AT&T Cybersecurity

AT&T Business

USM Central™

Operations Guide

Updated May 22, 2024

Contents

USM Central Web User Interface (UI) 5

USM Central Deployments 8

- USM Central Deployment Process 10
- USM Central Connections 10
- View Deployments 25

Alarms Management 29

- Alarms List View 31
- Selecting Alarms in Alarm List View 44
- Searching Alarms 45
- View Alarm Details 58
- Labeling the Alarms 73
- Alarm Status 79
- Create an Alarms Report 82

Vulnerabilities 84

- Vulnerabilities Page List View 85
- Searching Vulnerabilities 88
- View Vulnerabilities Details 92
- Labeling the Vulnerabilities 95
- Create Vulnerabilities Report 96

Configuration Issues 99

- Configuration Issues List View 100
- Searching Configuration Issues 103
- Viewing Configuration Issues Details 105
- Create Configuration Issues Report 107

Orchestration Rules Management 110

- Alarm Rules from the Orchestration Rules Page 111

Filtering Rules from the Orchestration Rules Page 115
Notification Rules from the Orchestration Rules Page 118
Suppression Rules from the Orchestration Rules Page 123
Response Action Rules from the Orchestration Rules Page 127

Saved Reports 133

System Events Management 138
USM Central System Events List View 139
Searching System Events 140
Viewing System Event Details 142

User Management 144
Creating Users 146
Role-Based Access Control (RBAC) in USM Central 148
Editing Users 151
Managing Your Profile Settings 154
Deleting Users 161
Configuring Web UI Session Timeout 162
Regulated Deployment Access 163
Using Multi-Factor Authentication 165
User Account Protections 168

USM Central Web User Interface (UI)

The LevelBlue USM Central web user interface (UI) provides access to your connected deployment so you can manage its security. From the USM Central web UI, you can view all essential information, like alarms, vulnerabilities, configuration issues, deployments, system events, system settings, and rules for each deployment. This interface enables you to connect existing deployments or create new ones. You can also create new users in the USM Central instance.

Note: The recommended screen resolution for viewing the USM Central web UI is 1440 pixels wide.

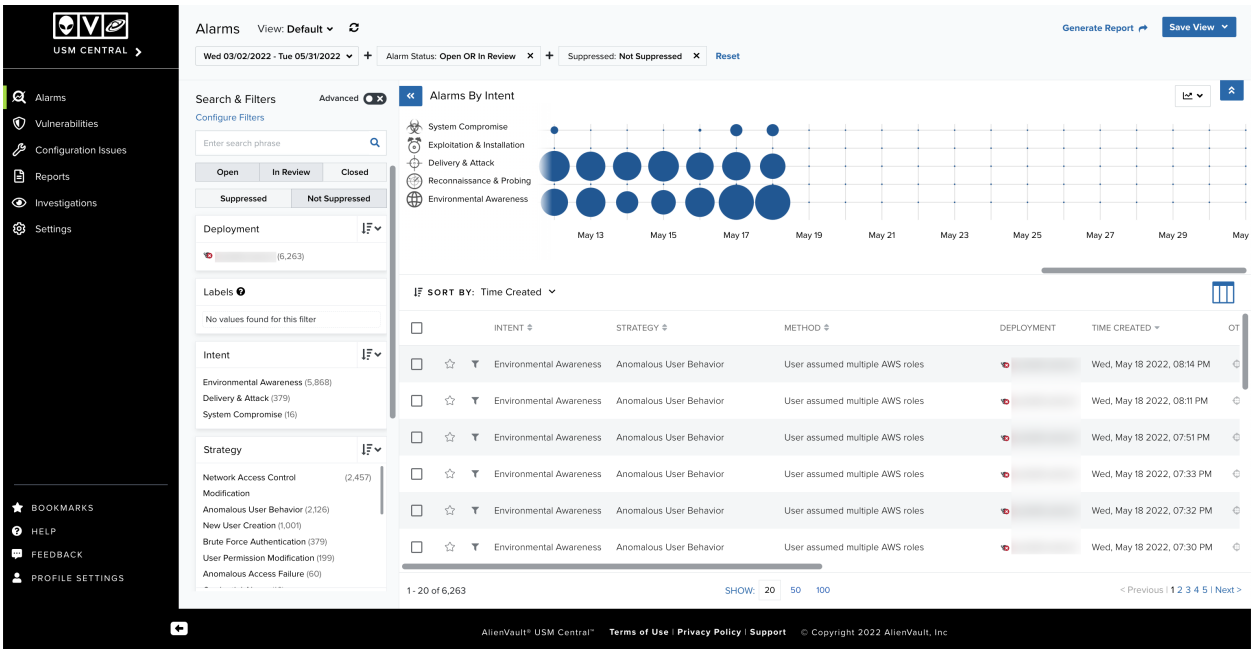
For the USM Central web UI to load successfully, it needs to access some external URLs in addition to the one reserved for the USM Central instance. If your company operates in a highly secure environment, you must change permissions on your firewall for USM Central to gain access. The following table summarizes the URLs that the USM Central web UI uses.

The following table shows the URLs used by USM Central.

URLs Used by USM Central

URL	Ports	Purpose
<your USM Central subdomain>.alienvault.cloud	443	USM Central ongoing communication
api-iam.intercom.io	443	USM Central in-product announcements
cdn.amplitude.com	8080	USM Central telemetry data collection
events.split.io	443	USM Central feature flags
sdk.split.io	8080	USM Central feature flags
www.google-analytics.com	443	USM Central website traffic analysis

The USM Central web UI runs in any standard web browsers. When you first log in, it displays the Alarms main page.



The main navigable elements and expand selections are provided consistently through the web UI. Use the ← and → icons to expand or collapse the left navigation pane.

Important: You can also load the default landing page by clicking the logo of USM Central located in the upper-left corner of the page.

Primary Menu

The primary menu provides access to the main functions or operations of USM Central. These include the following:

- **USM Central**: Displays a list of connected deployments. Select a deployment in the list to open the console for the deployment in another browser tab or page.

  Note: Either the admin IP address or the virtual private network (VPN) endpoint IP address must be routable from the browser for the link to work.

- **Alarms**: Displays alarms and enables the search, sorting, filtered selection, and visualization of the alarms. See Alarms Management for more information.
- **Vulnerabilities**: Displays vulnerabilities display and enables the management of the vulnerabilities. See Vulnerabilities for more information.
- **Configuration Issues**: Displays configuration issues and enables the management of the configuration issues. See Configuration Issues for more information.

- **Reports**: Displays reports that result from the export data that you c an find in alarms, vulnerabilities, and configuration issues, and enables the management of the reports. You can also choose the format of the report (PDF and CSV). See Saved Reports for more information.
- **Settings**: Provides access options to view and manage connected deployments. This option also enables you to manage users, system events, orchestration rules, and set a session timeout. See View Deployments, User Management, System Events Management, Orchestration Rules Management, and Configuring Web UI Session Timeout for more information.

Secondary Menu

The secondary menu provides access to the system configuration, the user profile information, the help link, and the bookmarked items:

- **Bookmarks**: The ★ icon enables you to see and access alarms, vulnerabilities, and configuration issues that you bookmarked for easy access. The number on the icon indicates the number of items bookmarked.
- **Help**: The ? icon includes these options:
  - **Documentation**: Links to online documentation.
  - **Support**: Links to the LevelBlue Support page.
- **Feedback**: The icon provides direct line of communication with the USM Anywhere team.
- **Profile Settings**: The icon includes these options:
  - **Profile**: Opens the profile settings page where you can change your full name, update your password, enable multi-factor authentication (MFA) for the account, configure an interval for auto-refreshing the alarms page. See Using Multi-Factor Authentication and Managing Your Profile Settings for more information.
  - **API Clients**: Opens the API Clients on the profile settings page. See API Clients for more information.
  - **Logout**: This option logout the user.

> **Note:** On the LevelBlue website, you can see the Introduction to USM Central video, which introduces you to USM Central and reviews its capabilities. This video includes a recorded demonstration of USM Central and an orientation to the web UI.

USM Central Deployments

USM Central enables you to centrally monitor multiple, distributed USM Anywhere and USM Appliance deployments from a single console.

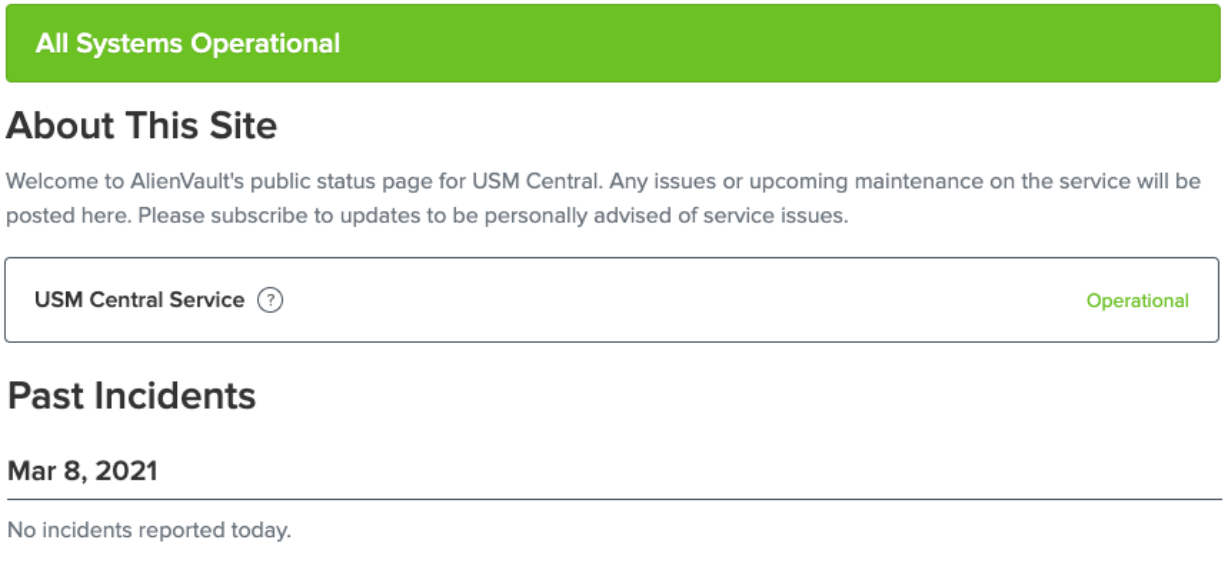
LevelBlue Managed Security Service Providers (MSSPs) and managed service providers (MSPs) that use the USM platform to provide security-monitoring services to their end customers can collect and investigate alarms within USM Central. In addition, USM Central gives MSSPs a consolidated view of the threats detected in their end-customer environments so that they can work efficiently and respond quickly to security incidents.

USM Central also enables large, heavily distributed organizations to connect multiple LevelBlue USM platform instances at various locations, and to centrally monitor and respond to all alarm activity across all deployments. This federated model is ideal for geographically distributed retail organizations, large enterprises with many departmental entities, and federal, state, and local governments with separate departments that require separate management but with centralized security monitoring. See USM Anywhere Data Security for more information on how data security is managed in the USM Central and USM Anywhere environments.

USM Central works best in the latest desktop version of the following web browsers:

- Google Chrome
- Mozilla Firefox

The USM Central updates occur automatically as new versions become available. The update is transparent, requires no action on your part, and runs in the background. If you want to be notified about the USM Central updates and incidents, subscribe to the USM CentralStatus page.



Topics covered in this section include:

USM Central Deployment Process 10

USM Central Connections 10

View Deployments 25

USM Central Deployment Process

The deployment process begins when a request for USM Central is received by a deployment either USM Anywhere or USM Appliance. There are three steps you need to complete your initial USM Central deployment.

Step 1: Register for LevelBlue USM Central

When you or your account manager contact LevelBlue and make a request for USM Central, LevelBlue will collect all the necessary information for deployment, including the email address that will be used to set up your initial user associated with the deployment.

Step 2: Activate the Account

After registering for LevelBlue USM Central, you will receive an email containing a link with instructions on how to set up your USM Central account. Click the link to set your password and activate your account.

Step 3: Connect Your Existing Deployments

Once USM Central is activated, you can connect your existing deployments of USM Anywhere and USM Appliance, and begin using USM Central.

See USM Anywhere Connections for connecting USM Anywhere deployments.

See USM Appliance Connections for connecting USM Appliance deployments.

Note: If you do not have existing deployments, see USM Anywhere Deployment Process or USM Appliance Deployments for instructions on how to configure your deployments prior to connecting them to USM Central.

USM Central Connections

To manage a deployment, you must connect the deployment within your USM Central instance. You need to initiate the connection from inside the USM Anywhere or USM Appliance environment. Once USM Centralreceives the connection request, you can accept or decline the connection.

Ports and Connectivity

Through USM Central, you can connect multiple instances of USM Anywhere or USM Appliance.

USM Anywhere uses private networking in the cloud. There is no extra port requirement.

The required port for integrating a USM Appliance instance into a USM Central instance is 443, so USM Appliance needs to be able to reach out to the endpoint. For instance, `mymssp-central.alienvault.cloud:443` where `mymssp-central` is the subdomain your LevelBlue Managed Security Service Providers (MSSP) provides.

Initiate a Deployment Connection

The request for connection initiates from the USM Anywhere or USM Appliance deployment. This creates a connection request that is displayed in the USM Central Deployments page.

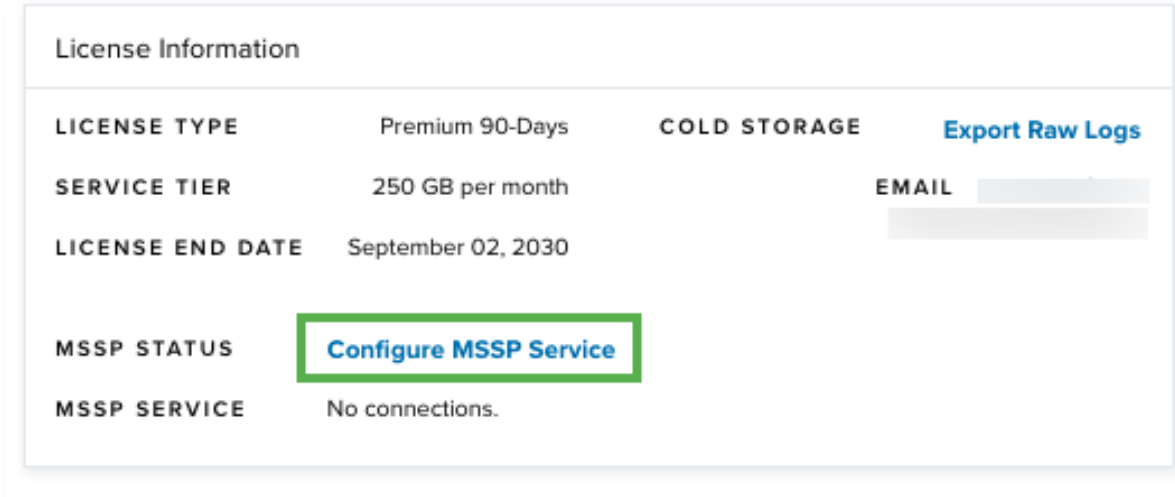
See USM Anywhere Connections and USM Appliance Connections for more information.

USM Anywhere Connections

To add a USM Anywhere deployment connection to a USM Central instance, you must initiate a connection from the USM Anywhere user interface (UI). If another user initiates the deployment connection, you must provide the domain for your USM Central instance.

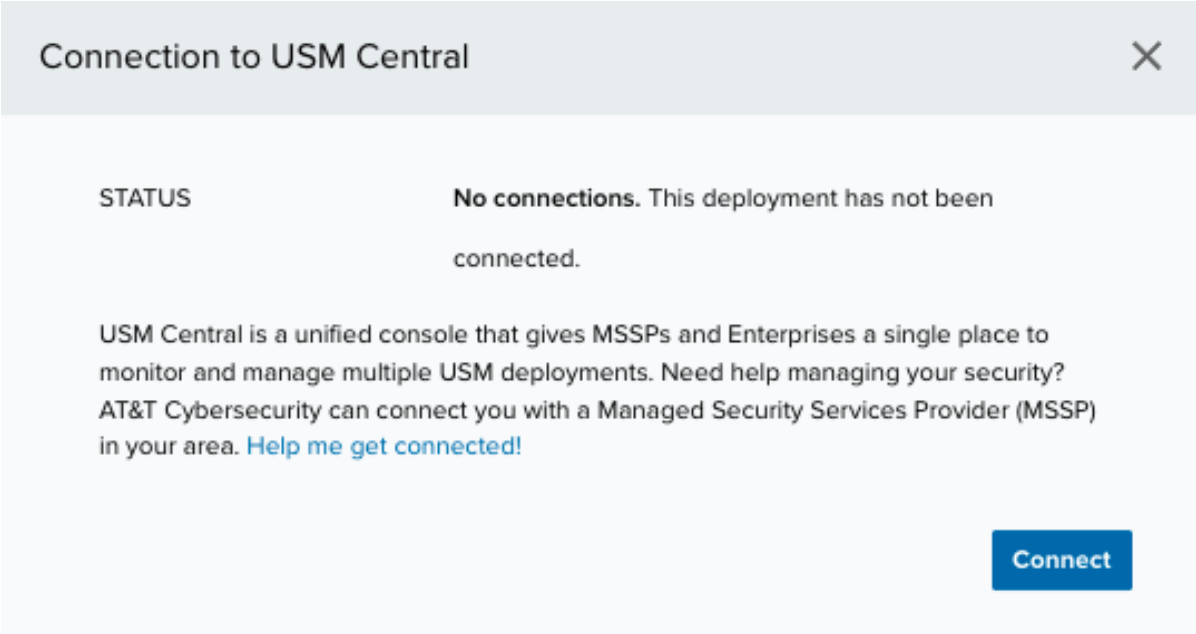
To initiate a connection to USM Central from USM Anywhere

1. In USM Anywhere, go to **Settings > My Subscription**.
2. Go to the License Information section.

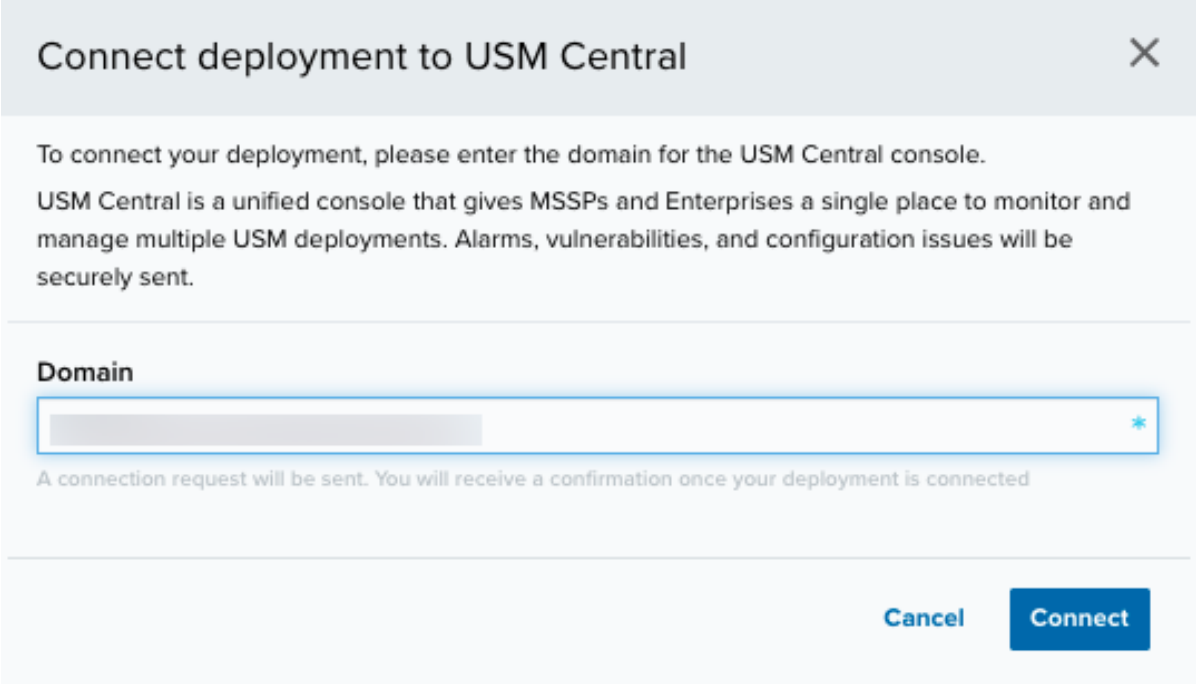


3. Click **Configure MSSP Service**.

   The Connect deployment to USM Central dialog box displays.

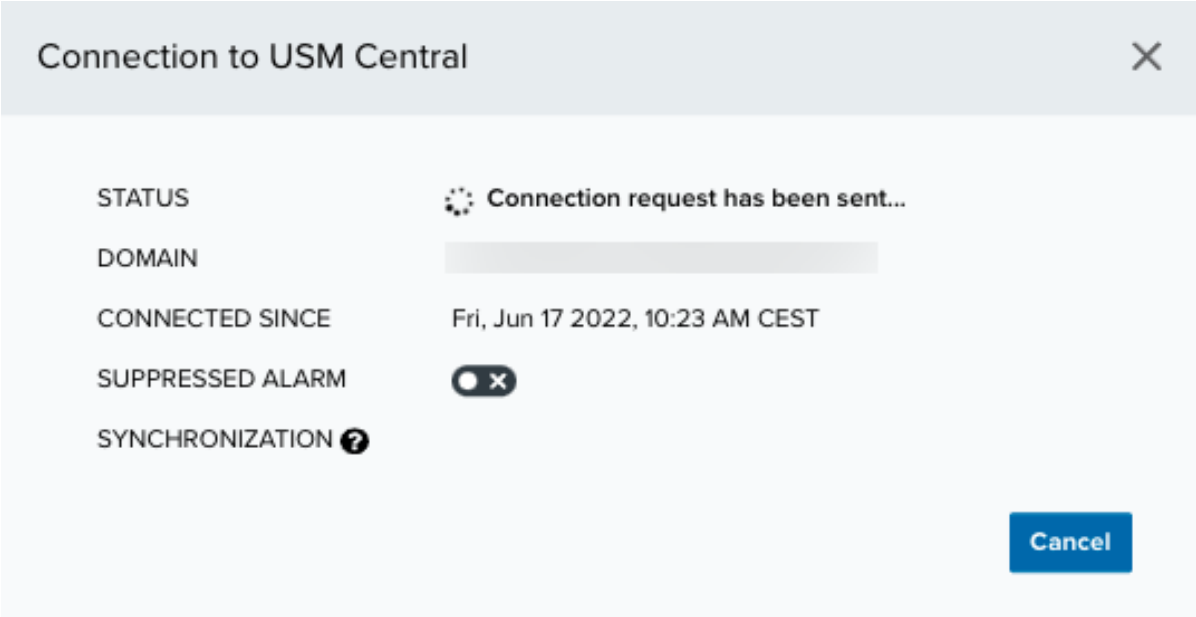


4. Click **Connect** and enter the domain for the USM Central instance.

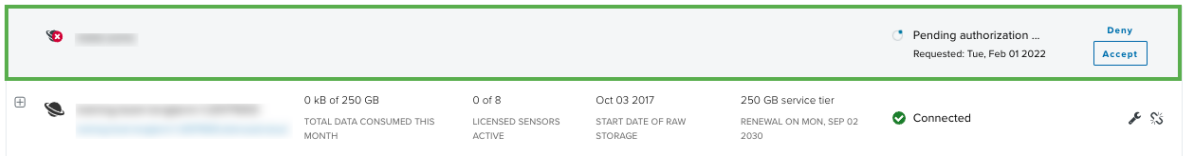


5. Click **Connect**.

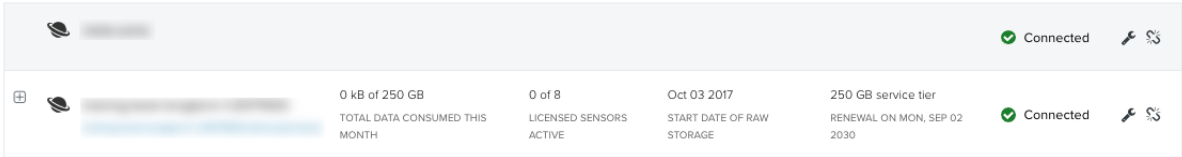
   From USM Anywhere, you see this dialog box.



