediated vulnerabilities of the selected organization. The number of vulnerabilities for each category is displayed vertically, ranging from 0 to the maximum number found, and the month/year is displayed horizontally. Hover the pointer over each bar for more information.
	Risk Distribution	Pie chart	Displays the risk distribution of vulnerabilities detected for the selected organization by High, Medium, and Low severities. Hover the pointer over each section of the chart for more information.

Category	Widget name	Widget type	Description
Scan - Charts	Affected Hosts vs Vulnerabilities	Bubble chart	Displays the Affected Hosts against their respective CVSS (Common Vulnerability Scoring System) Score of the vulnerabilities detected in the selected scan. The CVSS Score is displayed vertically ranging from 1 to 10, with 10 being the most severe. Affected Hosts are displayed horizontally, ranging from 0 to the total number of hosts in the scan. Hover the pointer over each bubble for more information.
	Lowest Score Host(s)	Bar chart	Displays up to five hosts with the lowest scores in the selected scan. The IP address of each host is displayed vertically, and the score of each host is displayed horizontally, ranging from 0 to 100. Hover the pointer over each bar for more information.
	Most Vulnerable Host (s)	Bar chart	Displays up to four of the most vulnerable hosts in the selected scan. The Medium and High risk vulnerabilities are displayed vertically, ranging 0 to 10, with 10 being the most severe, and the IP address of each host is displayed horizontally. Hover the pointer over each bar for more information.

Category	Widget name	Widget type	Description
	Risk Distribution	Pie chart	Displays the risk distribution of vulnerabilities detected for the selected scan by High, Medium, and Low severities. Hover the pointer over each section of the chart for more information.
	Score Trend	Line chart	Displays the number of vulnerabilities detected during the same scan over time. The number of vulnerabilities detected is displayed vertically, ranging from 0 to the maximum number found, and the date range is displayed horizontally. Hover the pointer over each dot for more information.
	Vulnerabilities Trend	Line chart	Displays the number of Medium and High risk vulnerabilities detected during the same scan over time. The number of vulnerabilities detected is displayed vertically, ranging from 0 to the maximum number found, and the date range is displayed horizontally. Hover the pointer over each dot for more information.

Category	Widget name	Widget type	Description
Asset Group - Charts	Affected Host Count Trend	Line chart	Displays the number of vulnerabilities detected for the selected asset group over time. The number of vulnerabilities detected is displayed vertically, ranging from 0 to the maximum number found, and the date range is displayed horizontally. Hover the pointer over each dot for more information.
	Affected Hosts vs Vulnerabilities	Bubble chart	Displays the Affected Hosts against their respective CVSS (Common Vulnerability Scoring System) Score of the vulnerabilities detected in the selected asset group. The CVSS Score is displayed vertically ranging from 1 to 10, with 10 being the most severe. Affected Hosts are displayed horizontally, ranging from 0 to the total number of hosts in the asset group. Hover the pointer over each bubble for more information.
	Lowest Score Host(s)	Bar chart	Displays up to five hosts with the lowest scores in the selected asset group. The IP address of each host is displayed vertically, and the score of each host is displayed horizontally, ranging from 0 to 100. Hover the pointer over each bar for more information.

Category	Widget name	Widget type	Description
	Most Vulnerable Host (s)	Bar chart	Displays up to four of the most vulnerable hosts in the selected asset group. The Medium and High risk vulnerabilities are displayed vertically, ranging 0 to 10, with 10 being the most severe, and the IP address of each host is displayed horizontally. Hover the pointer over each bar for more information.
	Risk Distribution	Pie chart	Displays the risk distribution of vulnerabilities detected for the selected asset group by High, Medium, and Low severities. Hover the pointer over each section of the chart for more information.

Category	Widget name	Widget type	Description
Organization/Scan/Asset Group - Informational	Risk Assessment	Varied	Displays the following five widgets: • The Asset Information widget displays the individual and total number of assets for the selected organization, scan, or asset group in Host(s), Safe, and At Risk categories. Asset Types are displayed at the bottom of the widget window. Hover the pointer over the circle chart for more information. • The Categories widget displays the number of assets for the selected organization, scan, or asset group in Compromise (high risk), Imminent Compromise (medium risk), and Hazardous (low risk) categories. Issue Types are displayed at the bottom of the widget window. Hover the pointer over the circle chart for more

Category	Widget name	Widget type	Description
			information. • The Main Categories widget displays the number of vulnerabilities per category for the selected organization, scan, or asset group. Click each category box to display results on the Vulnerability Scan Detailed Results page. • The Main Vulnerabilities widget displays the number of instances found in each of the main vulnerabilities for the selected organization, scan, or asset group. Click each category box to display results on the Vulnerability Scan Detailed Results page. • The Organization Monthly Trend widget displays the trend for Medium and High risk vulnerabilities in an organization for the past 12 months.

Category	Widget name	Widget type	Description
	Main Vulnerabilities	Categories	Displays the number of instances found in each of the main vulnerabilities for the selected organization, scan, or asset group. Click each category box to display results on the Vulnerability Scan Detailed Results page.
	Main Categories	Categories	Displays the number of vulnerabilities per category for the selected organization, scan, or asset group. Click each category box to display results on the Vulnerability Scan Detailed Results page.
	Categories	Circle chart	Displays the number of assets for the selected organization, scan, or asset group in Compromise (high risk), Imminent Compromise (medium risk), and Hazardous (low risk) categories. Issue Types are displayed at the bottom of the widget window. Hover the pointer over the circle chart for more information.
	High / Medium Count	Total counts	Displays the individual and total number of Medium and High risk vulnerabilities found for the selected organization, scan, or asset group.

Category	Widget name	Widget type	Description
	Asset Information	Total counts/circle chart	Displays the individual and total number of assets for the selected organization, scan, or asset group in Host(s), Safe, and At Risk categories. Asset Types are displayed at the bottom of the widget window. Hover the pointer over the circle chart for more information.
	Score	Total counts	Displays the Score of the selected organization, scan, or asset group, based on the total number of Hosts. Host scores range from 0 to 100, where higher scores represent greater security. A score of 0 indicates the host can be easily compromised and a score of 100 indicates a secure host with no Medium or High risk vulnerabilities.

Modes

The **Exec | DevOps** mode toggle at the top of the navigation bar is only available for users with Scanning and Administrator Account Types (users with the Reporting Account Type do not have access to the toggle), and provides the ability to switch between the two permission levels offered in beSECURE:

- **Exec**: Selecting this mode provides access to the Home, Reports, and More menu selections only, limiting the user to mostly scan results and reports. This mode is designed for Reporting users, which is ideal for managers and other decision makers.
- **DevOps**: Selecting this mode provides access to the Home, Scans, Admin, Results, and More menu selections, allowing full access to all of beSECURE's features and settings. This mode is designed for Scanning and Administrator users, which is ideal for system managers.

If you are a Scanning or Administrator in beSECURE, it is recommended to always use the DevOps mode while logged in so that you can access any setting or feature. Selecting the Exec mode provides visibility to what a Reporting user can see and will hide the Scans and Admin menu selections.

Viewing Events

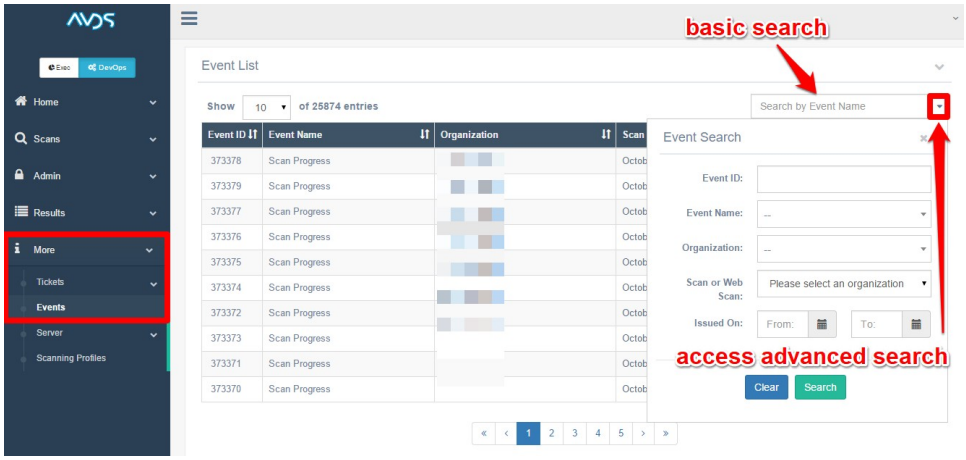
Events are actions a specific Scan Setting entity has taken. For example, events may include “scan complete,” “scan started,” “scan missed its schedule,” and similar actions.

To view events, click **More** > **Events**.

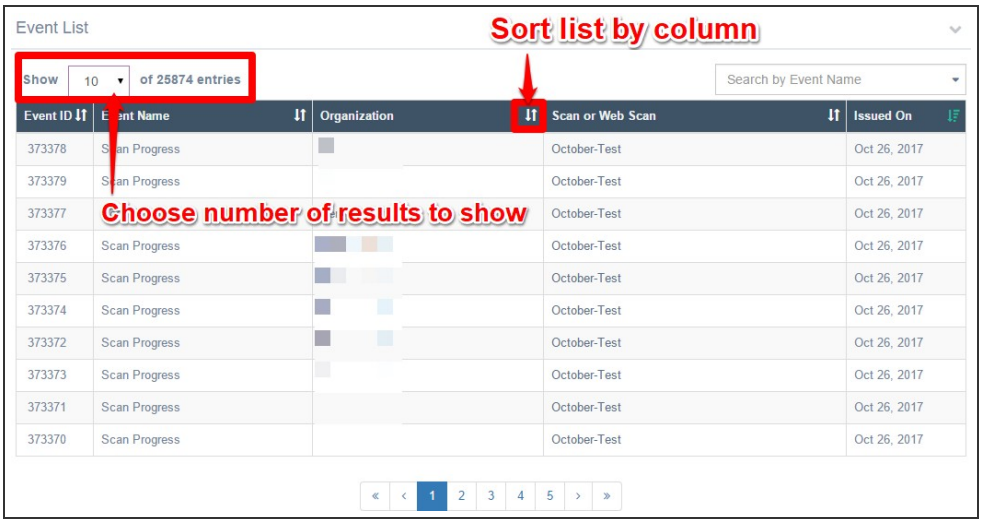
Search for a specific event using the **Search by Event Name** box. By default, the box performs searches by Event Name. To refine the search using additional criteria, click the box and enter information in the **Event ID**, **Organization**, **Scan or Web Scan**, and/or **Issued On date** boxes.

Use the drop-down list above the search results to change the number of results displayed. You can also use the arrows in the column headers to sort the data. To sort by Event Name, for example, click on the arrow icon in the header for that column. Its color will change to green to indicate that the data is sorted on that column. The vertical sequence of lines that appears next to the green arrow indicates whether it is an ascending or descending sort. To toggle the direction of the sort from ascending to descending or vice versa, click on that icon. Use the buttons that appear below the resulting table to page through the search results.

Click on an event to view the event details. The Event Details page displays the Event Name, Additional Information (if any), the Scan Name, and the Issued On date.

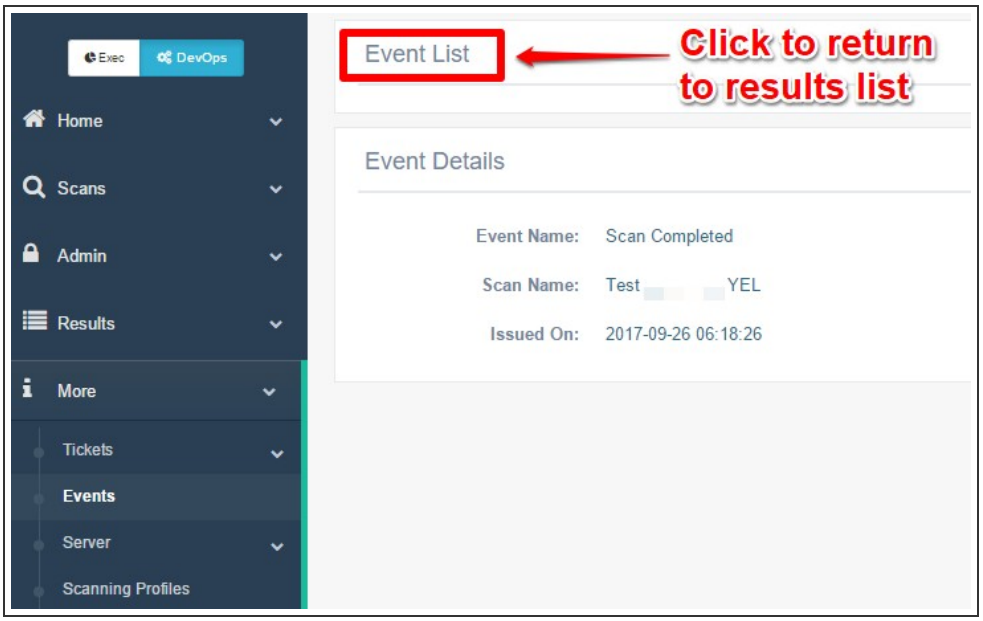


The Event List page.



The Event Details page.

In the example above, the scan completed on September 26, 2017 at 6:18 AM.



System Searches and Results

beSECURE Summary Results provide basic, aggregated information on the vulnerabilities found during a scan. The search parameters involve the Organization, Scan, Vulnerability Name, Category , Hostname / IP Address, Service and Port, Scan Number, Test ID , Summary, Impact, Solution, Output, Risk, CVSS Score, Vulnerability Age, Reference Search, OS Type, Asset Group, Scan Date, & Vulnerability ID. You can also tick the boxes for: Include Previous Scan Results, Show 'None' Risk, Show Unticketed, Show Ignored, & Return Dynamic Output.

You can search with multiple parameters even in the same field by using a comma. It is possible to change the columns that you see in the results using the columns visibility option.

Searches and results are available to all beSECURE system users.

To access searches and results, click **Results** > **Search** in the side navigation pane to open the Vulnerability Search page.

Searching with multiple queries

On the Vulnerability Search page, enter the values in the parameters you want to include in your search. For example, entering values in the Service and Port, Risk, and Vulnerability Age parameters and then clicking **Search** returns results that include those parameters.

Searching by Hostname/IP Address

1. On the Vulnerability Search page, click the Organization box to select your organization.
2. Enter the desired host name or IP address in the **Hostname / IP Address** box.
    a. To query multiple hostnames or IP addresses in a search, separate each with a comma (for example, 192.168.0.100,192.168.0.200).
    b. To query an exact match for a hostname, follow the name with the dollar sign character ($).
3. Click **Search** to perform a search.

Search by reference

1. On the Vulnerability Search page, click the **Reference Search** box and select the desired source.
2. Enter the string you want to query in the empty box to the right.
3. Click **Search** to perform a search.

Search by Asset Group

> **NOTE:** Asset Groups must be created by your organization beforehand. See *To create an Asset Group* under Assets for more information.

1. On the Vulnerability Search page, click the **Asset Group** box and select the desired Asset Group.

   > **NOTE:** Searches can only include one Asset Group.

2. Click **Search** to perform a search.

To save a search

1. After entering the values in the desired parameters, click **Saved Search(es)** in the upper-right corner of the Vulnerability Search page, and then click **Save Current Search**.
   a. To overwrite an existing saved search, click the **Update an existing Saved Search** box.
   b. To create a new saved search, enter the desired name in the Create a new Saved Search box.
2. Click **Save**.

> **NOTE:** Once a result of the search is received, you can download a report of these results in different formats e.g. pdf, xml, HTML, CSV.

Summary Results

beSECURE Summary Results provide basic, aggregated information on the vulnerabilities found during a scan. The reports show the Host(s), Scan Date, Total number of vulnerabilities found, number of High-risk and Medium-Risk vulnerabilities, an overall Score, and a vulnerability Trend indicator for each location associated within organization.

To access Summary Results

1. Click **Results** > **Summary**.
2. Click **Organization** box to select the desired organization to use.

The Vulnerability Scan Summary Results page.

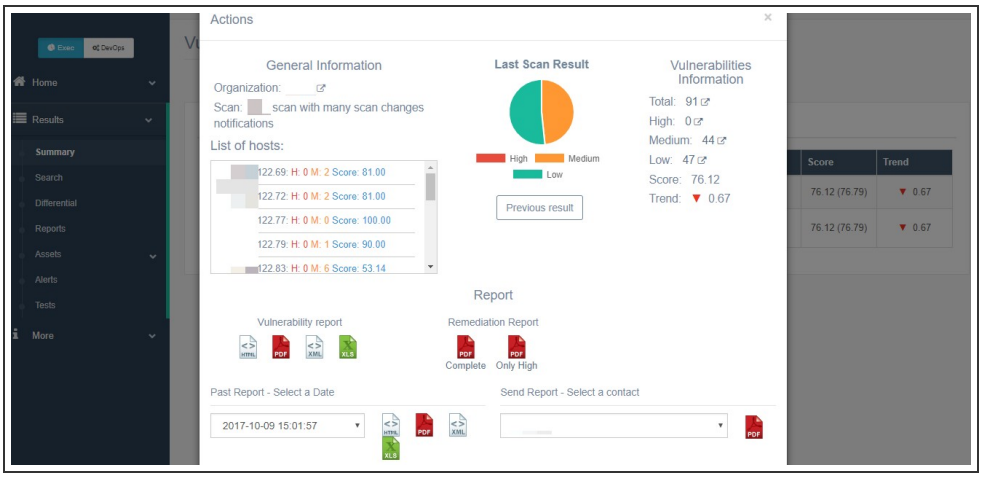
This page displays a hierarchy that shows the structure of the selected organization, as well as the vulnerability information accumulated for each location.

The summary shows up to two levels of an organization hierarchy. The top level is the organization itself (indicated by a green organizational chart icon in the first column). The direct sub–items appear beneath the organization. They are indicated by a scan icon (computer).

The page shows the following information:

Field	Description
Location	The location in the organization's hierarchy.
Host(s)	The number of hosts scanned, with the number of hosts from the previous scan in parentheses. Clicking on the first value in will open the Vulnerability Scan Detailed Results page.
Scan Date	The date of the most recent scan.
Total	The total number of vulnerabilities found. The integer in parentheses is the number of vulnerabilities found in the previous scan.
High	The number of high-risk vulnerabilities found. The integer in parentheses is the number of vulnerabilities found in the previous scan.
Medium	The number of medium-risk vulnerabilities found. The number in parentheses is the number of vulnerabilities found in the previous scan.
Score	The current score for the location on a scale of 0 to 100, with 100 representing the best possible score and a highly secure network. The number in parentheses is the score from the previous scan.
Trend	Indicates whether the target is becoming more or less secure, based on a comparison of the scores for the current and previous scans. An improvement in the Score due to fewer vulnerabilities is indicated by a green, upward-facing arrow. A drop in Score caused by an increase in vulnerabilities is indicated by a red, downward-facing arrow. A stable score is indicated by a yellow circle.

Clicking on a value in the **Location** column will bring up **Actions** window, which provides access to additional information and options for the selected **Location**.



The Actions window.

The General Information section of the Actions window shows the Organization, Scan, a list of hosts scanned, and the score for each host. By default, the Actions window displays the information for the first host in the list. To change the data displayed in the window, click on a different host.

The Last Scan Result section contains a pie chart that visualizes the proportions of high, medium, and low-risk vulnerabilities for the most recent scan of that location. You can compare the chart with the results from the previous scan by clicking the **Previous result** button. The Vulnerabilities Information section displays the same numbers shown on the Vulnerability Scan Summary Results page.

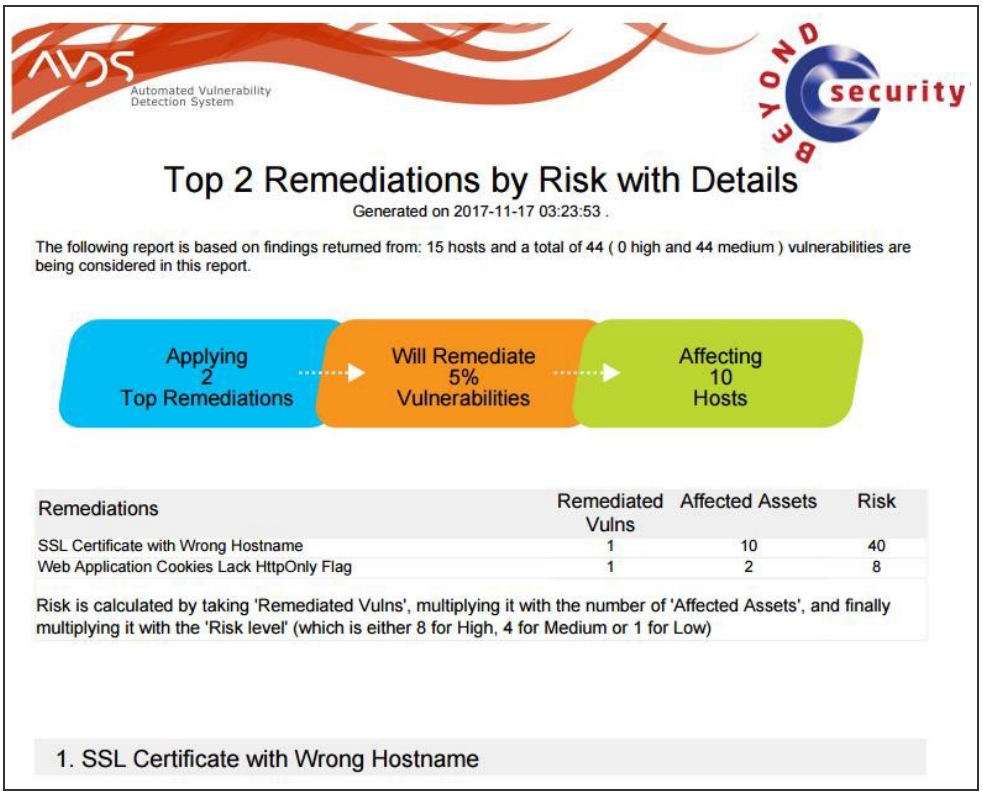
The Report section provides access to downloadable Vulnerability Reports and Remediation Reports. Vulnerability Reports provide details on the vulnerabilities found during a scan. In addition to the raw figures displayed in the Summary Results section of the beSECURE system, the reports also contain additional context, explanatory information, and possible solutions.

A Vulnerability Report in HTML format.

The reports are available in HTML, PDF, XML, and XLS formats. The HTML version of the report can be viewed in any web browser. It will automatically open in your default browser. The PDF version is a printer-friendly report. The third option is an XML machine–readable format that enables you to import the data into third-party reporting software. The XLS format is a Microsoft Excel-compatible CSV file. The XML and CSV formats contain tabular data only. Graphics are not included.

To generate a Vulnerability Report in a downloadable format, click the icon for the format you prefer. The HTML report will open in your browser. The other file formats will download to your machine automatically.

Remediation Reports suggest specific actions that will remediate selected vulnerabilities. For example, the following report suggests two actions that will remediate 5% of the vulnerabilities found during a scan of a particular Location.



A Complete Remediation Report.

Complete Remediation Reports suggest actions that address all types of vulnerabilities.
Only High Remediation Reports suggest actions that address high-risk vulnerabilities only.
These reports are available in PDF format only.

You can also send a report in PDF format to a contact person listed in the beSECUREE system. To do this, select the contact from the drop-down list at the bottom of the window, then click the **PDF** icon to the right.

Click the **Close** button to exit the Actions window.

For more information on reports, see the Reports section of this document.

Searching Vulnerabilities

The **Vulnerability Search** page enables fine–grained searches for specific vulnerabilities.

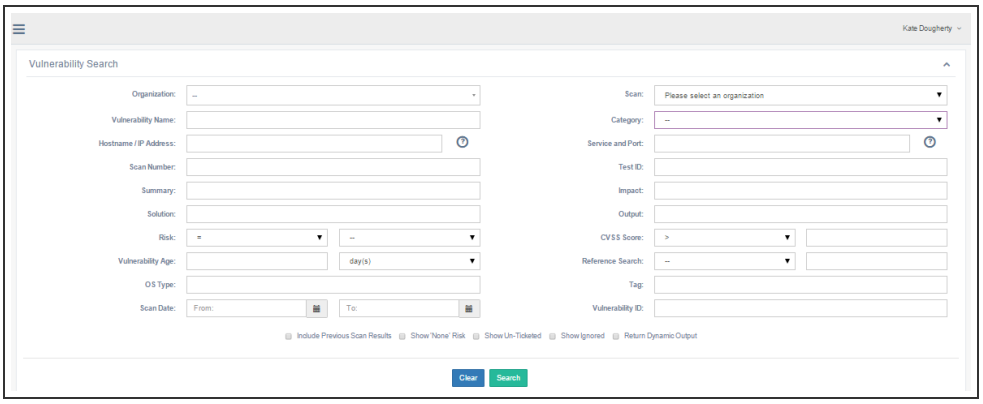
To search for vulnerabilities

1. Click **Results** > **Search**. This page presents the following search options:

Field	Description
Organization	The organization to search for.
Scan	The scan that identified the vulnerabilities. **NOTE:** An organization must be selected first.
Vulnerability Name	Searches for text in the descriptive name for the vulnerability.
Category	The category of vulnerability. beSECURE categorizes vulnerabilities according to their area of impact (web applications, encryption, etc.).
Hostname/IP Address	The hostname or IP address scanned. Use commas to separate multiple values. You can also use a dollar ($) sign to indicate that you want an exact match. By default, he system returns partial matches.
Service and Port	The service and port scanned. Separate the values with commas. For example, entering 80,443 will return the results for port 80 and port 443.
Scan Number	The number assigned to the scan. The Scan Number for the first scan of a target will be 1, the second scan will have the Scan Number 2, and so on.
Test ID	The ID for the beSECURE test that detected the vulnerability during the scan.
Summary	A summarized description of the test beSECURE conducted and the findings it revealed.
Impact	The potential impact of the vulnerability, such as unauthorized access or loss of data.
Solution	Potential solution(s) for resolving the vulnerability.
Output	Evidence that a web scan test was able to detect a vulnerability. This may be the name of a file in a format known to be vulnerable, sensitive information that can only be obtained by using the vulnerability, or some other indication of a vulnerability. **NOTE:** The Return Dynamic Output box must be checked for the Output to be displayed (see below). Output is available for web scans only.