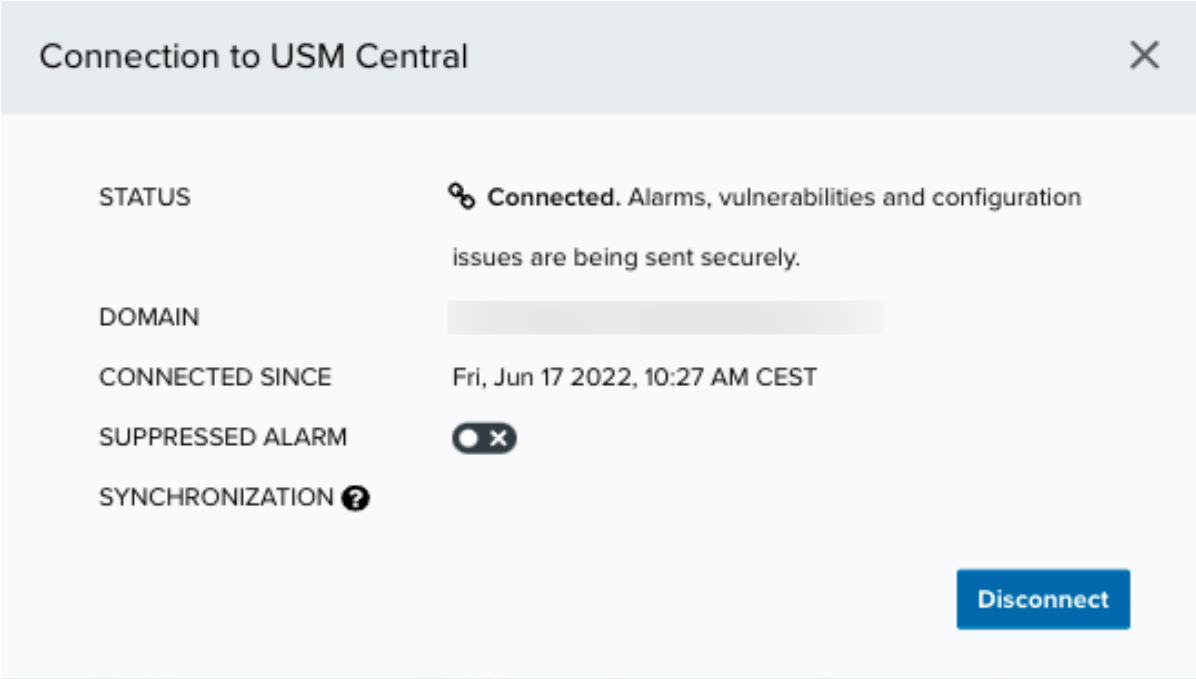
   The system sends a request to the USM Central. The connection is not complete until a USM Central user accepts the connection request.



6. Click **Accept**.
7. After several seconds, the deployment displays as **Connected** in USM Central.



This dialog box displays in USM Anywhere.



Important: Enable the suppressed alarm field to enable you to view and manage suppressed alarms in USM Central. If you enable this option, the load on USM Central increases.

Note: On LevelBlue website, you can see the Adding USM Anywhere to USM Central video, which describes how an existing USM Anywhere deployment is connected to USM Central. This video includes a recorded demonstration of the steps involved in configuring the connection and shows how the USM Anywhere information is represented.

Accept a Deployment Connection

As a user of USM Central, you can accept the connections initiated from a USM Anywhere deployment. This request is available in the USM Central web UI.

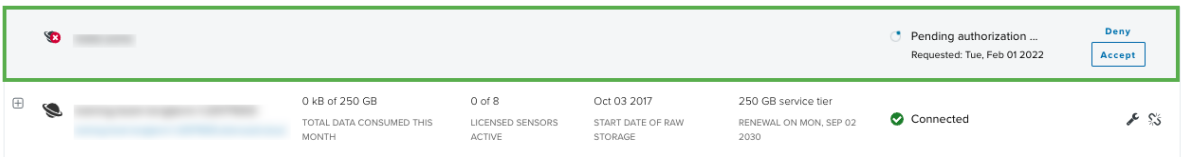
When you accept the connection, the deployment displays in your USM Central Deployments dashboard.

Your USM Central will receive alarms, vulnerabilities, and configuration issues from USM Anywhere connections.

To accept a connection in the USM Central web UI

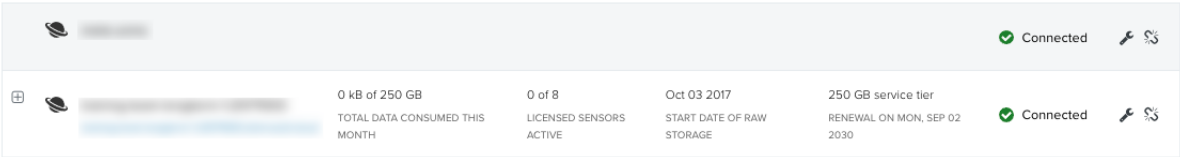
1. Go to **Settings > Deployments**.

   The new deployment displays.



2. Click **Accept**.

   After several seconds, the deployment displays as *Connected*.



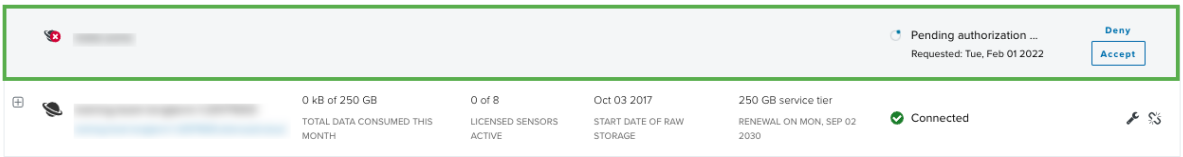
Decline a Connection

If you receive a request for connection by mistake or if there is some issue with making the connection, you can decline the connection request.

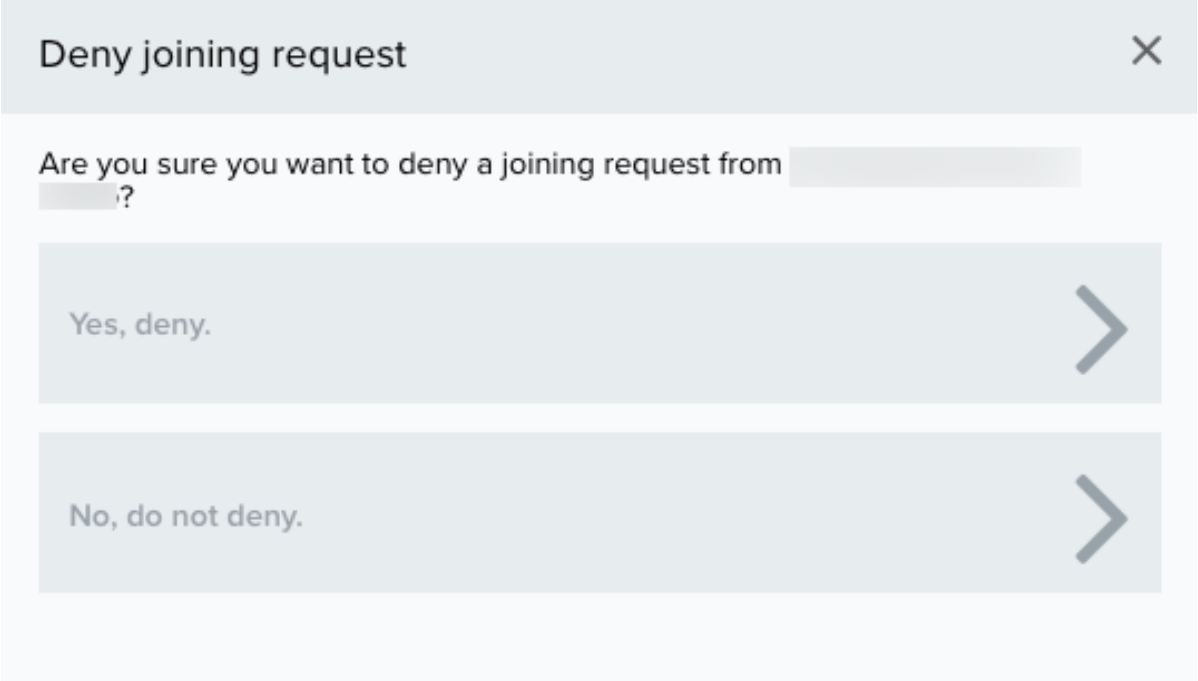
To decline a connection in the USM Central web UI

1. Go to **Settings > Deployments**.

   The new deployment displays.



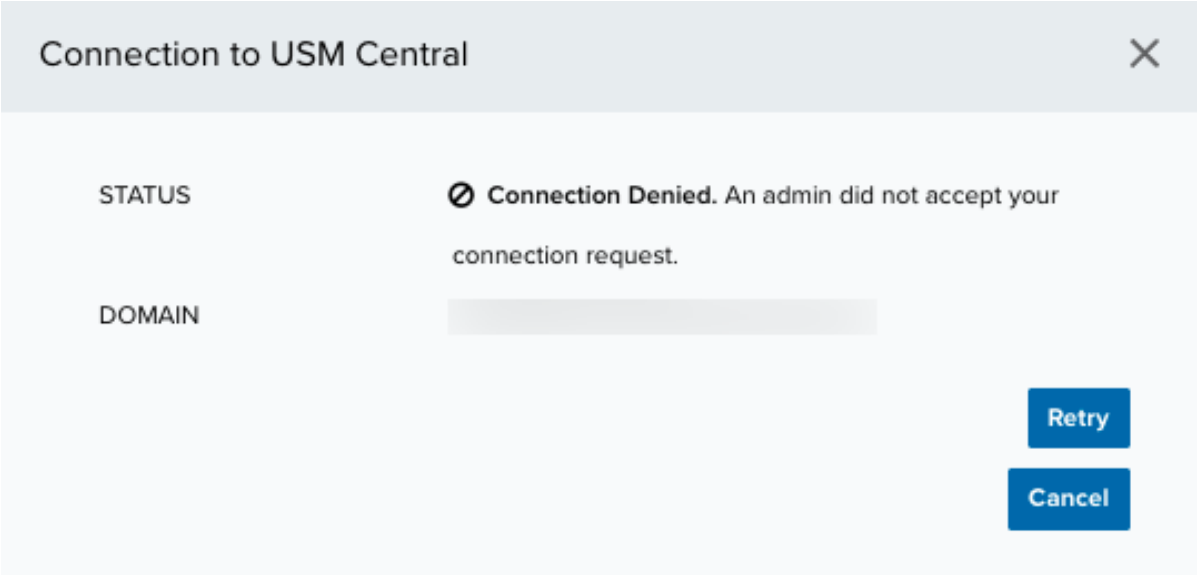
2. Click **Deny**.



   The connection doesn't display on the Deployments page of USM Central.

3. Go to your USM Anywhere instance and see that the status of the connections to USM

Central dialog box changes.



4. Click **Retry** if you want to try it again, or click **Cancel**.

Disconnect a Connection

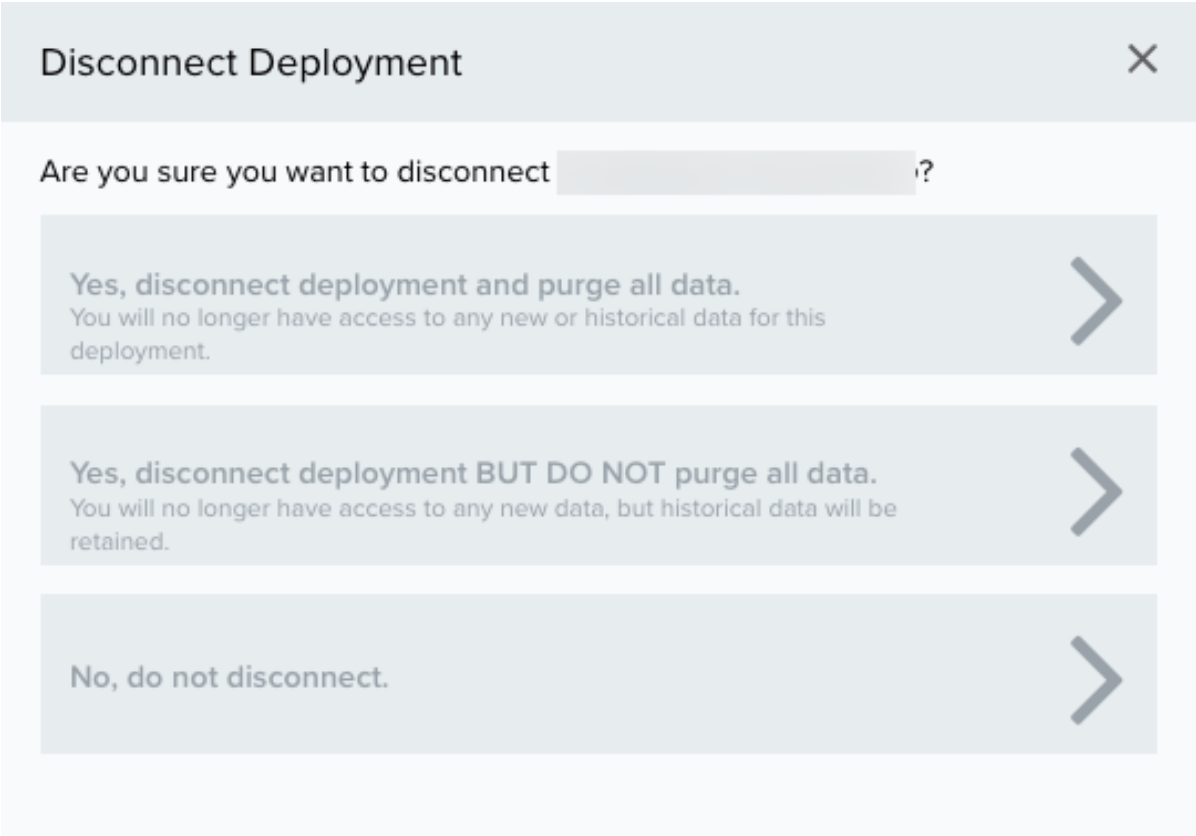
USM Anywhere and USM Central enable you to disconnect a connection.

To disconnect a connection from the USM Central web UI

1. Go to **Settings > Deployments**.

   Click the icon.

   The Disconnect Deployment dialog box opens.

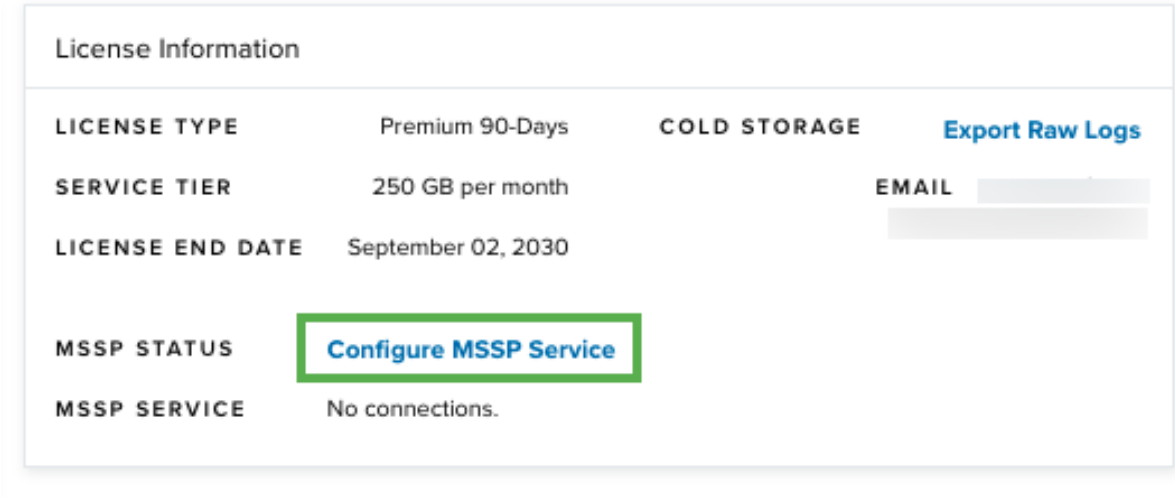


2. Choose one of these options:
   - **Yes, disconnect deployment and purge all data**: Use this option to disconnect the deployment and purge all historical data.
   - **Yes, disconnect deployment BUT DO NOT purge all data**: Use this option to disconnect the deployment. Alarms remain and your USM Anywhere shows them in the alarm list. The alarms are available if you connect the deployment again.
   - **No, do not disconnect**: Use this option to exit this dialog box without disconnecting the deployment.

To disconnect a connection from the USM Anywhere web UI

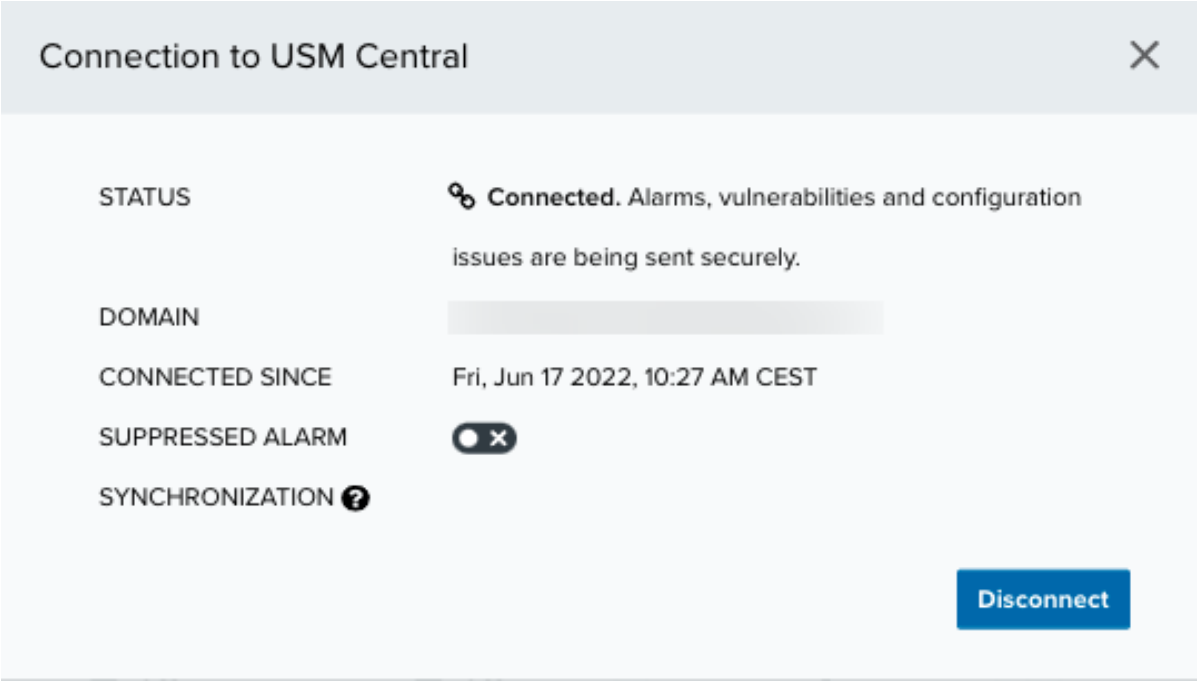
1. Go to **Settings > My Subscription**.

   Go to the License Information section.



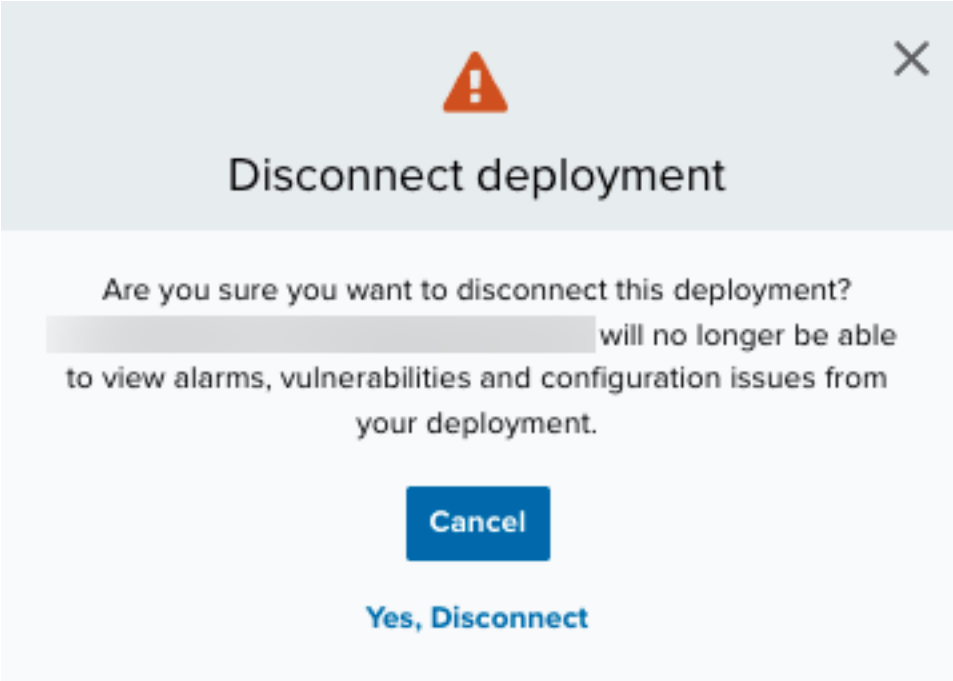
2. Click **Configure MSSP Service**.

   The Connection to USM Central dialog box opens.



3. Click **Disconnect**.

The Disconnect Deployment dialog box opens.



4. Click **Yes, Disconnect**.

USM Appliance Connections

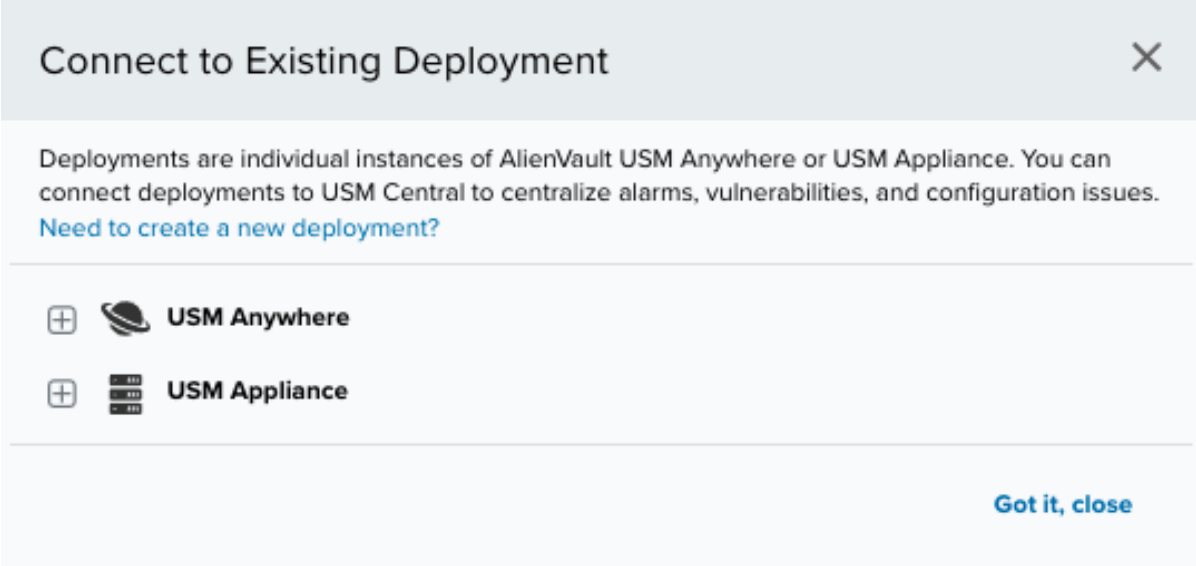
To add a USM Appliance deployment connection to a USM Central instance, you must initiate a connection from the USM Appliance web UI. The connection request from a USM Appliance deployment requires a token that you generate in the USM Central instance.

Important: Version 5.4.3 or later is required to add a USM Appliance deployment connection. Port 443 must be open between a USM Appliance and a USM Central instance.

To generate a token for a USM Appliance connection

1. In USM Central, go to **Settings > Deployments**.
2. Click **Connect to Existing Deployment**.

   The Connect to Existing Deployment dialog box opens.



3. Click the ⊞ icon next to USM Appliance.
4. Enter a name for the deployment that you want to connect.
5. Click **Generate Token**.
6. Click the icon to copy the token to your clipboard.

Connect to Existing Deployment

Deployments are individual instances of AlienVault USM Anywhere or USM Appliance. You can connect deployments to USM Central to centralize alarms, vulnerabilities, and configuration issues.
Need to create a new deployment?

USM Anywhere

USM Appliance

- Enter a name for the deployment and generate a token below.
- Log in to the Appliance deployment, navigate to **Configuration** > **Components** > **Servers**.
- Click **Connect To USM Central.**
- A connection request will be sent to your USM Central console.
- Enter the token to establish a connection. Once entered, the deployment will be automatically connected until sharing is terminated on either end.
- Show me the process

eyJzaWdBbGdvIjoiU0hBMjU2V2I0aFJTQSIsInRva2VuVHlwZSI6Ik1TU1BfVjVfQVVUSE9SSVpBVEIPTI9UT0tFTiIsInRva2VuSWQiOiIxODExNjY1OC1kNThiLTRkMDUtOTU2OC01YjMyNDMxMTM0NjMifQ==.eyJtc3NwSWQiOiJ0cmFpbmluZy10ZWFtLWNlbnRyYWwuYWxpZW52YXVsdC5jbG91ZCIsInRlbmFudE5hbWUiOiJhc2RmliwiY2xpZW50SWQiOiJ1bjJuWUJ4Mmx6UjNDQ2tkVm5uTXhNQ0VEYnhwMHBpcyIsIndoZW5Jc3N1ZWQiOjE2NDUwOTk2MjQ5MTcsInJlcXVlc3RlcklkIjoibmJhZW5hQGF0dC5jb20ifQ==.eyJzaWduYXR1cmUiOiJXdTM5MmtFazRRSWRSSlg3eStQWUc5a2ZRS2UwR0p1dm83UXM5RkJWV3V5azZsMGFsWURBR1dHWTIvL3FzN0ZNb0FFd0UyU0dJRi9DaDAvTWdtV2t0SXJoOWpSTGoyVWhFTUdjaXJja3dYWUJJTjFhOHovMm0rUTRkNXV5NWczRTE3bXBZTit2MlZWZUxFL3hHc2Z1d0hyc2ZWdXFYNWRqSVcyb29weHBKYXpMdWZlelBQZ2JRK24rSElxR0ZjczZ0RDRJbDJZTHdQNU95MIlvMkcrcGhpV05xYVRydk5RY09OU0Z4WjFPRFlqYkYzMWtOcHJkOVdRbC9xOGFCdktVakRzdGNHbDhrVk5vblhKNXZ3ZWlIZUVRbzBySnJBdDBHRVQ1SW43UFMrdHNmSXc4MFQvUzhDcUVhRnRDTVZQc0w3cEdJTkpkQm5BLzk3VUtETXI2QmdcdTAwM2RcdTAwM2QifQ==

Name of deployment:

This is the name that will be displayed in your USM Central console. No spaces or special characters.

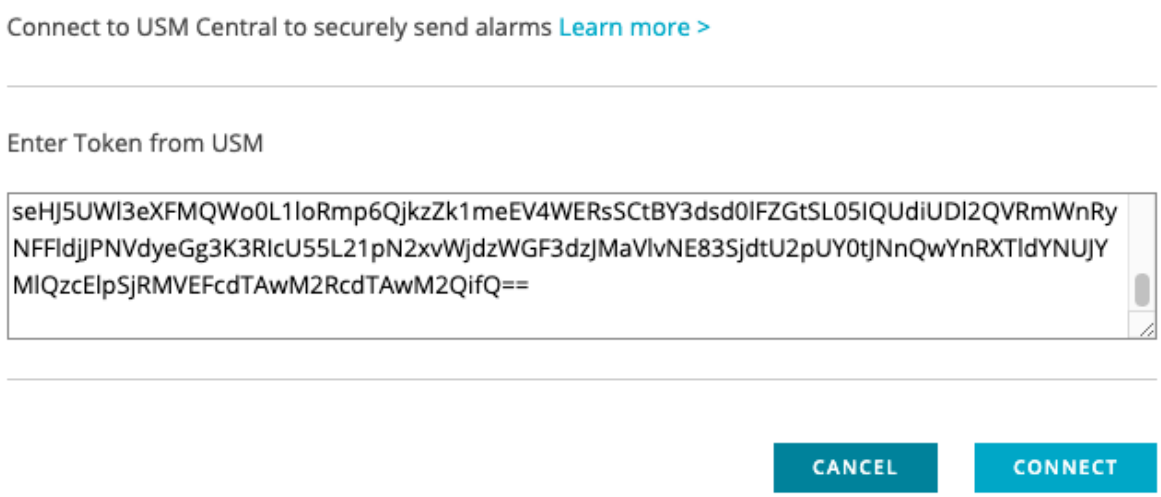
Generate Token

Got it, close

7. Paste the token into a secured file and send it to the user that is responsible for the USM Appliance deployment.
8. Click **Got it, close**.

To initiate a connection to USM Central from USM Appliance

1. In the USM Appliance web UI, go to **Configuration > Deployment > Components > Servers**.
2. Click the **Connect to USM Central** link.
3. Enter the token generated from USM Central.



4. Click **Connect**.

   The system sends a request to the USM Central.

   Upon acceptance, your USM Appliance deployment is automatically connected.

> **Note:** On the LevelBlue website, you can see the Adding USM Appliance to USM Central video, which describes how an existing USM Appliance deployment is connected to USM Central. This video includes a recorded demonstration of the steps involved in configuring the connection and shows how the USM Appliance information is represented.

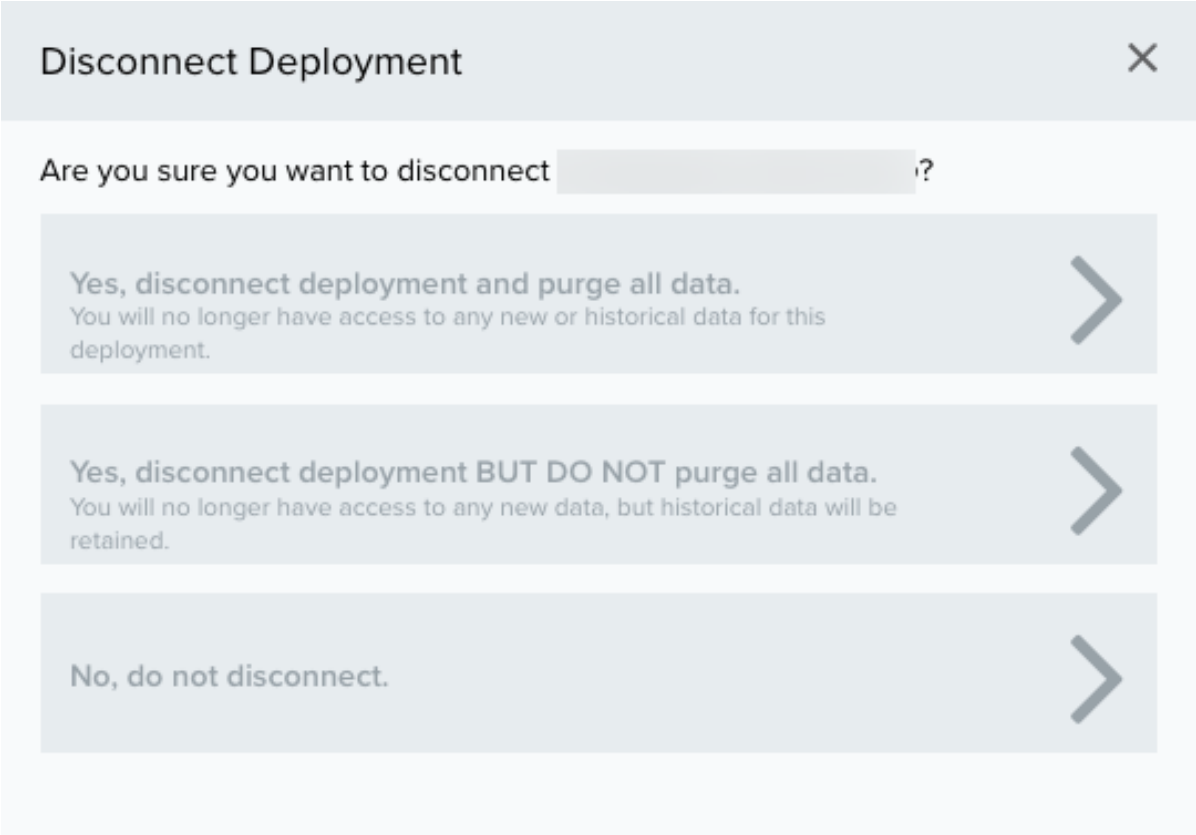
Disconnect a Connection

USM Appliance and USM Central enable you the option of disconnecting a connection.

To disconnect a connection from the USM Central web UI

1. Go to **Settings > Deployments.**
2. Click the icon.

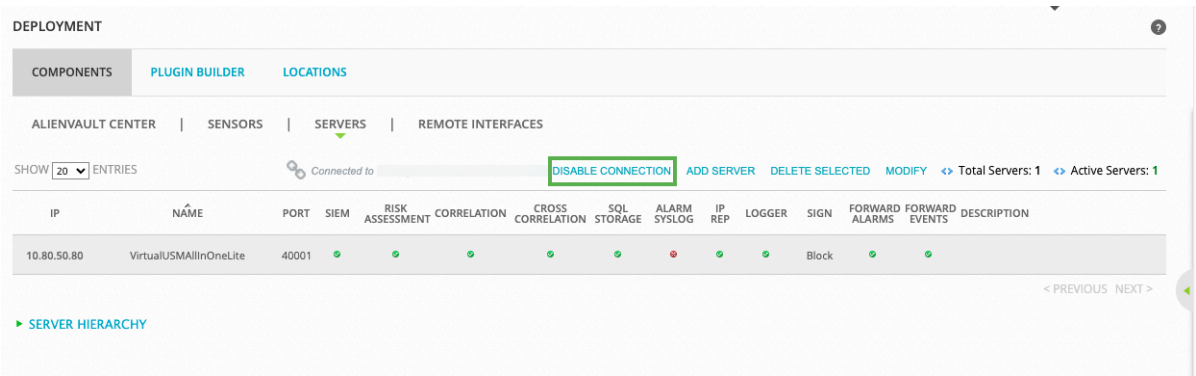
   The Disconnect Deployment dialog box opens.



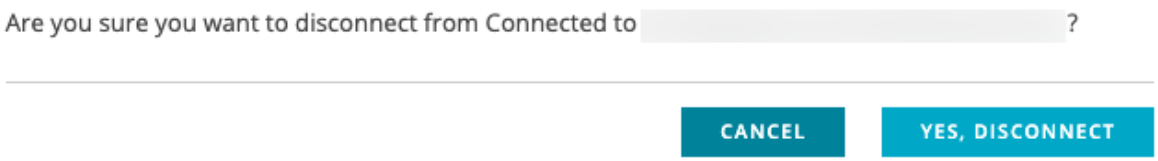
3. Choose one of these options:
   - **Yes, disconnect deployment and purge all data**: Use this option to disconnect the deployment and purge all historical data.
   - **Yes, disconnect deployment BUT DO NOT purge all data**: Use this option to disconnect the deployment. Alarms remain and are available if you connect the deployment again.
   - **No, do not disconnect**: Use this option to exit this dialog box without disconnecting the deployment.

To disconnect a connection from the USM Appliance web UI

1. In the USM Appliance web UI, go to **Configuration > Deployment > Components > Servers**.
2. Click **Disable Connection**.



A dialog box opens.



3. Click **Yes, Disconnect**.

View Deployments

In USM Central you can view multiple USM Anywhere and USM Appliance deployments. This enables you to easily drill down and investigate issues related to the connected environments. You can also modify the display name for a deployment to help identify it within the USM Central instance.

Deployment Status

The Deployments page lists all USM Anywhere and USM Appliance deployments associated with your USM Central environment. The list displays data consumption, sensors, storage, subscription, and connection status information for each deployment.

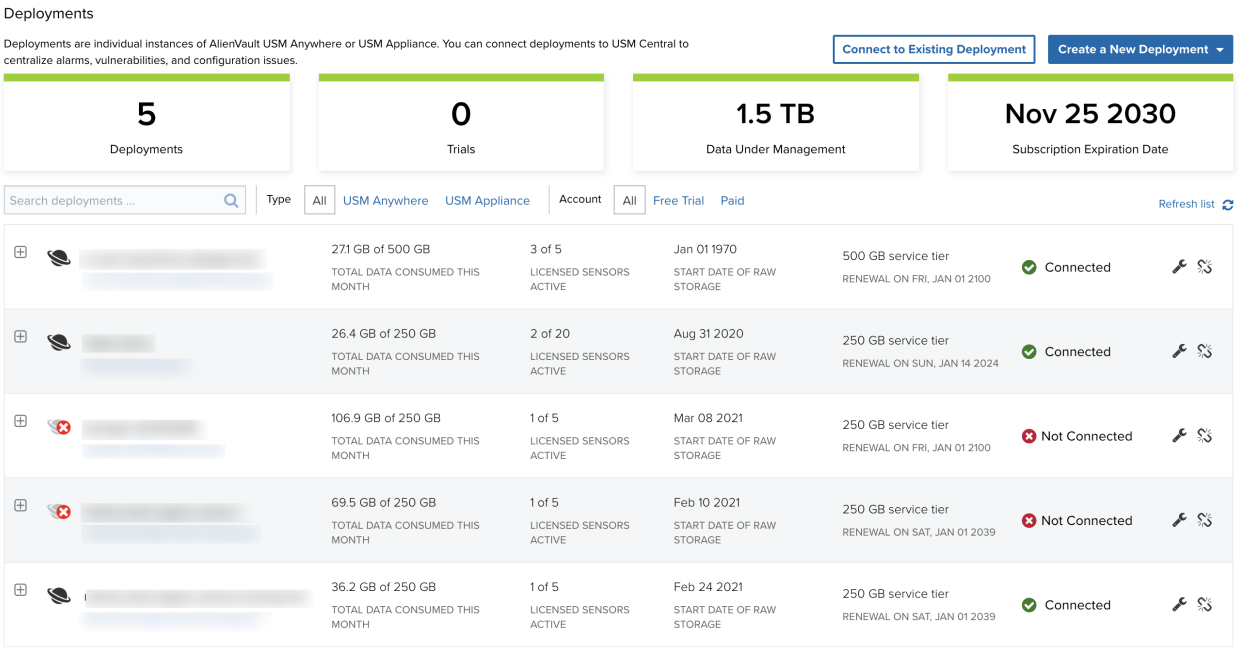
The following table shows the deployment status types.

Deployment Status Types

Status	Description
Connected	The deployment is connected to the USM Central environment.
Not Connected	The deployment is not currently connected to USM Central.
Connection Denied	A connection request was initiated from the deployment and the request was denied from the USM Central console.
Connection Request Sent	A connection request was initiated from the deployment and is awaiting an acceptance or denial. You can accept or decline the request in the USM Central console.
Connecting	The USM Central is waiting for a USM Anywhere connection. The USM Central is waiting until the token is entered in the USM Appliance.

Deployments Display

You can view all of your current deployments by navigating to **Settings > Deployments**. Here you can find the relevant data for all your deployments, including the number of deployments connected, subscription expiration dates, the amount of data under management, and the status of each individual deployment. You can also track the details of specific deployments, such as data usage, how many sensors are active, and the connectivity of the deployment. Click the ⊞ icon next to a deployment to expand its details.



Drill Down to a Specific Deployment

From USM Central, if your user role is Analyst or Manager, you can access any of the connected deployments without the need to log in. But if your user role is Read Only, you must enter your username and password to authenticate your access to the connected deployments.

To drill down to a specific deployment

1. Click the USM Central menu at the upper-left side of the page.

2. Click the deployment you want to access.

   Your browser opens a new tab or page to the web user interface (UI) for the deployment.

Create a New Deployment

If you want to connect to a deployment that does not yet exist, you can create a new USM Anywhere or USM Appliance deployment. After you create the new deployment, follow the instructions in USM Central Connections to connect it to your USM Central instance.

New USM Anywhere Deployment

Review the documentation for the USM Anywhere Deployment process and complete the tasks for a new deployment.

After a successful USM Anywhere deployment, follow the USM Anywhere Connections process to initiate a connection to USM Central.

New USM Appliance Deployment

Review the documentation for the USM Appliance Deployment process and complete the tasks for a new deployment.

After a successful USM Appliance deployment, follow the USM Appliance Connections process to initiate a connection to USM Central.

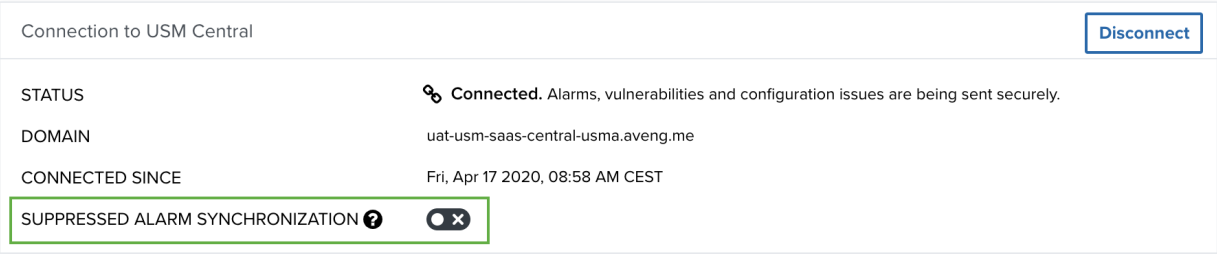
Alarms Management

USM Central provides a consolidated view of any alarms triggered within all of your connected deployments. The displayed alarms in USM Central are compiled from the connected deployments. An alarm consists of one or more events, based on the following:

- One or more rules performed by the correlation engine of USM Anywhere or USM Appliance, which analyzes these events for behavioral patterns. These rules look at and connect events to assess their priority and reliability and, when the system identifies a pattern, it generates an alarm, which requires attention and investigation. See Correlation Rules for more information.
- One orchestration rule, which is designed to raise an alarm when a particular type of event is found. See Orchestration Rules Management for more information.

USM Central displays the first 10 events associated with an alarm. If you need to see more events, you can drill into the specific deployment that created the original alert. See Drill Down to a Specific Deployment for more information.

Alarms in USM Anywhere that are suppressed or have a *closed* status are, by default, not forwarded to USM Central. You can have them forwarded from USM Anywhere by going to **Settings > My Subscription** in USM Anywhere and clicking the **Suppressed Alarm Synchronization** toggle.



Topics covered in this section include:

Alarms List View 31

Selecting Alarms in Alarm List View 44

Searching Alarms 45

View Alarm Details 58

Labeling the Alarms 73

Alarm Status 79

Create an Alarms Report 82

Alarms List View

Role Availability	Read-Only	Analyst	Manager

USM Central's Alarms page provides an overview of alarms triggered within connected deployments of USM Anywhere and USM Appliance. Here you can review all alarm activity, view only a select number of deployment alarms, or filter the alarms by specific details.

The Alarms page displays information on alarms. These are the different parts of the Alarms page:

- On the left side of the page are the search and filters options. Use filters to delimit your search.
- At the top of the page, you can see any filters you have applied, and you have the option to create and select different views of the alarms.
- The main part of the page is the list of alarms, where each row describes an individual alarm. Click an alarm to open a summary view. See Viewing Alarm Details for more information. Each alarm includes a check box that you can use to select it. You can select all alarms in the same page by clicking the check box in the first column of the header row. You can also select all the alarms in the system. See Selecting Alarms in Alarm List View for more information.

If you want to analyze the data, you can maximize the screen and hide the filter pane. Click the « icon to hide the filter pane. Click the icon to expand the filter pane.

Refreshing the page

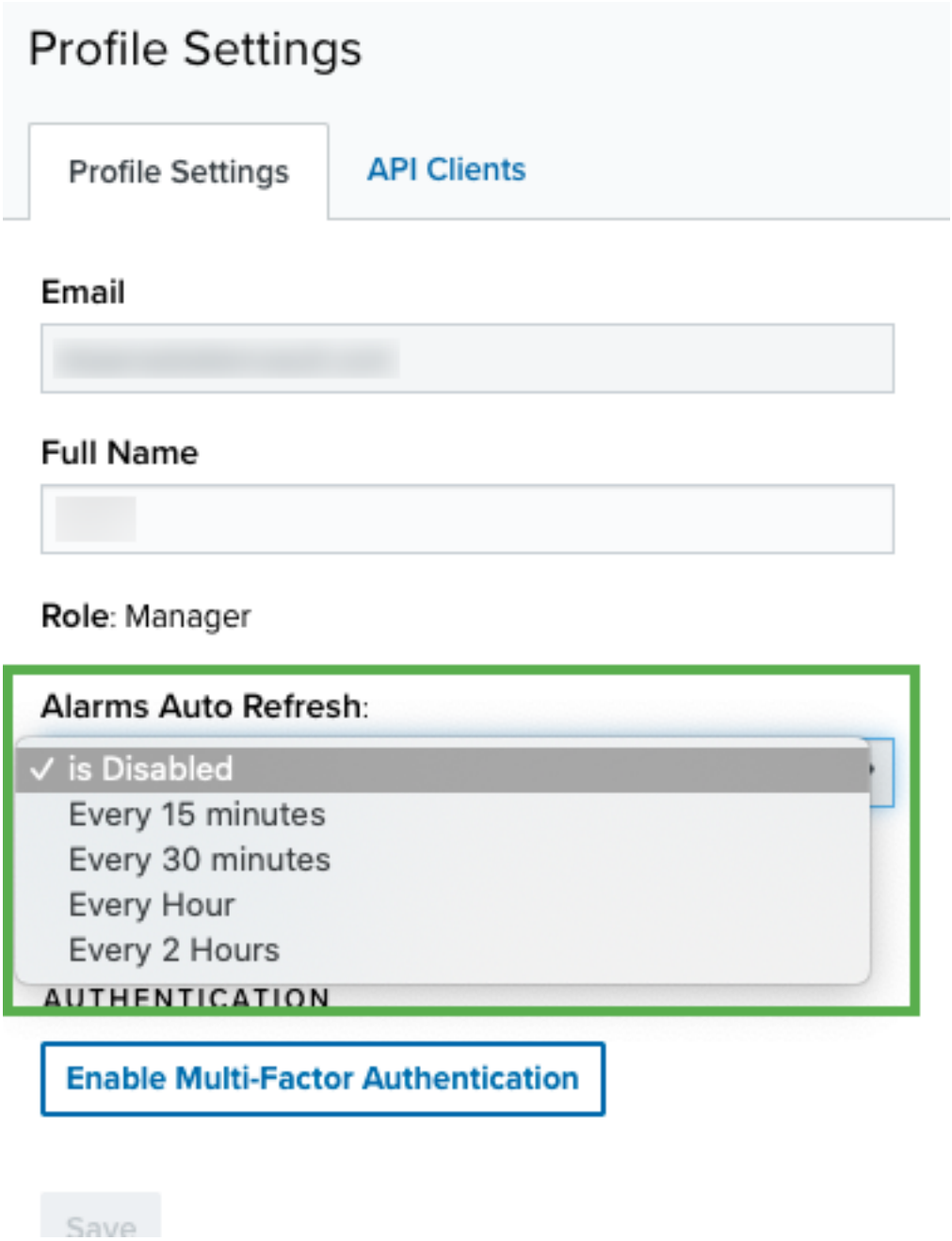
USM Central gives you the option of refreshing the page automatically in a period of time that you can configure.

Following the name of the view, you can click the icon to stop the auto-refresh countdown and refresh the page manually.

There is an auto-refresh countdown that refreshes the page at a regular interval. The number inside the blue circle indicates the remaining time until the next refresh. See Managing Your Profile Settings to configure this interval.

To enable the auto refresh option

1. At the bottom of the expanded pane of the USM Central web user interface (UI), hover over the profile settings options, and select **Profile**.
2. Click the **Alarms Auto Refresh** field and select **Every 15 Minutes**, **Every 30 Minutes**, **Every Hour**, or **Every 2 Hours**. Select **is Disabled** if you don't want the alarms to automatically refresh.