Field	Description
Risk	The level of risk assigned to the vulnerability. The first drop-down list in this field allows users to search for vulnerabilities with a risk level thatis equal to, (=), greater than (>), less than (<), greater than or equal to (>=), or less than or equal to (<=) the risk level selected from the second drop-down list(High, Medium, Low, or None).
CVSS Score	The CVSS score for the vulnerability.
Vulnerability Age	The age of the vulnerability, as an integer. Use the drop-down list to the right of the text field to indicate whether the number entered represents day(s), week(s), or month(s).
Reference Search	Searches for a specified CVE, CERT, CSC (Cisco), or KB (Microsoft Knowledge Base) item.
OS Type	The type of operating system the remote target runs.
Scan Date	Searches scans that fall within a date range. Use the calendar widgets to enter begin and end dates.
Vulnerability ID	The ID for a specific vulnerability.
Include Previous Scan Results	Whether to include results from previous scans.
Show 'None' Risk	Whether to show vulnerabilities that are not associated with a risk level.
Show Un-Ticketed	Whether to show vulnerabilities that aren't associated with a ticket.
Show Ignored	Whether to show vulnerabilities that have been marked Ignore.
Return Dynamic Output	Activates the Output field above. **NOTE:** Output is available for web scans only.

2. Search using one or three parameters:
    a. Vulnerability name - A string search (you can write a part of the name)
    b. Vulnerability ID - for a specific vulnerability on a specific IP/DNS
    c. Test ID - for all the places this vulnerability shows
3. When finished entering search parameters, click the **Search** button. The Vulnerability Scan Detailed Results page appears.



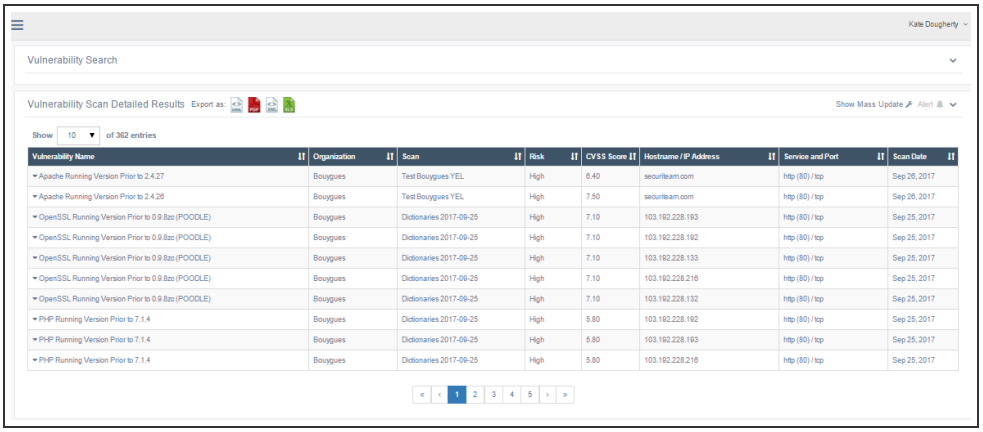
The Vulnerability Search page.

This page displays a list of vulnerabilities that match the search criteria. It presents the following default information about each vulnerability:

Field	Description
Vulnerability Name	A descriptive name for the vulnerability.
Organization	The name of the organization associated with the vulnerability.
Scan	The name of the scan that found the vulnerability.
Risk	The risk level associated with the vulnerability. Values are High, Medium, Low, and None.
CVSS Score	The CVSS Score for the vulnerability.
Hostname/IP Address	The host address or IP address of the affected host.
Service and Port	The service and port affected by the vulnerability. Separate the values with commas. For example, entering 80, 443 will return the results for port 80 and port 443.
Scan Date	The date the scan took place.

Field	Description
Vulnerability ID	
Port	
Service	
Protocol	
Category	
Ticket Status	

Field	Description
Ticket Assigned To	
Ticket State	



The Vulnerability Scan Detailed Results page.

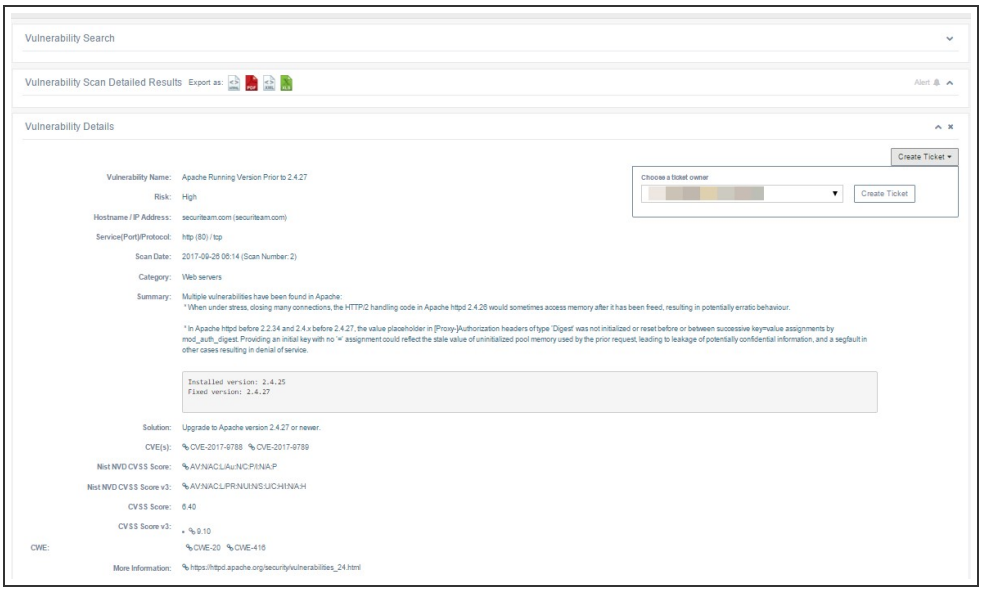
You can export a copy of the list by clicking the icon for the file format you prefer at the top of the page. The list can be exported in HTML, PDF, XML, or XLS format. Click on an entry in the list to view the Vulnerability Details.

Viewing vulnerability details

The Vulnerability Details page shows detailed information about a specific vulnerability and ways to resolve that vulnerability. The system presents the following information on vulnerabilities:

Field	Description
Vulnerability Name	A descriptive name for the vulnerability.
Risk	The risk level associated with the vulnerability. Values are High, Medium, Low, and None.
Hostname / IP Address	The host address or IP address of the affected host.
Service (Port) Protocol	The affected scan setting service, composed of the service name, port number, and scan setting protocol.
Scan Date	The date and time the scan took place.
Category	The category of vulnerability. beSECURE categorizes vulnerabilities according to their area of impact (web applications, encryption, etc.).

Field	Description
Summary	A summary of the vulnerability that gives extended details about the vulnerability, the affected products, and if possible, ways to recreate the situation caused by the vulnerability.
Solution	Potential solution(s) for resolving the vulnerability.
CVE(s)	The Common Vulnerabilities and Exposures (CVE) ID number for the vulnerability. Click on the value to view details about the CVE at NIST.gov.
Nist NVD CVSS Score	The CVSS severity score for the vulnerability. The CVSS is an independent system that scores vulnerabilities on a scale from 1 to 10. A score of 10 indicates a critical vulnerability, while 0 represents negligible risk.
Nist NVD CVSS Score v3	The severity score for the vulnerability on the updated CVSS Score v3 scale. Click on the value to view details about the CVE at NIST.gov.
CWE	The Common Weakness Enumeration ID for the vulnerability. CWE is an industry standard for indicating vulnerability type.
More Information	Provides links to external websites that contain further information about the vulnerability, including the CVE, Microsoft's knowledge base, and securiteam.com.
Test ID	The ID for the beSECURE test that detected the vulnerability during the scan.
Vulnerability ID	The ID for the vulnerability.
Vulnerability Age	The age of the vulnerability, as the number of days that have elapsed between the first and last time beSECURE detected it.



The Vulnerability Details page.

Vulnerabilities are categorized by three main risk levels. High-risk vulnerabilities can allow an attacker to gain elevated privileges on a vulnerable machine, and should be addressed as top priority. Medium- risk vulnerabilities are weaknesses that either expose sensitive data to an attacker or facilitate a denial of service. Low-risk vulnerabilities allow preliminary information–gathering for an attacker, or pose risks that are not entirely security-related. Security policies are considered low-risk. The system categorizes results that pose no security threat but show interesting information about the target as None.

The Vulnerability Details page also provides access to ticketing functionality. If a ticket does not exist for a vulnerability, you may create one by clicking on the **Create Ticket** button. If there is an existing ticket for a vulnerability, a **View Ticket** button will appear instead. For more information, see Tickets.

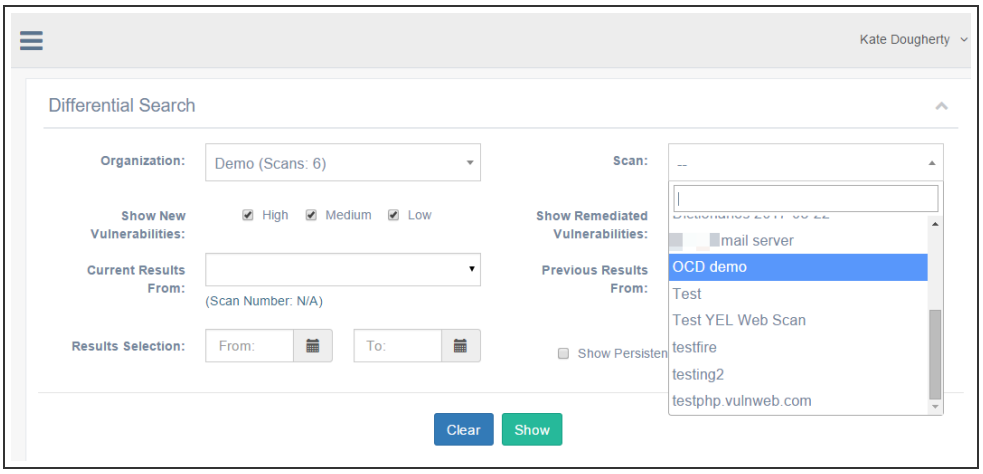
Differential Search

Differential reports allow you to monitor changes between two scan events for an organization. This functionality allows you to track performance in terms of:

- The actions taken to address vulnerabilities
- The amount of time that elapses before vulnerabilities are addressed

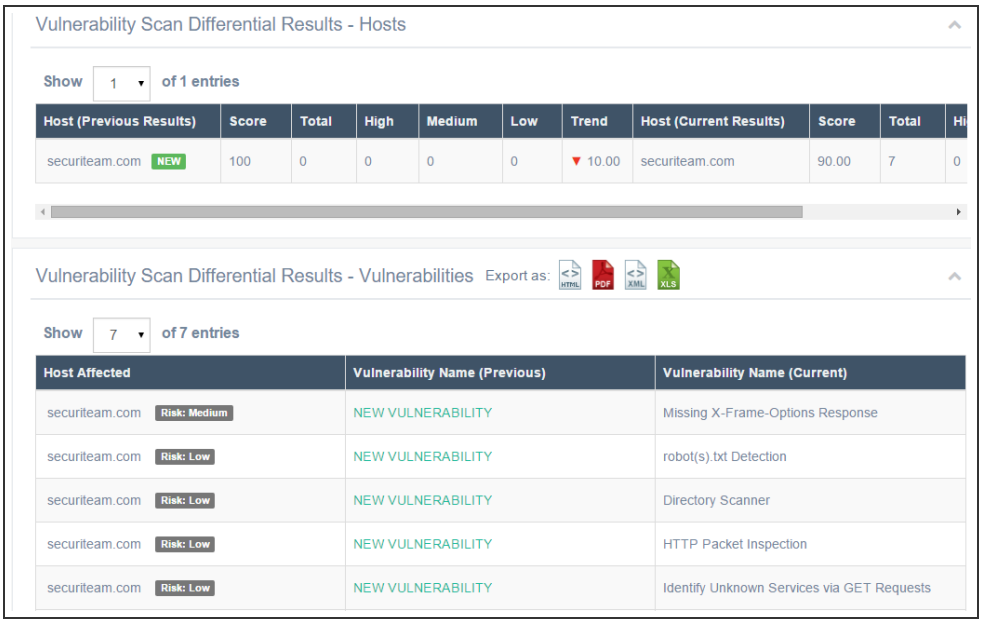
To run a differential search

1. Click **Results** > **Differential** in the sidebar.
2. Fill out the following search fields (from left to right):
    a. Choose your Organization from the drop-down list. The number of saved scans available appears in parentheses next to the Organization name. The Scan field on the right will populate with the available scans for that Organization.
    b. Choose a Scan from the drop-down list.
    c. The **High**, **Medium**, and **Low** boxes for the Show New Vulnerabilities field are selected by default. Disable if desired.
    d. The **High**, **Medium**, and **Low** boxes for the Show Remediated Vulnerabilities field are selected by default. Disable if desired.
    e. In the Current Results From field, select the date of a recently run scan.
    f. In the Previous Results From field, select the date of an earlier scan.
    g. In the Results Selection field, choose a date range to narrow the results to a shorter period between the scan dates you selected in steps e and f above.
    h. Check the checkbox for Show Persistent Vulnerabilities, if desired.
    i. Check the checkbox for Show Open Ports, if desired.
    j. Click the Show button to view the results, or the Clear button to start over.



The Differential Search page.

The results screen shows results by Host and results by Vulnerability.



The Differential Search results page.

The Vulnerability Scan Differential Results – Hosts section displays the following information:

Field	Description
Host (Previous Results)	The host scanned during the previous scan.
Score	The host's overall score.
Total	The total number of vulnerabilities found.
High	The number of high-risk vulnerabilities found.
Medium	The number of medium-risk vulnerabilities found.
Low	The number of low-risk vulnerabilities found.
Trend	Indicates whether the target is becoming more or less secure, based on a comparison of the Scores for the current and previous scans.
Host (Current Results)	The host scanned during the current scan.
Score	The host's overall score.
Total	The total number of vulnerabilities found.
High	The number of high-risk vulnerabilities found.

Field	Description
Medium	The number of medium-risk vulnerabilities found.
Low	The number of low-risk vulnerabilities found.

In the image below, for example, secureiteam.com was the host or target in the previous and current scans. The previous results show a perfect overall score of 100, with no vulnerabilities found. In the current results, however, beSECURE found a total of seven vulnerabilities, and the host's overall score fell to 90. The Trend column reflects this 10-point drop. For more information on how beSECURE calculates scores, see the Scoring section of this document.

The Hosts section of the Vulnerability Scan Differential Results page.

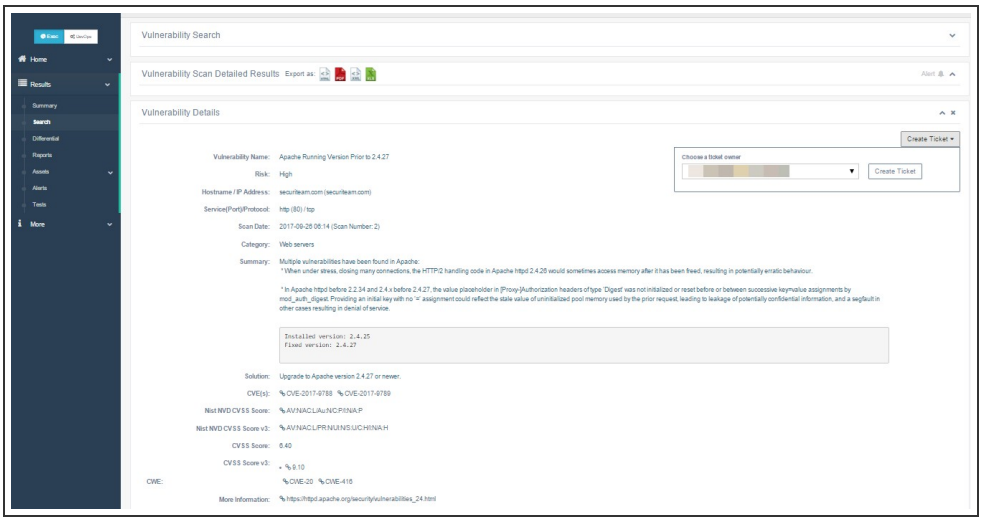
The Vulnerability Scan Differential Results – Vulnerabilities section displays the following information:

Field	Description
Host Affected	The host scanned. A label for the vulnerability risk for the host appears next to the host name.
Vulnerability Name (Previous)	A descriptive name for the vulnerability found in the previous scan. The value "New Vulnerability" will appear if the vulnerability was not discovered in the previous scan. The value "Remediated" will appear if a vulnerability discovered during a previous scan does not appear in the current scan.
Vulnerability Name (Current)	A descriptive name for the vulnerability found in the current scan.

To export the results in HTML, PDF, XML, or XLS format, click the icon for the format that appears above the results table.

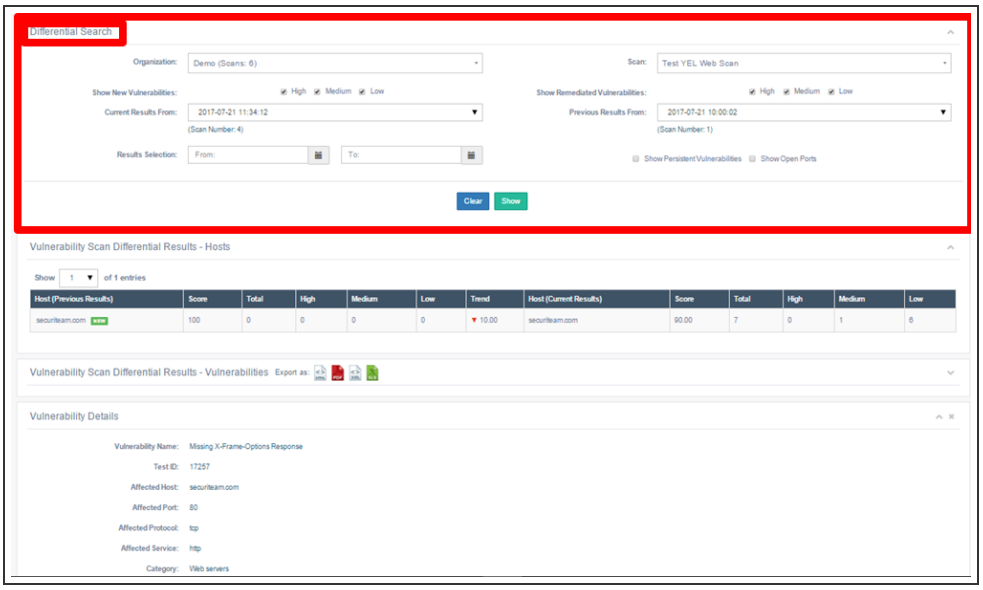
The Vulnerabilities section of the Vulnerability Scan Differential Results page.

Click on a row to view the vulnerability details.



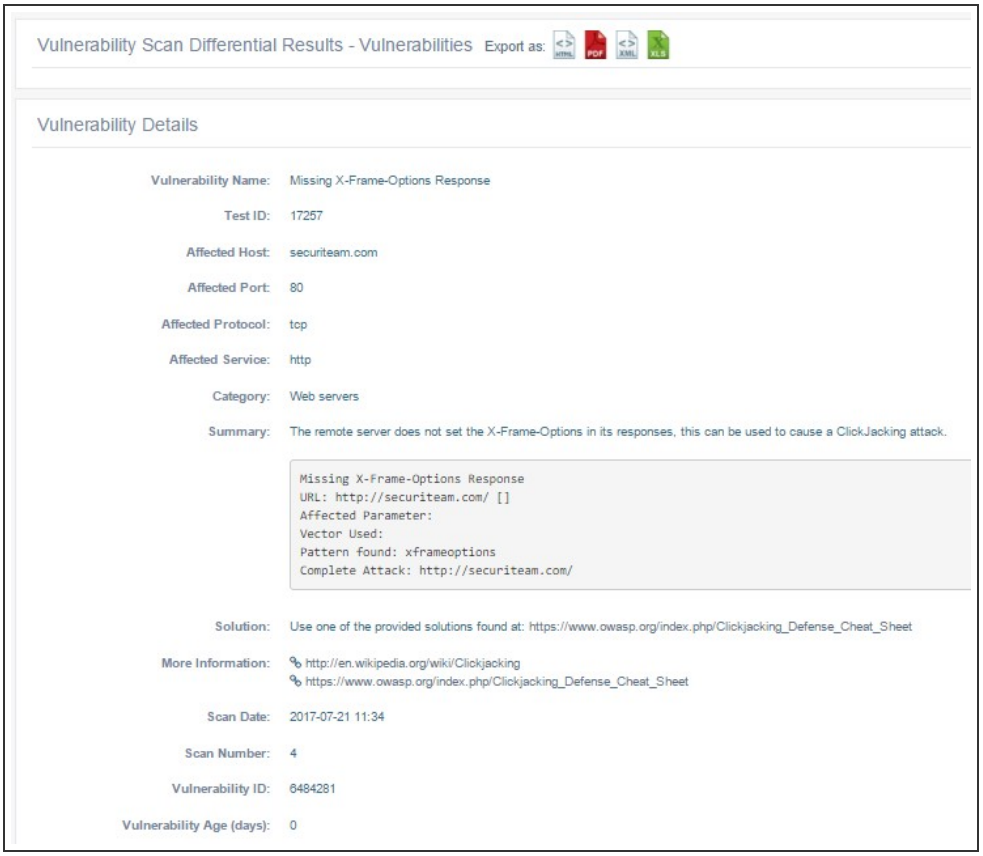
The Vulnerability Details page.

The links at the top of the page provide access other areas of the Differential Results section within the same page. For example, clicking Vulnerability Scan Differential Results – Hosts will open a panel containing the Host results. Clicking **Differential Search** will open another panel containing the search interface, so you can run another Differential Search within the same page.



The Vulnerability Scan Differential Results page, with the Differential Search panel expanded.

Click on a result to see the vulnerability details.



The Vulnerability Details page.

The Vulnerability Details page displays the following information:

Field	Description
Vulnerability Name	The name of the vulnerability.
Test ID	The ID for the beSECURE test that detected the vulnerability during the scan.
Affected Host	The host scanned.
Affected Port	The affected port.
Affected Protocol	The affected protocol (for example, tcp).
Affected Service	The affected service (for example, http).
Category	The category the vulnerability falls under.
Summary	A descriptive summary of the vulnerability.
Solution	Provides suggestions for how to address the vulnerability.
More Information	Links to more information about the vulnerability.
Scan Date	The date of the scan.
Scan Number	The number assigned to the scan. The Scan Number for the first scan of a target will be 1, the second scan will have the Scan Number 2, and so on.
Vulnerability ID	The ID for the vulnerability.
Vulnerability Age (days)	The age of the vulnerability, as the number of days that have elapsed between the first and last time it was detected.

Scoring

The beSECURE system scores vulnerabilities, assets, networks, and organizations. The vulnerability score is based on the severity of the vulnerability. The asset score is based on the asset. Finally, the organization score is based on the average score for all of the networks under an organization.

Vulnerability Score

beSECURE calculates a vulnerability's score based on its risk factor (High, Medium or Low), as well as the Common Vulnerability Scoring System (CVSS). The CVSS numeric base scores represent the innate characteristics of each vulnerability.

While the CVSS also uses categorical Low, Medium, and High severity rankings, these qualitative rankings are simply mapped from the numeric CVSS scores:

- Low severity – A vulnerability with a CVSS base score of 0.0-3.9.
- Medium severity– A vulnerability with a base CVSS score of 4.0-6.9.
- High severity – A vulnerability with a CVSS base score of 7.0-10.0.

In certain cases, some of the information typically used to generate CVSS scores may be unavailable. This typically happens when a vendor announces a vulnerability but declines to provide certain details. When this occurs, Beyond Security's analysts will assign CVSS scores based on the information available.

CVSS Vector Definitions

beSECURE also provides a vector describing the components used to calculate the CVSS score. This provides users of the score confidence in its correctness and insight into the nature of the vulnerability.

CVSS vectors always include base metrics and may contain temporal metrics. See the Common Vulnerability Scoring System User Guide for detailed descriptions of CVSS metrics and their possible values.

CVSS Base Vectors

CVSS vectors containing only base metrics take the following form: (AV:[R,L]/AC:[H,L]/Au:[R,NR]/C:[N,P,C]/I:[N,P,C]/A:[N,P,C]/B:[N,C,I,A])

The letters in brackets represent the possible values of a CVSS metric. One option is chosen for each set of brackets. Letters outside the brackets are mandatory and must be included in a valid CVSS vector. Each letter or pair of letters is an abbreviation for a metric or metric value within CVSS. The abbreviations are defined as follows.

- Example 1: (AV:L/AC:H/Au:NR/C:N/I:P/A:C/B:C)
- Example 2: (AV:R/AC:L/Au:R/C:C/I:N/A:P/B:N)

Metric	Possible Values
AV = AccessVector (Related exploit range)	• R = Remote • L = Local
AC = AccessComplexity (Required attack complexity)	• H = High • L = Low

Metric	Possible Values
Au = Authentication (Level of authentication needed to exploit)	• R = Required • NR = Not Required
C = ConfImpact (Confidentiality impact)	• N = None • P = Partial • C = Complete
I = IntegImpact (Integrity impact)	• N = None • P = Partial • C = Complete
A = AvailImpact (Availability impact)	• N = None • P = Partial • C = Complete
B = ImpactBias (Impact value weighting)	• N = Normal • C = Confidentiality • I = Integrity • A = Availability

CVSS Temporal Vectors

CVSS vectors containing temporal metrics are formed by appending the temporal metrics to the base vector. The temporal metrics appended to the base vector take the following form:

/E:[U,P,F,H]/RL:[O,T,W,U]/RC:[U,Uc,C]

- Example 1: (AV:L/AC:H/Au:NR/C:N/I:P/A:C/B:C/E:U/RL:O/RC:U)
- Example 2: (AV:R/AC:L/Au:R/C:C/I:N/A:P/B:N/E:P/RL:T/RC:Uc)

Metric	Possible Values
E = Exploitability (Availability of exploit)	• U = Unproven • P = Proof-of-concept • F = Functional • H = High

Metric	Possible Values
RL = RemediationLevel (Type of fix available)	• O = Official-fix • T = Temporary-fix • W = Workaround • U = Unavailable
RC = ReportConfidence (Level of verification that the vulnerability exists)	• U = Unconfirmed • Uc = Uncorroborated • C = Confirmed

beSECURE provides links to the NVD CVSS calculator by creating a hyperlink that includes the CVSS vector. This works for both base and temporal vectors. The hyperlinks take the following form.