3. Click **Save**.

Alarm by Intent Graph

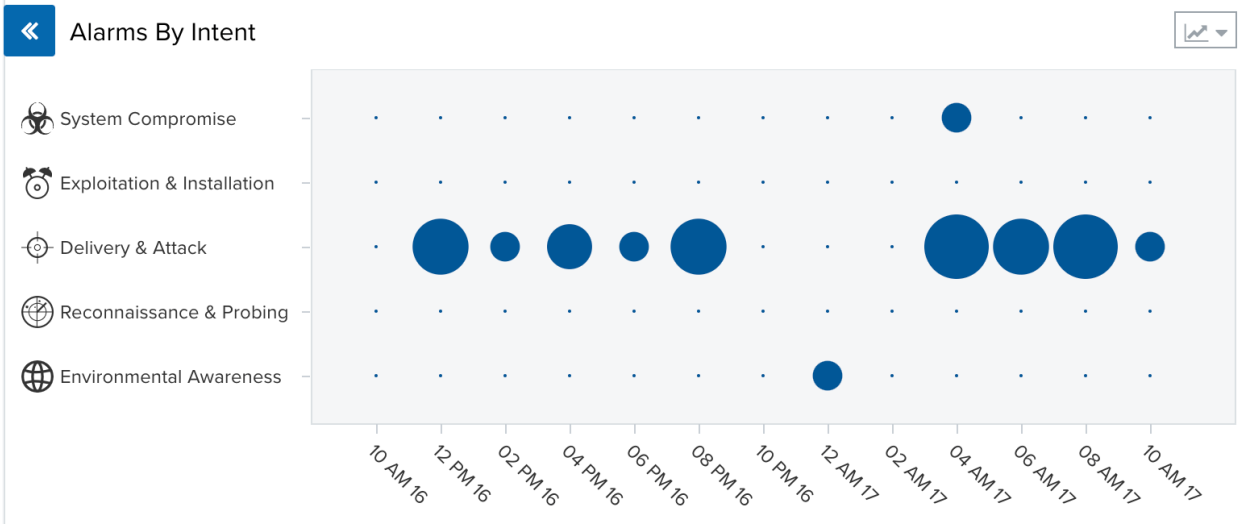
The Alarms by Intent graph in the middle of the page provides a graphical representation of alarms by intent. Blue circles indicate the number of times that an alarm in an intent showed. A bigger circle indicates a higher number of alarms. You can hover over each of the circles to

get the actual number of different types of intent. In addition, if you click any of the blue circles, they display only the alarms corresponding to that circle. You can change the displayed period of time by clicking the **Last 24 Hours** filter.

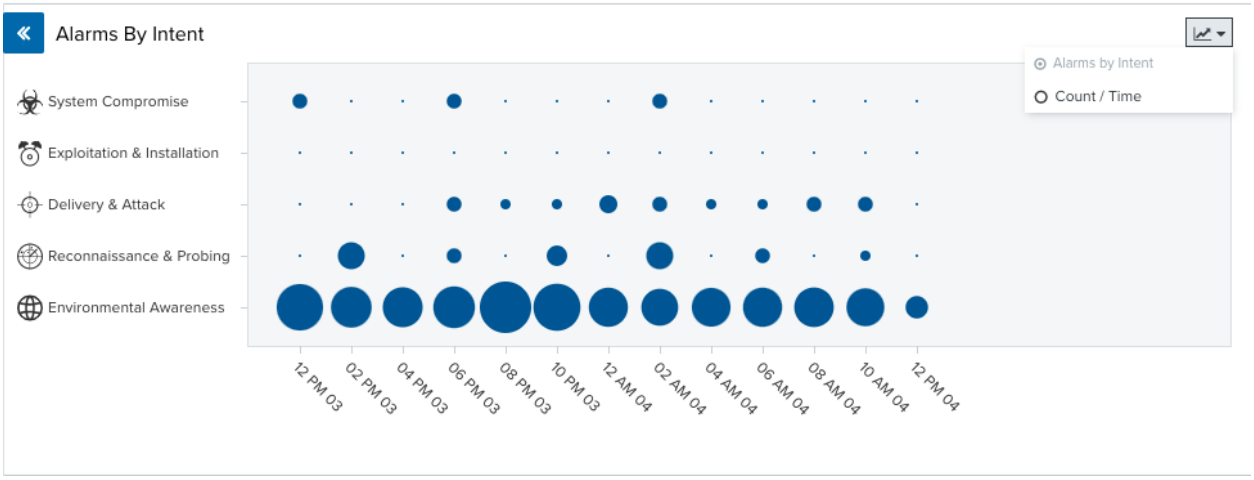
Alarms graphed by intent are sorted into five different categories, which are represented by the graphic icons in the display:

- Delivery & Attack ( )
- Environmental Awareness ( )
- Exploitation & Installation ( )
- Reconnaissance & Probing ( )
- System Compromise ( )

If you want to analyze the data and see the additional columns without having to scroll left and right, you can maximize the screen and hide the filter pane. Click the « icon to hide the filter pane. Click the icon to expand the filter pane.



Use the icon to change the alarms view, which is by default, Alarms by Intent.



Alarms List View

Role Availability	Read-Only	Analyst	Manager

USM Central's Alarms page provides an overview of alarms triggered within connected deployments of USM Anywhere and USM Appliance. Here you can review all alarm activity, view only a select number of deployment alarms, or filter the alarms by specific details.

The Alarms page displays information on alarms. These are the different parts of the Alarms page:

- On the left side of the page are the search and filters options. Use filters to delimit your search.
- At the top of the page, you can see any filters you have applied, and you have the option to create and select different views of the alarms.
- The main part of the page is the list of alarms, where each row describes an individual alarm. Click an alarm to open a summary view. See Viewing Alarm Details for more information. Each alarm includes a check box that you can use to select it. You can select all alarms in the same page by clicking the check box in the first column of the header row. You can also select all the alarms in the system. See Selecting Alarms in Alarm List View for more information.

If you want to analyze the data, you can maximize the screen and hide the filter pane. Click the « icon to hide the filter pane. Click the ▼ icon to expand the filter pane.

Refreshing the page

USM Central gives you the option of refreshing the page automatically in a period of time that you can configure.

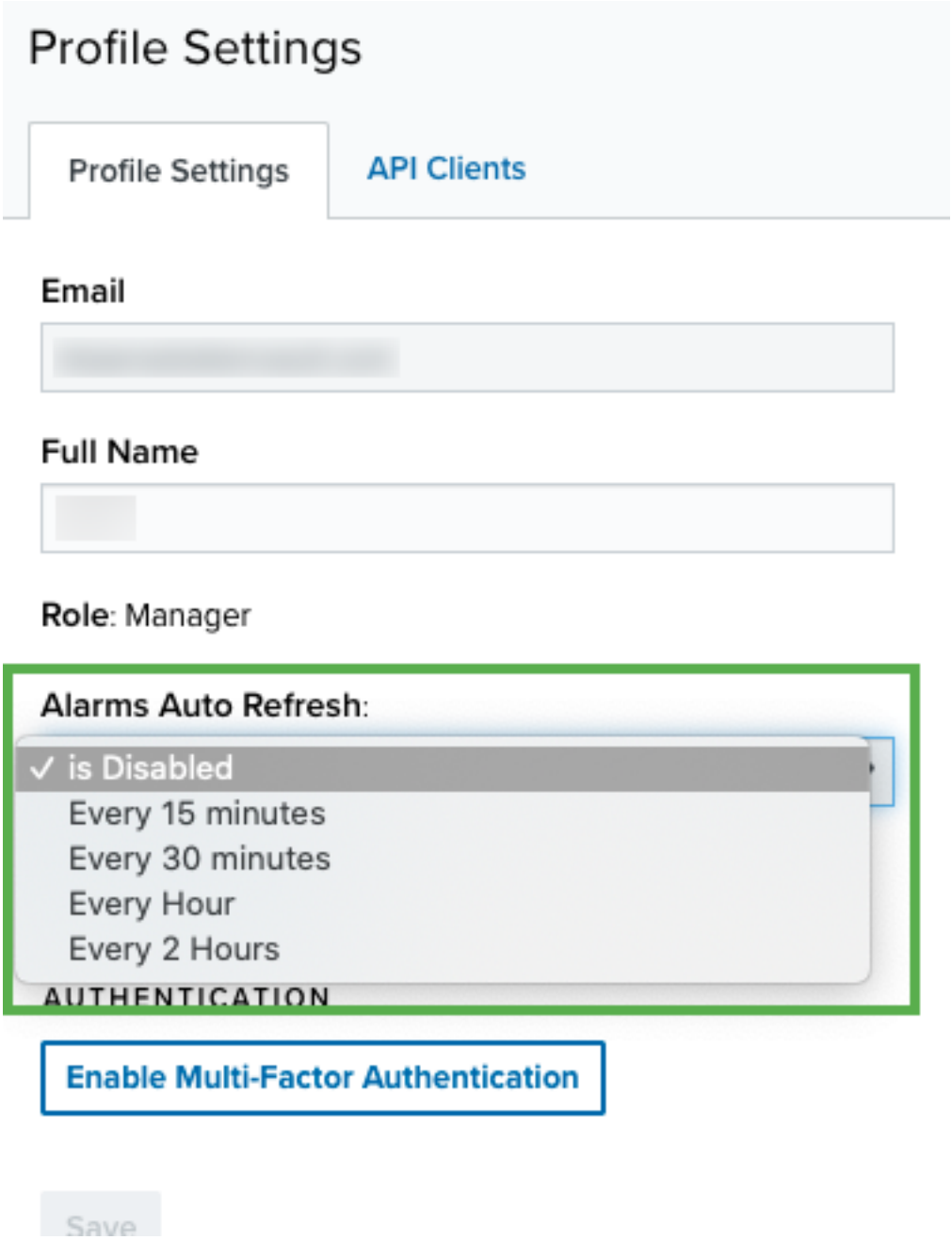
Following the name of the view, you can click the icon to stop the auto-refresh countdown and refresh the page manually.

There is an auto-refresh countdown that refreshes the page at a regular interval. The number inside the blue circle indicates the remaining time until the next refresh. See Managing Your Profile Settings to configure this interval.

To enable the auto refresh option

1. At the bottom of the expanded pane of the USM Central web user interface (UI), hover over the profile settings options, and select **Profile**.
2. Click the **Alarms Auto Refresh** field and select **Every 15 Minutes**, **Every 30 Minutes**, **Every Hour**, or **Every 2 Hours**. Select **is Disabled** if you don't want the alarms to

automatically refresh.



3. Click **Save**.

Alarm by Intent Graph

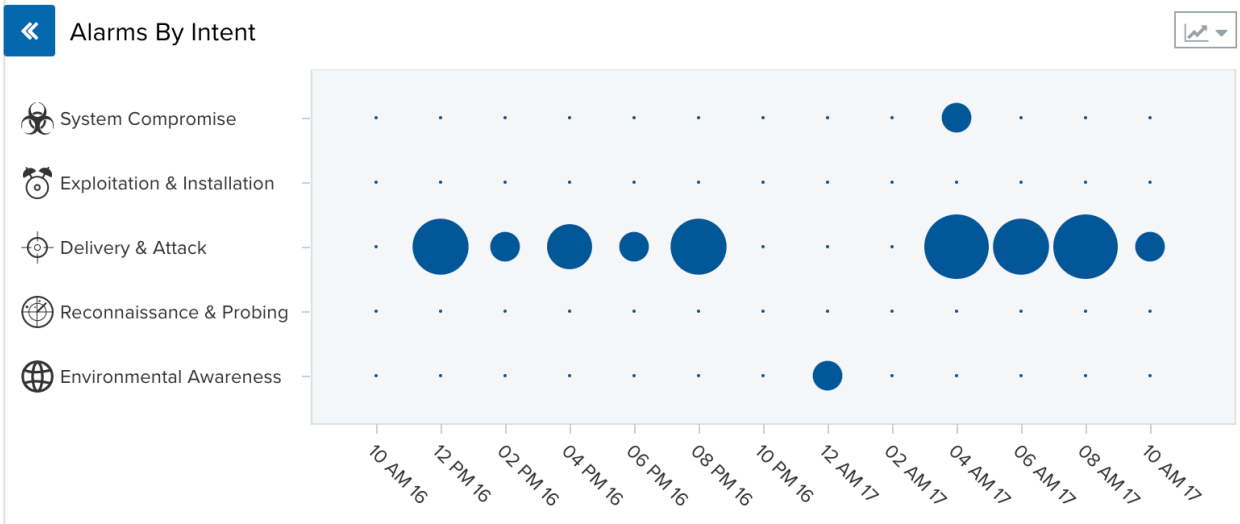
The Alarms by Intent graph in the middle of the page provides a graphical representation of alarms by intent. Blue circles indicate the number of times that an alarm in an intent showed. A bigger circle indicates a higher number of alarms. You can hover over each of the circles to

get the actual number of different types of intent. In addition, if you click any of the blue circles, they display only the alarms corresponding to that circle. You can change the displayed period of time by clicking the **Last 24 Hours** filter.

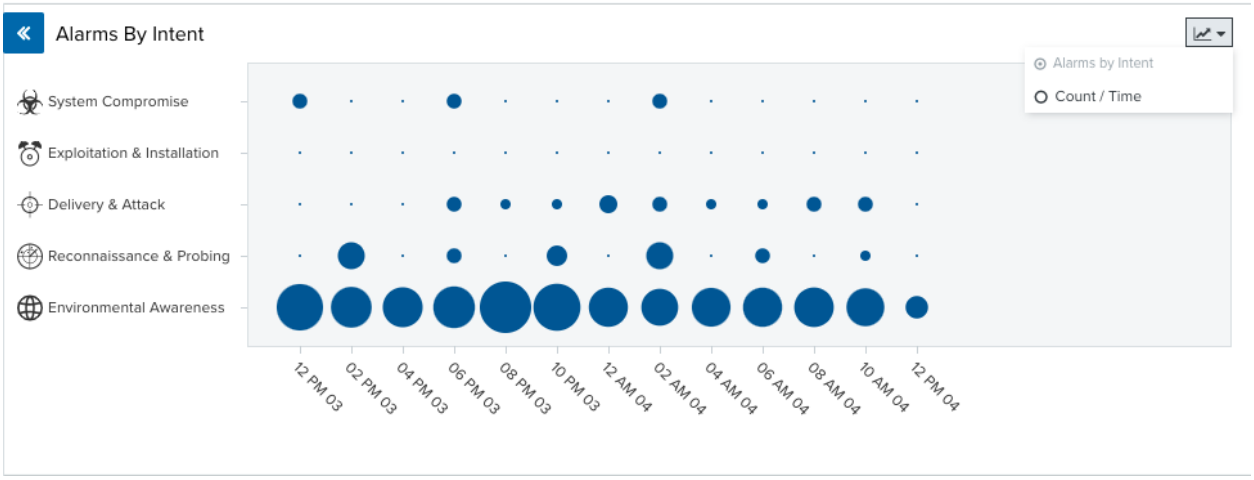
Alarms graphed by intent are sorted into five different categories, which are represented by the graphic icons in the display:

- Delivery & Attack ( )
- Environmental Awareness ( )
- Exploitation & Installation ( )
- Reconnaissance & Probing ( )
- System Compromise ( )

If you want to analyze the data and see the additional columns without having to scroll left and right, you can maximize the screen and hide the filter pane. Click the « icon to hide the filter pane. Click the icon to expand the filter pane.



Use the icon to change the alarms view, which is by default, Alarms by Intent.



Configuring Columns on Alarms

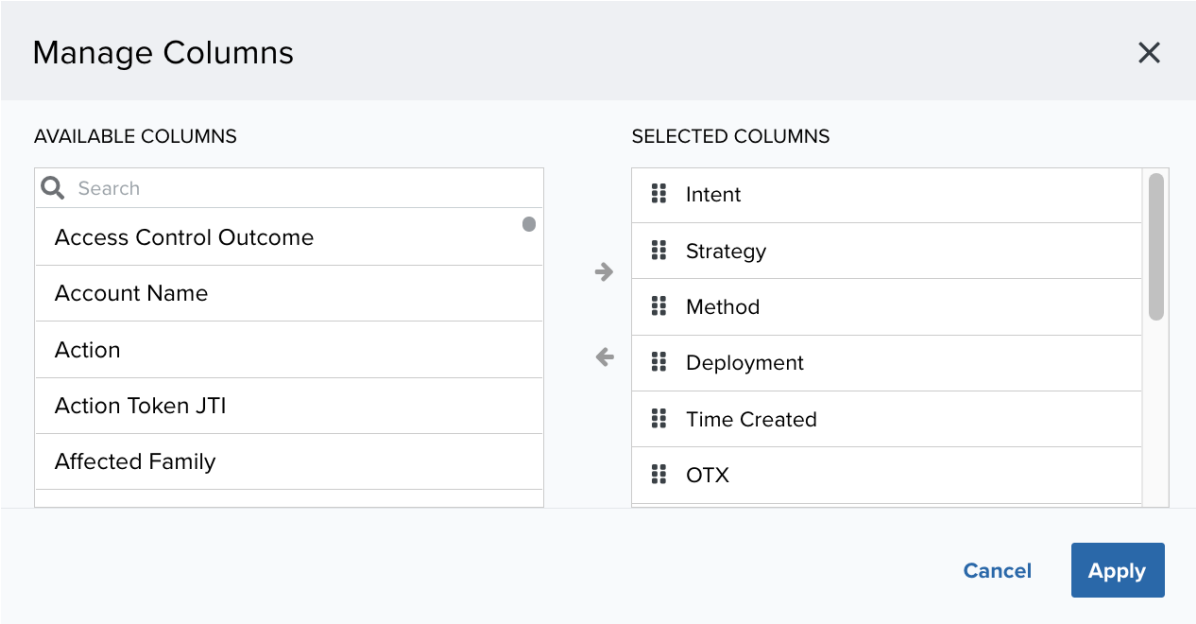
Role Availability	Read-Only	Analyst	Manager

Within the page, you can configure the columns and fields that display in the list view. You can also save your configuration settings for later use.

To configure your columns

1. From the alarms list view, click the icon.

   The Manage Columns dialog box opens.



2. Search the columns you want to have in the list view by using the search field.
3. Use the and icons to select or deselect from the available columns.
4. You can order the columns by clicking and dragging the column to the desired place.
5. Click **Apply**.

Note: If you generate a report when you have set custom columns, your report keeps the columns you have configured.

Important: If you want to keep your configuration, you need to save it by selecting **Save View > Save As**. Otherwise, your custom view is not kept when you move to another feature. See Alarms Views for more information.

Priority Field for Alarms

Role Availability	Read-Only	Analyst	Manager

In USM Central, all alarms have a Priority field, which indicates the importance of the alarm. This is a measurement to determine the impact of the alarm in the network.

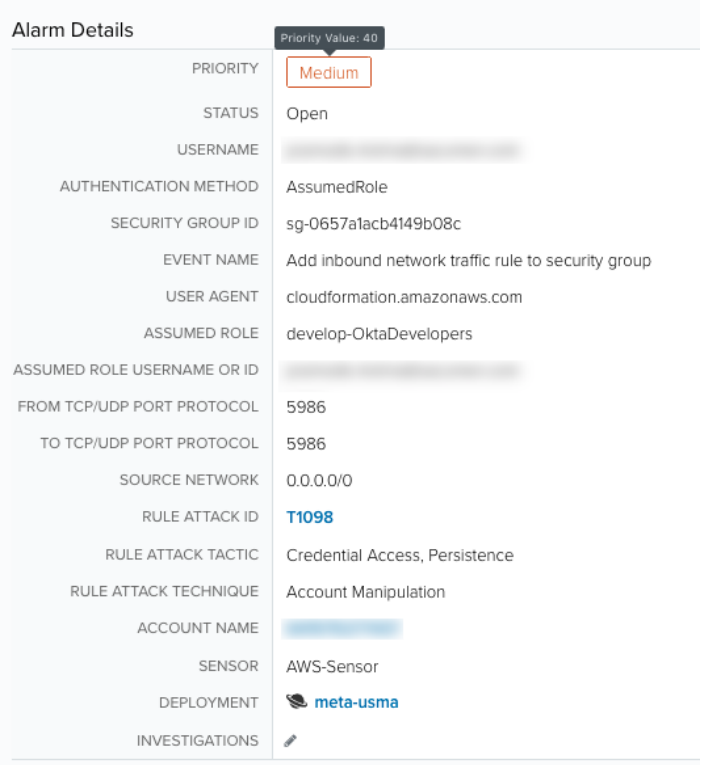
The Priority field can display Low, Medium, or High. This text comes from correlation and orchestration rules. When you create an orchestration rule, you must enter a priority value between 0 and 100. LevelBlue Labs™ creates the correlation rules and include a value. The LevelBlue Labs team sets the value for the correlation rules depending on how critical the alarm is.

The displayed text in the column of alarms depends on the value that the rule has according to this table:

Priority Field for Alarms

Displayed text	Value in the rule
Low	Between 0 and 33
Medium	Between 34 and 66
High	Between 67 and 100

Open the details of an alarm to learn the exact value of the priority level. See View Alarm Details for more information. After you are in the Alarm Details page, hover over the priority text and a dialog box will show you the exact value.



See Correlation Rules and Orchestration Rules Management for more information.

Alarms Views

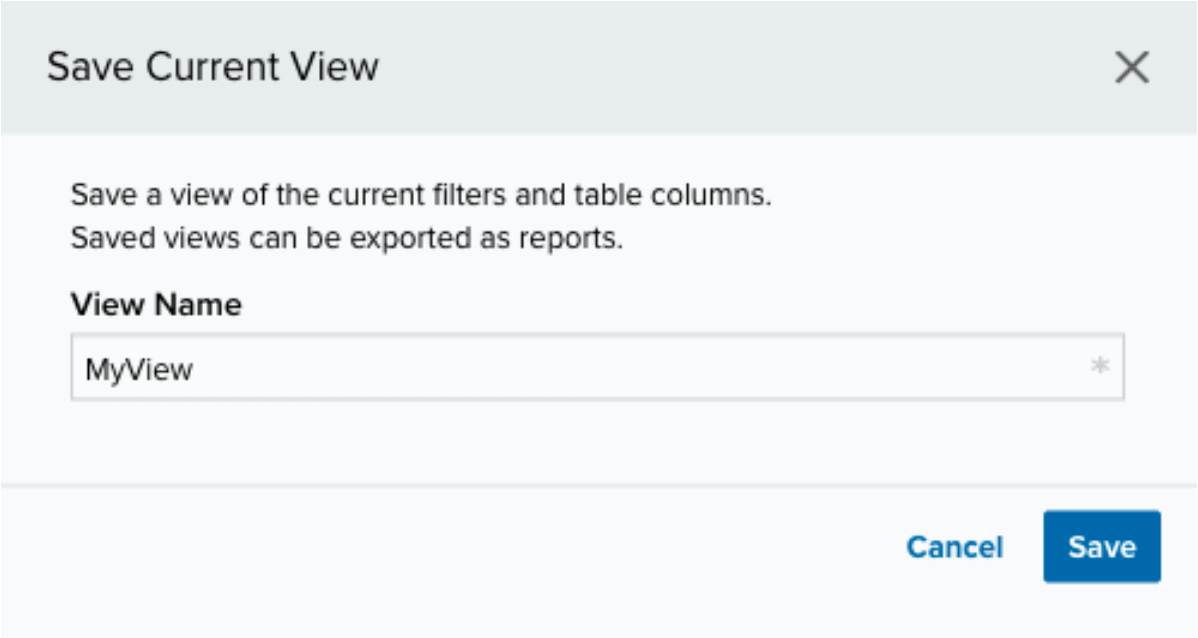
Role Availability	Read-Only	Analyst	Manager

You can configure the view you want for the list of items in the page.

To create a view configuration

1. From the list view, click the icon.
2. Use the and icons to pass the items from one column to another and select the columns you want to see.
3. Click **Apply**.
4. If you want to delimit the search, select the filters you want to apply.
5. Go to **Save View > Save As**.

The Save Current View dialog box opens.



6. Enter a name for the view.
7. Click **Save**.

   The created view is already selected.

To select a configured view

1. From the ist view, click **View** above the filters.
2. Click **Saved Views**, and then select the view you want to see.
3. Click **Apply**.

To delete a configured view

1. From the Alarms list view, click **View** above the filters.
2. Click **Saved Views**, and then click the 🗑 icon next to the saved view you want to delete.

   A Settings Delete dialog box opens to confirm the deletion.
3. Click **Accept**.

> **Important:** The 🗑 icon does not display if the view is selected.

Note: . You can only delete the views you have created .

Selecting Alarms in Alarm List View

Role Availability	Read-Only	Analyst	Manager

USM Central enables you to select an alarm or multiple alarms to add a label to the selected alarms.

To select a single alarm

- Select the checkbox to the left of the alarm.

To select multiple alarms

- Select the checkbox of each alarm that you want to include.
- You can go to the next page and select more alarms. USM Central does not preserve the selection on the previous page.

To select all the alarms on the same page

- Select the checkbox in the first column of the header row.

To select all the alarms returned from a search or all the alarms in the system

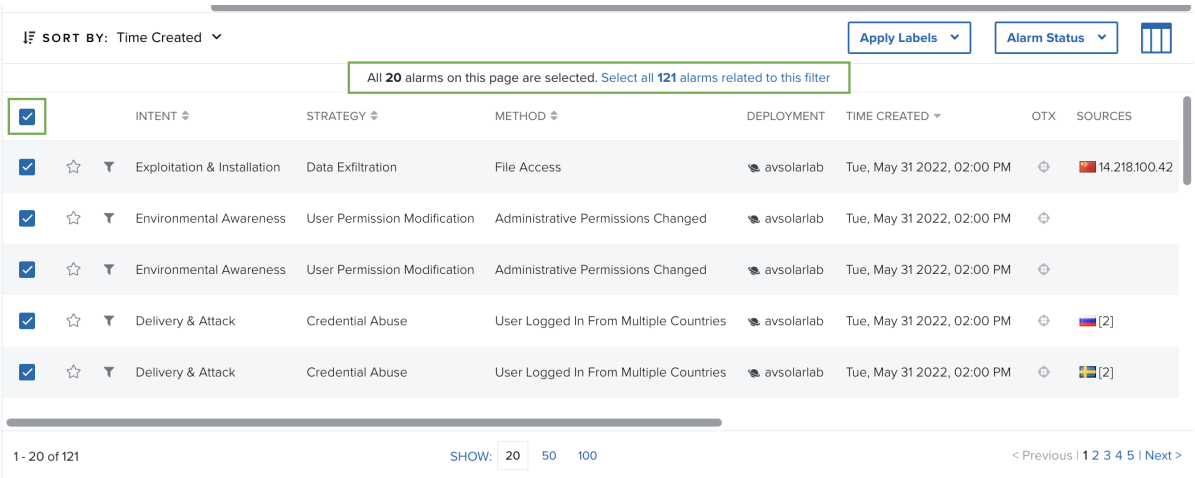
1. Select all the alarms on the page.

   Text similar to the following example displays above the alarm table:

   ```
   All 20 alarms on this page are selected. Select all 121 related to this filter
   ```

   where

121 is the number of alarms in the system.



2. To select all the alarms, click **Select all 121 related to this filter**.

Searching Alarms

Role Availability	Read-Only	Analyst	Manager

USM Central includes the option of searching items of interest on the page. There are several filters displayed by default. You can either filter your search or enter what you are looking for in the search field.

You can configure more filters and change which filters to display by clicking the **Configure Filters** link located in the upper-left side of the page. The management of filters is similar to that for assets. See Managing Filters for more information.

The following table lists the filters you see on the page.

Filters Displayed by Default in the Main Alarms Page

Filter Name	Meaning
Last 24 Hours	Identify alarms triggered in the last hour, 24 hours, 7 days, 30 days, or 90 days. You can also configure your own period of time by clicking the **Custom Range** option. This option enables you to customize a range. When you click **Custom Range**, a calendar opens. You can choose the first and last day to delimit your search by clicking the days on the calendar or entering the days directly. Then select the hours, minutes, and seconds by clicking the specific box. Finally, select **AM** or **PM**.
Open/In Review/Closed	Filter alarms by Alarm Status. See Alarm Status for more information.
Suppressed	Filter suppressed alarms.
Not Suppressed	Filter hidden suppressed alarms. The suppressed alarms are hidden by default.
Deployment	Filter alarms by the connected individual instances of USM Anywhere or USM Appliance.
Labels	Filter alarms by the applied labels. See Labeling the Alarms for more information.
Intent	Filter alarms by the purpose of the alarm. It can be Delivery & Attack, Environmental Awareness, Exploitation & Installation, Reconnaissance & Probing, and System Compromise. See Intent for more information.
Strategy	Filter alarms by the type of attack. See Strategy for more information.
Method	If known, filter alarms by the method of attack or infiltration associated with the indicator that generated the alarm. See Method for more information.
Sensors	Filter alarms by the associated USM Anywhere Sensor. See USM Anywhere Sensor Management for more information.

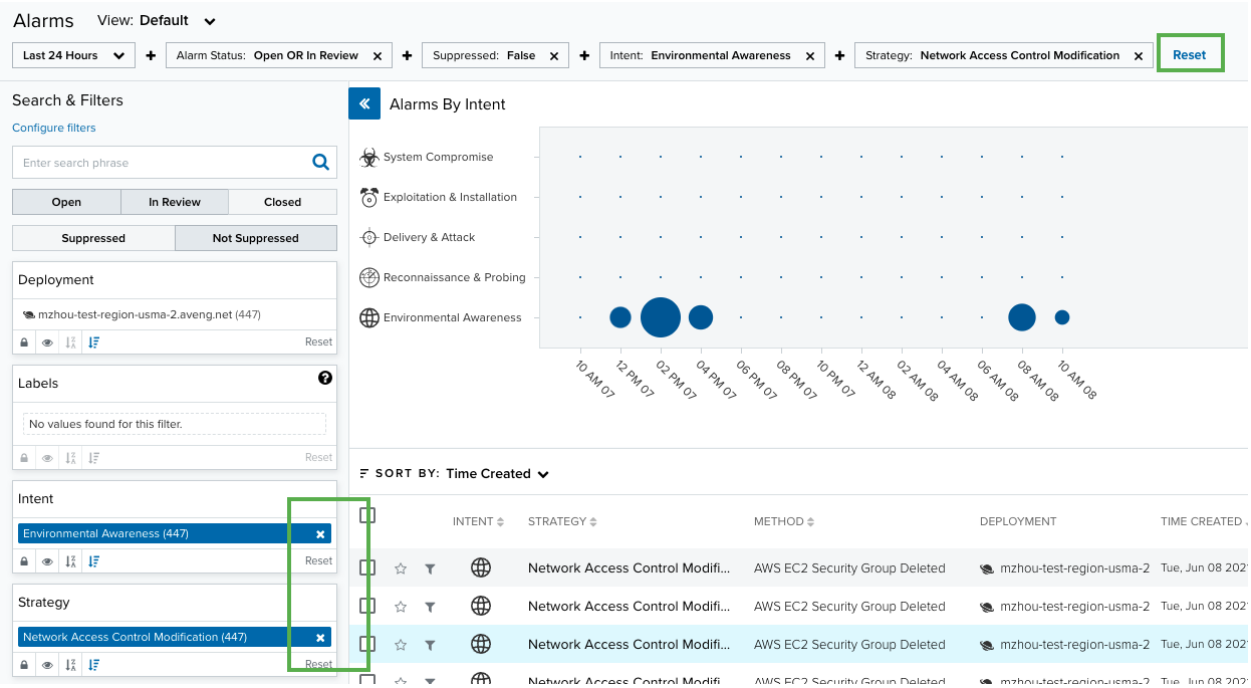
The number between brackets displayed by each filter indicates the number of items that matches the filter. You can also use the filter controls to provide a method of organizing your search and filtered results.

The following table shows the icons displayed with each filter box.

Icons Next to the Filter Title

Icon	Meaning
A Z Z A	Sort the filters alphabetically.
	Sort the filters by number of items that matches them

In the upper-left side of the page, you can see any filters you have applied. Remove filters by clicking the ✕ icon next to the filter. Or clear all filters by clicking **Reset**.



Note: When applying filters, the search uses the logical AND operator if the used filters are different. However, when the filter is of the same type, the search uses the logical OR operator.

Those filters that have more than 10 options include a Filter Value search field for writing text and making the search easier.

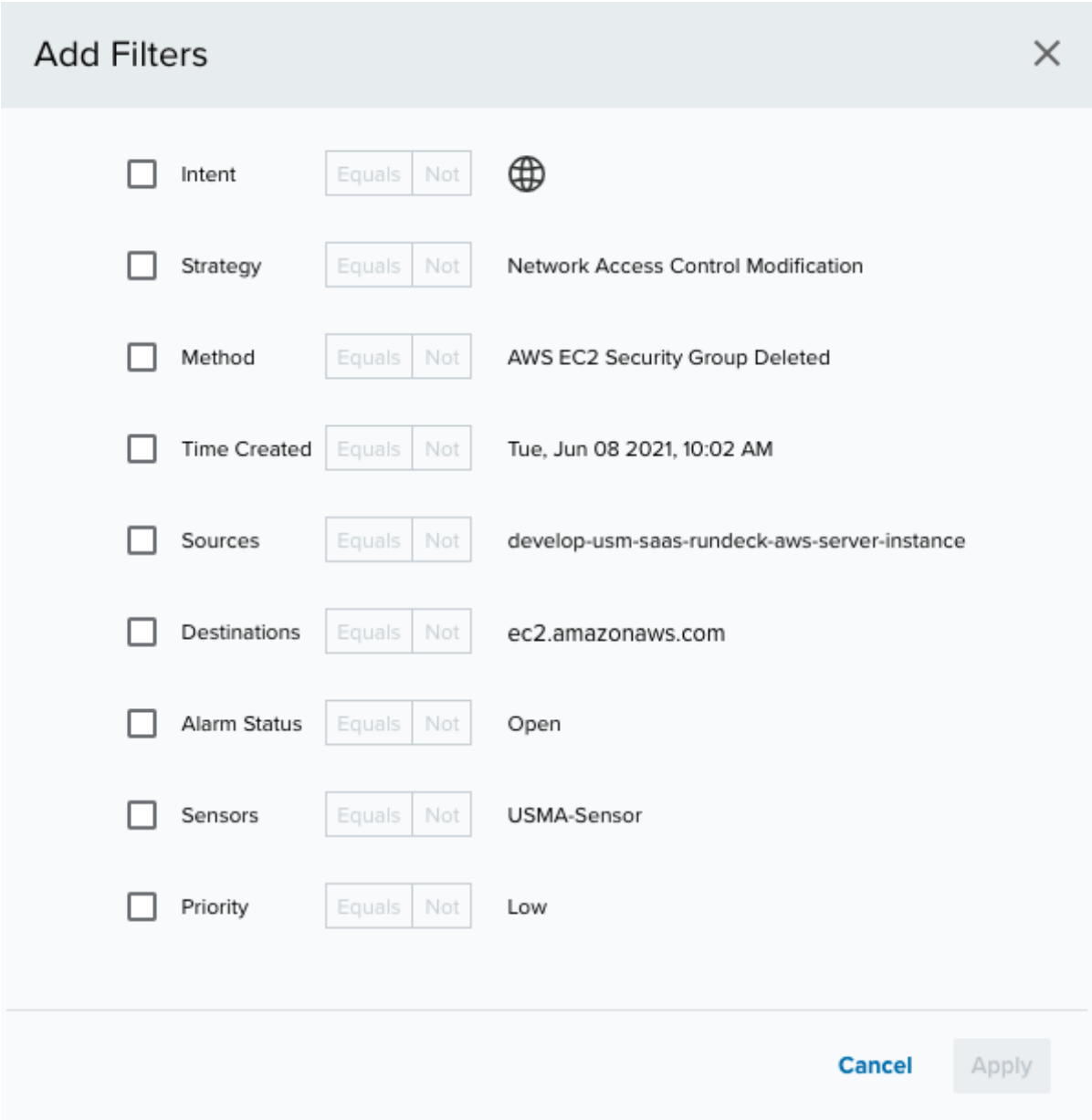
Filtering Alarms by Row Fields

USM Central includes a column with the icon in the list view in the alarms page. Use this icon to add filters to your search. When you click this icon, a dialog box opens with the specific fields of that row.

To filter alarms by row fields

1. Go to **Alarms** to open the list view in the Alarms List View page.
2. Click the icon of the row to which you want to add the filters.

   The Add Filters dialog box opens.



3. Select the fields that you want to filter during your search and click **Equals** or **Not** to limit your search.
4. Click **Apply**.

   The result of your search displays with the filters applied.

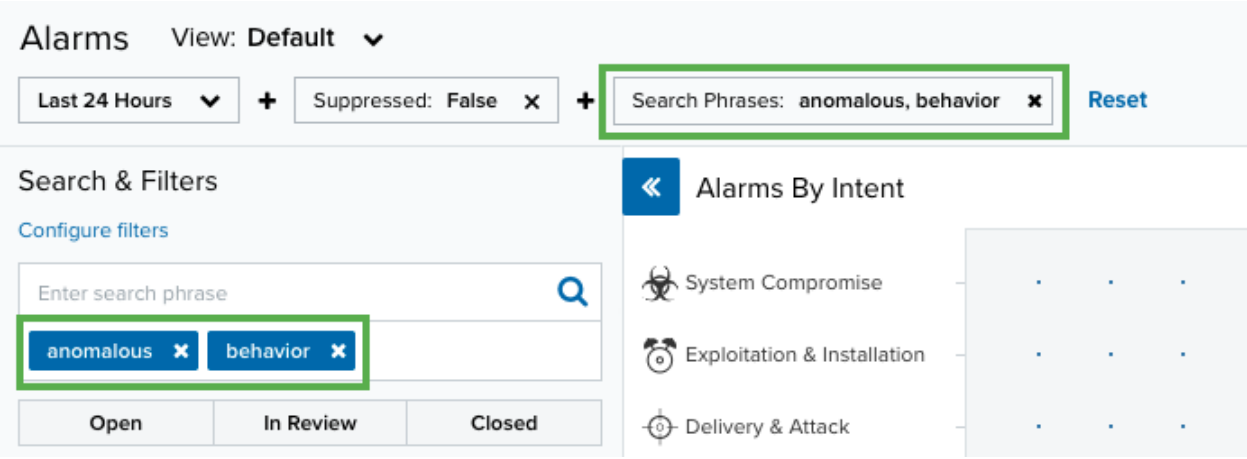
To search for Alarms using the search field

1. Go to **Alarms**.
2. Enter your query in the search field.

   If you want to search for an exact phrase having two or more words, you need to put quotation marks around the words in the phrase. This includes email addresses (for example, "bob@mycompany.com").

   Note: Wildcard characters are considered as literal characters.

3. Click the icon.



The result of your search displays with the items identified.

Filtering Alarms

You can use filters to delimit the number of alarms that display in the List view in the Alarms page. You can also save filter views to easily use later. Your active filters will be used for reports exports.

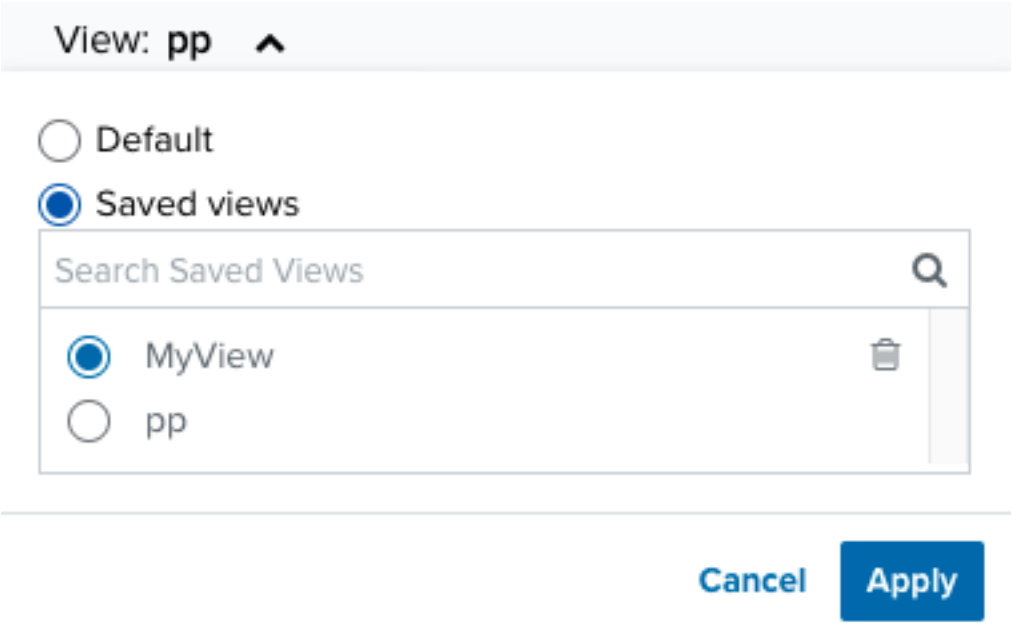
To search alarms using a filter

1. Go to **Alarms**.
2. Click a filter.

   The result of your search displays the identified alarms.

To save a filter configuration

1. Go to **Alarms** and select the filters you want to use in your saved view.
2. Select the **Save View** drop-down list and then click **Save as**.
3. Enter a name for the view and click **Save**. You can now load this view from the View drop-down list.

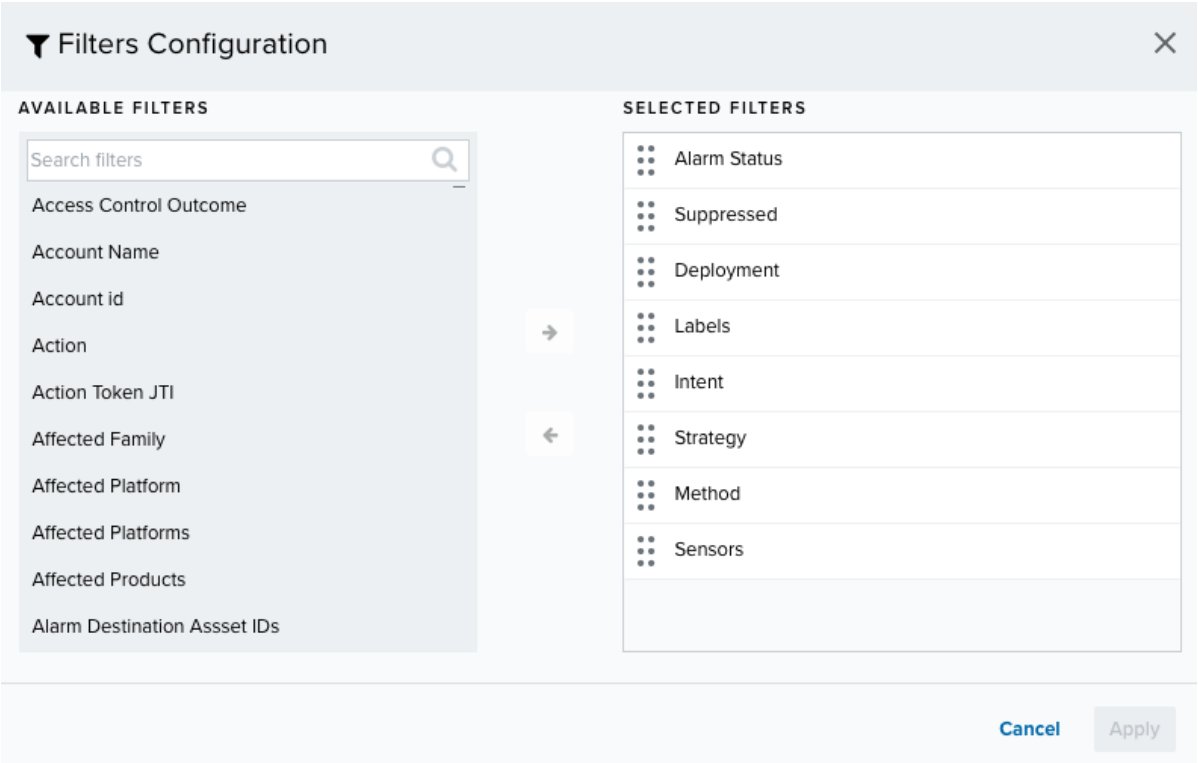


Note: If you have changed the configuration of the alarms within the List view columns, this configuration will also be saved together with the filter configuration. See Alarms List View for more information.

To add or delete filters from the Search & Filters area

1. Go to **Alarms**.
2. Click the **Configure Filters** link at the bottom of the Search & Filters sidebar to open the Filters Configuration window.

3. Click the arrow icons ( ) and ( ) to pass the items from the Available Filters and Selected Filters columns, and then click **Apply**.



Searching Alarms by Using the Search Field

Role Availability ✔ **Read-Only** ✔ **Analyst** ✔ **Manager**

Use the search field to enter queries and refine your search. You can enter free text, use wildcards, and use advanced search syntax. When searching, keep in mind the accepted query string syntax list in this table.

Accepted Query String Syntax

Type of Query	Meaning	Example
Standard query with a blank space between terms	By default, a space between query terms is considered an implicit “OR”.	denylist malicious
Literal, using double quotes " "	Matches fields that contain the full term. Literal searches are case-sensitive. **Note:** This type of query will not match any searches in the raw log because raw logs are tokenized. **Note:** IP addresses and FQDNs are considered literal searches, so they don't require quotation marks.	"Event from asset not received"
Boolean operators or using parentheses AND, OR, NOT, ( )	Including AND or OR between two search terms will search for results that match both of those terms. Including NOT between two search terms will exclude results that match the second term, even though they otherwise match your query. Parentheses can be used to group terms for higher precedence relative to the rest of your query. Parentheses are also used to designate subsearches.	(http OR tcp) AND ftp
Wildcards, asterisk *	Appending an asterisk to the end of a term within your query will search for results that begin with your search term. An asterisk cannot be used at the beginning of a search query.	instance*

Accepted Query String Syntax (Continued)

Type of Query	Meaning	Example
Wildcards, question mark ?	Embedding a question mark in the middle of a term will search for results that otherwise match your query, no matter the value in the position held by the question mark in your search term. A question mark cannot be used at the beginning of a search query.	qu?ck
Regular expression (regex), using /expression/	Regular expression inside forward slash characters. A dialog box opens to confirm the search. **Note:** The characters ", *, ?, (, and) are special characters included in expressions. If you want to search by these characters, you need to manually escape them by preceding them with a backslash.	/Describe.*Instances/
OTX pulse	Pulses are collections of Indicators of Compromise (IOCs). You need to insert the word *pulse* followed by a colon and the pulse ID or URL.	pulse:59432536c1970e343ce61bf0

Any characters may be used in a query, but certain characters are reserved and must be escaped. The reserved characters are these:

+ - = & | > < ! { } [ ] ^ " ~ : \ /

Use a backslash (for example, "\>") to escape any reserved character (including a backslash).

To search for Alarms using the search field

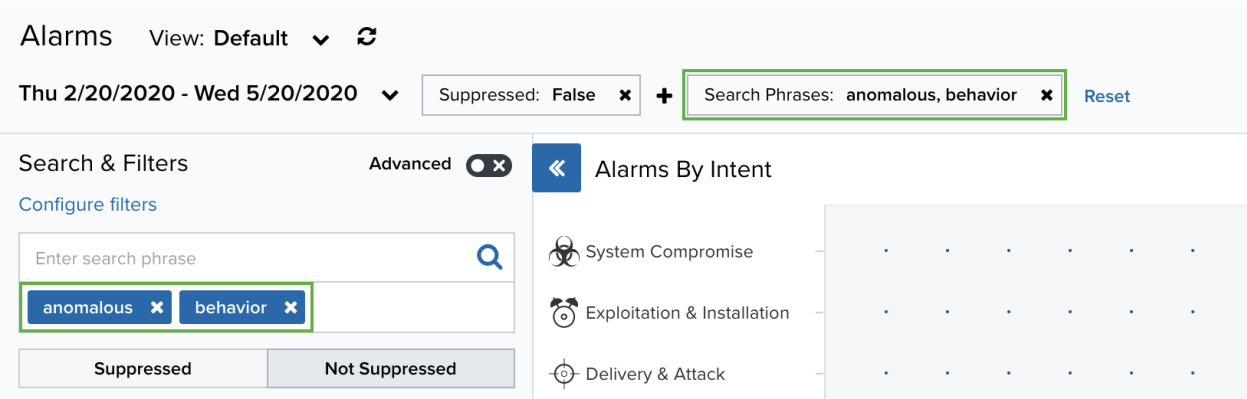
1. Go to **Alarms**.
2. Enter your query in the search field.

   If you want to search for an exact phrase having two or more words, you need to put quotation marks around the words in the phrase. This includes email addresses (for

example, "bob@mycompany.com").

> **Note:** Wildcard characters are considered as literal characters.

3. Click the icon.



The result of your search displays with the items identified.

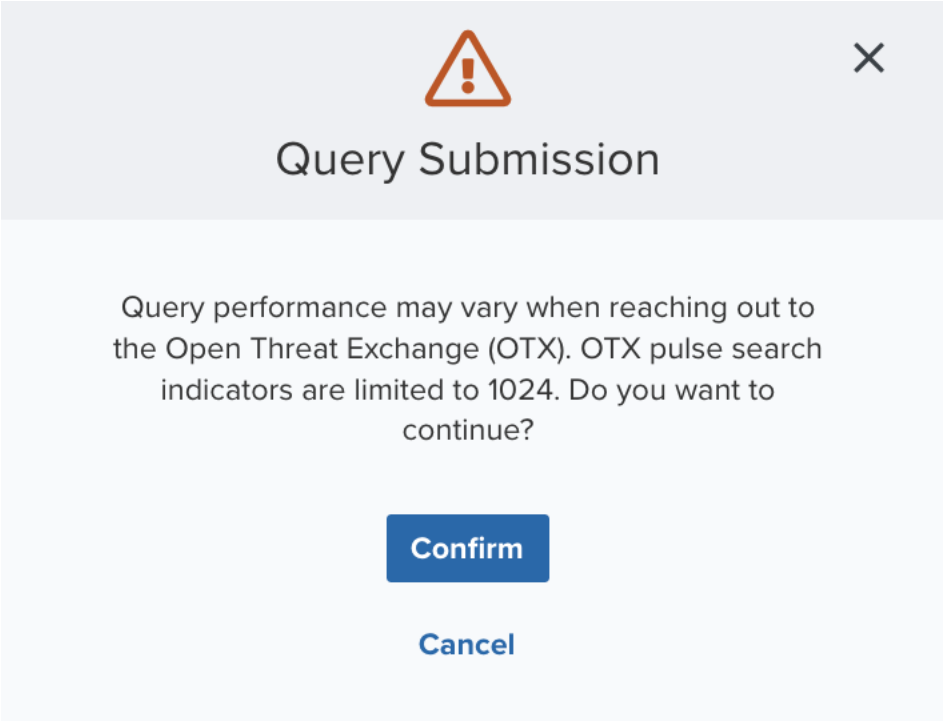
Searching Alarms by Using the Pulse ID

You can use the search field to search alarms by pulse identification (ID). Pulses are collections of IOCs, reported by the LevelBlue Labs™ Open Threat Exchange® OTX™ community, on which other community members review and comment. Pulses provide you with a summary of the threat, a view into the software targeted, and the related IOCs, reported by the OTX community worldwide. See Open Threat Exchange® and USM Anywhere for more information.