- Example base vector hyperlink to CVSS calculator: http://nvd.nist.gov/cvss.cfm?vector=(AV:L/AC:H/Au:NR/C:N/I:P/A:C/B:C)
- Example temporal vector hyperlink to CVSS calculator: http://nvd.nist.gov/cvss.cfm?vector=(AV:L/AC:H/Au:NR/C:N/I:P/A:C/B:C/E:U/RL:O/RC:U)

Host Score

Host scores range from 0 to 100, where higher values represent greater security. A score of 0 indicates that the host can be easily compromised, while a value of 100 indicates a secure host with no High or Medium risk vulnerabilities.

The score for a host or asset is determined by summing the scores for all of the vulnerabilities present on the host, and then averaging them. High, Medium, and Low risk vulnerabilities are weighted differently. More weight is applied to High risk vulnerabilities, while Low risk vulnerabilities have no weight. Weighting is done according to the following calculation:

$$hostscore = (\frac{1}{2})^{(numberofhigh)} * (\frac{9}{10})^{(numberofmedium)}$$

Network Score

The score for a network or group of assets is determined by averaging all of the scores for the hosts present. A weight is added to each group of hosts. This allows you to assign certain hosts greater importance than others. The added weight can help beSECURE users

decrease the importance of certain hosts (such as printers) when calculating the overall score for a network or group of assets while assigning greater importance to other hosts, such as production servers. The network score is calculated in the following way:

$$\frac{\Sigma\left(\frac{(averagescore) * (hostcount)}{(101 - weight)}\right)}{\Sigma\left(\frac{(hostcount)}{(101 - weight)}\right)}$$

In the equation above, host weights are averaged together. The higher the weight, the larger the influence on the network score. Assigning a group of hosts a weight of 1 or even 0 (zero) will make their influence unnoticeable or ignored, respectively.

Organization Score

An organization's score is based on the recursive average of the scores for all of the scans/networks that fall under it. If an organization has sub-organizations, beSECURE will also include their scores in its averaging algorithm.

Reports

While beSECURE reports are available from various areas of the Results menu, the Reports sub-area serves as a central location for generating and viewing custom reports.

Viewing Reports

To view previously requested reports:

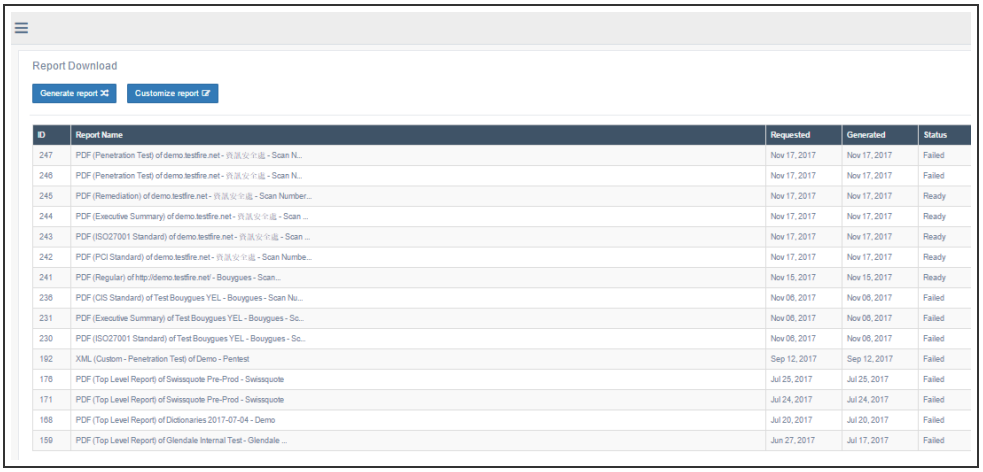
1. From the home page, click **Results** > **Reports**.

A list of previously generated reports will appear (if any). The list shows the following information about each report:

Field	Description
ID	An ID for the report.
Report Name	A descriptive name for the report.
Requested	The date the report was requested.
Generated	The date the report was generated.
Status	The status of the report. Values are Queued, Ready, and Unviewed.

Hovering over an entry will cause a window with more information to appear.

If the Status of the report is Ready, clicking on the report will cause it to open in a browser, or download to your machine.



The Reports page.

Generating Reports

To generate a report:

1. Go to **Results** > **Reports**. A list of previously generated reports will appear (if any).
2. Click **Generate Report**.
3. Complete the form that appears. The form has the following fields:

Field	Description
Organization (required)	The organization to scan.
Scan	The previously run scan to report on.
Scan Date	The date and time the scan occurred.
Report Type (required)	The type of report to create (Executive Summary, HIPAA, etc.). Default is Regular.
Hide Host Information Section	Whether to hide the Host Information section of the report, which contains port scan results, data on the scan process, and other information that is not related to vulnerabilities.

4. Click the **Generate** button. The report request will enter the queue. Reports are typically generated within five minutes.

Customizing Reports

beSECURE allows users to control the information that appears in a report.

To customize a report:

1. Go to **Results** > **Reports**. A list of previously generated reports will appear (if any).
2. Click the **Customize Report**. The customize report window will open.

3. Complete the form that appears. The form has the following fields:

Field	Description
Customization Name	A name for the customization.
Report Name	The name of the report.
Format (required)	The output format for the report. Values are PDF (default) and XML.
Report Type	The type of report to create. Values are Complete (default), Filtered, and Differential.
Report Style (required)	The style of report to create (Executive Summary, HIPAA,etc.) Default is Regular.
Hide Host Information Section	Whether to hide the Host Information section of the report.

4. Click the **Modify** button to save the changes.

To delete the report customization entirely, click the **Delete** button.

Assets

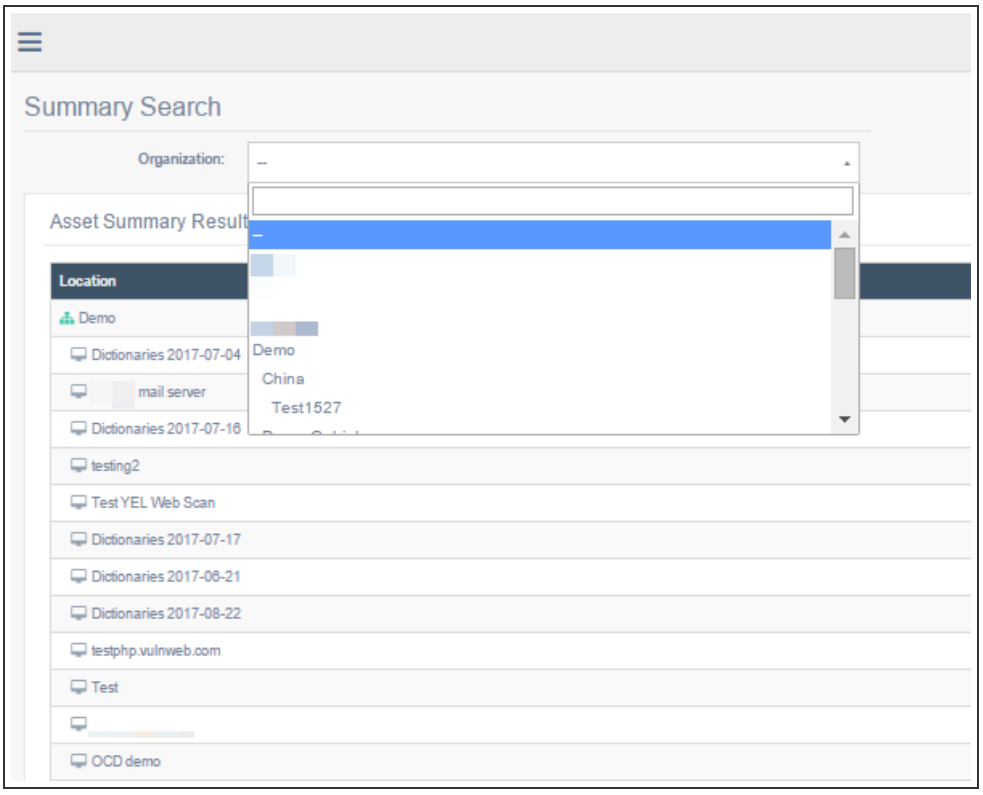
Assets are hostnames or IP addresses. Asset groups are used as a filtration option. An asset group can be created using hosts from multiple scans or from the same scan.

An Asset represents the hostname or IP address entered into beSECURE. Each asset is assigned a value to represent its the hostname or IP address has on the score for the network that contains the asset, as well as the score of the Organization containing the Network.

By default, all assets are given a Value of Normal. However, changing the Value assigned to an asset gives you greater control over weighting and scores. Valid Values range from 0 (Ignore) to 100 (High). A value of Normal represents the median value of 50, and gives no special weight to the host in question.

To view Assets

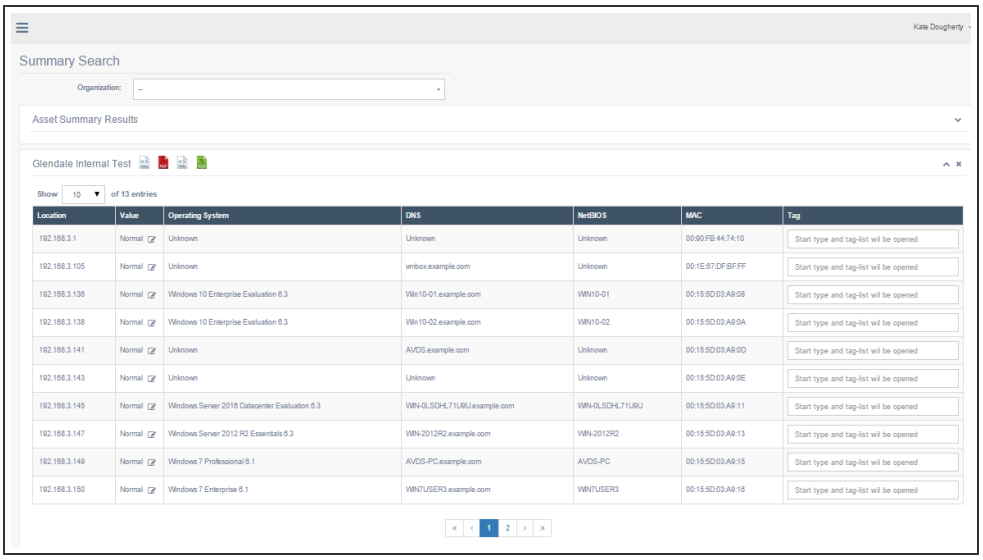
1. Click **Results** > **Assets**.
2. Click **Summary**.



The Asset Summary page.

3. To filter the list, choose an organization from the drop-down list at the top of the page. You may also use the navigation buttons at the bottom to page through the list. Click on an entry to view its details.

The Asset Summary Results page appears. This page shows the Location, Value, Operating System, DNS, NetBIOS name, MAC, and tag for each asset. To export this information, click the icon for the output format you prefer. Results can be exported as HTML, PDF, XML, or XLS files.



The Asset Summary Results page.

All of the assets in the image above have the default Value of Normal. They affect the Network and Organization score equally.

To change the Value for an asset in order to adjust its weight in the scoring process, click the edit icon that appears next to the Value, and then choose a new Value from the box.

The Assets Search page allows you to locate a specific asset more efficiently. To search assets:

1. Click **Results** > **Assets** > **Search**.
2. Enter search parameters. The Assets Search page contains the following fields:

Field	Description
Organization	The organization associated with the asset.
Scan	The scan associated with the asset. Note: An organization must be selected first.
Hostname/IP Address	The name or IP address range for the host scanned.
Operating System	Filters by the target's operating system.
DNS	The FQDN or Internet Host name of the target.
NetBIOS	The NetBIOS name.
MAC	The hardware address of the target machine.
Recursively	Whether to search recursively. While a standard search occurs at the main organization level, a recursive search examines the selected organization and all of the sub-organizations under it.
Hide No-Results	Whether to hide targets with no vulnerabilities.

3. Click the **Search** button.

Alerts

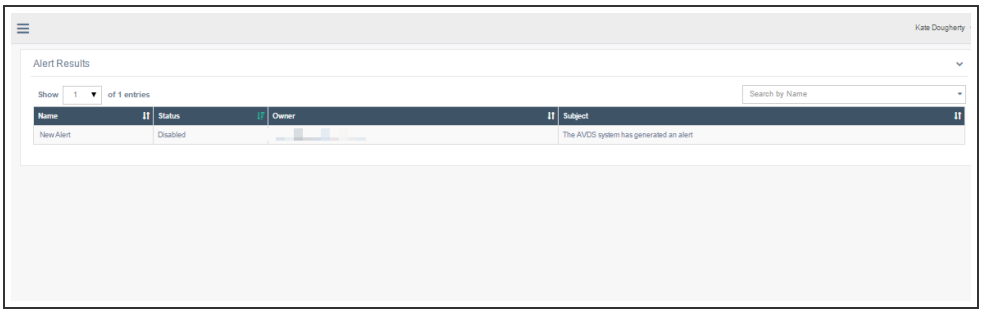
An alert is a user-defined search that triggers an email to the user when it returns results. For example, an alert might send an email whenever a high-risk vulnerability is found. The alerts area of the beSECURE system displays a list of alerts the system has generated.

To access alerts:

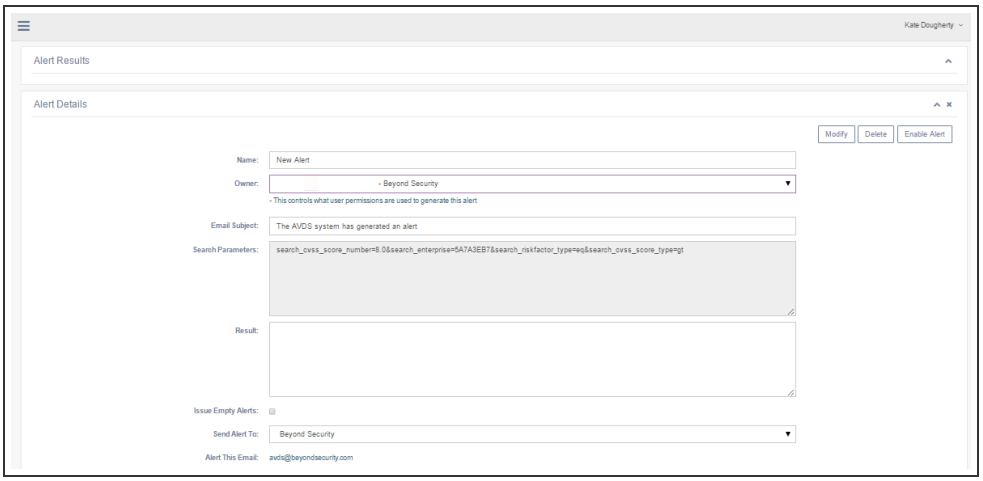
1. Click **Results** > **Alerts**. The list of system-generated alerts shows the following information about each alert:

Field	Description
Name	The name of the alert.
Status	The status of the alert. Values are Disabled and Enabled
Owner	The user who owns the alert.
Subject	The subject of the email message that was sent to the contact person.

2. Click on an alert to see the alert details



The Alert Results page.



The Alert Details page.

The Alert Details page displays the following information:

Field	Description
Name	The name of the alert.
Owner	The user who owns the alert.
Email Subject	The subject of the email message that will be sent to the contact person.
Search Parameters	The search parameters that should generate the alert.
Result	The results of a "test run" of the alert. This information is useful for debugging.
Issue Empty Alerts	Whether to issue empty alerts to indicate that no results were found.
Send Alert To	The contact person the alert should be sent to.
Alert This Email	The email address the alert should be sent to.

To modify the alert, edit the form fields, then click **Modify**.

To delete the alert, click **Delete**.

To enable the alert, click **Enable Alert**.

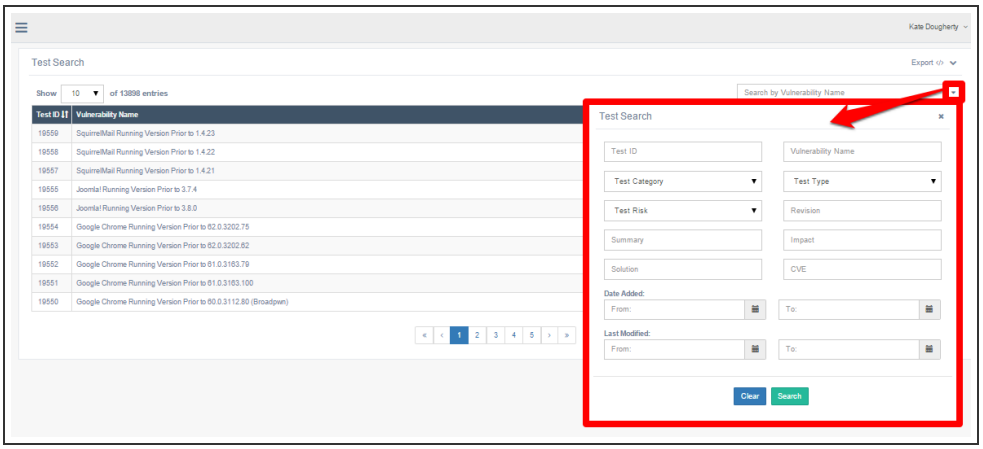
Tests

Each beSECURE scan runs multiple Tests designed to detect vulnerabilities. The Tests area of the beSECURE system provides an overview of the Tests included in a scan.

To access Tests:

1. Click **Results** > **Tests**. The Test Search page provides the following information about each test:

Field	Description
Test ID	The ID for the test that detected the vulnerability.
Vulnerability Name	A descriptive name for the vulnerability.
Test Category	The category the test falls into. Each category is designed to detect different types of vulnerabilities.
Test Risk	The vulnerability risk level the test is designed to detect. Values are None, Low, Medium, and High.
Date Added	The date the test was added.
Last Modified	The date the test was last modified.



2. Use the search box to search for a test by Vulnerability Name, or click the arrow in the search box to open the advanced search options. The advanced search allows you to retrieve tests based on the following fields:

Field	Description
Test ID	The ID for the test.

Field	Description
Vulnerability Name	Searches for text in the descriptive name for the vulnerability.
Test Category	The category the test falls into. Each category is designed to detect different types of vulnerabilities.
Test Type	The type of test. Values are Attack, DoS (denial ofservice), Informational (data-gathering only; do not uncover vulnerabilities), and Scanner(configure how the scanner preforms the scan in terms of speed, authentication usage, web scanning settings, etc.).
Test Risk	The vulnerability Risk level the test is designed to detect. Values are None, Low, Medium, and High.
Revision	The version of the test (for example, “1stgeneration,” “2ndgeneration,” etc.).
Summary	A summarized description of the test and the findings it revealed.
Impact	The potential impact of the vulnerability, such as unauthorized access or loss of data.
Solution	Potential solution(s) for resolving the vulnerability.
CVE	The Common Vulnerabilities and Exposures (CVE) ID number for the vulnerability.
Date Added	The date the test was added.
Last Modified	The date the test was last modified.

Click on a result to see the vulnerability details associated with the test. For more information on the details the system provides, see the ***Viewing vulnerability details* on page 29** section of this document.

Test Details table

Field	Description
Vulnerability Name	A descriptive name for the vulnerability.
Risk	The risk level associated with the vulnerability. Values are High, Medium, Low, and None.

Field	Description
Hostname / IP Address	The host address or IP address of the affected host.
Service (Port) Protocol	The affected scan setting service, composed of the service name, port number, and scan setting protocol.
Scan Date	The date and time the scan took place.
Category	The category of vulnerability. beSECURE categorizes vulnerabilities according to their area of impact (web applications, encryption, etc.).
Summary	A summary of the vulnerability that gives extended details about the vulnerability, the affected products, and if possible, ways to recreate the situation caused by the vulnerability.
Solution	Potential solution(s) for resolving the vulnerability.
CVE(s)	The Common Vulnerabilities and Exposures (CVE) ID number for the vulnerability. Click on the value to view details about the CVE at NIST.gov.
Nist NVD CVSS Score	The CVSS severity score for the vulnerability. The CVSS is an independent system that scores vulnerabilities on a scale from 1 to 10. A score of 10 indicates a critical vulnerability, while 0 represents negligible risk.
Nist NVD CVSS Score v3	The severity score for the vulnerability on the updated CVSS Score v3 scale. Click on the value to view details about the CVE at NIST.gov.
CWE	The Common Weakness Enumeration ID for the vulnerability. CWE is an industry standard for indicating vulnerability type.
More Information	Provides links to external websites that contain further information about the vulnerability, including the CVE, Microsoft's knowledge base, and securiteam.com.
Test ID	The ID for the beSECURE test that detected the vulnerability during the scan.
Vulnerability ID	The ID for the vulnerability.
Vulnerability Age	The age of the vulnerability, as the number of days that have elapsed between the first and last time beSECURE detected it.

Tickets

A vulnerability may be assigned a ticket. Unlike vulnerabilities, tickets are actionable items. Tickets allow all system users to track the course of action taken to eliminate a vulnerability. Users can update the status of a ticket, change a ticket's due date, add comments, and more through the tickets area.

Viewing Tickets

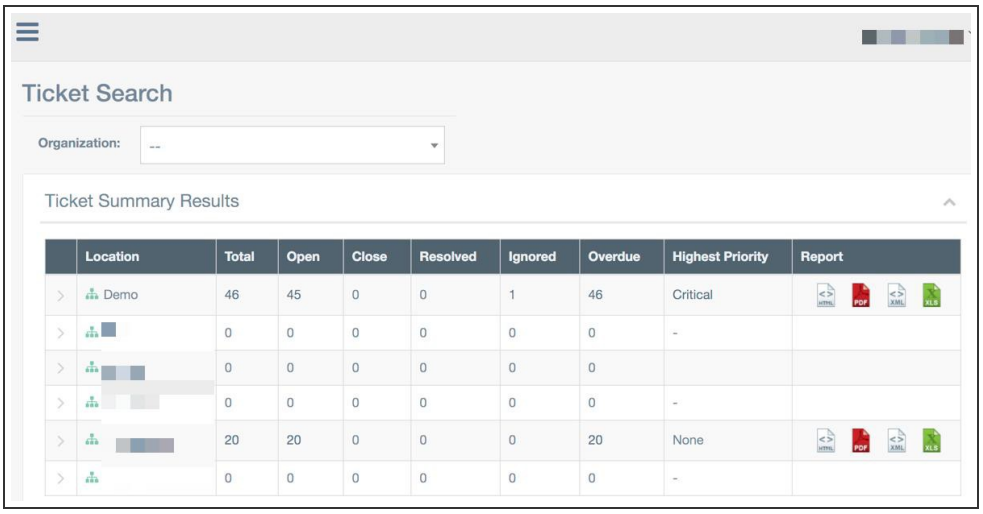
To view tickets:

1. Click **More** > **Tickets**.
2. Click **Summary**.

By default, the Ticket Summary page displays information for all organizations. To display the tickets for a specific organization, select an organization from the drop-down list at the top of the page.

The results show the following information for each organization:

Field	Description
Location	The organization, scan, or host.
Total	The total number of tickets.
Open	The number of open tickets.
Close	The number of closed tickets.
Resolved	The number of resolved tickets.
Ignored	The number of ignored tickets.
Overdue	The number of overdue tickets.
Highest Priority	The priority level of the highest-priority ticket.
Report	Contains icons for downloading a summary report in HTML, PDF, XML, or XLS format.



The Ticket Summary page.

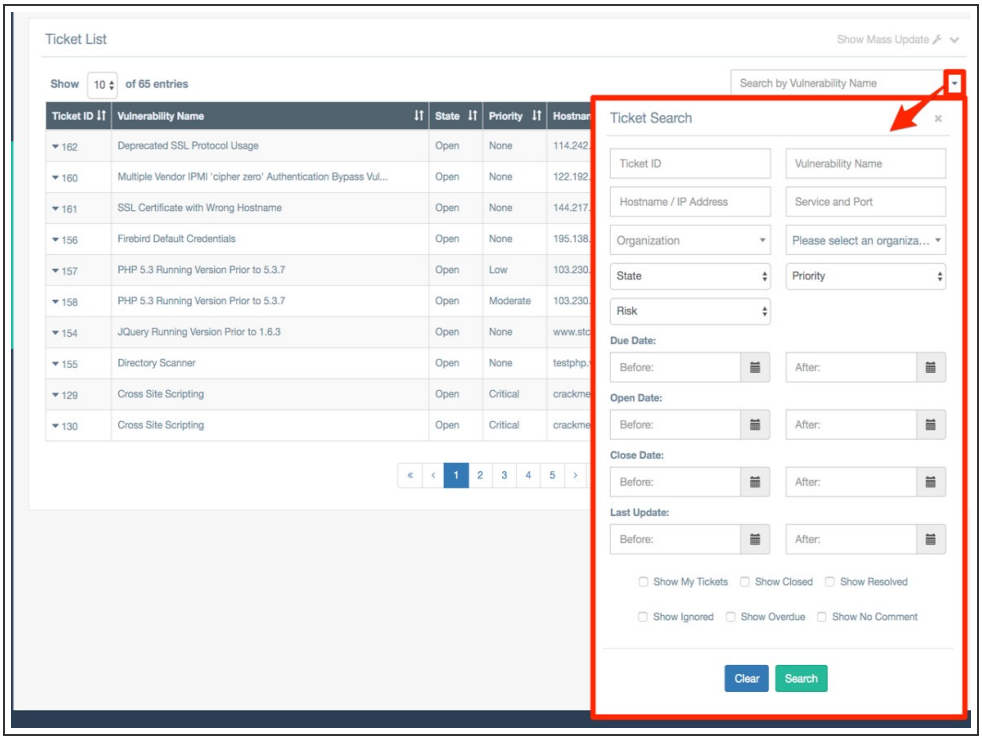
Click on the value in a cell to see all related tickets. In the image above, for example, clicking on the number **45** would bring up a list of 45 open tickets for the Demo location.

Searching Tickets

To search tickets:

1. Click **More** > **Tickets**.
2. Click **Search**.

   By default, the Ticket List page displays all of the tickets for an organization. The basic search allows you to search by Vulnerability Name by entering text in the search box at the top right. To access the advanced search, click the arrow at the end of the search box. A search window with additional options will appear.



The Ticket List page, with the advanced search expanded.

The advanced search screen provides the following options:

Field	Description
Ticket ID	The ID for the ticket.
Vulnerability Name	A descriptive name for the vulnerability.
Hostname/IP Address	The host name or IP address for the host associated with the ticket.
Service and Port	The service and port affected by the vulnerability. Separate the values with commas. For example, entering 80, 443 will return the results for port 80 and port 443.
Organization	The organization associated with the ticket.
State	The status of the ticket (open, ignore, resolved, or closed). For more information, see the Tickets section of this document.
Priority	How urgent the ticket is. Values are None, Low, Moderate, Important, and Critical.
Risk	The level of risk associated with the vulnerability in the ticket. Values are High, Medium, Low, and None.

Field	Description
Due Date	The date the ticket is due. Enter before and after dates to return tickets due within a specific time range.
Open Date	The date the ticket was opened. Enter before and after dates to return tickets due within a specific time range.
Close Date	The date the ticket was closed. Enter before and after dates to return tickets due within a specific time range.
Last Updated	The date the ticket was last updated. Enter before and after dates to return tickets due within a specific time range.
Show My Tickets	Includes tickets assigned to the current user.
Show Closed	Includes tickets that have been closed.
Show Resolved	Includes tickets that have been resolved.
Show Ignored	Includes tickets that have been marked Ignore.
Show Overdue	Includes tickets that are overdue.
Show No Comment	Shows tickets that don't have comments describing the action taken.

3. If using the advanced search, enter your search criteria and click the **Search** button.
4. Use the **Next** and **Previous** links at the bottom of the page to navigate through your results.

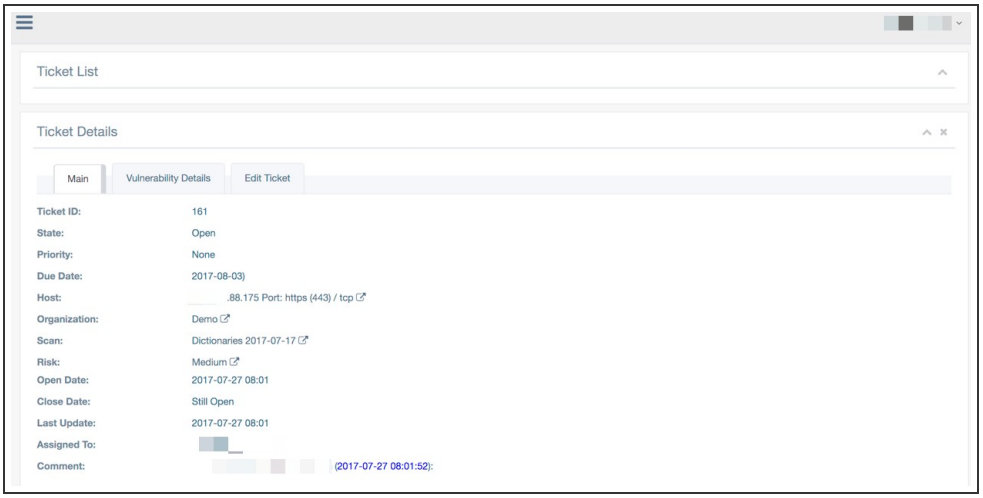
   Click on a ticket to view the Ticket Details page.

Viewing Ticket Details

The Ticket Details page displays the following information about a ticket:

Field	Description
Ticket ID	The ID for the ticket.
State	The status of the ticket (open, ignore, resolved, or closed). For more information, see the Tickets section of this document.
Priority	How urgent the ticket is. Values are None, Low, Moderate, Important, and Critical.
Due Date	The date the ticket is due. Enter before and after dates toreturn tickets due within a specific time range.

Field	Description
Host	The host name or IP address, port, and protocol for the host associated with the ticket.
Organization	The organization associated with the ticket.
Scan	The scan associated with the ticket. Note: An organization must be selected first.
Risk	The level of risk associated with the vulnerability in the ticket. Values are High, Medium, Low, and None.
Open Date	The date the ticket was opened. Enter before and after dates to return tickets due within a specific time range.
Close Date	The date the ticket was closed. Enter before and after dates to return tickets due within a specific time range.
Last Updated	The date the ticket was last updated. Enter before and after dates to return tickets due within a specific time range.
Assigned To	The email address for the user the ticket is as signed to.
Comment	A field for optional comments.



The Ticket Details page.

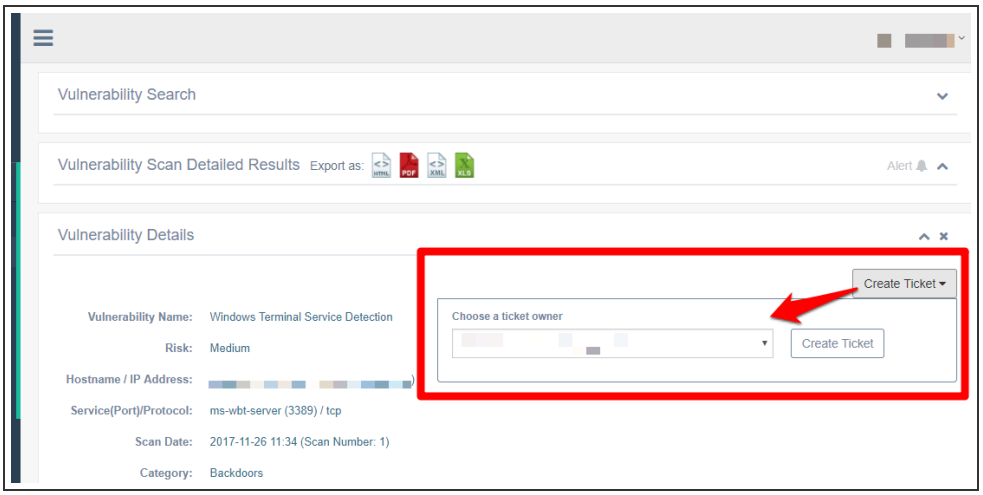
To return to the ticket list, click **Ticket List** at the top of the screen.

Creating Tickets

Tickets are created through the Vulnerabilities List page, rather than the tickets area. One ticket can be created from each vulnerability. A user who can view the vulnerability information will also be able to view the ticket.

To create a ticket:

1. Follow the steps listed in the Searching Vulnerabilities section of this guide
2. Select a vulnerability from the results list.
3. Click **Create Ticket**.
4. Choose a ticket owner from the drop-down list, and then click **Create Ticket**.



Creating a new ticket from a vulnerability.

Ticket State

A Ticket may have one of the following states: **Open**, **Closed**, **Resolved**, **Ignored**, or **Overdue**. The state **Closed** can only be assigned to tickets whose vulnerabilities are no longer present. Tickets marked **Ignored** are not displayed in the system.

To Set a Ticket to the Ignore State

1. Select the desired ticket from the Ticket List to display its details.
2. Click the **Edit** tab.
3. Click the **Action** box, and then select **Ignore**.
4. Optionally, add a comment as to why this ticket is now ignored, providing visibility to other users to why this action was taken.
5. Click **Save**.

Ticket Priority

A ticket can also be assigned one of the following priorities: **None**, **Low**, **Moderate**, **Important**, or **Critical**. **Critical** tickets will appear at the top of the ticket list.

Ticket Due Date

The due date option sets a deadline for resolving a ticket. Tickets with due dates that have passed will appear at the top of the list. In addition, the closer a ticket's upcoming due date is to the current date, the higher it will appear on the list.

Administrative Functions

The Admin area of the beSECURE system enables authorized users to manage accounts, organizations, contacts, security profiles, servers, alarms, and audits. Access to the Admin area is limited to users with Scanning User and Administrator account types. It is available under **DevOps** mode only.

Managing Organizations

The organizations area allows Scanning Users and Administrators to create, modify, and delete organizations and manage organization logos.

Creating an Organization

To create a new Organization:

1. Log in to beSECURE with administrative privileges.
2. Make sure the **DevOps** role is selected.
3. Click **Admin** > **Organizations**.
4. Click **List**.
5. Click the plus sign button  button at the bottom right.
6. Complete the form on the Organization Details page that appears. At a minimum, enter the **Organization Name** and whether **Scan Range Overlapping** is **Allowed** or **Not Allowed**. Both of these fields are required. You can also select a **Parent Name** and **Logo**.

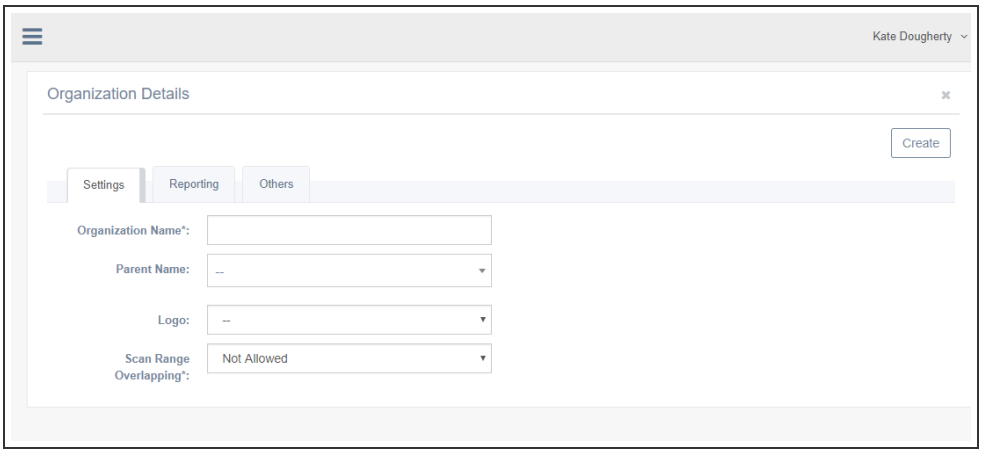
   > **NOTE:** Setting **Scan Range Overlapping** to **Not Allowed** prevents users from scanning the same target machine twice. This avoids confusion and additional charges for unnecessary scans.

7. Review the information on the Reporting tab.
   a. By default, the user who creates the organization becomes the contact person. However, the contact person can be changed at any time.

      > **NOTE:** If an account isn't associated with the Organization, only accounts with Administrator authorization will be able to view the vulnerability information for that Organization and its sub–Organizations.

b. The **Scan Starts** and **Scan Finishes** boxes are also checked by default. This means that the organization's contact person will receive an email notification whenever a scan starts or finishes. To prevent the contact person from receiving the notifications, uncheck the boxes.

8. Optionally, complete the form on the Others tab.
   a. The **Used By** field indicates the other scans that use this organization, if any.
   b. The **Comment** field is a free-text field for entering notes.
9. Click **Create**.



The Organization Details page.

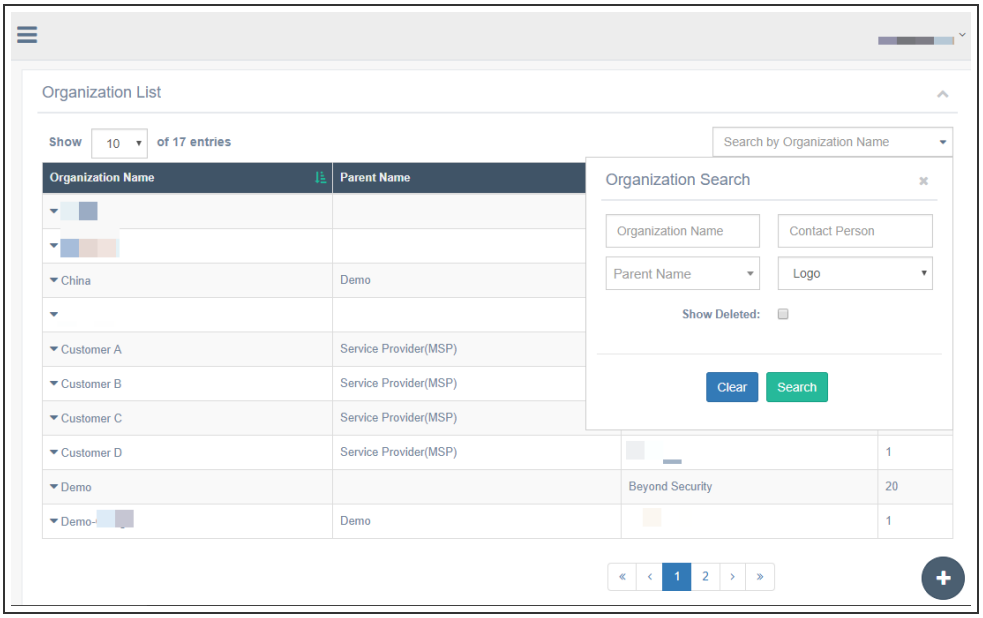
10. Enter information about the organization. You will need to fill out the following basic fields:

Field	Description
Organization Name (required)	The name of the organization. Required.
Parent Name	The name of the organization's parent.
Logo	The organization's logo. Choose from the drop-down list. If an organization doesn't have a logo assigned to it, the default system logo will be used.
Scan Range Overlapping (required)	Values are Allowed and Not Allowed (default). Required. **NOTE:** Setting Scan Range Overlapping to Not Allowed prevents users from scanning the same target machine twice. This avoids confusion and additional charges for unnecessary scans.

Modifying an Organization

To modify an organization:

1. Log in to beSECURE with administrative privileges.
2. Make sure the **DevOps** role is selected.
3. Click **Admin** > **Organizations**.
4. Click **List**.
5. Enter an organization name in the search box at the top to search for a specific Organization, or click the drop-down arrow in the search box to open the advanced search options. The advanced search provides additional options for searching by contact person, parent name, and logo. If you would like to include deleted organizations in your search, check the Search Deleted box. You may also use the navigation buttons at the bottom to page through the list of organizations.



The Organization List page, with the advanced search expanded.

6. Click on a result to open the Organization Details page. The Settings tab is the default tab. The options on this tab allow you to modify the following settings:

Field	Description
Organization Name (required)	The name of the organization.
Parent Name	The name of the organization's parent.

Field	Description
Logo	The logo for the organization. Choose from the drop-down list. If the logo doesn't appear in the list, go to Admin › Organizations › My Logo to upload it. The supported file types are JPEG, BMP, SVG, and GIF. The maximum file size that can be uploaded is 1MB. If an organization doesn't have a logo assigned to it, the default system logo will be used.
Scan Range Overlapping (required)	Values are Allowed and Not Allowed (default). Required. **NOTE:** Setting Scan Range Overlapping to Not Allowed prevents users from scanning the same target machine twice. This avoids confusion and additional charges for unnecessary scans.

Modifying an Organization's Permissions

The Permissions tab determines which users are allowed to modify, change, and delete the organization entry.

To add a new owner to an organization, click on the username on the Available side of the Owned By section. This will move that entity over to the Assigned area. To remove a current owner, click the **X** at the end of the green box in the Assigned area. This will move that entity back to the Available section.

To add a new association, click on the username on the Available side of the Associations section. This will move that entity over to the Assigned area. To remove a current owner, click the **X** at the end of the green box in the Assigned area. This will move that entity back to the Available section.

Modifying an Organization's Contact Person and Notifications

You can modify the contact person and the notifications the contact person receives from the Organization Details area. To do this, click on the Reporting tab. This tab will allow you to select a different contact person from the drop-down list, or check/uncheck the notification options available to the Contact Person (when a Scan Starts or Scan Finishes).

Deleting an Organization

The beSECURE system allows you to delete an organization in the event that a mistake in the entry, change in company structure, or similar event occurs.

To delete an organization:

1. Log in to beSECURE with administrative privileges.
2. Make sure the **DevOps** role is active.
3. Click **Admin** > **Organizations**.
4. Click **List**.
5. Enter an organization name in the search box at the top to search for a specific organization, or click the arrow in the search box to open the advanced search options. The advanced search provides additional options for searching by **Contact Person**, **Parent Name**, and **Logo**. You may also use the navigation buttons at the bottom to page through the list of organizations.
6. Select an organization from the search results.
7. Click **Delete** at the top right of the Organization Details page.

> **NOTE:** Attempting to delete an organization that is being used by other active parties in the system will be denied, and the following error message will appear: “Cannot delete the item as it is associated with one or more items.” Click on the plus sign in the error message box to view the entities in the system that are actively using the organization.

Restoring an Organization

To restore an Organization that was deleted by mistake:

1. Log in to beSECURE with administrative privileges.
2. Make sure the **DevOps** role is active.
3. Click **Admin** > **Organizations**.
4. Click **List**.
5. Click the drop-down arrow in the search box to open the advanced search.
6. Select **Show Deleted**.
7. Run a search for the organization.
8. Select the appropriate deleted item from the search results.
9. Click on the plus sign button  to view the Organization Details page.
10. Click **Undelete**.

Managing Account Profiles

An account profile defines a user role. Each new user is assigned an Account Profile that determines their beSECURE system permissions. There are three default account profiles:

Account Profile	Description
Administrator	Users with this account profile have complete system access.
Scanning User	Scanning Users may only manage items they have been specifically granted access to by the Admin or the user who created them.
Reporting User	Reporting Users have read-only access to scan results, assets, and tickets.

An account profile can be associated with one or more organizations, and can own multiple objects (accounts, scans, contacts, etc.) in the system. This grants users with that profile access to the specified objects. If a user is granted ownership of an item that is already owned by its profile, the ownership will not be effective.

All of the accounts with a specific account profile will have the same privileges, associations, and ownerships. For example, Group A, having ownership over Scan Setting C will give authorization to any user belonging to Group A. You can create, view, and modify account profiles through the Account Pro- files area.

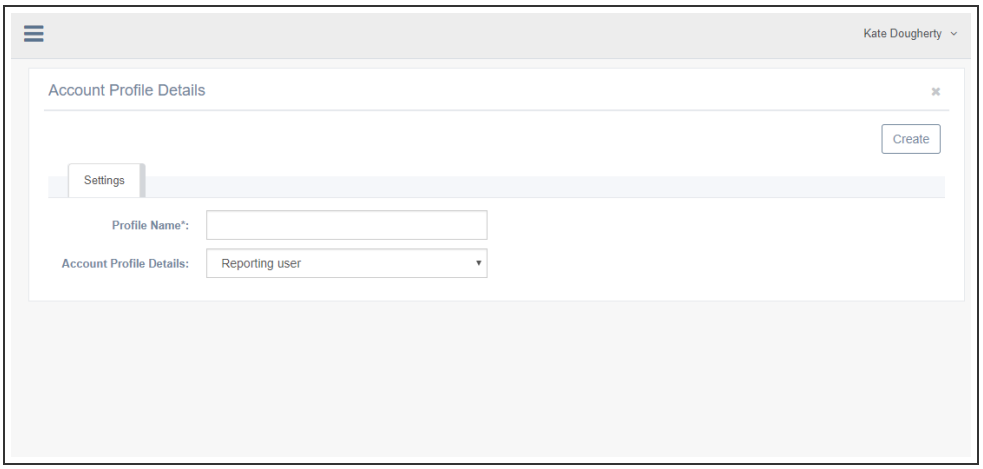
Creating an Account Profile

To create a new account profile:

1. Log in to beSECURE with administrative privileges.
2. Make sure the **DevOps** role is selected.
3. Click **Admin** > **Accounts** > **Account Profiles**.
4. Click the plus sign button at the bottom right corner.
5. Complete the basic information form that appears. The available fields are:

Field	Description
Profile Name (required)	A name for the account profile.
Account Profile Details	The profile type, or permissions associated with the account profile. Values are Reporting User, Scanning User, and Administrator. This value cannot be changed after the account profile has been created. A user cannot create an account with privileges higher than their own.

6. Click the Create button.

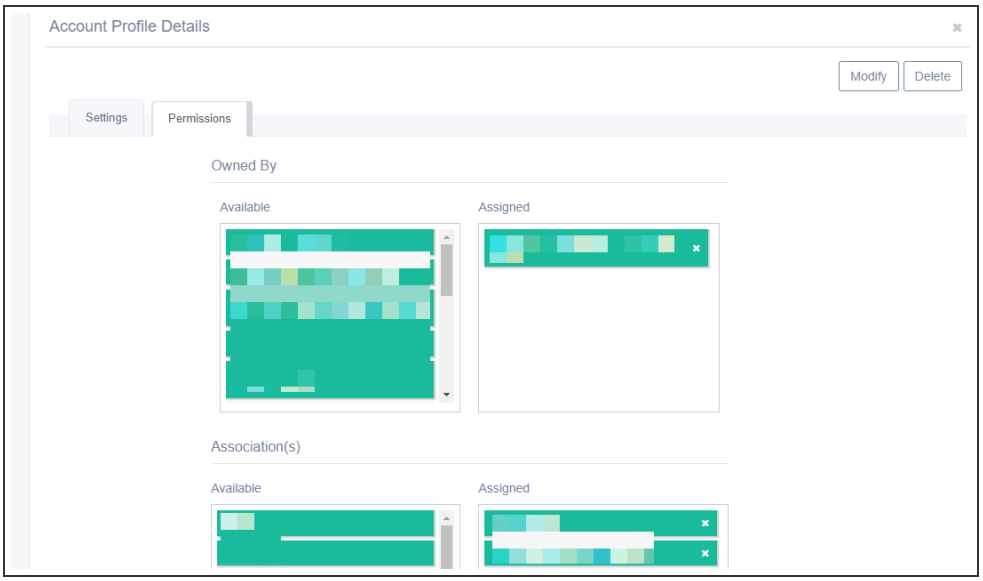


The Account Profile Details page.

Modifying an Account Profile

To modify an account profile:

1. Log in to beSECURE with administrative privileges.
2. Make sure the **DevOps** role is selected.
3. Click **Admin** > **Accounts** > **Account Profiles**.
4. Enter text in the search box at the top right to search by **Profile Name**. You may also use the navigation buttons at the bottom to page through the list of account profiles.
5. Select an account profile from the list.
6. Optionally, modify the basic settings for the account profile (**Profile Name**, **Used By**, and **Comment**) on the Settings tab.
7. Click the **Permissions** tab to modify the permissions for the account profile. If the account profile has one or more managers, they will appear in the Assigned area. To add a new manager, click on the username on the Available side of the Owned By section. This will move that entity over to the Assigned area. To remove a current manager, click the **X** at the end of the green box in the Assigned area. This will move that entity back to the Available section.
8. Optionally, modify the **Associations** below the **Owned By** section. The Associations section determines which users and administrators can access the scan results of their parent organization. An account profile without assigned owners will automatically be owned by any Administrator account in the system.



The Permissions tab of the Account Profile Details page.

9. Click **Modify**.

Deleting an Account Profile

To delete an account profile:

1. Log in to beSECURE with administrative privileges.
2. Make sure the **DevOps** role is selected.
3. Click **Admin** > **Accounts** > **Account Profiles**. A list of existing account profiles will appear. Enter text in the search box at the top right to search by **Profile Name**. You may also use the navigation buttons at the bottom to page through the list of account profiles.
4. Select an account profile from the list.
5. Click **Delete**.

> **NOTE:** An account profile that is in use by other active parties in beSECURE cannot be deleted.

Restoring an Account Profile

To restore an account profile that was deleted by mistake:

1. Log in to beSECURE with administrative privileges.
2. Make sure the **DevOps** role is selected.
3. Click **Admin** > **Accounts** > **Account Profiles**.

4. Click the arrow in the search box to open the advanced search.
5. Select **Show Deleted**.
6. Click **Search**.
7. Select the appropriate deleted item from the list of results.
8. Click **Undelete**.

Managing Security Profiles

A security profile defines the security settings for an account, such as password strength and session timeout. Users with administrative privileges can view information about security profiles and create new security profiles through the Security Profiles area.

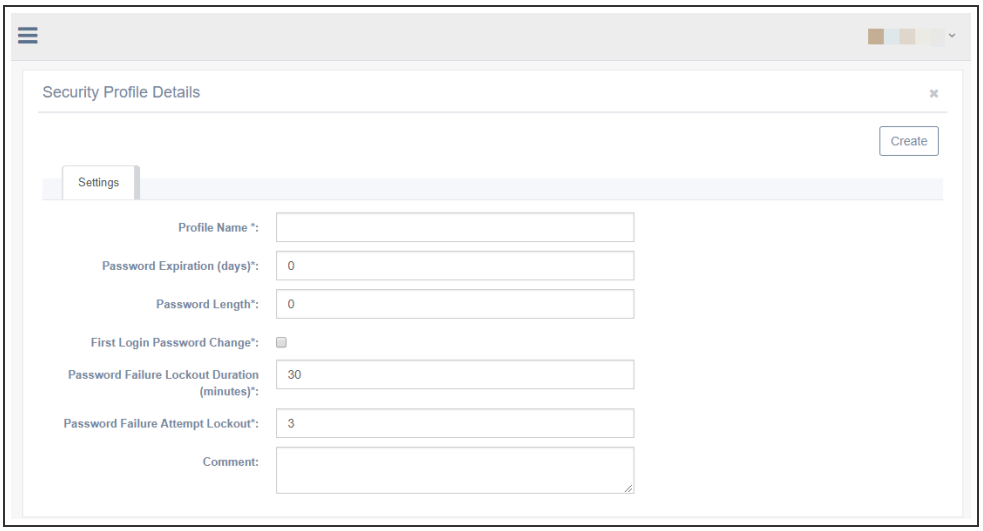
Creating a Security Profile

To create a security profile:

1. Log in to beSECURE with administrative privileges.
2. Make sure the **DevOps** role is selected.
3. Click **Admin** > **Accounts** > **Security Profiles**.
4. Click the plus sign button at the bottom right and complete the form that appears. The form has the following fields:

Field	Description
Profile Name (required)	A name for the security profile.
Password Expiration (required)	The number of days before passwords for accounts associated with this security profile expire.
Password Length (required)	The required password length.
First Login Password Change (required)	Default is 30.
Password Failure Lockout Duration (required)	The number of failed login attempts before an account is locked out. Default is 3.
Comment	A field for optional comments.