To search alarms by using the pulse ID

1. Go to **Activity > Alarms**.
2. Enter your query in the Enter search field. Either paste the full URL or insert the word *pulse* followed by a colon and the pulse. For example, enter: **https://otx.alienvault.com/pulse/59432536c1970e343ce61bf0** or **pulse:59432536c1970e343ce61bf0**.
3. Click the icon.

4. The Query Submission dialog box opens.



5. Click **Confirm** to continue.

   The result of your search displays with the items identified. This result matches entries containing IOCs in your environment.

Standard and Advanced Modes on Alarms

Role Availability	Read-Only	Analyst	Manager

USM Central enables you to toggle the mode of search. The available modes are Standard and Advanced. You can change from one mode to the other by clicking the icon or clicking the icon located in the upper left corner of the page.

Standard Mode

This mode enables you to select one value per filter at the same time, and then the search is automatically performed. This mode is on by default.

To activate the standard mode when the advanced mode is on

1. Go to **Alarms**.
2. In the upper-left corner of the page, click the icon.
3. This turns the icon gray, .

> **Note:** If you exit the advanced mode and the selected filters are not compatible with the standard mode, a warning dialog box opens to inform you the current filters will be removed.

Advanced Mode

Advanced mode enables you to select more than one value per filter at the same time. This mode is off by default.

To activate the advanced mode

1. Go to **Alarms**.
2. In the upper-left corner of the page, click the icon to activate the advanced mode.

   This turns the icon green, .

To perform a search in the advanced mode

1. Go to **Alarms**.
2. In the upper-left corner of the page, click the icon to activate the advanced mode.

   This turns the icon green, .

3. Click the filters that you want to select.

   The selected filters display inside a dashed rectangle.

4. In the lower-left corner of the page, click **Apply Filters**. Or in the upper side of the page, click **Apply**.

   Apply Filters

   The result of your search displays.

To search all values of a filter

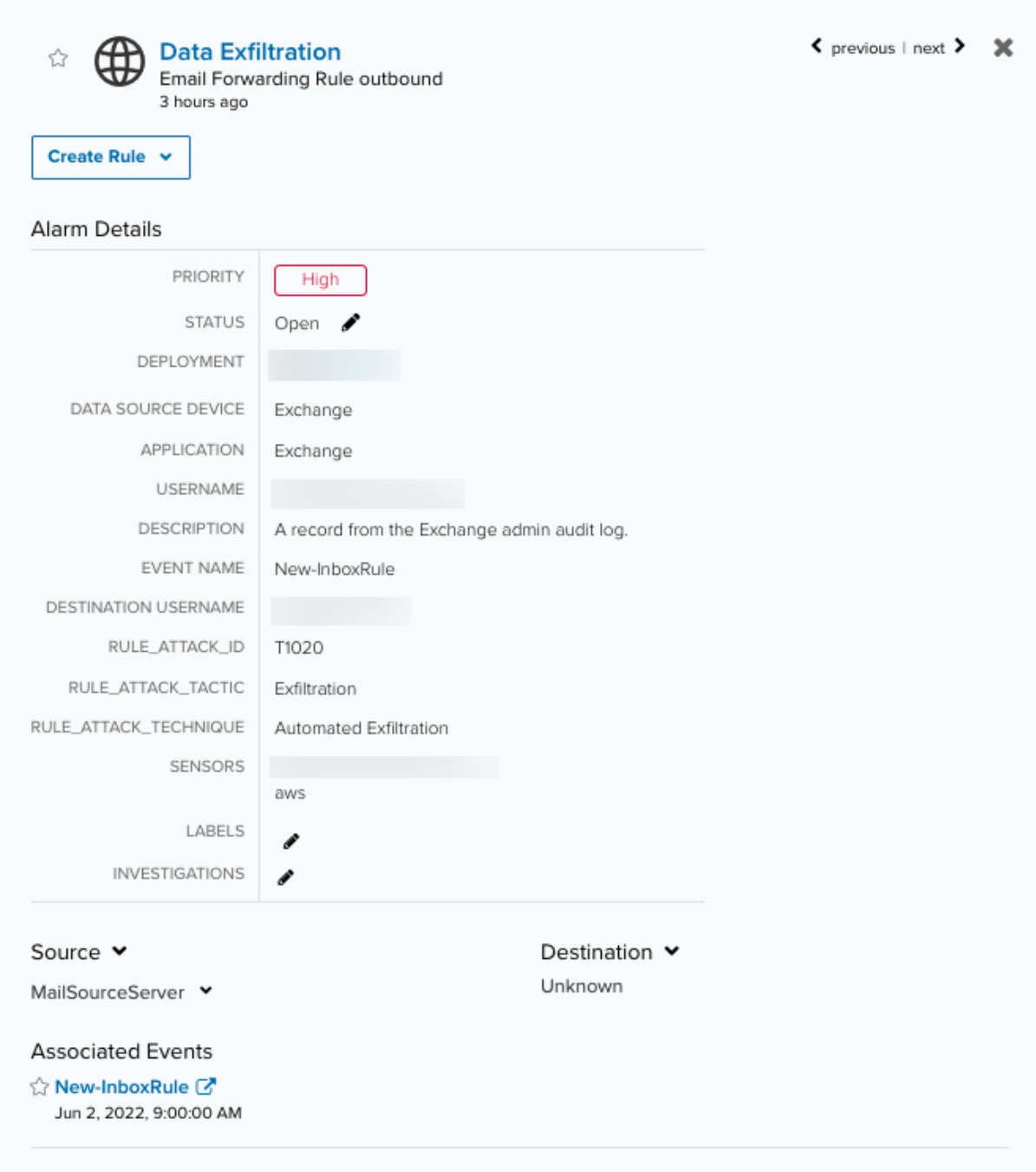
1. Go to **Alarms**.
2. In the upper-left corner of the page, click the icon to activate the advanced mode.
3. Select a filter title to select all filters below that title.

View Alarm Details

The alarm details view provides in-depth information on an alarm and provides easy access to the alarm within the related deployment. When you use this feature to access the alarm at the deployment level, you can perform further investigation, as well as create associated rules for that deployment based on characteristics of the alarm.

To view the details of an alarm

1. Go to **Alarms**.
2. Click the alarm to display a summary view, and then click the alarm name to open the full details of the alarm.



Click the ★ icon to bookmark an item for quick access.

Note: You can view your bookmarked items by going to the secondary menu and clicking the ★ icon. This will display all of your bookmarked items and provide direct links to each of them.

Not all alarms found during monitoring are necessary in managing your environment because they do not pose a security threat. Frequently, there are alarms that create a noisy environment, making it difficult to monitor other alarms that require more attention. You can identify these alarms and suppress them by using a rule.

The Alarms Details page includes this alarm management function that is supported for your assigned user role:

- **Create Rule**: See Creating Rules from Alarms for more information.

The alarm details include the main fields that identify an alarm. You can edit or add values into these fields:

- **Status**: This field indicates the status for the alarm: open, in review, or closed. You can click the icon to edit the field and apply a status. See Alarm Status for more information.
- **Labels**: This field indicates if the alarm has been classified by using a label. You can click the icon to manage the labels of the alarm. See Labeling the Alarms for more information.
- **Investigations**: This field indicates if the alarm has been associated to an investigation. You can click the icon to edit the field and enter the title or the number that identifies each investigation.
- **HTTP Hostname**: If the alarm includes this field, you can search for events by using it. See Searching Events from the Details of an Alarm for more information.
- **DNS RR Name**: If the alarm includes this field, you can search for events by using it. See Searching Events from the Details of an Alarm for more information.

To investigate the alarm in its specific deployment environment, click the link in the Deployment field.

Below the alarm details, you can see the source, the destination, the associated alarm if it exists, the associated events, a description, and a recommendation to fix the problem.

Your environment can have sources and destinations included in the inventory and those not included in the inventory. Assets included in the inventory display their names in blue, and assets not included in the inventory display their names in gray.

The icon located next to the source and destination fields enables you to access these options:

- **Search Pivot**: Identify alarms triggered in the last hour, 24 hours, 7 days, 30 days, or 90 days. You can also configure your own period of time by clicking the **Custom Range** option. This option enables you to customize a range. When you click the icon, a calendar opens. You can choose the first and last day to delimit your search by clicking the days on the calendar or entering the days directly. Then select the hours, minutes, and seconds by clicking the specific box. Finally, select **AM** or **PM**.
- **Find Source or Destination in Events**: Use this link to search events having the same source or destination as the alarm.
- **Find Source & Destination in Events**: Use this link to search events having the same source and destination as the alarm.

The icon located next to the asset enables you to access these options:

- **Add to current filter**: Use this option to add the asset name as a search filter.
- **Look up in OTX**: This option searches the IP address of the source asset in the Open Threat Exchange page. See Using OTX in USM Anywhere for more information.
- **Full Details**: See Viewing Assets Details for more information.

The icon located next to the asset enables you to access these options:

- **Add to current filter**: Use this option to add the asset name as a search filter.
- **Look up in OTX**: This option searches the IP address of the source asset in the Open Threat Exchange page. See Using OTX in USM Anywhere for more information.

3. Click the link of an associated event to open its details page.

   The Associated Events list displays all events associated with the alarm.

4. In the upper right corner, click **Previous** and **Next** to navigate between items.
5. Click the icon to close the dialog box.

> **Note:** See the Searching Events from the Details of an Alarm page for more information about the options in the HTTP Hostname, DNS RR Name, Source, and Destination fields.

Creating Rules from Alarms

USM Central enables you to create and manage your own orchestration rules from the Alarms Details page, which is the easiest way to configure an orchestration rule. You can also create and manage your rules for all your deployments from the rules page in the Settings menu. Once you have created a rule, you can also copy it and make modifications for alternate uses or for use in other deployments.

You can create these rules:

- **Alarm Suppression Rule**: You can create a rule to suppress alarms that match a particular set of criteria. See Creating Suppression Rules from the Alarms Page and Suppression Rules from the Orchestration Rules Page for more information.
- **Notification Rule**: You can create a notification rule according to a method. See Creating Notification Rules from the Alarms Page and Notification Rules from the Orchestration Rules Page for more information.

Creating Suppression Rules from the Alarms Page

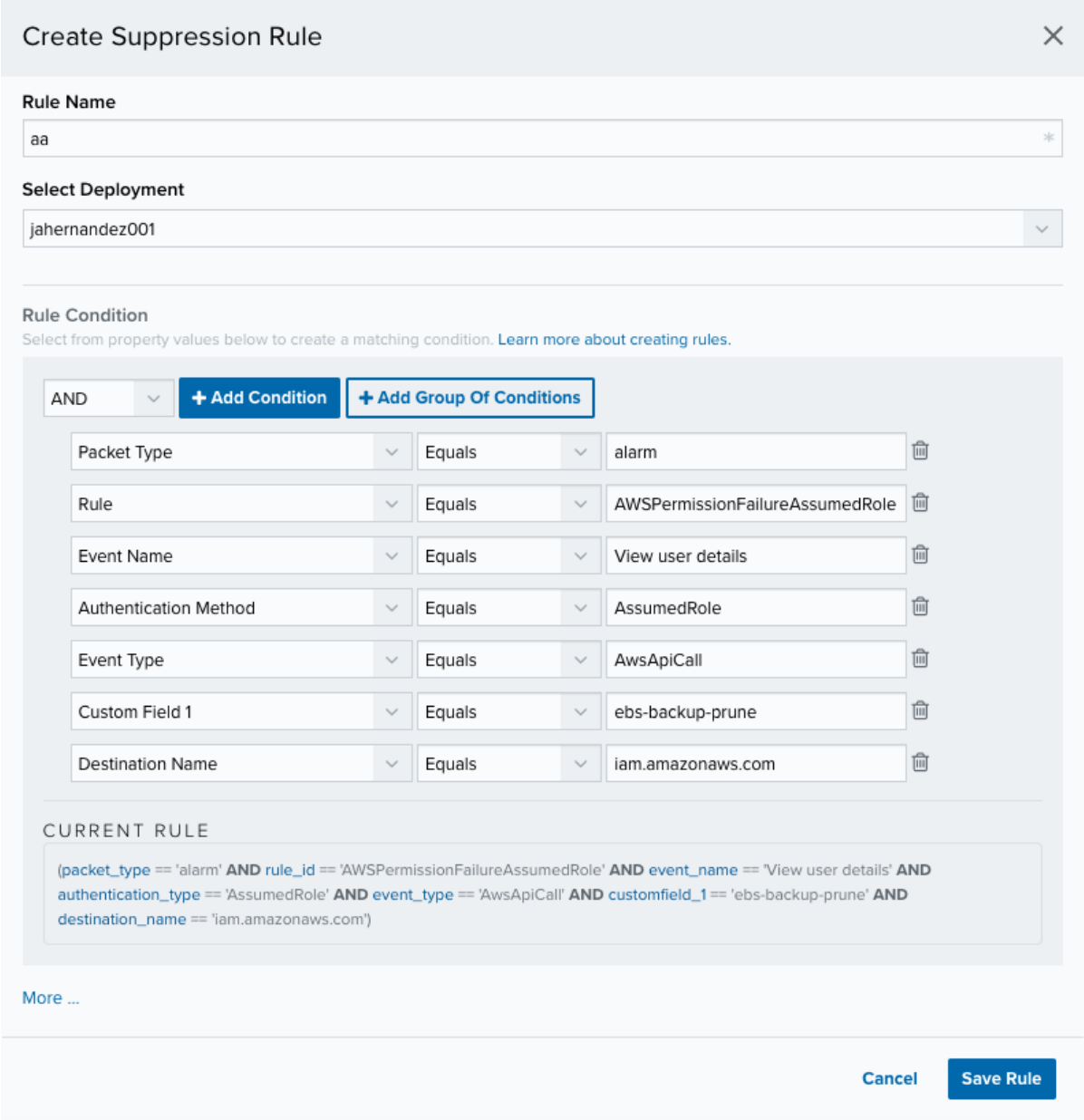
Role Availability	Read-Only	Analyst	Manager

There are cases where the alarms in USM Central are false positives, and you may want to suppress these kinds of alarms to prevent the false positives from flooding your system. To suppress an alarm, you need to create a suppression rule. USM Central applies the suppression rule to similar alarms from the current day (up to 10 K alarms) and to future alarms. Existing alarms are suppressed but kept open, while future alarms are suppressed and closed.

To create a suppression rule from the Alarms page

1. Go to **Alarms**.
2. Locate the alarms that you want to include in the suppression rule.

   See Searching Alarms for more information.
3. Click the alarm that you want to suppress.
4. Click **Create Rule > Create Alarm Suppression Rule**.



5. Enter a name for the rule.
6. Select a deployment.
7. You have already suggested property values to create a matching condition, but if you want to add new property values, click **Add Condition**.

> **Note:** If the field is related to the name of a country, you should use the country code defined by the ISO 3166.

> **Note:** The Sources or Destinations field needs to match the universally unique identifier (UUID) of the event or alarm. You can use the Source Name or Destination Name field instead.

8. (Optional.) Click **Add Group** to group your conditions.

> **Note:** See Operators in the Orchestration Rules for more information.

9. (Optional.) Click the **More** link to include a multiple occurrence parameter.

   Modify these two options:

   - **Occurrences:** Specify the number of event occurrences that produce a match on the conditional expression to trigger the rule. You can enter the number of occurrences or use the arrow to scroll the value up or down. You need to enter a number between 1 and 100.
   - **Length:** Specify the length of the timespan used to identify a match for multiple occurrences. Enter the number and choose a value of seconds, minutes, or hours.

     This duration identifies the amount of time that transpires from the beginning to the end of the occurrence. If the number of occurrences is not met within this period, the rule is not a match.

     In this example, the rule applies when the configured conditions happen five times every three hours.

   These two options function together to specify the number of occurrences within a time period that will produce a match for the rule. For example, you can define a rule to trigger an alarm for an unauthorized access attempt when a failed SSH login occurs three times within a five-minute window.

10. Click **Save Rule**.

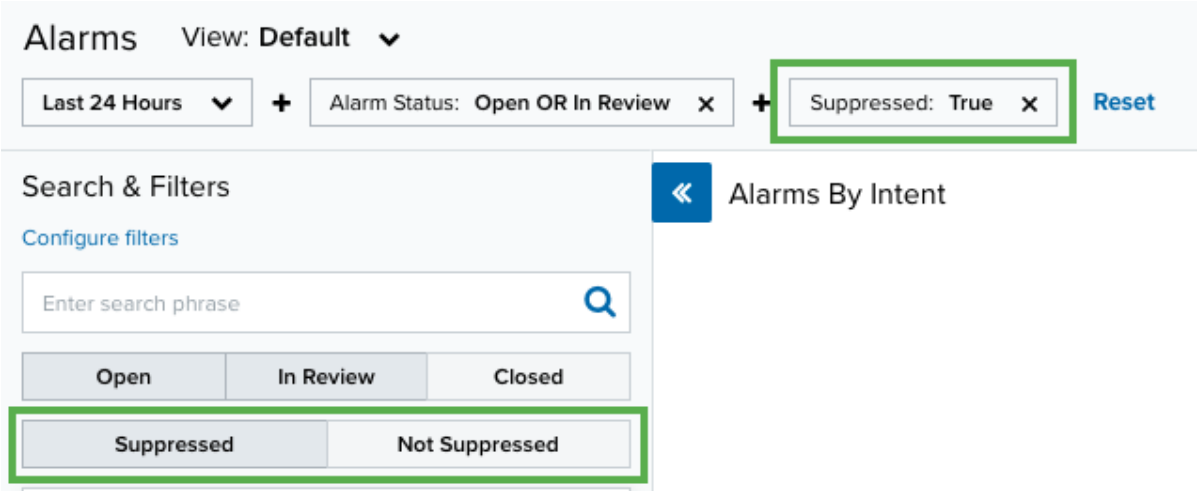
    The suppression rule has been created. You can see it from **Settings > Rules > Suppression Rules**. See Suppression Rules from the Orchestration Rules Page for more information.

Important: It takes a few minutes for an orchestration rule to become active.

Suppressed alarms remain in the system but are hidden in the web user interface (UI) by default. If you want to see these alarms, click **Suppressed** in the Search & Filters area. The suppressed alarms will be displayed in the table along with the other alarms. Use the following instructions if you want to display just the suppressed alarms.

To only display the suppressed alarms

1. Go to **Alarms**.
2. In the Search & Filters area, click **Not Suppressed** to remove the *Suppressed: False* filter, and then click **Suppressed** to add the *Suppressed: True* filter.



3. Click **Closed** to include the closed alarms.
4. To see alarms suppressed by a certain rule, in the upper-left corner of the page, click the **Configure Filters** link.
5. In the Search filters field, enter **Suppress**.
6. Select the **Suppress Rule Name** filter.
7. Click the → icon to pass the selected filter from the available filters to the selected ones.
8. Click **Apply**.

   The page reloads and the Suppress Rule Name filter is added in the lower left corner.
9. Search the Suppress Rule Name filter and click the rule. If no rule name displays, it is because of these reasons:

- There are no alarms suppressed by the rule.
- The Suppressed filter is not enabled.

See Searching Alarms for more information about the icons below the filters.

Note: You can save the view for later use. See Alarms Views for more information about how to create a configuration view.

To show triggered alarms rules

1. Go to **Settings > Rules** to open the All Orchestration Rules page.
2. In the Create an Alarm row, click the icon.

   The Alarms List View page opens. The page includes Rules Name as a filter so that you can see how many alarms match the selected rule.

Creating Notification Rules from the Alarms Page

Role Availability	Read-Only	Analyst	Manager

You can create your own notification rules from the Notification Rules from the Orchestration Rules Page or from the Alarms Details page, which is the easiest way to configure the matching conditions.

To create a notification rule from the Alarms page

1. Go to **Alarms**.
2. Search the alarms that you want to include in the notification rule and click one of them.

   See Searching Alarms for more information.
3. Select **Create Rule > Create Notification Rule**.
4. Enter a name for the rule.
5. Select a deployment.
6. Select a notification method:
   - **Amazon SNS:** This method requires the setup of the Amazon Simple Notification Service (SNS) API call from the USM Anywhere server. There is no limit to the number of Amazon SNS endpoint notifications sent. However, this method requires having an Amazon Web Services (AWS) account for setup and use. The Amazon SNS allows the

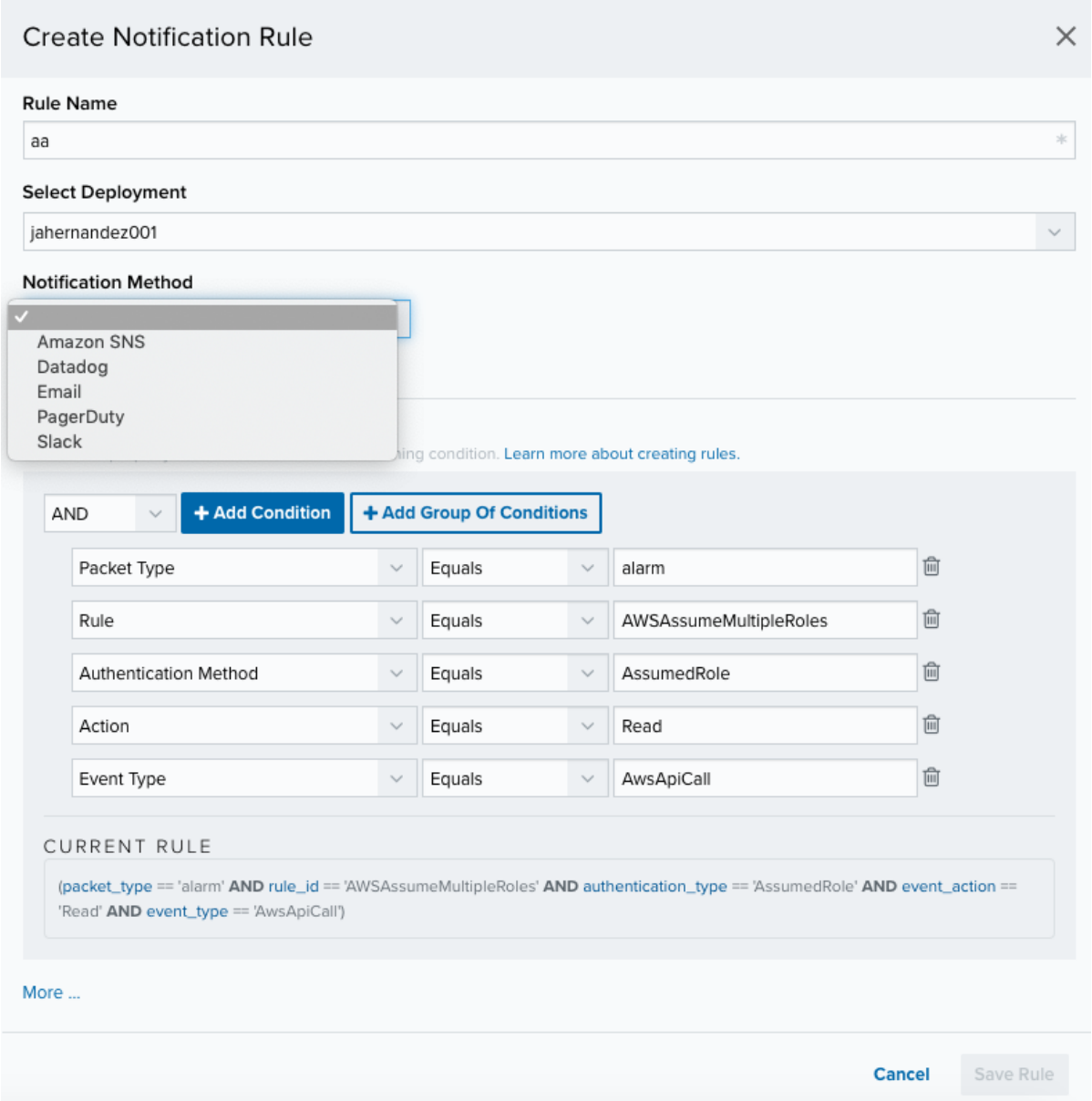
first 1000 email notifications per month to fall into the free messaging tier. See Sending Notifications Through Amazon SNS in the *USM Anywhere Deployment Guide* for more information.