5. Click **Create**.



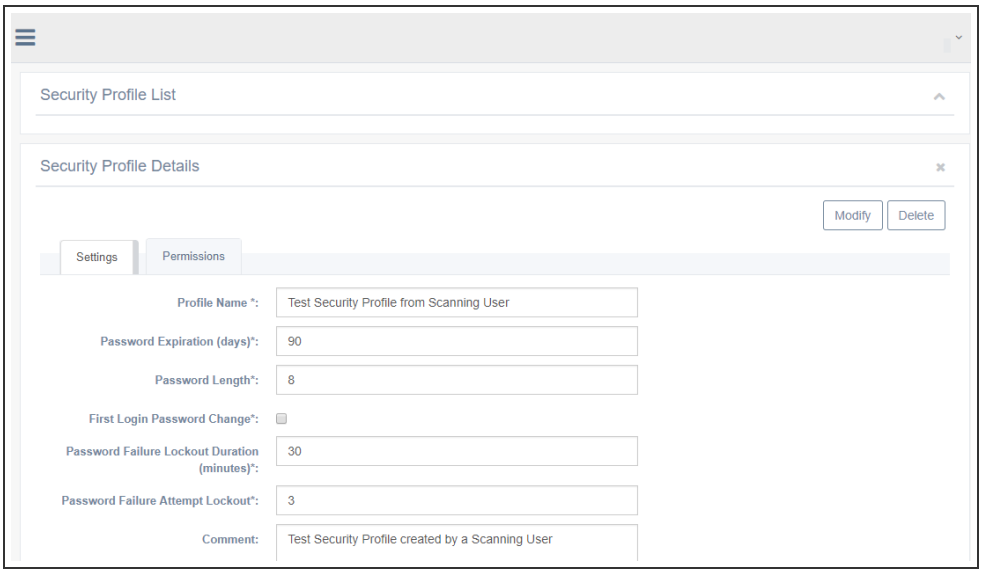
The Security Profile Details page.

NOTE: New security profiles must be more restrictive than the system security profile. The password expiration value must be shorter or equal to the system security profile value, and the password must be longer than the system security profile.

Modifying a Security Profile

To modify a security profile:

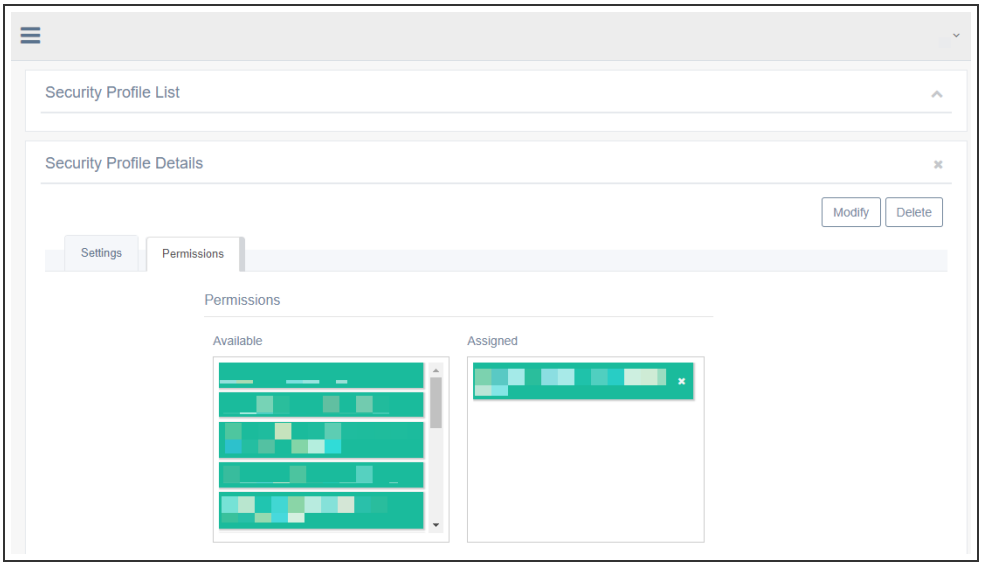
1. Log in to beSECURE with administrative privileges.
2. Make sure the **DevOps** role is selected.
3. Click **Admin** > **Accounts** > **Security Profiles**.
4. Enter text in the search box at the top right to search by **Profile Name**. You may also use the navigation buttons at the bottom to page through the list of security profiles.
5. Select a security profile from the list.
6. Optionally, modify the basic settings on the **Settings** tab.



Modifying the Settings on the Security Profile Details tab.

7. Click the **Permissions** tab to modify permissions for the Security Profile. If there are any current managers for the Security Profile, they will appear in the Assigned area. To add a new manager, click on the username in the Available area of the Owned By section. This will move that entity over to the Assigned area. To remove a current manager, click the X at the end of the green box in the Assigned area. This will move that entity back to the Available section.

> **NOTE:** A security profile without assigned owners is automatically owned by any Administrator account in the system.



8. Click **Modify**.

> **NOTE:** A user cannot modify an existing security profile to have a weaker security profile than their own. If the user tries to set a shorter password length or a longer expiration interval for the password, an error message will appear.

Deleting a Security Profile

To delete a security profile:

1. Log in to beSECURE with administrative privileges.
2. Make sure the **DevOps** role is selected.
3. Click **Admin** > **Accounts** > **Security Profiles**.
4. Enter text in the search box at the top right to search by **Profile Name**. You may also use the navigation buttons at the bottom to page through the list of security profiles.
5. Select a security profile from the list.
6. Click **Delete**.

> **NOTE:** A security profile that is in use by other active parties in the beSECURE system cannot be deleted.

Restoring a Security Profile

To restore a security profile that was deleted by mistake:

1. Log in to beSECURE with administrative privileges.
2. Make sure the **DevOps** role is selected.
3. Click **Admin** > **Accounts** > **Security Profiles**.
4. Click the arrow in the search box to open the advanced search.
5. Select **Show Deleted**.
6. Click **Search**.
7. Select the appropriate deleted item from the list of results.
8. Click **Undelete**.

Managing Accounts

The Accounts area allows users with administrative privileges to create and configure beSECURE user accounts. You can also add contacts and users to your account and update passwords in this section.

Creating a New Account

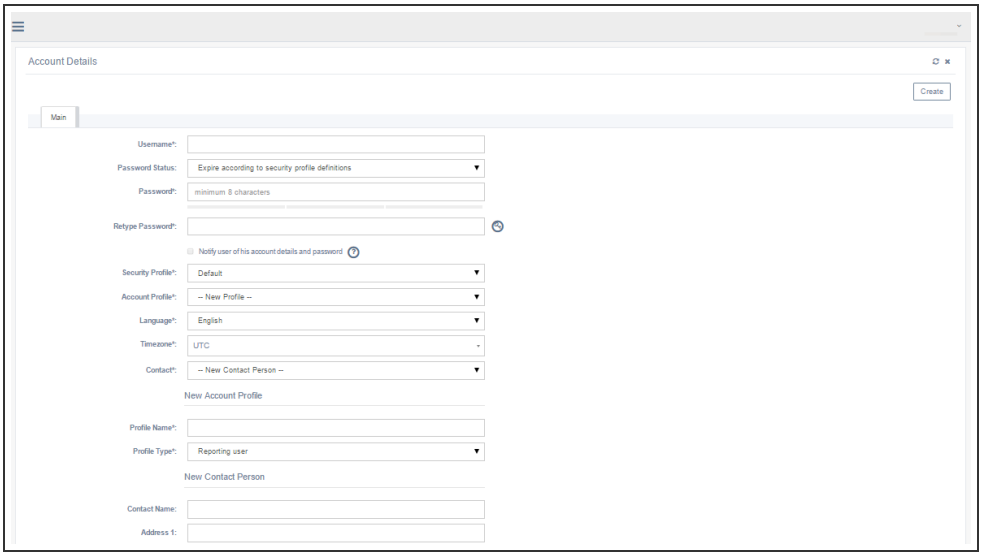
To create a new beSECURE user account:

1. Log in to beSECURE with administrative privileges.
2. Make sure **DevOps** Mode is selected.
3. Click **Admin** in the sidebar.
4. Click **Accounts**.
5. Click **List**.
6. Click the plus sign button at the bottom right.
7. Complete the **Account Details** page form.
8. Click **Create** at the top right and complete the form that appears. The form has the following fields:

Field	Description
Username (required)	The username to associate with the account.
Password Status	The password's validity or expiration status. Values are Expired, Expires in 30 days, and Never expires.
Password (required)	A password for the account.
Retype Password (required)	A password verification field.
Security Profile (required)	The security profile to associate with the account.
Account Profile (required)	The account profile to associate with the account.
Language (required)	The language to use with this account.
Timezone (required)	The time zone to associate with the account.

Field	Description
Contact (required)	The name of the contact person associated with the account. The default is New Contact Person.When the default value is selected, the New Contact Person section is visible. Use that section to enter personal details about the user. You may also select an existing user from the drop-down list.
Profile Name (required)	The name of the profile.
Profile Type (required)	The profile type.
New Contact Person	Visible when the Contact field is set to the default value of New Contact Person. Enter the user's name, address, phone number, and email in this section.

A user who creates a new account is automatically authorized to manage that account, and may also authorize other users to manage it.

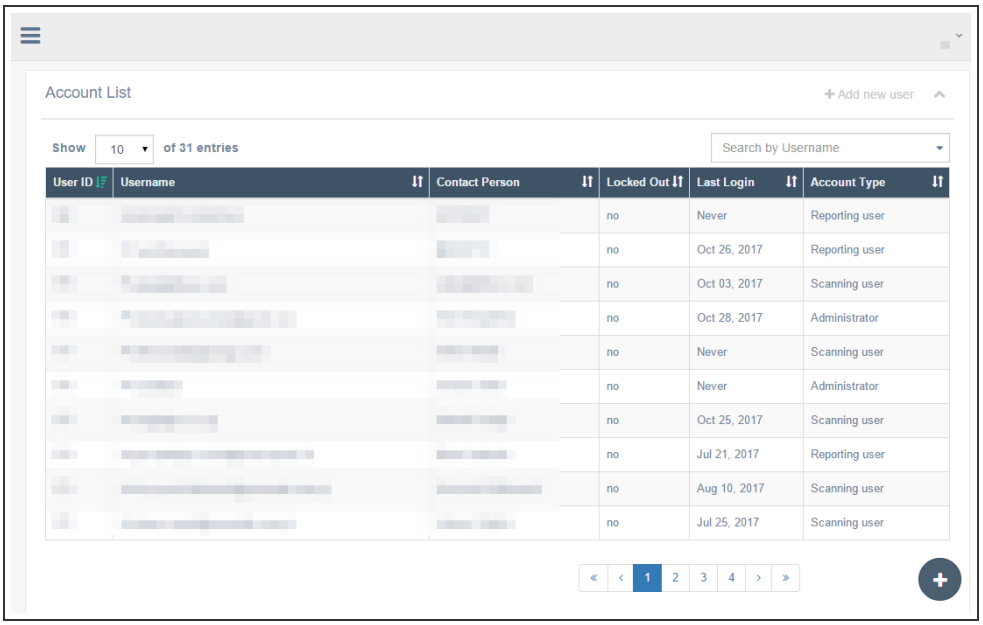


Creating a new user account.

Modifying an Account

You can modify the details for an existing account from the Account List page. Editable settings include username, password, security profile, account profile, language, time zone, and more. To modify the details associated with a user account:

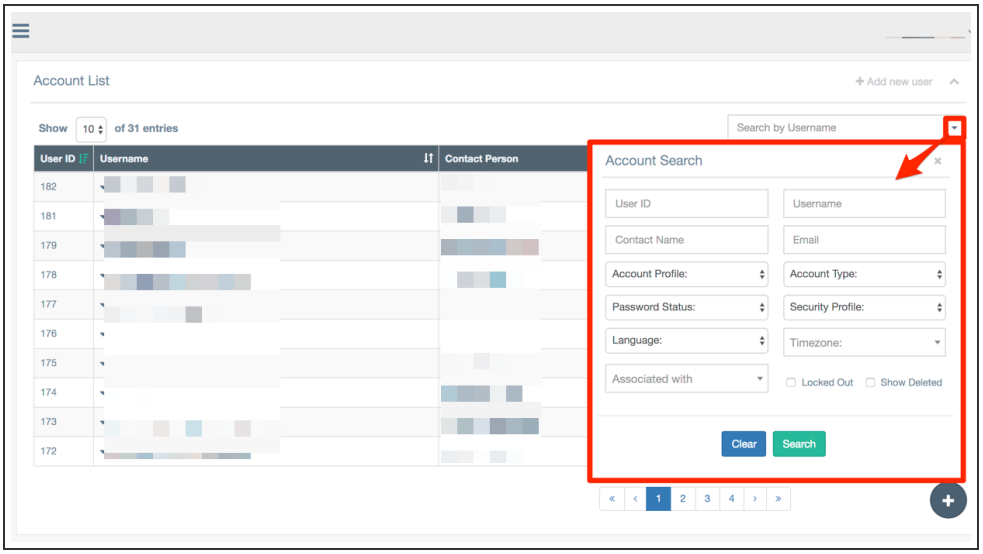
1. Log in to beSECURE with administrative privileges.
2. Make sure **DevOps** Mode is selected.
3. Click **Admin** in the sidebar.
4. Click **Accounts**.
5. Click **List**. The results table displays the User ID, Username, Contact Person, whether the person is Locked Out, the Last Login, and Account Type for each account. Enter text in the search box at the top right to search accounts by username, or click the arrow in the box to open the advanced search options. You may also use the navigation buttons at the bottom to page through the results.



The Account List page.

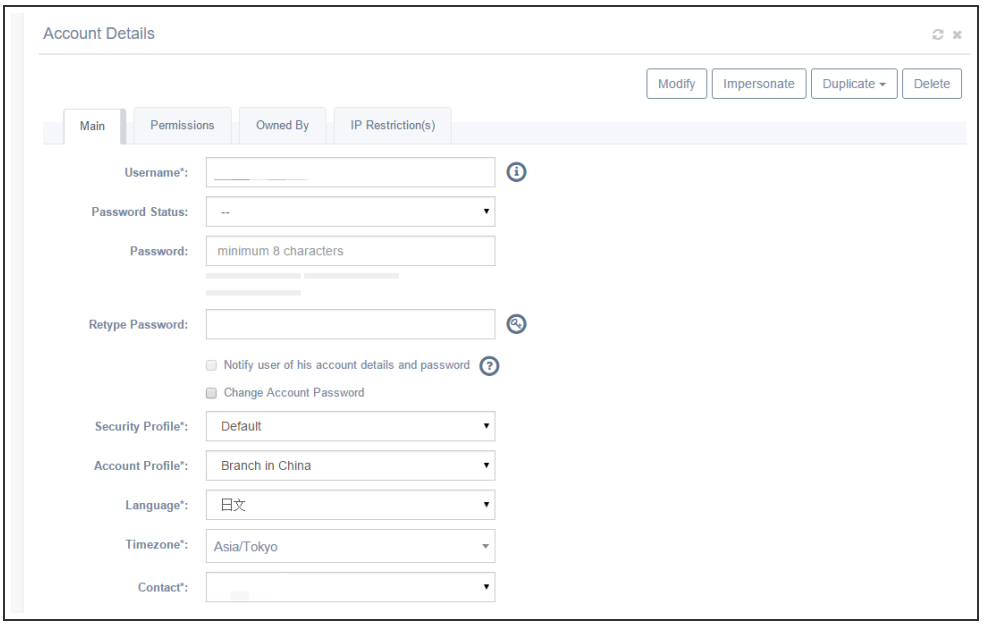
Field	Description
User ID	The user ID associated with the account.
Contact Name	The name of the contact person associated with the account.
Account Profile	The role of the account. Values are Administrator, Reporting User, and Scanning User.
Password Status	The password's validity or expiration status. Values are Expired, Expires in 30 days, and Never expires.
Language	The language associated with the account.
Associated With	The organizations the account is associated with.

Field	Description
Username	The username used to log in to the system. This field is required when creating a new account.
Email	The email address associated with the account.
Account Type	The level of privilege associated with the account.
Security Profile	The security profile associated with the account.
Timezone	The time zone associated with the account.
Locked Out	Whether the account is locked out.
Show Deleted	Includes deleted accounts in search results.



The advanced Account Search.

6. Click on an account in the results table to access the Account Details page.



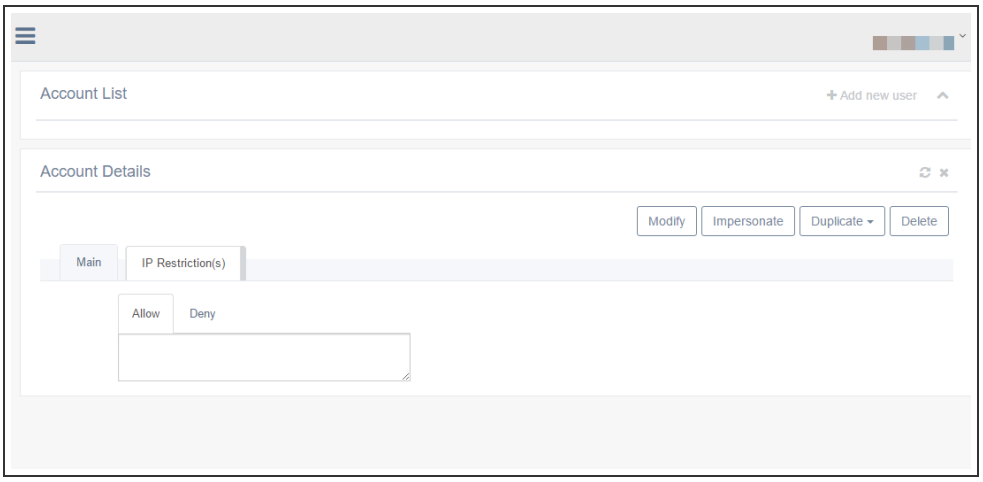
The Account Details page.

Depending on the account type, the Account Details area will have up to four tabs: Main, Permissions, Owned By, and IP Restriction(s). The Main tab, which is the default tab, has the following fields:

Field	Description
Username (required)	The username used to log in to the system. This field is required when creating a new account.
Password Status	The password's validity or expiration status. Values are Expired, Expires in 30 days, and Never expires.
Password	Used when changing the account password.
Retype Password	Used for verification when creating or changing the account password.
Security Profile (required)	The security profile associated with the account.
Account Profile (required)	The role of the account. Values are Administrator, Reporting User, and Scanning User.
Language (required)	The language the beSECURE system uses for the account.
Timezone (required)	The time zone associated with the account.
Contact (required)	The name of the contact person associated with the account.

Restricting IPs for an Account

The IP Restrictions tab enables administrators to allow or deny access to the system through specific IP addresses. Denying an IP address helps prevent unauthorized users from logging in to the system.



The IP Restrictions tab of the Account Details page.

Managing Account Passwords

To change an beSECURE account password:

1. Log in to beSECURE with administrative privileges.
2. Make sure the **DevOps** mode is selected.
3. Click **Admin** > **Accounts** > **List**.
4. Click on the account.
5. Enter a new password in the **Password** field (the password must contain a minimum of eight characters).
6. Re-enter the new password in the **Retype Password** field.
7. If you're creating a new account for someone else or changing a user's password and would like to send a notification to the user's email address, select **Notify user of account details and password**.
8. Select **Change Account Password**.
9. Click **Modify**.

Deleting an Account

To delete an account:

1. Log in to beSECURE with administrative privileges.
2. Make sure **DevOps** mode is selected.
3. Click **Admin** in the sidebar.
4. Click **Accounts**.
5. Click **List**.
6. Select the account you want to delete from the list.
7. Click **Delete**.

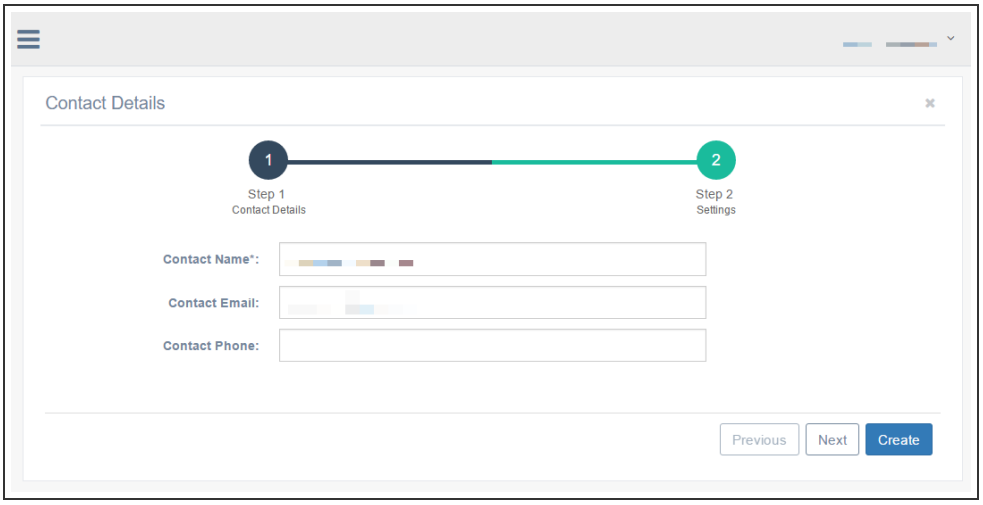
Managing Contacts

Contacts are users who receive beSECURE email notifications about scan results, scan events (when a scan starts or finishes), alerts, and alarms. You can view information about contacts and create new contacts through the Contacts area.

Creating a Contact

To create a new contact:

1. Log in to beSECURE with administrative privileges.
2. Make sure the **DevOps** mode is selected.
3. Click **Admin** > **Accounts** > **Contacts**.
4. Click the plus sign button at the bottom right corner and enter the **Contact Name** (required), **Contact Email**, and **Contact Phone** fields on the form that appears.
5. Click **Next** to continue to the second page of the form and enter address information, or **Create** to create the contact with basic information only.



The Contact Details landing page.

Modifying a Contact

To modify an existing contact:

1. Log in to beSECURE with administrative privileges.
2. Make sure the **DevOps** mode is selected.
3. Click **Admin** > **Accounts** > **Contacts**.
4. Enter text in the search box at the top right to search by contact name. You may also use the navigation buttons at the bottom of the page to page through the list of contacts.
5. Select a contact from the results list.
6. Follow the prompts to modify the contact details.
7. Click **Modify**.

Deleting a Contact

To delete a contact:

1. Log in to beSECURE with administrative privileges.
2. Make sure the **DevOps** mode is selected.
3. Click **Admin** > **Accounts** > **Contacts**.
4. Select the contact you want to delete from the list.
5. Click **Delete**.

Managing Group Contacts

A group contact is an email list that enables the system to send messages to multiple users at once. You can view information about group contacts and create new group contacts through the Group Contacts area.

Creating a Group Contact

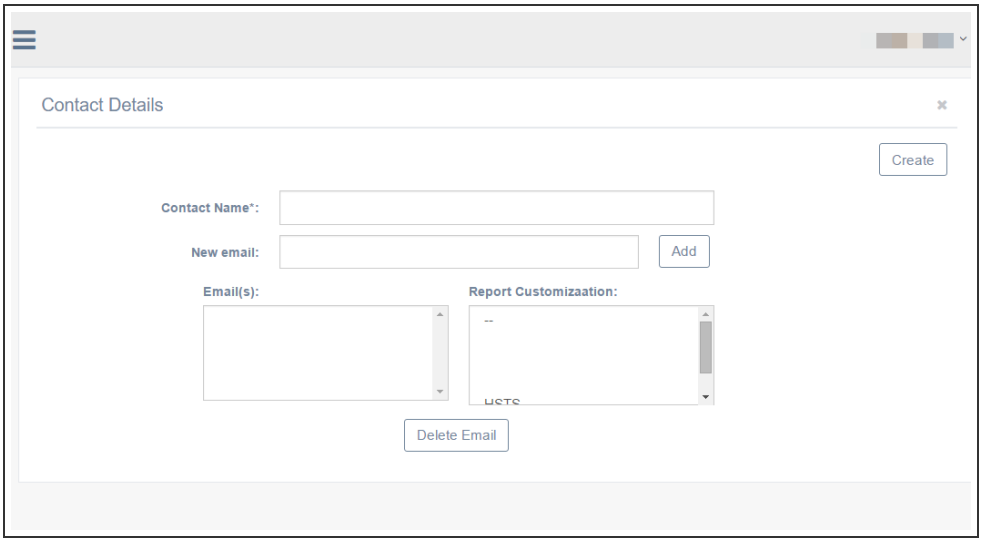
To create a group contact:

1. Log in to beSECURE with administrative privileges.
2. Make sure the DevOps role is selected.
3. Go to Admin > Accounts > Group Contacts.

4. Click the + button at the bottom right corner and complete the basic information form that appears. The available fields are:

Field	Description
Contact Name (required)	A name for the group contact.
New email	A field for adding a new email address.
Email(s)	Displays the email addresses that have already been added to the group contact.
Report Customization	The type of report customization the corresponding user in the Email(s) section should receive.

5. Click the Create button.



The Group Contact Details page.

Modifying a Group Contact

To modify an existing group contact:

1. Log in to beSECURE with administrative privileges.
2. Make sure the DevOps role is selected.
3. Go to Admin > Accounts > Group Contacts. A list of existing group contacts will appear.
4. Enter text in the search box at the top right to search by group contact name. You may also use the navigation buttons at the bottom to page through the list of group contacts.
5. Select a group contact from the results.

6. Modify the group contact details.
    a. To remove a user from the group contact, click on the email address in the Email(s) field, then click the Delete Email button.
7. When finished, click the Modify button.

Deleting a Group Contact

To delete a group contact:

1. Log in to beSECURE with administrative privileges.
2. Make sure the DevOps role is selected.
3. Go to Admin > Accounts > Group Contacts. A list of existing group contacts will appear. Enter text in the search box at the top right to search by group contact name. You may also use the navigation buttons at the bottom of the page to page through the list.
4. Select the Group Contact you want to delete from the list.
5. Click the Delete button.

Managing Active Users

Active users are users at your organization who are currently using the beSECURE system.

Viewing Active Users

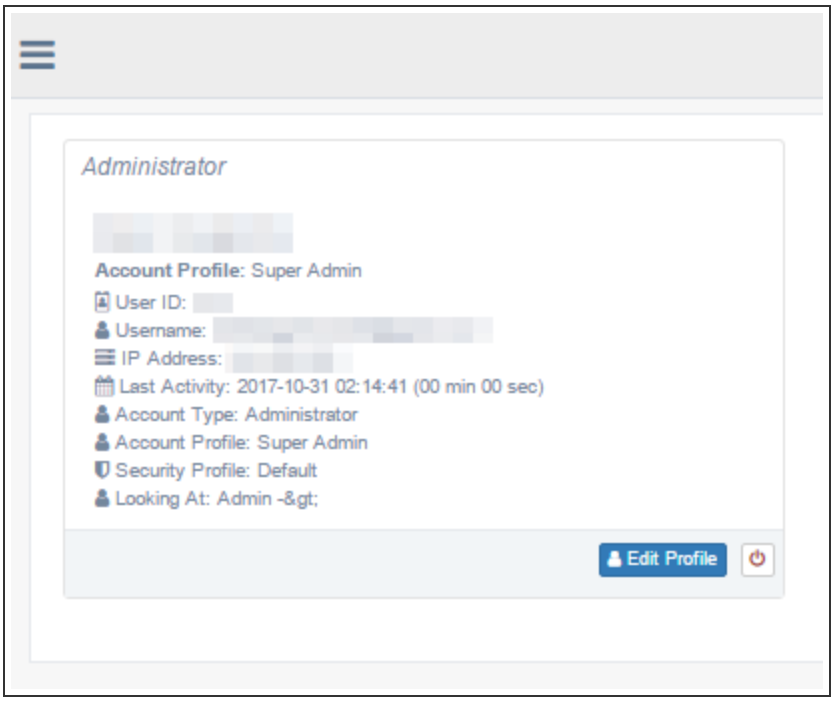
To view active users:

1. Log in to beSECURE with administrative privileges.
2. Make sure the **DevOps** mode is selected.
3. Click **Admin** > **Active Users**.

The Active Users page displays the following information for each active user:

Field	Description
Name	The user's name.
Account Profile	The role of the account. Values are Administrator, Scanning User, and Reporting User.
User ID	The user's User ID.
Username	The user's username. This is typically an email address.

Field	Description
IP Address	The IP address of the machine the user is using.
Last Activity	The date and time of the user's last activity.
Account Type	The level of privilege or access associated with the account.
Security Profile	The security profile associated with the user account.
Looking At	The section of the beSECUREE system the user is accessing.



The Active Users screen.

You can disconnect an active user from the system by clicking on the power button at the bottom right of his or her "card." This will prevent the user from accessing the system.

Modifying Active Users

To modify an active user, click on the **Edit Profile**. This redirects you to the Account Details page, where you can edit the active user's account.

Managing Scan Settings

Scan settings are available to Scanning Users and Administrators. The Scans area allows these users to:

- Create entries containing specific scan setting information
- Modify existing scan setting information
- Delete scan setting information
- Undelete scan setting information
- Modify a scan's schedule
- Enable a scan
- Disable a scan

Creating a Scan Setting Entry

To create an entry containing specific scan setting information:

1. Log in to beSECURE with administrative privileges.
2. Make sure the **DevOps** mode is selected.
3. Click **Scans**.
4. Click **Scan Settings**. A list of existing scans will appear (if any).
5. Click the plus sign  button at the bottom right.

6. Fill out the form on the Settings tab (default).
    a. The required fields on the Main sub-tab are:

Field	Description
Scan Name (required)	A name for the scan.
LSS (required)	The LSS to use for the scan.
Organization (required)	The organization associated with the scan.
Hostname/IP Address Range (required)	The name or IP address range for the host to scan. Use the Import button to import a CSV file, or the Resolve button to resolve the host. **NOTE:** Hostnames/IP addresses provided must be unique for the specified Parent Organization, two different Scans assigned to the same organization should have no common target hosts. Use a comma or a new lines to separate different IPs or Hostnames. Use network dividers such has /8 (A-class) or /24 (C-class) to define subnets. Use '-' to define ranges (For the last digits only, i.e. 192.168.1.100-120).

    b. Click on the **Authentication** sub-tab to enter a Windows username, Windows password, and Windows domain (optional).
    c. Click on the Hostname / IP Address Range sub-tab to import a CSV file of IP address ranges or resolve the IP addresses to include and exclude (optional).
    d. Click on the **Additional Settings** sub-tab to enter a port range, SNMP community name, scanning profile type, and tests to exclude (optional).

> **NOTE:** Unchecking the “ping hosts” check box on this sub-tab will cause the scan to skip the first phase where it attempts to detect live hosts in the range provided. This will cause the scan to run on hosts that do not answer Scan Setting ping and do not listen to standard ports. This is beneficial when scanning high security Scan Settings like a DMZ. However, unchecking this box may also cause the scan to run much longer. This is because all of the possible Scan Settings in the range will be scanned, even if there are no actual machines configured to that IP address.

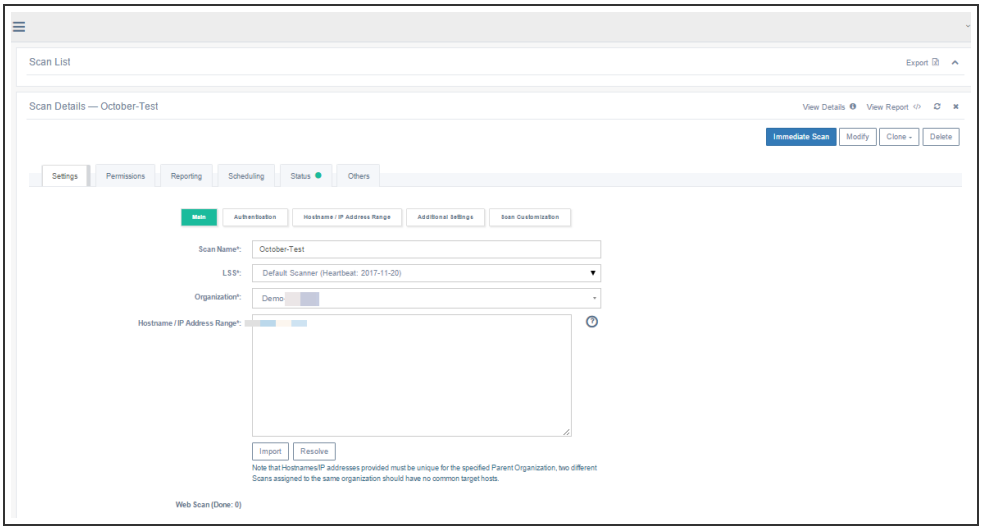
7. Click on the **Permissions** tab to assign additional managers for the scan setting entry (optional). Click on an email/address name under the Available section to move it to the Assigned section. This will assign that user as a manager for the scan

setting. A scan setting without assigned owners will automatically be owned by any Administrator account in the system.

8. Click on the **Reporting** tab to configure settings for reports. Available settings include:

Field	Description
Contact Person (required)	The contact person who should receive reports and notifications.
Notifications	The notifications to send. Values are Scan Starts, Scan Finishes, and Scan Result Change(s).
Customization Name	A saved report customization.
Report Name	The name of the report to send.
Format	The format for the report.
Report Type	Values are Complete, Filtered, and Differential.
Report Style	Values are Regular, SOX, PCI (compliance), HIPAA, ISO 27001/2, OWASP, CIS, Remediation, Microsoft Patches, Penetration Test, Top Level Report, and Executive Summary.

9. When finished, click **Create**.



The Scan Details page.

Creating a new scan setting only registers it on the IS. A request to register the Scan Setting on the selected scanning device will occur on the next synchronization or communication cycle between the IS and LSS. Until the LSS accepts the registration request, the following

message will appear in the Scan Setting details: “The scan has not yet been confirmed by the scanner. You cannot modify its scan setting until it is confirmed.”

Once the LSS has accepted the scan setting registration, a new section in the scan setting details form will appear. This section will allow the user to configure the scanning routine and to enable the scan on the remote scanning device.

If the scanning device is changed once the original scanning device has accepted the registration, a warning will be generated saying: “Changing a scanner will cause the scan to be disabled on the original scanner and a new scan will be created on the new scanner.”

Creating a Schedule for a Scan Setting Entry

Adding a scanning schedule to a scan setting entry allows you to run automated scans on a periodic basis. A schedule consists of a reference date (the date the schedule is calculated) and a routine, which can be daily, weekly, monthly or once (a one-time scan). In order to provide a schedule for a Scan Setting entry, you must create the scan setting first, then go back and modify it.

1. Log in to beSECURE with administrative privileges.
2. Make sure the **DevOps** mode is selected.
3. Click **Scans**.
4. Click **Scan Settings**.
5. Enter text in the search box at the top right to search by Scan Name, or click the arrow in the search box to run an advanced search.
6. Select the Scan Settings entry you want to add a schedule to.
7. Click the **Scheduling** tab.

8. Enter the schedule details. The Scheduling tab includes the following fields:

Field	Description
Date Last Scanned	The date and time this scan setting was last used, if applicable.
Next Scheduled Scan	The date of the next scheduled scan. Will be null if a schedule hasn't been added to the scan setting yet.
Last Scan Number	The ID number for the last scan. The scan number for the first scan of a target will be 1, the second scan will have the scan number 2, and so on.
Scan Duration	The duration of the last scan.
Scan Timezone (required)	The time zone associated with the scan.
Reference Date	The date the schedule is based on.
Routine	Values are Unscheduled, Daily, Weekly, Monthly, and Once. For more information, see the 14.8.2.1. About Routines section below.
Time Range	The hours during which the scan can be initiated.
Time Range Behavior	The behavior of the time range. For example, you can use this field to specify that a scan shouldn't run during the hours in red, and that scans should resume during the hours in green. By default, green indicates the start time and active period, while red is the inactive period.

9. Click **Modify Schedule**.

About Routines

For daily and weekly routines, you must also enter an integer in the field below your choice. This number represents the interval. For example, to scan every 5 days, select Daily, then enter the number 5 in the next field.

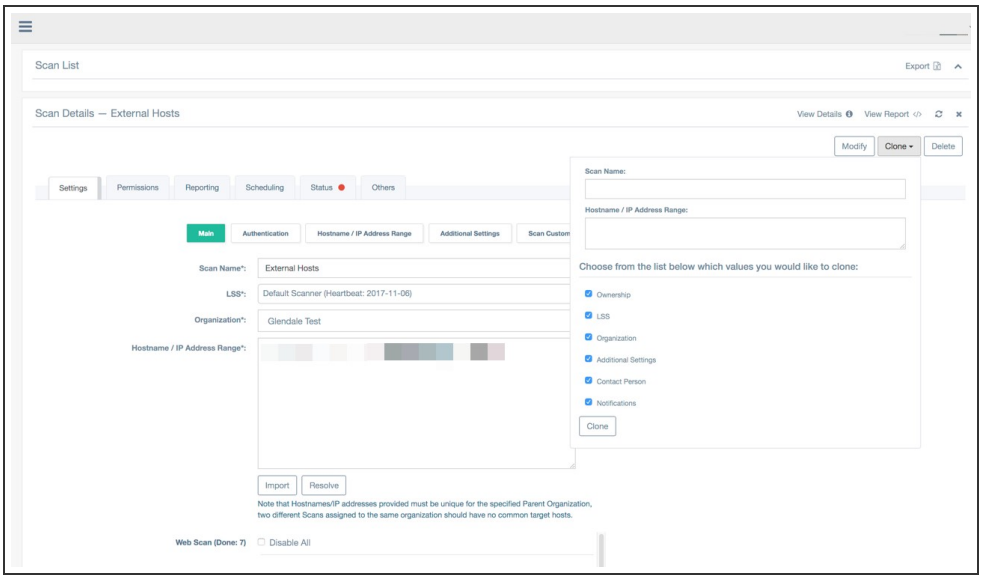
There are two options for the monthly routine. You may choose to scan on a certain day of the month, or the first, second, third, or fourth Sunday, Monday, etc. of the month. For the Once routine, the specific date for the scan should be entered. For example, you would enter 2018–03–05 to scan on March 5, 2018.

Each scan has a starting time that is determined by a matrix of 24 hours. If it is marked by green, the scan can begin at that time. If it is marked in red, it cannot begin at that time. There are two parameters affecting the scan start time: the fixed time frame and the number of scans that can be conducted simultaneously by the LSS. If the time frame does not allow for a scan because the maximum number of scans is being conducted on the LSS, the system will generate an alarm.

Modifying a Scan Setting Entry

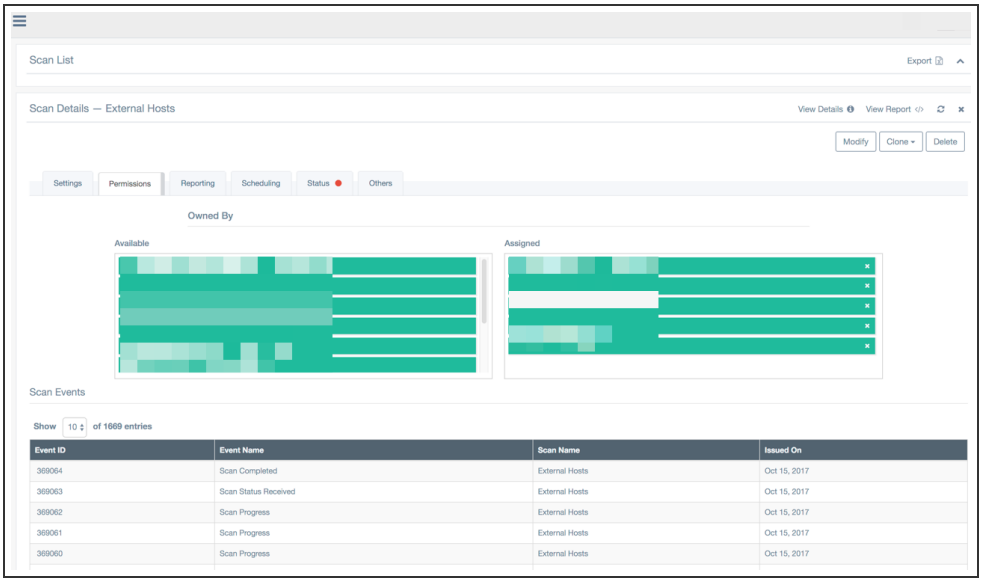
To modify the settings for a scan:

1. Log in to beSECURE with administrative privileges.
2. Make sure the **DevOps** mode is selected.
3. Click **Scans**.
4. Click **Scan Settings**.
5. Enter text in the search bar at the top to search by Scan Name, or click the arrow in the search box to open the advanced search options. Select **Show Deleted** in the advanced search options to include deleted scans in your search. You may also use the navigation buttons at the bottom to page through the list of scan setting entries.
6. Click on a scan in the results list.
7. Edit the scan details. For tab and setting details, see the Creating a Scan Setting Entry section of this user guide.
    a. You can also click Clone to clone the settings associated with another scan, either by Scan Name or Hostname / IP Address Range. The fields that can be cloned include Ownership, LSS, Organization, Additional Settings, Contact Person, and Notifications.
8. Click **Modify**.



The Scan Details page.

The user who creates a new scan setting entry is automatically authorized to manage it, and to add other managers. To view a list of the accounts authorized to manage an entry, click the Permissions tab. Authorized managers appear under Owned By › Assigned. To add a new manager, click on the email address/name for the manager under Available. The manager will now appear under Assigned. To remove an existing manager, click on the email address/name for the manager under Assigned to move it back to the Available section.



The Permissions tab of the Scan Details page.

When a new scan setting is created, the LSS must confirm its creation. The scan cannot be enabled or scheduled for scanning without this confirmation. As soon as confirmation is given, two additional actions are made available. These are Modify Schedule and Enable/Disable Scan. The Scan Setting default is disabled and doesn't have a schedule. To activate a scan, it must be enabled and a schedule must be provided.

Cloning a scan

Cloning a scan is an option made for your comfort - Create a scan in a way that's even faster than the "Create new scan" widget. Just click on a scan, clone it and inherit all its settings.

1. Select the **DevOps** mode.
2. Click **Scans** > **Scans list**.
3. Select a preexisting scan on the Scans List page.
4. Click the **Clone** button the upper-right corner of the Scans Details page.
5. Enter a name for the scan in the **Scan Name** box.
6. Enter an IP address, a range of IP addresses, or FQDNs in the **Hostname / IP Address Range** box. To include multiple entries, separate each with a comma (for example, 192.168.0.100,192.168.0.200).
7. Optionally, disable any value(s) you do not want to include in your scan clone.
8. Click **Clone**.
9. Click **Scan List** from the side navigation pane to access your newly cloned scan.

Deleting a Scan Setting Entry

To delete a scan settings entry:

1. Log in to beSECURE with administrative privileges.
2. Make sure the **DevOps** mode is selected.
3. Click **Scans**.
4. Click **Scan Settings**.
5. Enter text in the search bar at the top to search by **Scan Name**, or click the arrow in the search box to open the advanced search options. You can also use the navigation buttons at the bottom to page through the list of scan setting entries.
6. Click on a scan in the results list.
7. Click **Delete**.

> **NOTE:** A scan setting that is in use by other active parties in beSECURE cannot be deleted.

Restoring a Scan Setting Entry

To restore a scan setting that was deleted by mistake:

1. Log in to beSECURE with administrative privileges.
2. Make sure the **DevOps** mode is selected.
3. Click **Scans**.
4. Click **Scan Settings**.
5. Click the drop-down arrow in the search box to open the advanced search.
6. Select **Show Deleted**.
7. Click **Search**.
8. Select the appropriate deleted item from the list of results.
9. Click **Undelete**.

Errors

The following errors may be generated by scan settings.

Time Range

The scanner may not be able to perform a scan on time due to a heavy load or other causes. If this occurs, beSECURE will generate an alarm with the message “The scanner has missed the schedule of one of the scans.”

Reference Date

Supplying a scanning routine without a reference date will cause an error.

Conflicting IP Addresses/Hosts

All of the IP addresses and hosts in the scan setting's range must be unique to the parent organization the scan setting was placed in. Any of the following actions will generate an error message:

- Attempting to create or modify an existing scan setting with a range or host that exists in another scan setting in the same organization.
- Attempting to move an existing scan setting to an organization that already has one or more IP addresses or hosts of that scan setting.

If these situations occur, you may click the plus sign in the error message to view the conflicting hosts or IP addresses.

Managing Web Scan Settings

Web Scan Settings are available to Scanning Users and Administrators. Users with administrative privileges can:

- Create entries containing specific web scan setting information
- Modify existing web scan setting information
- Delete web scan setting information
- Undelete web scan setting information
- Modify a web scan's schedule
- Enable a web scan
- Disable a web scan

Creating a Web Scan Setting Entry

To create an entry containing specific web scan setting information:

1. Log in to beSECURE with administrative privileges.
2. Make sure the **DevOps** mode is selected.
3. Click **Scans**.
4. Click **Web Scan Settings**.
5. Click the plus sign button at the bottom right.
6. Fill out the details on the **Settings** tab and **Main** sub-tab (you will see these by default). The following fields are required:

Field	Description
Web Scan Name (required)	A name for the web scan.
LSS (required)	The LSS to use for the web scan.

Field	Description
Organization (required)	The organization to associate with the web scan.
Scan (required)	The saved scan to use.
Hostname (required)	The name of the host (for example, www.example.com).

7. Optionally, edit the information on the **Configuration** sub-tab. The available fields are:

Field	Description
URL testing limit (required)	An integer for the maximum amount of testing Dynamic Pages gathered by the crawling processes. Default is 500.
Page visiting limit (required)	An integer for the maximum amount of previously unvisited pages (links) the crawler will visit during the crawling processes. Contains sub-options for handling hosts that match a given regular expression and skipping links that match a given regular expression. Default is 500.
Automatically start crawling site	If the checkbox is enabled, once you create the record, the hostname will be automatically entered into the Static Pages. Every new web scan entry created will also create two new Static Pages: http://hostname/ and https://hostname/.
Automatically start scanning	Indicates whether the scan should start as soon as the first crawling process finishes.
Recrawl before starting to scan	Indicates whether the scan should start as soon as the first crawling process finishes.
Turn off duplicate script detection	By enabling this option, cases such as `article_about_life.php?id=1` and `article_about_feelings.php?id=1` will be regarded as two different Dynamic Pages. While by not enabling this, they will be regarded as the same. By not enabling this, only parameters names are looked at, while by enabling it, the filename will be looked at as well.

8. Optionally, click the **Reporting** tab to change the **Contact Person**. The default is the user who created the web scan setting entry.
9. Click **Create**.

Modifying a Web Scan Setting Entry

To modify the settings for a web scan:

1. Log in to beSECURE with administrative privileges.
2. Make sure the **DevOps** mode is selected.
3. Click **Scans**.
4. Click **Web Scan Settings**.
5. Use the navigation buttons at the bottom to page through the list, or enter text in the search bar at the top to search by Scan Name. You can also click the arrow in the search box to open and run an advanced search.
6. Select **Show Deleted** in the advanced search options to include deleted scans in your search.
7. Click on a web scan in the list.
8. Edit the web scan details. For tab and setting details, see the Creating a Web Scan Setting Entry section of this guide.
9. Click **Modify**.

Deleting a Web Scan Setting Entry

To delete a web scan settings entry:

1. Log in to beSECURE with administrative privileges.
2. Make sure the **DevOps** role is selected.
3. Click **Scans**.
4. Click **Web Scan Settings**.
5. Use the navigation buttons at the bottom to page through the list, or enter text in the search bar at the top to search by Scan Name. You can also click the arrow in the search box to open and run an advanced search.
6. Click on a web scan in the list.
7. Click **Delete**.

Restoring a Web Scan Setting Entry

To restore a web scan setting that was deleted by mistake:

1. Log in to beSECURE with administrative privileges.
2. Make sure the **DevOps** mode is selected.
3. Click **Scans**.
4. Click **Web Scan Settings**.
5. Click the arrow in the search box to open the advanced search.
6. Select **Show Deleted**.

7. Click **Search**.
8. Select the appropriate deleted item from the list of results.
9. Click **Undelete**.

Managing Logos

Scanning Users and Administrators have permissions to upload, modify, and delete company logos for organizations. An organization's logo will appear in system reports. The beSECURE system supports logos in JPEG, BMP, SVG, and GIF formats. The maximum file size that can be uploaded is 1MB.

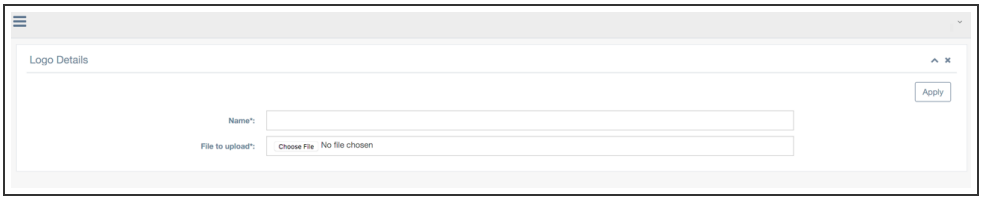
Uploading a Logo

To upload a company logo to the beSECUREsystem:

1. Log in to beSECURE with administrative privileges.
2. Make sure the **DevOps** mode is selected.
3. Click **Admin** > **Organizations** > **My Logo**.
4. Click the plus sign button at the bottom right.
5. Enter a name for the logo in the **Name** box.
6. Click **Choose File**, then browse to the file's location on your machine and select it.

   > **NOTE:** Logos exceeding 1 MB in size will be truncated to 1 MB. size must not exceed 1 MB.

7. Click **Apply**.



The Logo Details page.

Modifying a Logo

To modify a company logo in the beSECURE system:

1. Log in to beSECURE with administrative privileges.
2. Make sure the **DevOps** mode is selected.
3. Click **Admin** > **Organizations** > **My Logo**.
4. Select the logo you wish to modify from the Logo List.
5. Modify the basic settings (Name or File, optional).

   > **NOTE:** If changing the file, the Logo size must not exceed 1 MB. If the size is exceeded, the image will be truncated to 1 MB.

6. Optionally, to change logo permissions, click the **Permissions** tab. By default, the user who uploads the image is automatically authorized to manage it and assign it to other managers. To assign a manager, click on a username under the Available section. This will move the entity over to the Assigned section. To remove a manager, click the x at the end of the username in the Assigned section.

   > **NOTE:** If there are no assigned managers, any Administrator account in the system will be able to manage the logo.

7. Click **Modify**.

Deleting a Logo

To delete a logo from the beSECURE system:

1. Log in to beSECURE with administrative privileges.
2. Make sure the **DevOps** mode is selected.
3. Click **Admin** > **Organizations** > **My Logo**.
4. Select the logo you wish to modify from the Logo List.
5. Click **Delete**.

> **NOTE:** A logo that is in use by other active parties in the beSECURE system cannot be deleted. Click the plus sign in the error message box to view the entities that are actively using the logo.

Restoring a Logo

To restore a logo that was deleted by mistake:

1. Log in to beSECURE with administrative privileges.
2. Make sure the **DevOps** mode is selected.
3. Click **Admin** > **Organizations** > **My Logo**.

4. Click the arrow in the search box to open the advanced search.
5. Select **Show Deleted**.
6. Click **Search**.
7. Select the appropriate deleted item.
8. Click **Undelete**.

Managing Licenses

The Licenses area allows Scanning Users and Administrators to create and modify entries containing specific license information for licenses used by LSS assets.

Every system must have at least one license, with no regex, named the default license. The intention of this license is to “catch” any IP that was not caught in any other license in the system by its regex policy.

License utilization is calculated according to the initial quantity, amount consumed, and the amount remaining.

Creating a License Entry

To create a new License entry:

1. Log in to beSECURE with administrative privileges.
2. Make sure the **DevOps** mode is selected.
3. Click **Admin** > **Deployment** > **Licenses**.
4. Click the plus sign button at the bottom right.
5. Enter a **License Name** and **License Key** in the corresponding boxes.
6. Click **Modify**.

Modifying a License Entry

To modify a License entry:

1. Log in to beSECURE with administrative privileges.
2. Make sure the **DevOps** mode is selected.
3. Click **Admin** > **Deployment** > **Licenses**. To show deleted licenses, click the drop-down arrow in the search box, select **Search Deleted**, and then click **Search**.
4. Click on the license to edit.