- **Datadog:** This method requires the creation of a Datadog API key and additional steps. See Sending USM Anywhere Notifications to Datadog in the *USM Anywhere Deployment Guide* for more information.
- **Email:** This method sends the notification by email. You need to enter information for the email subject and enter a destination email address. Multiple comma-separated email addresses are possible. This method uses a built-in integration with the Amazon Simple Email Service (SES) function and is limited to a maximum of 200 emails per rolling 24-hour period. The only user-customizable information available is the email subject line.

  > **Note:** The rolling 24-hour, 200-email limit refers to all email accounts. For example, you can have a rule with multiple emails, which counts as a single email delivery. Alternately, if you have several rules with several emails, each of these counts as an individual email account. Sensor-disconnect emails do not count against this number because they are critical and are only sent to users whose role is manager.

  Select the **Sanitize Email Content** checkbox to replace detailed email contents with a generic message and a link that requires user authentication to view further information.

- **PagerDuty:** This method is performed using an integration in the product, and user setup is required. See Sending USM Anywhere Notifications to PagerDuty in the *USM Anywhere Deployment Guide* for more information.
- **Slack:** This method makes use of a user-created *Slack Webhook* integration. Slack integration can also be performed using Amazon SNS. See Sending USM Anywhere Notifications to Slack in the *USM Anywhere Deployment Guide* for more information.



7. You have already suggested property values to create a matching condition, but if you want to add new property values, click **Add Condition**.

> **Note:** If the field is related to the name of a country, you should use the country code defined by the ISO 3166.

> **Note:** The Sources or Destinations field needs to match the universally unique identifier (UUID) of the event or alarm. You can use the Source Name or Destination Name field instead.

8. (Optional.) Click **Add Group** to group your conditions.

   Note: See Operators in the Orchestration Rules for more information.

9. (Optional.) Click the **More** link to include a multiple occurrence parameter.

   Modify these two options:

   - **Occurrences:** Specify the number of event occurrences that produce a match on the conditional expression to trigger the rule. You can enter the number of occurrences or use the arrow to scroll the value up or down. You need to enter a number between 1 and 100.
   - **Length:** Specify the length of the timespan used to identify a match for multiple occurrences. Enter the number and choose a value of seconds, minutes, or hours.

     This duration identifies the amount of time that transpires from the beginning to the end of the occurrence. If the number of occurrences is not met within this period, the rule is not a match.

     In this example, the rule applies when the configured conditions happen five times every three hours.

   These two options function together to specify the number of occurrences within a time period that will produce a match for the rule. For example, you can define a rule to trigger an alarm for an unauthorized access attempt when a failed SSH login occurs three times within a five-minute window.

10. Click **Save Rule**.

    The notification rule has been created. You can see it from **Settings > Rules > Notification Rules**. See Notification Rules from the Orchestration Rules Page for more information.

Searching Events from the Details of an Alarm

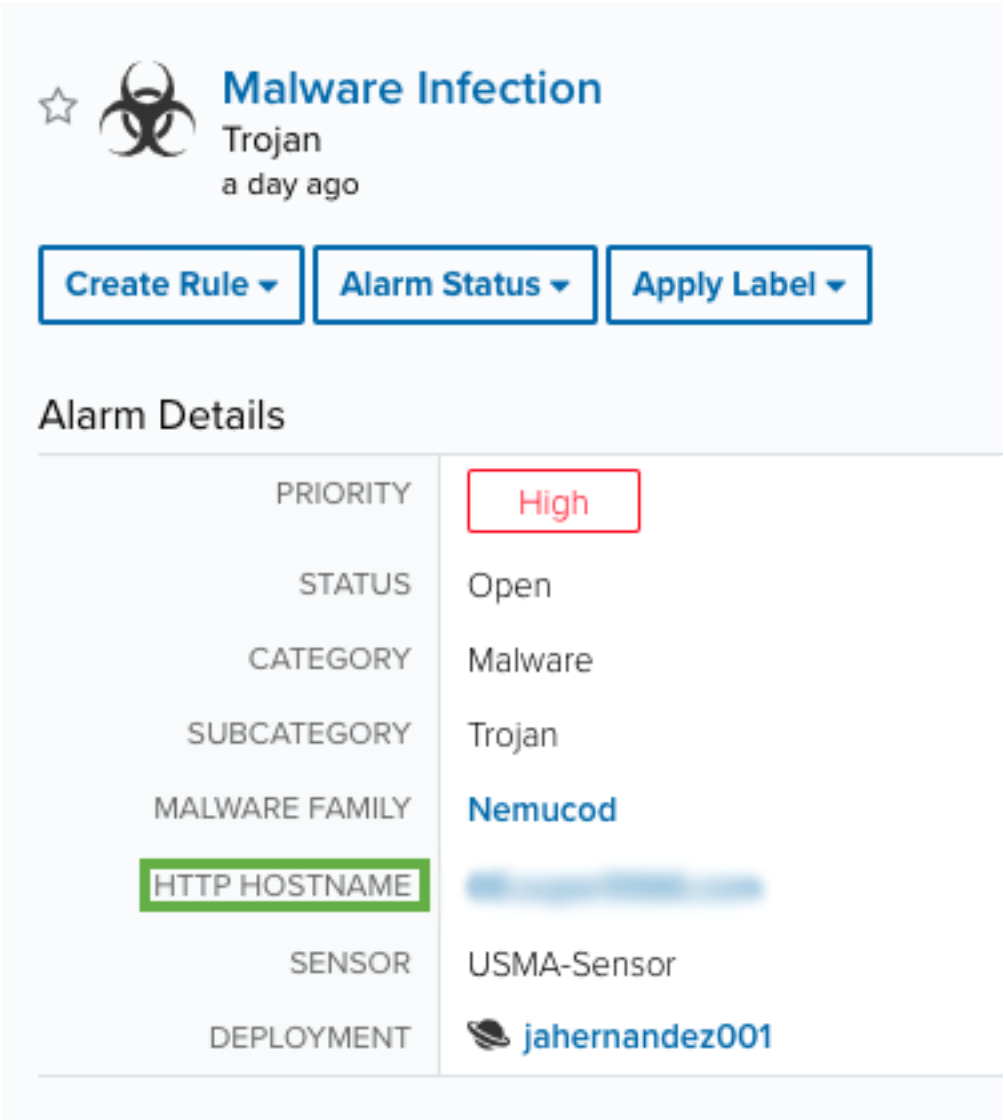
USM Central enables you to search for events from the details of an alarm using the selected value as a filter in the search.

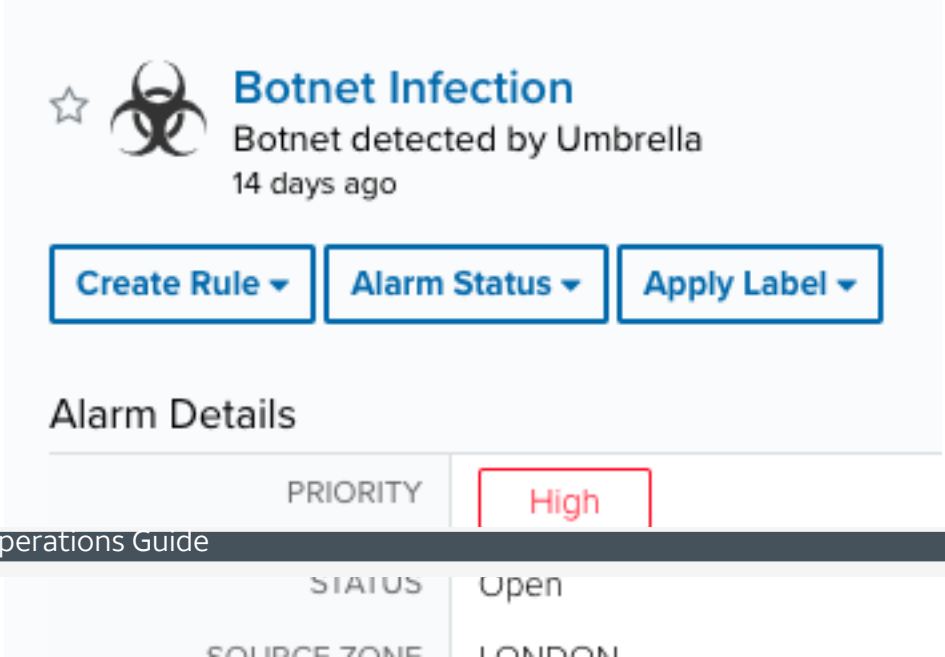
The HTTP Hostname or the DNS RR Name fields

All alarms that include the fields HTTP Hostname or the DNS RR Name give you the option of searching for events by using these fields. The alarm needs to include these fields.

To configure the HTTP Hostname or the DNS RR Name filters

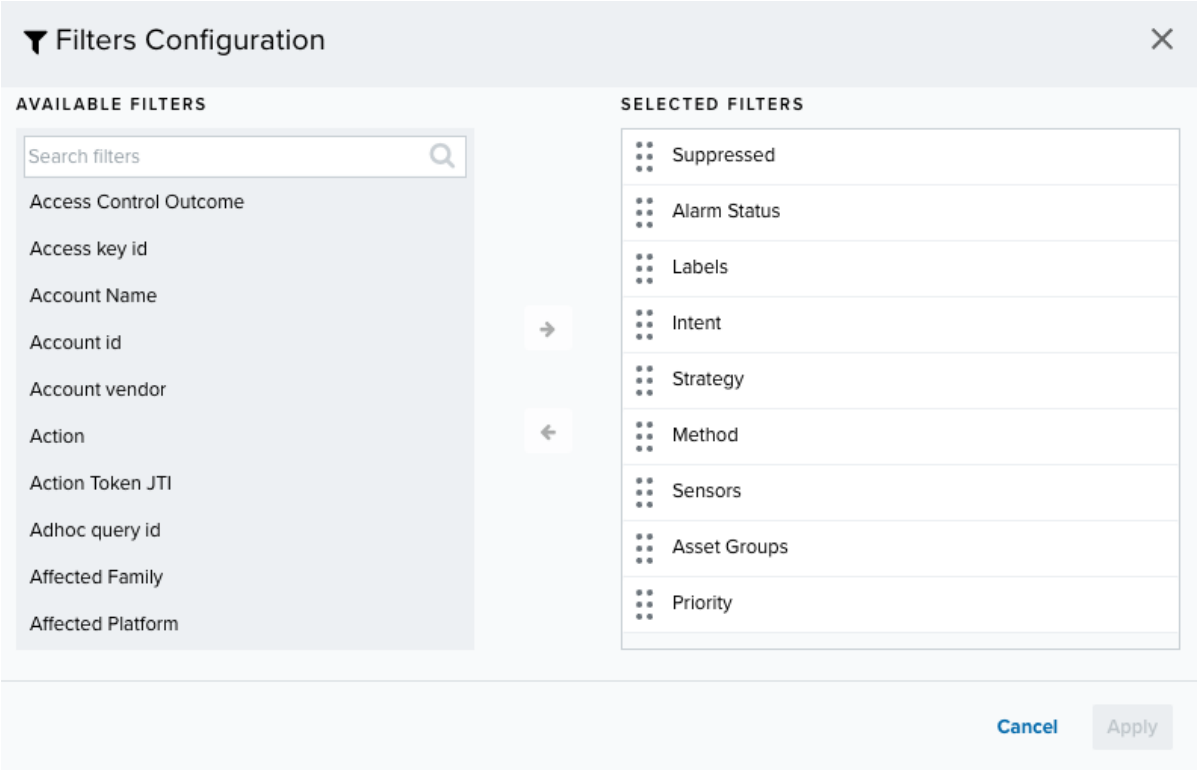
1. Go to **Alarms**.





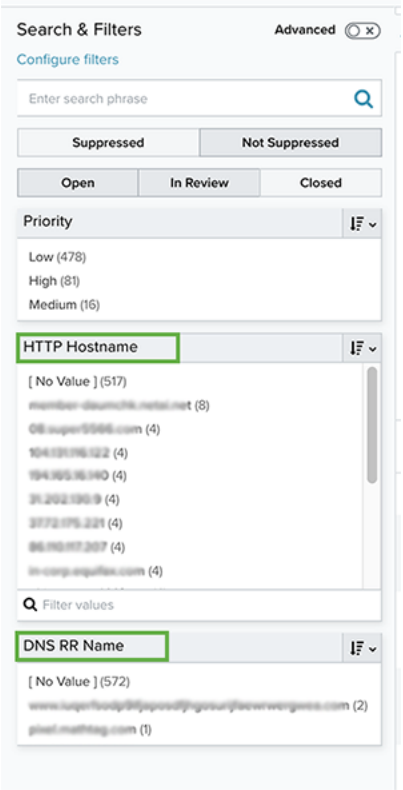
To configure the HTTP Hostname or the DNS RR Name filters

1. Go to **Alarms**.
2. In the upper-left side of the page, click the **Configure Filters** link.



3. In the search filters box, enter **HTTP** or **DNS** and select the desired filter.
4. Use the → and ← icons to pass the items from one column to the other.
5. Click **Apply**.

   The selected filters display.



Labeling the Alarms

Role Availability | Read-Only | ✔ Analyst | ✔ Manager

Labels can be applied to alarms in USM Central to streamline the alarm management process by enabling you to create and distribute labels across all other connected deployments from your instance of USM Central.

Label Management with Connected Deployments

Because of the way that USM Central handles its own labels and the inherited labels of the connected deployments, there are a few things that are important to understand and consider:

- USM Central automatically collects and displays all labels from connected deployments. You can only edit these inherited labels and apply them to alarms in their individual deployment of USM Anywhere.

- You can apply the labels you've created in USM Central to alarms in both USM Anywhere and USM Central. You can only edit these labels in USM Central, but not in USM Anywhere.
- In cases where an identically named label exists in both USM Anywhere and USM Central, USM Central will assume control of the label's management.
- Similarly, if you would like to have USM Central assume ownership of an active label in USM Anywhere, you can recreate the label in USM Central using the same naming conventions. This will make the distribution and editing of the labels exclusive to USM Central.

You can see the label management in USM Central and USM Anywhere in the following table.

Label Management in USM Central and USM Anywhere

	Apply Labels to Alarms in Anywhere	Edit/Delete Labels in Anywhere	Apply Labels to Alarms in Central	Edit/Delete Labels in Central
Label Created in Anywhere	Yes	Yes	No	No
Label Created in Central	Yes	No	Yes	Yes

Best Practices for Label Management

Because of the way that labels are managed across USM Central and the connected deployments, it is important to have a manageable plan for label implementation. For example, given that labels created in USM Central can be applied in all connected deployments, their application will be more broadly used than deployment-specific labels. It would be useful to have an easily identifiable naming convention for the USM Central labels that is applicable to all deployments.

It is important to keep in mind that labels created in USM Central that share a name with a label in a connected deployment, will take control of the inherited label as well. So if a label needs to be able to be edited in USM Anywhere, you'll want to avoid using the same name for a label in USM Central. Alternately, if you have similar types of labels across your USM Anywhere deployments that you would prefer to manage at a more “global” level in USM Central, it would be best to make them all share the same name before creating a label of that name in USM Central. That way they can all be rolled up at once into USM Central.

You can't edit or delete the set of default labels:

- Closed
- False Positive
- In Progress
- Open

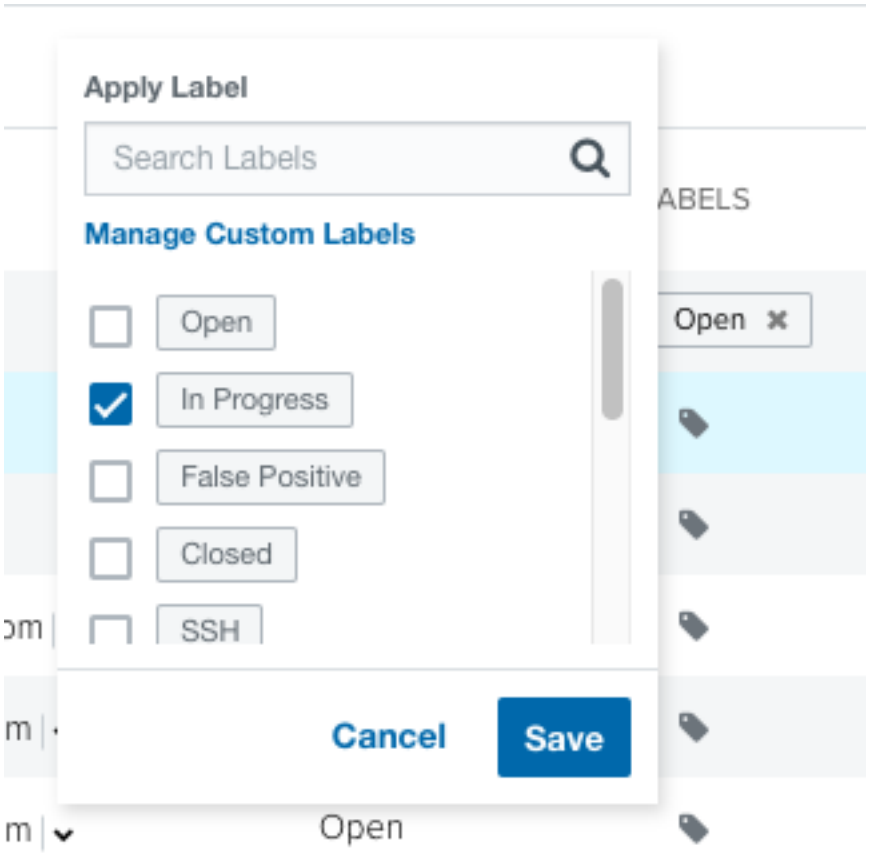
Alarm Label Usage

USM Central enables you to create, edit, and delete your own labels. You can apply a label to one or more alarms. You can also apply multiple labels to the same alarm. To distinguish between labels and statuses, see Differences between Statuses and Labels.

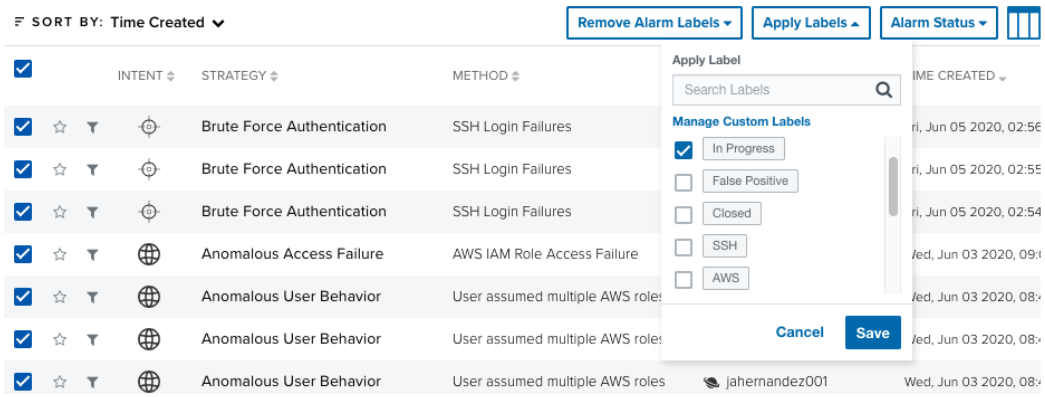
To label an alarm from the Alarms main page

1. Go to **Alarms**.
2. Search for the alarm or alarms to which you want to apply a label.
3. Complete one of these options:

- Click the icon in the labels column of the alarm you want to label, select the label, and click **Save**.



- Select the checkbox to the left of an alarm, click **Apply Labels**, select the label, and click **Save**.



To label an alarm from the Alarms Details page

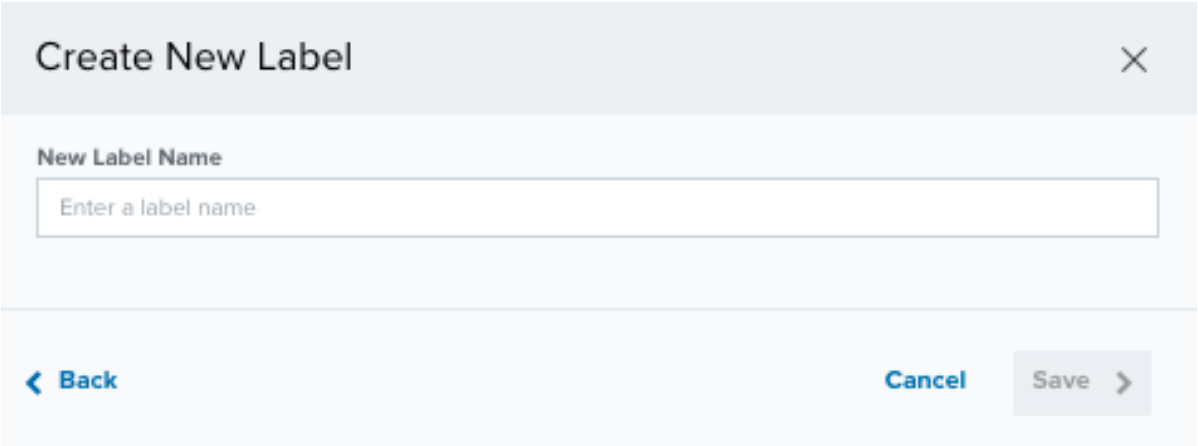
1. Go to **Alarms**.
2. Search for the alarm to which you want to apply a label.

   See Searching Alarms for more information.
3. Click the alarm.
4. Click **Apply Labels** and select a label.
5. Click **Save**.

To create a new label

1. Go to **Alarms**.
2. Select the checkbox to the left of an alarm.

   You can also select several alarms or select all alarms at the same time by selecting the first checkbox in the column.
3. Click **Apply Labels**.
4. Click **Manage Custom Labels**.
5. Click **Create New Label**.



6. Enter a name for the label.
7. Click **Save**.

To edit a label

1. Go to **Alarms**.
2. Select the checkbox to the left of an alarm.

   You can also select several alarms or select all alarms at the same time by selecting the first checkbox in the column.

3. Click **Apply Labels**.
4. Click **Manage Custom Labels**.
5. Click the icon next to the label you want to edit.
6. Modify the name of the label.
7. Click the icon to apply the changes.

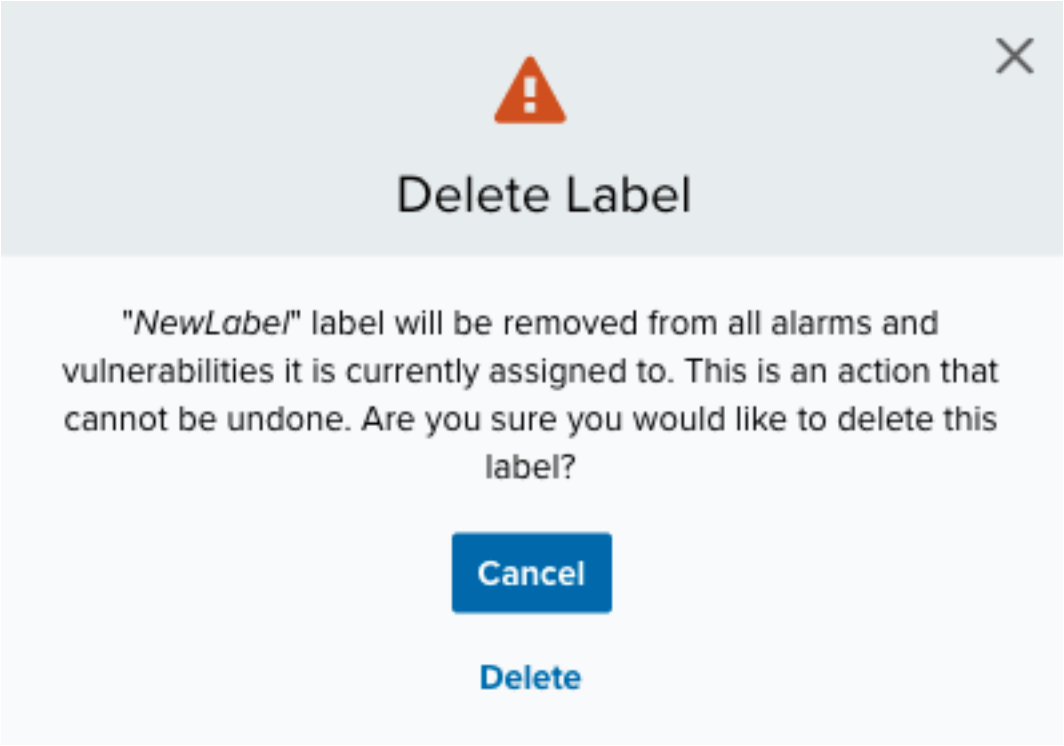
To delete a label

1. Go to **Alarms**.
2. Select the checkbox to the left of an alarm.

   You can also select several alarms or select all alarms at the same time by selecting the first checkbox in the column.