5. Edit the license details. Enter a **License Name** and **License Key** in the corresponding boxes.
6. Optionally, click the **Permissions** tab to assign managers to the License. Click on a username under the Available section to move it to the Assigned section. (A license without an assigned owner will automatically be owned by any Administrator account in the system.) To remove a manager, click the **X** at the end of the username under the Assigned section. This will move the entity back to the Available section.
7. Optionally, add or change a comment.
8. Click **Modify**.

Managing LSS Entities

The LSS area of the beSECURE allows Scanning Users and Administrators to create and manage LSS assets.

Creating an LSS Entity

To create a new LSS entity:

1. Log in to beSECURE with administrative privileges.
2. Make sure the **DevOps** mode is selected.
3. Click **Admin** > **Deployment** > **LSS**.
4. Click the plus sign button at the bottom right.

5. Fill out the form that appears. The form has the following fields:

Field	Description
LSS Name (required)	The name of the LSS.
Server ID (required)	The ID for the server. Note that this value cannot be changed once it has been submitted. This ensures proper connectivity between the LSS and the IS.
Network Address (required)	The network address.
Parent IS (required)	The IS server, or management server that controls the LSS. In most cases, this is the server you're using, and there will be no other available selections.
Scan Data Retention (required)	The number of days to retain the data.
Encryption Key (required)	The LSS encryption key. > **NOTE:** This key must be kept secret, as it is used in the communication between the LSS and the IS. In case of suspected key compromise, immediately replace the key by generating a new one on the LSS as described in the LSS installation guide.
Secure Connection	Enables a secure connection when checked.
Secure Connection (required)	The initiator of the connection (IS or LSS). This field determines the direction of the communication.
Contact Person (required)	The contact person for the LSS.
Comments	A field for optional comments.

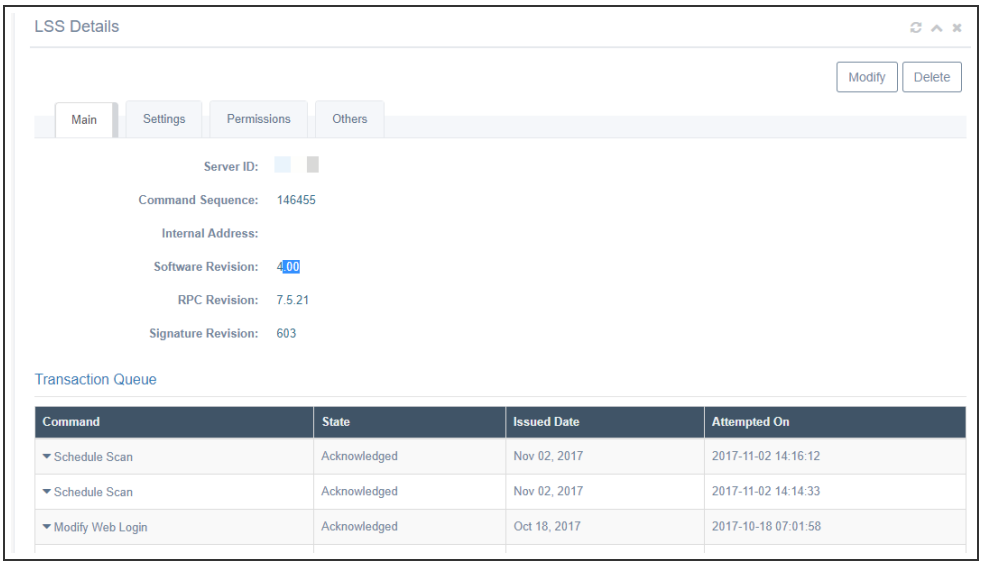
6. Click **Apply**.

> **NOTE:** The communication direction must be set correctly in both the IS and LSS. If an LSS is placed within an internal Scan Setting, the communication direction preferred is “LSS initiates connections.” This can be chosen from the “communication direction” drop–down box and must be set accordingly in the LSS interface. Alternatively, in the instance that the LSS is placed on the Internet, or direct access is available from the IS to the LSS, it is preferable to set the “IS initiates connections” which can be chosen from the “communication direction” drop–down box and must be set accordingly in the LSS interface.

Modifying an LSS Entity

To modify an existing LSS entity:

1. Log in to beSECURE with administrative privileges.
2. Make sure the **DevOps** mode is selected.
3. Click **Admin** > **Deployment** > **LSS**.
4. Enter text in the search box to search by LSS Name or click the arrow in the search box to open the advanced search options. You may also use the navigation buttons at the bottom to page through the list.
5. Select an LSS from the list. The LSS Details page will appear. This page shows basic details about the LSS, the Transaction Queue, and License Utilization.



The LSS Details page.

6. Optionally, click the **Settings** tab to modify the LSS settings. For details on LSS settings, see the Creating an LSS Entity section of this guide.

7. Optionally, click the **Permissions** tab to assign or delete managers for the LSS. Click on a username under the Available section to move it to the Assigned section. To remove a manager, click the **X** at the end of the username under the Assigned section. This will move the entity back to the Available section.

   > **NOTE:** An LSS without assigned owners will automatically be owned by any Administrator account in the system.

8. Optionally, click the **Others** tab to change the **Contact Person** for the LSS.
9. Click **Modify**.

Deleting an LSS Entity

To delete an LSS entity:

1. Log in to beSECURE with administrative privileges.
2. Make sure the **DevOps** mode is selected.
3. Click **Admin** > **Deployment** > **LSS**.
4. Select the desired LSS to delete.
5. Click **Delete**.

> **NOTE:** An LSS that is in use by other active parties in the beSECURE system cannot be deleted. Click the plus sign in the error message box to view the entities that are actively using the LSS.

Restoring an LSS Entity

To restore an LSS that was deleted by mistake:

1. Log in to beSECURE with administrative privileges.
2. Make sure the **DevOps** mode is selected.
3. Click **Admin** > **Deployment** > **LSS**.
4. Click the arrow in the search box to open the advanced search.
5. Select **Show Deleted**.
6. Click **Search**.
7. Select the desired deleted item.
8. Click **Undelete**.

Managing Servers

The Server area of the beSECURE system allows users to manage Settings, Maintenance, System Security, Tasks, Notifications, Ticket, Translation, Integration, and Billing. Access to the server screens is limited to users whose account type is Administrator.

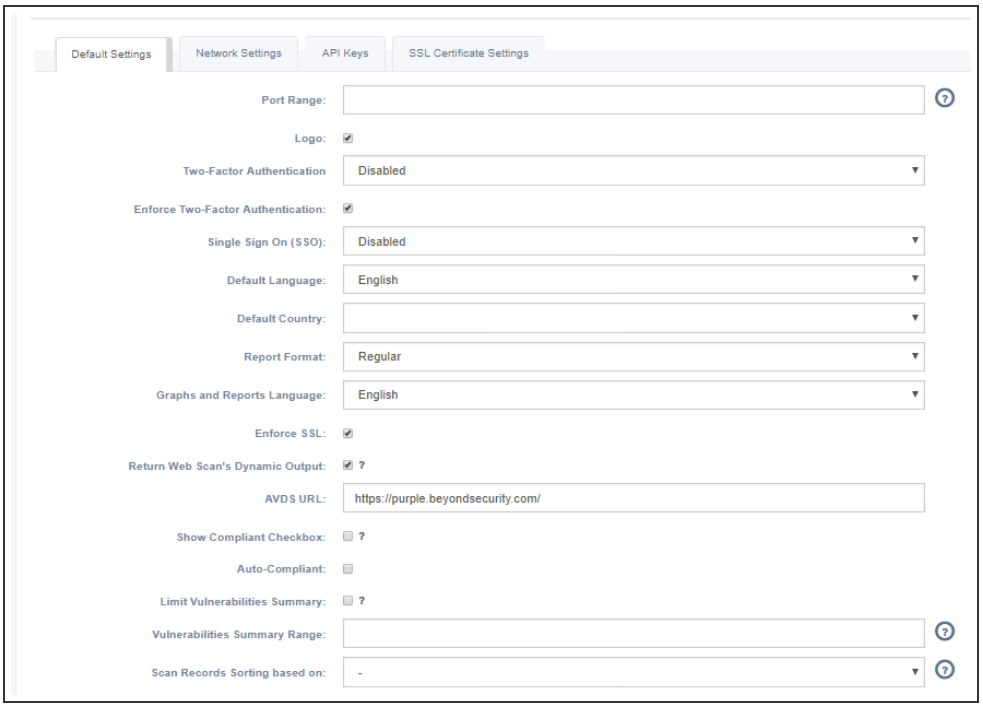
Server Settings

To manage server settings:

1. Log in to the beSECURE system with administrative permissions.
2. Click **More** > **Server**.
3. Click **Settings**.
4. Optionally, edit the settings on the **Default Settings** tab. This tab has the following fields:

Field	Description
Port Range	Examples: 1-65535; 135, 139, 445, 1026, 3389 By leaving this field empty, LSS will use the default port range (1-1024 and well known port list).
Logo	The logo to associate with the server.
Two-Factor Authentication	Values are Disabled and FIDO UNF (Universal 2nd Factor).
Enforce Two-Factor Authentication	A toggle indicating whether to enforce two-factor authentication.
Single Sign On (SSO)	Values are Disabled, LDAP, SAM, Active Directory, and RADIUS.
Default Language	The language to associate with the server.
Default Country	The country to associate with the server.
Report Format	The format for reports. Values are Regular, SOX, PCI, HIPAA, ISO 27001/2, and CIS.
Graphs and Report Language	The language that should be used for graphs and reports.
Enforce SSL	A toggle indicating whether to enforce SSL.

Field	Description
Return Web Scan's Dynamic Output	Web scans return the dynamic output of the request (the request sent to the server, and the server response) to ease the debugging and understanding of where the vulnerability lies on the remote server. By enabling this checkbox, that content will be included in the report. Otherwise, it will be omitted.
beSECURE URL	The root beSECURE URL the system should use inside reports and emails when linking to more information on the beSECURE website.
Show Compliant Checkbox	Marks a certain Organization, Scan, or Host as compliant (in terms of security). If this is checked, the Compliant checkbox will appear at Vulnerabilities > Summary tab.
Auto-Compliant	Whether to automatically mark items with no High or Medium-risk vulnerabilities as compliant. The default is ON.
Limit Vulnerabilities Summary	Determines whether the Reports > Summary table will display a limited amount of rows or the full number of rows on large implementations of beSECURE. Limiting the number of rows may prevent the browser from overloading.
Vulnerabilities Summary Range	Determines the number of rows displayed in the Reports > Summary table.
Scan Records Sorting based on	Defines how the Result and Summary scan records are sorted. The choices are Asset Score and Asset Value.
Prevent Duplicate Scan Name	Prevent users from creating to scans under the Scan Settings menu that have the same Scan Name.

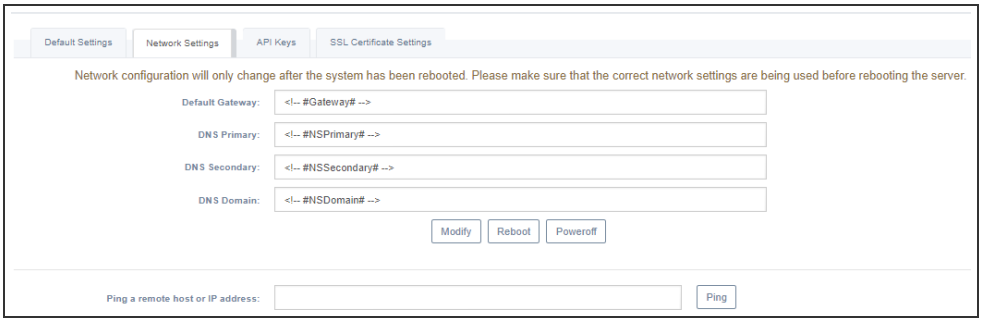


The Settings page under the Server menu.

5. Optionally, click the **Network Settings** tab to edit the **Default Gateway**, **DNS Primary**, **DNS Secondary**, and **DNS Domain** settings.
   a. Click **Modify**.
   b. Click **Reboot**.

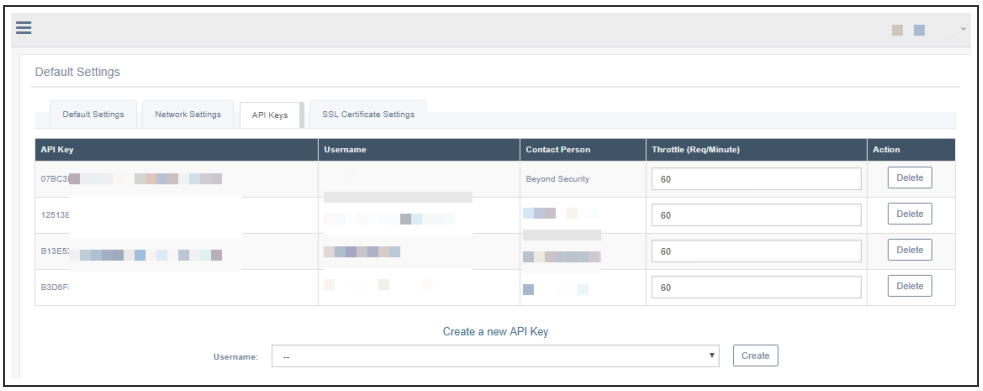
      > **NOTE:** New network configurations do not take effect until the system is rebooted.

   c. Optionally, power the system down by clicking **Poweroff**.
   d. Optionally, enter a remote host or IP address in the box at the bottom of the page to ping that host using the new configuration.
6. When finished, click **Modify**.



The Network Setting tab.

7. Click the **API Keys** tab to create, modify, or delete an API key.
    a. To create a new API key, select a username from the list bix at the bottom of the page and then click **Create**.
    b. To delete an API key, click **Delete** at the end of the row.



The API Keys tab.

8. Optionally, click the **SSL Certificate Settings** tab to edit those settings:
    a. Upload the desired Certificate File.
    b. Upload the desired Key File.
    c. Click **Change**.

WARNING: Placing invalid or malformed certificates/keys will make your beSECURE server inaccessible, if in doubt ask your local Beyond Security support staff to place the new key and certificate for you.

Server Maintenance

The Maintenance area provides detailed information about system uptime, load averages, total memory, free memory, total swap, free swap, disk usage, and RPC log. You can “awaken” the RPC service into action by clicking on the wake–up button.

System Security

The System Security area of the beSECURE system controls password requirements and session timeout settings. beSECURE automatically assigns baseline default settings. A leaner profile cannot be used in the system.

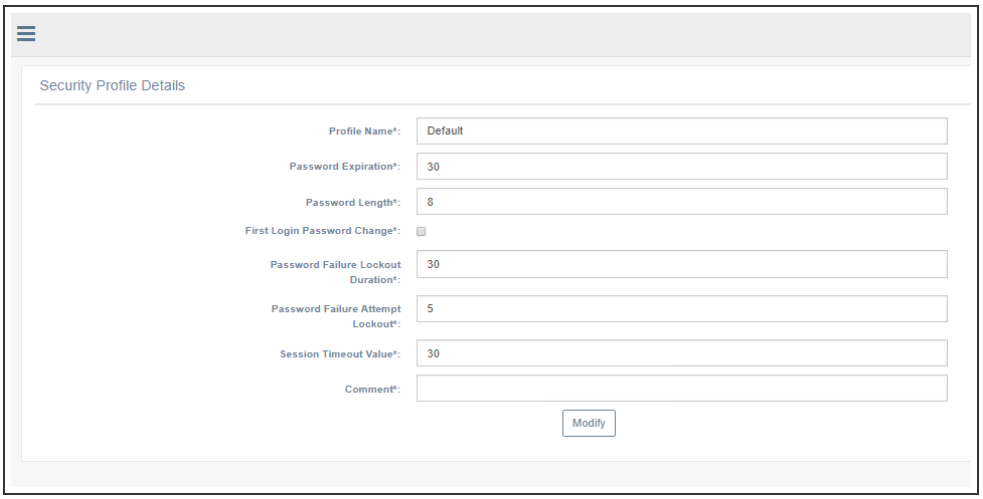
To modify the default System Security settings:

1. Log in to the beSECURE system with administrative permissions.
2. Click **More** > **Server**.
3. Click **System Security**.

4. Modify the settings as desired. The Security Profile Details page has the following fields:

Field	Description
Profile Name (required)	The name of the security profile.
Password Expiration (required)	The number of days before passwords expire. The default is 30 days.
Password Length (required)	The minimum password length. The default is 8 characters.
First Login Password Change (required)	A toggle indicating whether the user must change their password the first time they Log in to the beSECURE system.
Password Failure Lockout Duration (required)	The amount of time a user is locked out of the system after failing to enter the correct password while attempting to log in. The default is 30 minutes.
Password Failure Attempt Lockout (required)	The number of failed password entry attempts before the system locks the user out. The default is 5.
Session Timeout Value (required)	The number of minutes of inactivity before the system logs the user out. The default is 30.
Comment (required)	A comment explaining the change to the Security Profile.

5. Click the **Modify**.



The Security Profile Details page.

Managing Server Hierarchies

The Server Hierarchy provides a view of the relationships between the actual scanning devices and the information servers that show which scanning device reports to which information server. It is automatically generated by the beSECURE system as users install and integrate LSS entities. Hierarchy controls are available in DevOps Mode only.

The process for installing and integrating an LSS on a system is described in the ***Creating an LSS Entity* on page 98**section of this guide.

After a new LSS has been configured according to specifications, you will need to connect that LSS to an existing IS. The LSS reports to the IS, which is called the “associated IS.”

Connecting an LSS

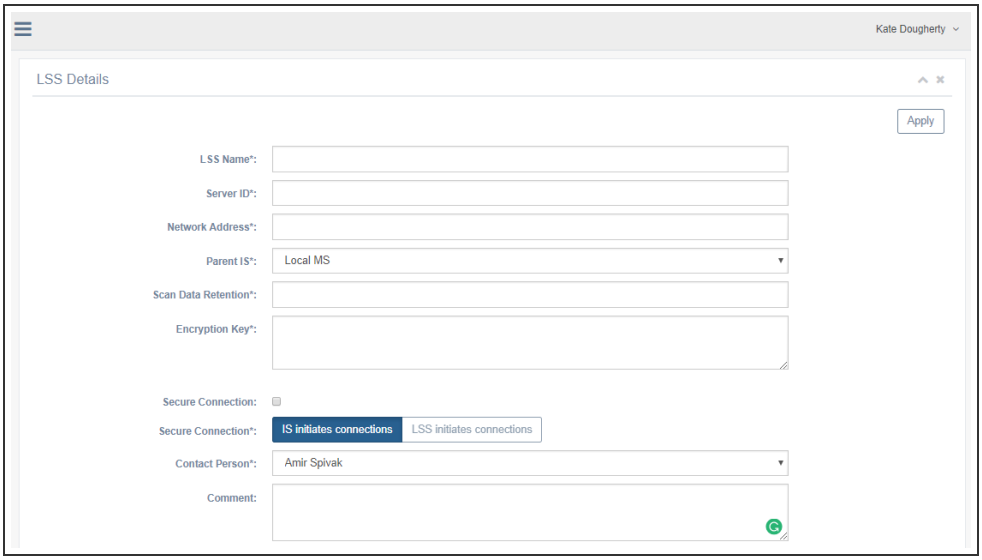
To connect an LSS with an existing IS:

1. Log in to the beSECURE system with administrative permissions.
2. Click **Admin** > **Deployment** > **LSS**.
3. Click the plus sign button to create a new LSS entity.
4. Specify the LSS details in the form that opens. The available fields are:

Field	Description
LSS Name (required)	The name of the LSS.
Server ID (required)	The ID for the server. **NOTE:** This value cannot be changed once it has been submitted. This ensures proper connectivity between the LSS and the IS.
Network Address (required)	The network address.
Parent IS (required)	The IS server, or management server that controls the LSS. In most cases, this is the server you're using, and there will be no other available selections.
Scan Data Retention (required)	The number of days to retain the data.

Field	Description
Encryption Key (required)	The LSS encryption key. **NOTE:** This key must be kept secret, as it is used in the communication between the LSS and the IS. In case of suspected key compromise, immediately replace the key by generating a new one on the LSS as described in the LSS installation guide.
Secure Connection	Enables a secure connection when checked.
Secure Connection (required)	The initiator of the connection (IS or LSS). This field determines the direction of the communication.
Contact Person (required)	The contact person for the LSS.
Comments	A field for optional comments.

5. Click **Apply**.



The LSS Details page.

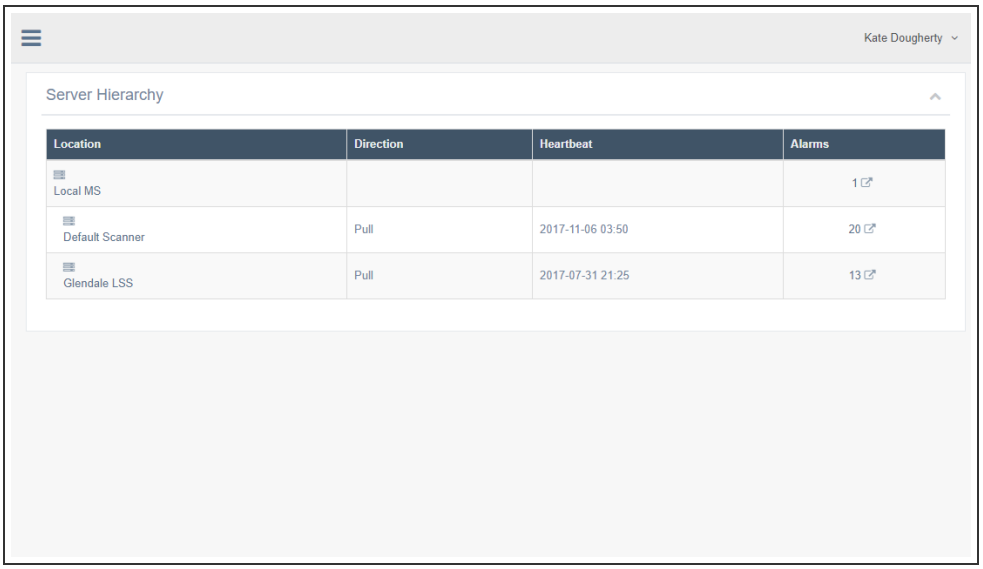
6. Follow the testing procedure to ensure that the LSS has been defined correctly and the IS communicates properly with the new LSS. (The procedure is described fully in the Creating an LSS Entity section of this document.)
7. Repeat steps to add as many scanning devices as the system requires.

Viewing Server Hierarchies

To view an existing Server Hierarchy:

1. Log in to the beSECURE system with administrative permissions.
2. Click **Admin** > **Deployment** > **Server Hierarchy**. This page shows the following information:

Field	Description
Location	The location in the server hierarchy.
Direction	The direction of data movement in the client/server relationship. Values are Pull and Push.
Heartbeat	The date and time of the last connection between the remote scanner and the beSECURE system. This field indicates whether the remote scanner is still active.
Alarms	The number of alarms associated with the Location. Click on the number in this field to go to the Alarm List for the Location. You can also view Alarms under Admin > Alarms.



The Server Hierarchy page.

Managing Notifications

You can configure the beSECURE system to send notifications when certain events related to scans and tickets occur. For example, the contact person for the organization may wish to receive notices when a scan is completed or a ticket is created. For information on configuring a contact person, see the Managing Contacts section of this document.

To manage Notification Settings:

1. Log in to the beSECURE system with administrative permissions.
2. Click **More** > **Server**.
3. Click **Notifications**. The Notification Settings page will appear. This page displays the Active Notifications at the top, current settings in the middle, and a list of sent notifications at the bottom.
4. Optionally, modify the Active Notifications. The choices are:

Field	Description
Scan Completed	Sends a notification when a scan finishes.
Scan Started	Sends a notification when a scan starts.
Ticket Created	Sends a notification when a ticket is created.
Ticket Assigned	Sends a notification when a ticket is assigned.
Ticket Unassigned	Sends a notification when a ticket is unassigned.
Ticket Remediated	Sends a notification when a ticket is remediated.
Ticket Status Change	Sends a notification when the status of a ticket changes.
Ticket Assigned	Sends a notification when a ticket is assigned.
Scan Completed with Report Attachment	Sends a notification and report when a scan finishes. Requires the Scan Completed notification to be enabled.
Scan Changes with Report Attachment	Sends a notification and report when a scan changes. Requires the Scan Changes notification to be enabled.

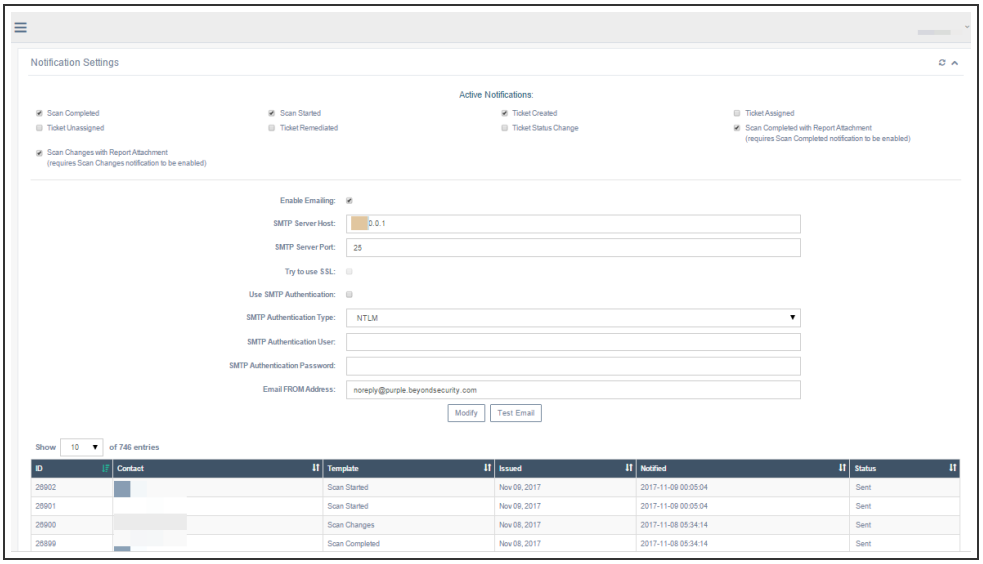
5. Optionally, modify the Notification Settings. The available fields are:

Field	Description
Enable Emailing	Enables email notifications.
SMTP Server Host	The SMTP server host.
SMTP Server Port	The SMTP server port.
Try to use SSL	Whether to attempt to use SSL
Use SMTP Authentication	Whether or not to use SMTP Authentication.
SMTP Authentication Type	The type of SMTP authentication server.
SMTP Authentication User	The user name to use for the SMTP authentication server.
SMTP Authentication Password	The password to use for the SMTP authentication server.

Field	Description
Email FROM Address	The email address the notification should originate from.

6. Click **Modify**.

To send a test email notification, click **Test Email**.



The Notification Settings page.

Managing Ticketing System Settings

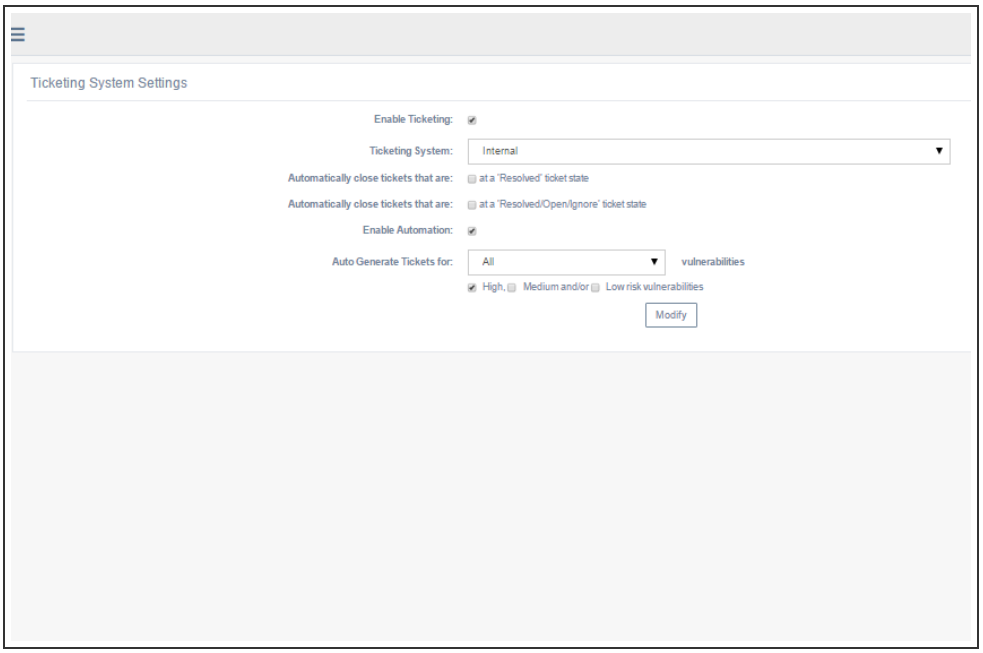
The Ticketing System Settings area allows users to enable ticketing and configure ticketing settings, such as the ticketing system to use, and whether to automatically generate and close tickets. To access this area:

1. Log in to the beSECURE system with administrative permissions.
2. Click **More** > **Server**.
3. Click **Ticketing**.
4. Modify the settings as desired. The fields are:

Field	Description
Enable Ticketing	Whether to enable ticketing.

Field	Description
Ticketing System	Whether to use beSECURE Internal ticketing system, or an external one. Selecting “External” expands a panel containing fields for the External URL, Email, subject, and Template.
Automatically close tickets that are at a ‘Resolved’ ticket state	Whether to automatically close resolved tickets.
Automatically close tickets that are at a ‘Resolved/Open/Ignore’ ticket state	Whether to automatically close tickets marked Resolved/Open/Ignore.
Enable Automation	Whether to enable auto-generation of tickets.
Auto Generate Tickets for	If Enable Automation is checked, this will determine whether tickets are auto- generated for all vulnerabilities, or for new vulnerabilities only. The three checkboxes for high, medium, and low-risk vulnerabilities allow you to limit ticket auto-generation to specific vulnerability types.

5. Click **Modify**.

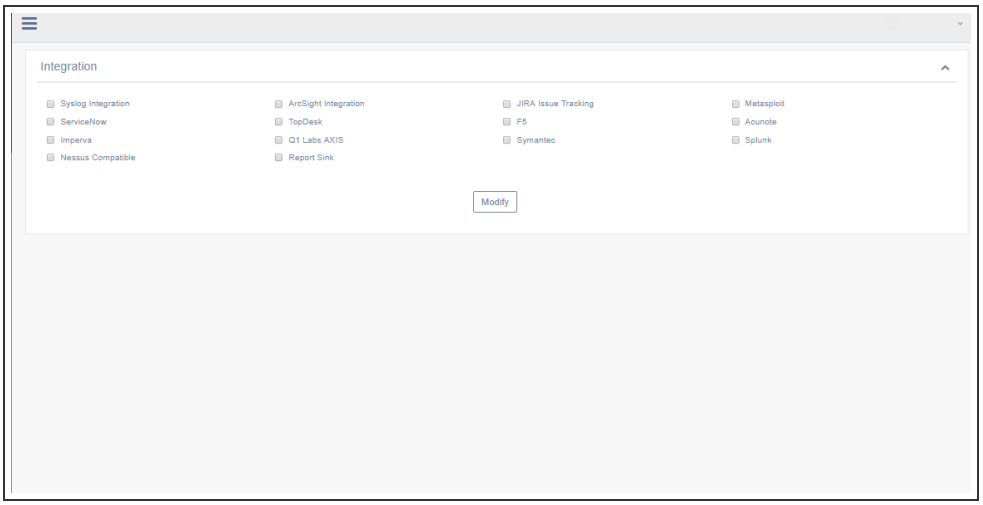


The Ticketing System Settings page.

Managing Integrations

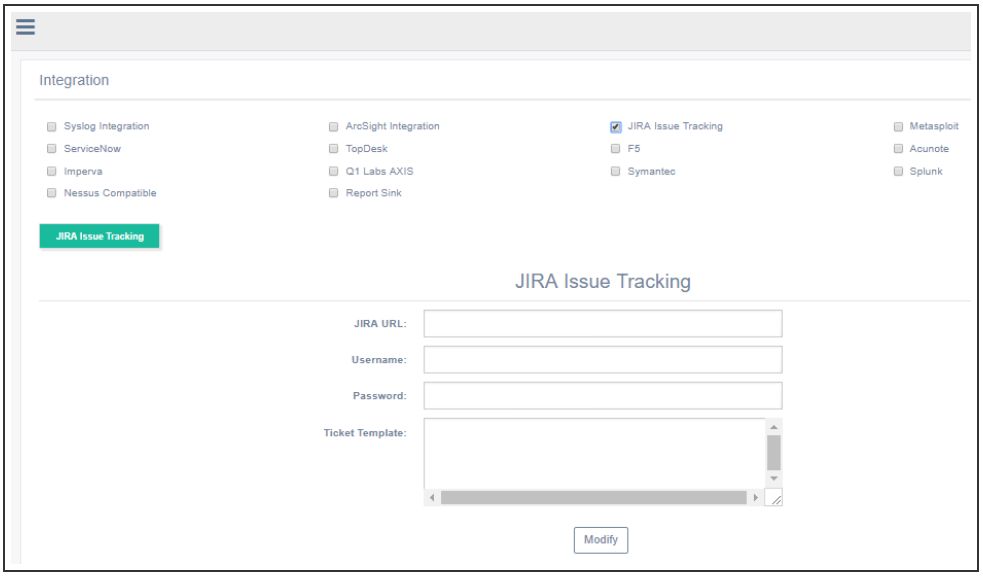
beSECURE offers more than a dozen third-party integrations with providers like Service Now, Jira, Symantec, Service Now, and many other services. To manage your integrations:

1. Log in to the beSECURE system with administrative permissions.
2. Click **More** > **Server**.
3. Click **Integration**.



The Integration list page.

4. Select the Integration to modify.
5. A panel with configuration options specific to the Integration you selected will open.



Configuration options for Jira integration. These fields appear upon clicking the Jira Issue Tracking box.

6. Edit the settings for the integration.
7. Click **Modify**.

Viewing Tasks

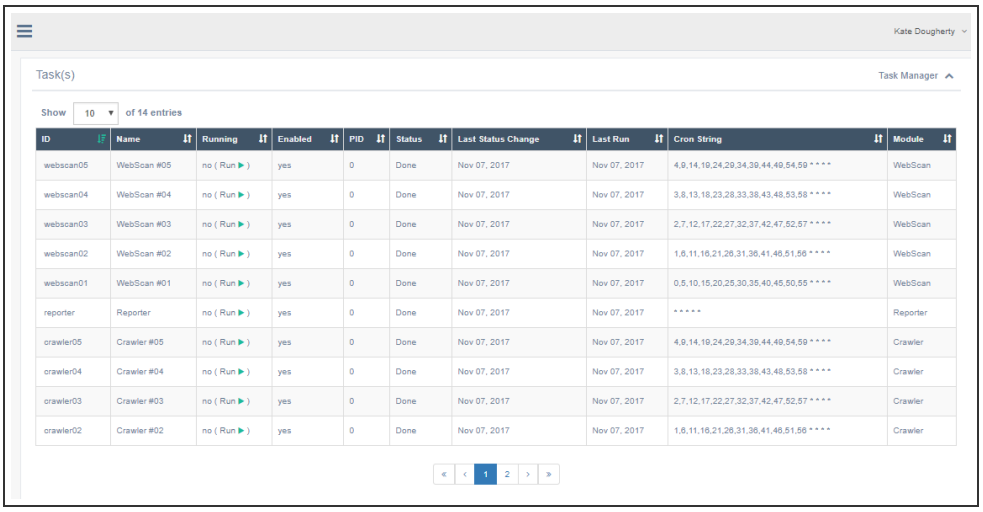
Tasks are actions the system performs every few minutes, hours, or days. Tasks include backing up a database, initiating a scan, exporting scan results to a third-party server, sending an alert to a user, and other actions.

To view the Tasks the system has performed:

1. Log in to the beSECURE system with administrative permissions.
2. Click More > Server. The menu will expand.
3. Click Tasks. A list of tasks will appear.

The Task(s) List displays the following information:

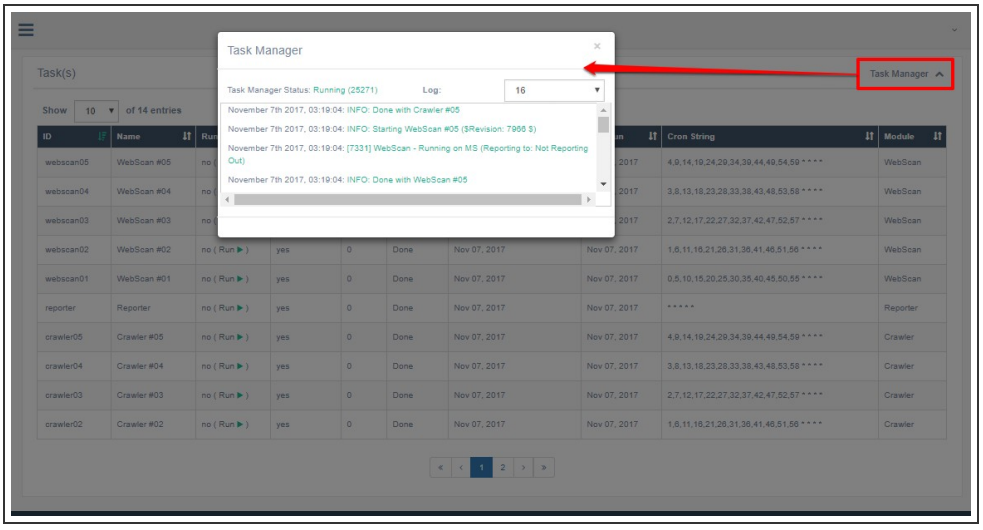
Field	Description
ID	The ID for the task.
Name	The name of the task.
Running	Whether the task is running or not.
Enabled	Whether the task is enabled or not.
PID	The process ID the beSECURE system has assigned to the task.
Status	The status of the task.
Last Status Change	The date the status of the task last changed.
Last Run	The date the task was last run.
Cron String	The cron string that describes the details of the schedule.
Module	Values are Mailer, Web Scan, Crawler, Maintenance, Alert, Billing, and Reporter.



The Task List page.

Task Manager

Click on Task Manager at the top of the page to see additional options. This will open the Task Manager window, which displays the Task Manager's log.



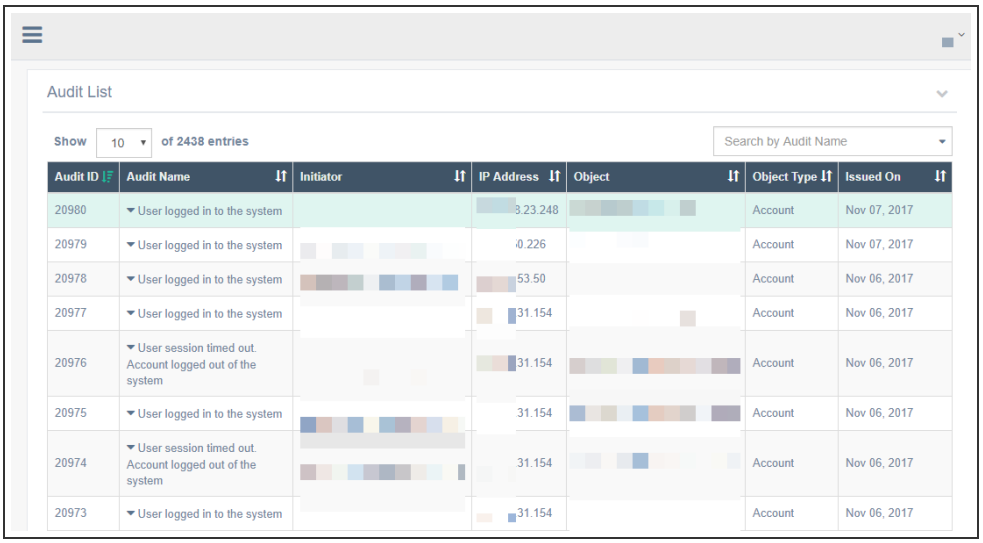
The Task Manager window.

Viewing Audits

The Audit area allows Scanning Users and Administrators to obtain audit logs of all the actions performed in the system. An audit shows the action, the initiator of the action, and the time and date of the action.

To access the Audits area:

1. Log in to beSECURE with administrative privileges.
2. Make sure the **DevOps** mode is selected.
3. Click **Admin** > **Audit**.

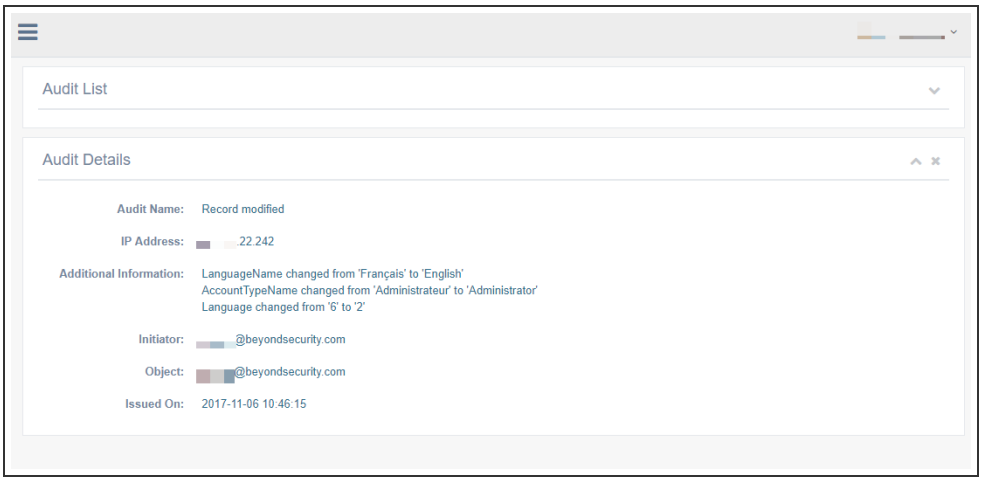


The Audit List page.

4. This page shows the following information for each audit:

Field	Description
Audit ID	The ID for the audit.
Audit Name	The name of the audit.
Initiator	The entity that initiated the audit.
IP Address	The IP address the user who triggered the Audit accessed the beSECURE system from.
Object	An object in the beSECURE system (for example, an account, scan, organization, contact, etc.). The system creates an audit trail for each object, and adds to the trail whenever a user creates, modifies, deletes, or restores an object.
Object Type	The type of object the audit was created for.
Issued On	The date the audit was issued.

5. Click on the desired audit to view. The Audit Details page will appear.



The Audit Details page.

Viewing Alarms

The alarms area of the beSECURE system provides detailed information on alarms. A user can view the alarms corresponding to the Assets an administrator has assigned them to.

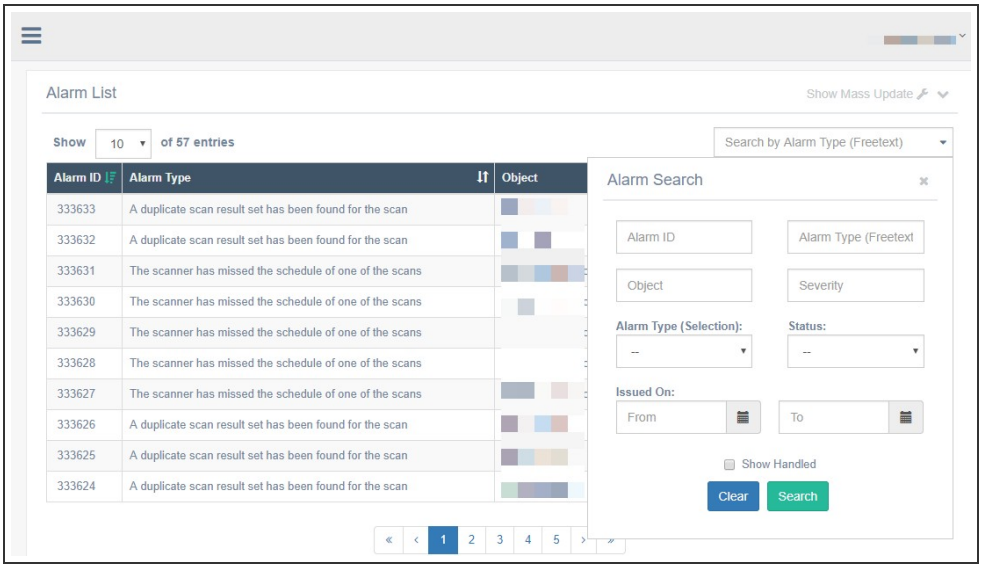
Accessing Alarms

To access the Alarms area:

1. Log in to beSECURE with administrative privileges.
2. Make sure the **DevOps** mode is selected.
3. Click **Admin** > **Alarms**.
4. Use the navigation buttons at the bottom to page through the list or enter text in the search bar at the top to search by Alarm Type. You can also click the arrow in the search box to open the advanced search options. These include:

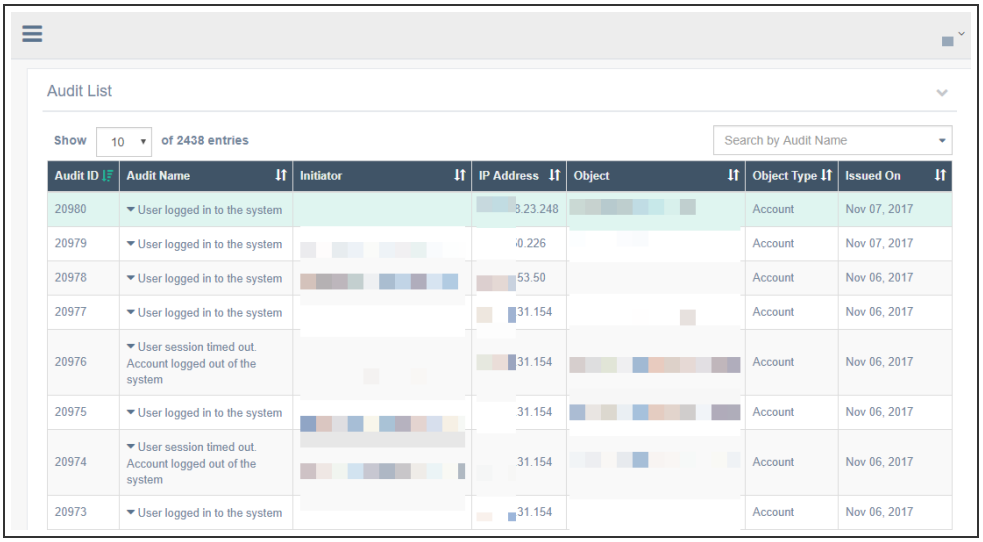
Field	Description
Alarm ID	The ID for the alarm.
Alarm Type (free-text search)	A free-text search for Alarm Type.
Object	An object in the beSECURE system (for example, an account, scan, organization, contact, etc.).
Severity	An integer representing the severity level of the alarm.

Field	Description
Alarm Type (List)	The type of alarm. Choose from the options in a drop-down list.
Status	The status of the Alarm. Choose from Unacknowledged, Acknowledged, Handled, and Under Investigation.
Issued On	The date the alarm was generated. Enter a From date and To date to narrow the search results to a specified time range.
Show Handled	A toggle for including or excluding alarms withthe status Handled in the search results.



The Alarm List page.

5. Click on an alarm in the list.



The Audit Details page.

The Audit Details page displays the following information:

Field	Description
Alarm ID	The ID for the alarm.
Alarm Type	The type of alarm.
Additional Information	The scan number and network that generated the alarm.
Object	An object in the beSECURE system (for example, an account, scan, organization, contact, etc.).
Severity	An integer from 1 (lowest) to 10 (highest) representing the severity level of the alarm.
Issued On	The date the alarm was issued.
Status	The status of the alarm. Values are Unacknowledged, Acknowledged, Handled, and Under Investigation.

Modifying an Alarm

New alarms enter the system with the status Unacknowledged. They appear on the Alarm List and the Home page.

To change the status of an alarm:

1. Log in to beSECURE with administrative privileges.
2. Make sure the **DevOps** role is selected.
3. Click **Admin** > **Alarms**.
4. Enter text in the search bar at the top to search by Alarm Type, or click the arrow in the search box to open the advanced search options. You can also use the navigation buttons at the bottom to page through the list of alarms.
5. Select the alarm to edit from the list.
6. Click the button corresponding to the new status. For a new alarm, the choices are **Acknowledge**, **Handled**, and **Under Investigation**.
7. Confirm your choice in the confirmation window that appears.

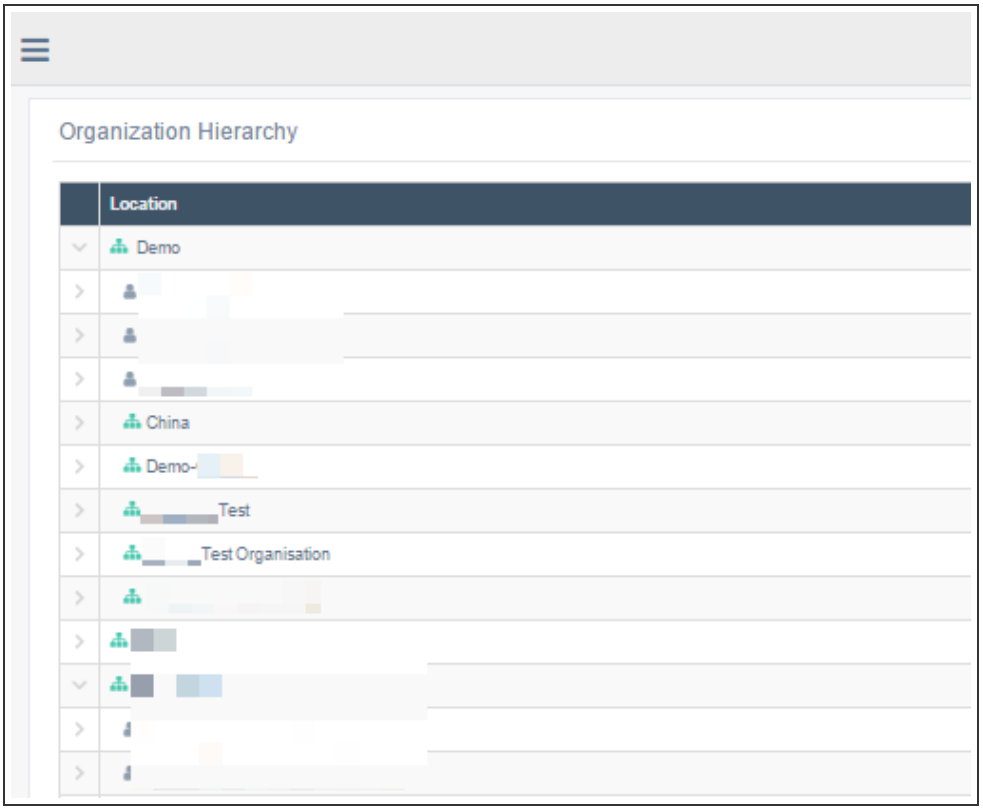
> **NOTE:** The beSECURE system will register the action you take in the alarm tracking database. It will also appear on the Alarm Details page.

Viewing Organization Hierarchies

The beSECURE system allows you to define complex, multi-level organizational structures. For example, a large company might have “Headquarters” as the main, or parent, organization, with sub- Organizations for the sales department, marketing department, London office, and so on. The Organization Hierarchies area provides an overview of your Organization’s structure.

To view an Organization Hierarchy:

1. Log in to beSECURE with administrative privileges.
2. Make sure **DevOps** mode is selected.
3. Click **Admin** > **Organizations** > **Organization Hierarchy**.



The Organization Hierarchy page.

One or more organizations may appear on this page. An organization is indicated by a green organizational chart icon. To expand the hierarchy for an organization, clicking on the arrow in the first column. For example, in the image above, the hierarchy for the Organization named Demo has been expanded to reveal three sub-entities. In this case, they are users, as indicated by the gray “person” icon. Machines are indicated by a scan icon (computer).

Clicking on a name in the hierarchy will open the Details page for that entity.