3. Click **Apply Labels**.
4. Click **Manage Custom Labels**.

5. Click the icon next to the label you want to delete.



6. Click **Delete** to confirm the deletion.

Alarm Status

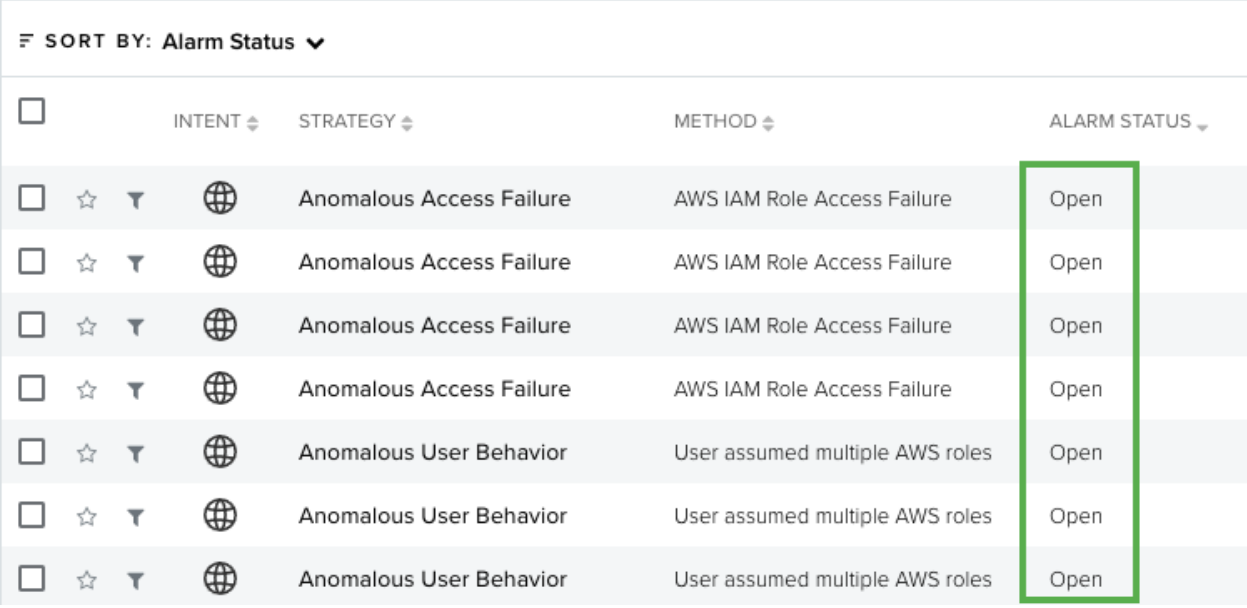
USM Central includes a set of statuses, which you can use to classify your alarms, track alarm status, and search alarms using statuses as a filter. Statuses are shared across both USM Central and USM Anywhere, so when an alarm status is updated in both environments will reflect the updated status.. See Searching Alarms for more information on how to search alarms.

You can't edit or delete the set of default statuses:

- Open
- In Review
- Closed

USM Central enables you to apply just one status to an alarm. You can't apply multiple statuses to the same alarm. See Differences between Statuses and Labels to distinguish between label and status.

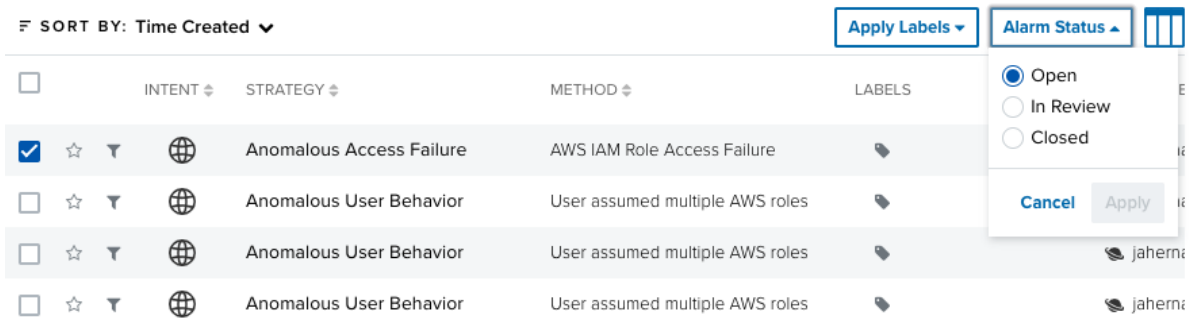
Note: The alarms that have the "closed" status will not display in the Alarm list view.



To apply a status to an alarm from the Alarms main page

1. Go to **Alarms**.
2. Search for the alarm you want to apply a status.

   See Searching Alarms for more information.
3. Select the checkbox to the left of the alarm.
4. Click **Alarm Status** and select a status.



5. Click **Apply**.

To apply a status to an alarm from the Alarms Details page

1. Go to **Alarms**.
2. Search for the alarm you want to apply a status.

   See Searching Alarms for more information.
3. Click the alarm.
4. Click **Alarm Status** and select a status.
5. Click **Apply**.

To bulk set the alarm status

1. Go to **Alarms**.
2. Select all of the alarms to which you want to apply a status by selecting the checkbox to the left of an alarm.

   See Searching Alarms for more information. You can also select several alarms or select all alarms at the same time by selecting the first checkbox in the column.
3. Click **Alarm Status** and select a status.
4. Click **Apply**.

To search for alarms having a status

1. Go to **Alarms**.
2. Click the filter to select the name of the status on the left pane.

   The alarm list displays the alarms that have the selected status.

Differences between Statuses and Labels

USM Central includes several statuses and labels you can use to classify your alarms. A status is a property of the alarm and a label is a tag you can assign to an alarm.

These are the main differences:

- You can add all the labels you need, but you are not able to create a new alarm status.
- You can apply a label to more than one alarm, but you are not able to apply more than one status to an alarm.
- Alarms that have the "Closed" status will not display in the List view in the Alarms page.

Create an Alarms Report

You can create a PDF or CSV report of the alarms directly from the alarms page.

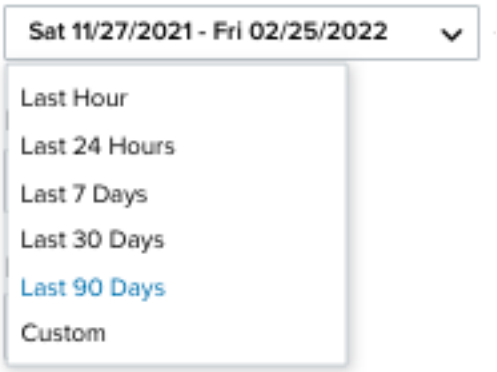
Important: LevelBlue recommends Google Chrome as the preferred browser for generating reports. The use of alternative browsers may result in poor formatting.

To create an alarms report

1. Go to **Alarms**.
2. Use filters to define the content you want to display in your report.
3. Click **Generate Report** to open the Configure Report dialog box.

   The filters selected and displayed for the page view are the ones that are populated in the report.

4. Click **Edit Filters** if you want to modify the selected filters, and then **Continue to Filters**. Do the modifications you need, and then click **Edit Report**.
5. Click the date field if you want to choose a different date range.



   Choose **Last Hour**, **Last 24 Hours**, **Last 7 Days**, **Last 30 Days**, **Last 90 Days**, or **Custom Range** to set a particular date range.

6. Under the Format section, select either **CSV** or **PDF** for the format of the report.
7. Under the Repeat section, select if you want to generate the report again.

   If you want to generate the report again, choose **Never**, **Daily**, **Weekly**, **Bi-weekly**, or **Monthly**.

8. Enter an email address to send the report.

9. Select the **Send to my Email Address** option to add your email automatically.
10. Select the **Enable link expiration** option.

    This link is delivered by email and expires in 14 days.

11. Click **Next**.
12. In the Report Name field, enter a name for the report.

    This name will be displayed in the Saved Reports page.

13. (Optional.) Add a description that will be included.
14. Under the Number of records section, choose the maximum number of records to include on the report: **20**, **50**, **100**, **500**, **1000**, or **2500**.
15. If you have chosen the PDF format, you will see the Graphs section, which you can use to include additional views.

    You can add or remove graphs included in the report by clicking the → and the ← icons.

16. Select **Save & Run** if you wish to keep the report in your Saved Reports page and receive the report in the indicated email.
17. Click **Run** to run the report.

Vulnerabilities

USM Anywhere delivers vulnerability assessment as part of a complete package of security monitoring and management capabilities for efficient threat detection. Vulnerability assessment is important because to improve security in your network, you first need to know what is vulnerable.

Vulnerability assessment is used for defining, identifying, classifying, and prioritizing the vulnerabilities in the system. The universal open and standardized method for rating IT vulnerabilities and determining the urgency of response is the Common Vulnerability Scoring System (CVSS). This method assigns severity scores to vulnerabilities. Scores range from 0 to 10, with 10 being the most severe.

USM Anywhere works on both CVSS version 3 (CVSSv3) and the previous version 2 (CVSSv2) for scoring.

USM Central displays a list of vulnerabilities detected on your connected deployments, enabling you to easily scan for potential threats on your deployments and drill down to an item on that deployment.

Note: See About Vulnerability Assessment for more information.

Important: USM Central currently only forwards vulnerabilities from USM Anywhere and not USM Appliance.

Topics covered in this section include:

Vulnerabilities Page List View 85

Searching Vulnerabilities 88

View Vulnerabilities Details 92

Labeling the Vulnerabilities 95

Create Vulnerabilities Report 96

Vulnerabilities Page List View

USM Central's Vulnerabilities page provides an overview of vulnerabilities detected within connected deployment of USM Anywhere. The vulnerabilities main page lists vulnerabilities in reverse chronological order (the most recent item displays first). Here you can review all vulnerability activity, view only a select number of deployment vulnerabilities, or filter the vulnerabilities by specific details.

Go to **Vulnerabilities** to open the page.

The Vulnerabilities page displays information on vulnerabilities. These are the different parts of the page:

- On the left side of the page are the search and filters options. Use filters to delimit your search.
- At the top of the page, you can see any filters you have applied, and you have the option to create and select different views of the .
- The main part of the page is the list of , where each row describes an individual . Click an to open a summary view. See for more information.

If you want to analyze the data, you can maximize the screen and hide the filter pane. Click the « icon to hide the filter pane. Click the ▼ icon to expand the filter pane.

The following table displays the list of the default columns found in the List view.

Default Columns Found in the List View

Column / Field Name	Description
Last Seen	Last date on which the vulnerability was seen in the asset. The displayed date depends on your computer's time zone.
Vulnerability ID	The associated Common Vulnerabilities and Exposures (CVE) identification (ID) when there is a CVE ID to display.
Vulnerability Name	The name of the vulnerability.
Deployment	Name of the deployment on which the vulnerability has been detected.
Labels	Label applied to the vulnerability. See Labeling the Vulnerabilities for more information.
Asset	The asset that is vulnerable.

Default Columns Found in the List View(Continued)

Column / Field Name	Description
Severity	The severity of the vulnerability. Values are High, Medium, and Low.
Score	The score in the Common Vulnerability Scoring System (CVSS). See Common Vulnerability Scoring System SIG for more information.
First Seen	Detection date of the vulnerability in the asset. The displayed date depends on your computer's time zone.

From the list of vulnerabilities, you can click any individual vulnerability row to display more information on the selected vulnerability. See View Vulnerabilities Details for more information.

Click the icon next to the asset name to access these options:

- **Add to current filter**: Use this option to add the asset name as a search filter.
- **Look up in OTX**: This option searches the IP address of the asset in the LevelBlue LevelBlue Labs Open Threat Exchange® (OTX™) page. See Using OTX in USM Anywhere for more information.
- **Full Details**: See Viewing Assets Details for more information.

You can choose the number of items to display by selecting **20**, **50**, or **100** below the table. You can classify some columns by clicking the icons to the right side of the heading. You can sort the item information in ascending or descending order.

Click **Generate Report** to open the Configure Report dialog box. See Create Vulnerabilities Report for more information.

Click the icon to bookmark an item for quick access.

Note: You can view your bookmarked items by going to the secondary menu and clicking the icon. This will display all of your bookmarked items and provide direct links to each of them.

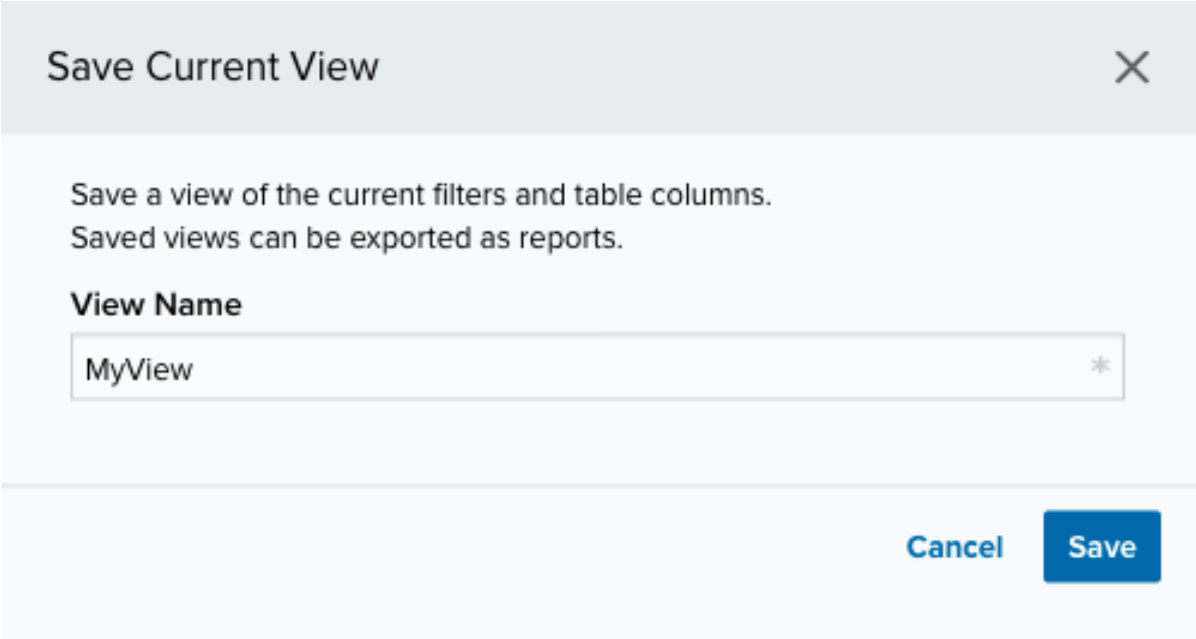
Views

You can configure the view you want for the list of items in the page.

To create a view configuration

1. From the list view, select the filters you want to apply.
2. Go to **Save View > Save As**.

   The Save Current View dialog box opens.



3. Enter a name for the view.
4. Click **Save**.

   The created view is already selected.

To select a configured view

1. From the ist view, click **View** above the filters.
2. Click **Saved Views**, and then select the view you want to see.
3. Click **Apply**.

To delete a configured view

1. From the Vulnerabilities list view, click **View** above the filters.
2. Click **Saved Views**, and then click the 🗑 icon next to the saved view you want to delete.

A Settings Delete dialog box opens to confirm the deletion.

3. Click **Accept**.

Important: The icon does not display if the view is selected.

Note: . You can only delete the views you have created .

Searching Vulnerabilities

USM Central includes the option of searching items of interest on the page. There are several filters displayed by default. You can either filter your search or enter what you are looking for in the search field.

This table shows the filters displayed by default in the main Vulnerabilities page.

Filters Displayed by Default in the Main Vulnerabilities Page

Filter Name	Meaning
Last 24 Hours	Identify vulnerabilities triggered in the last hour, 24 hours, 7 days, 30 days, or 90 days. You can also configure your own period of time by clicking the **Custom Range** option. This option enables you to customize a range. When you click **Custom Range**, a calendar opens. You can choose the first and last day to delimit your search by clicking the days on the calendar or entering the days directly. Then select the hours, minutes, and seconds by clicking the specific box. Finally, select **AM** or **PM**.
Active/Inactive	Filter vulnerabilities by the active or inactive vulnerabilities.
Deployment	Filter vulnerabilities by the name of the deployment on which the vulnerability has been detected.
Labels	Filter vulnerabilities by the labels applied to the vulnerability. See Labeling the Vulnerabilities for more information.
Vulnerability Name	Filter vulnerabilities by the name of the vulnerability.
Severity	Filter vulnerabilities by the severity of the vulnerability. Values are High, Medium, and Low. See About Vulnerability Severity for more information.
Asset	Filter vulnerabilities of the asset that is vulnerable.

To search for Vulnerabilities using the search field

1. Go to **Vulnerabilities**.
2. Enter your query in the search field.

   If you want to search for an exact phrase having two or more words, you need to put quotation marks around the words in the phrase. This includes email addresses (for example, "bob@mycompany.com").

   Note: Wildcard characters are considered as literal characters.

3. Click the icon.

Filtering Vulnerabilities

You can use filters to delimit the number of vulnerabilities that display in the List view in the Vulnerabilities page. You can also save filter views to easily use later. Your active filters will be used for reports exports.

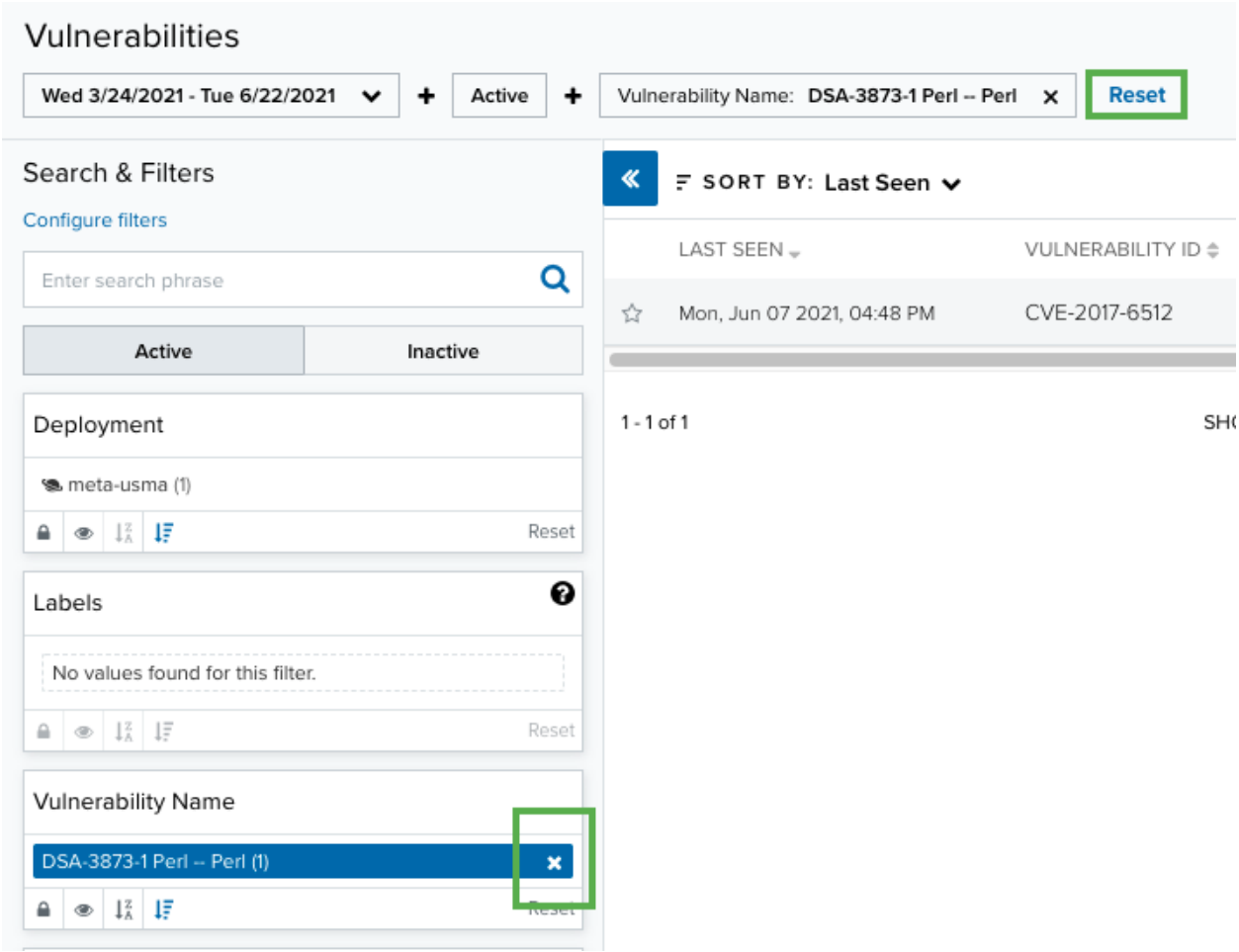
The number between brackets displayed by each filter indicates the number of items that matches the filter. You can also use the filter controls to provide a method of organizing your search and filtered results.

The following table shows the icons displayed with each filter box.

Icons Next to the Filter Title

Icon	Meaning
	Sort the filters alphabetically.
	Sort the filters by number of items that matches them

In the upper-left side of the page, you can see any filters you have applied. Remove filters by clicking the icon next to the filter. Or clear all filters by clicking **Reset**.



Note: When applying filters, the search uses the logical AND operator if the used filters are different. However, when the filter is of the same type, the search uses the logical OR operator.

Those filters that have more than 10 options include a Filter Value search field for writing text and making the search easier.

To search vulnerabilities using a filter

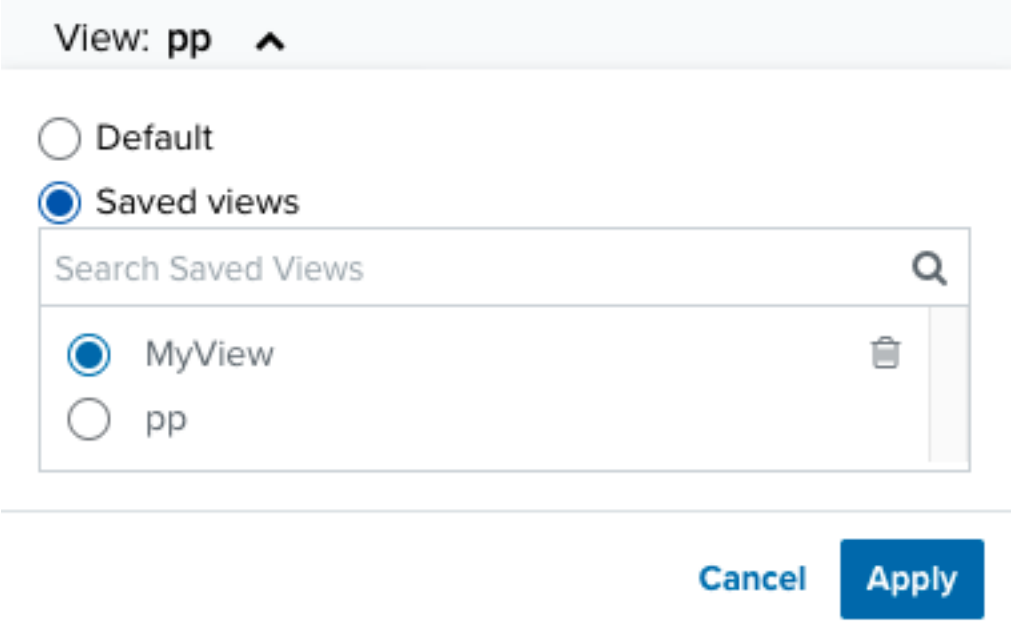
1. Go to **Vulnerabilities**.
2. Click a filter.

   The result of your search displays the identified vulnerabilities.

To save a filter configuration

1. Go to **Vulnerabilities** and select the filters you want to use in your saved view.
2. Select the **Save View** drop-down list and then click **Save as**.
3. Enter a name for the view and click **Save**.

   You can now load this view from the View drop-down list.

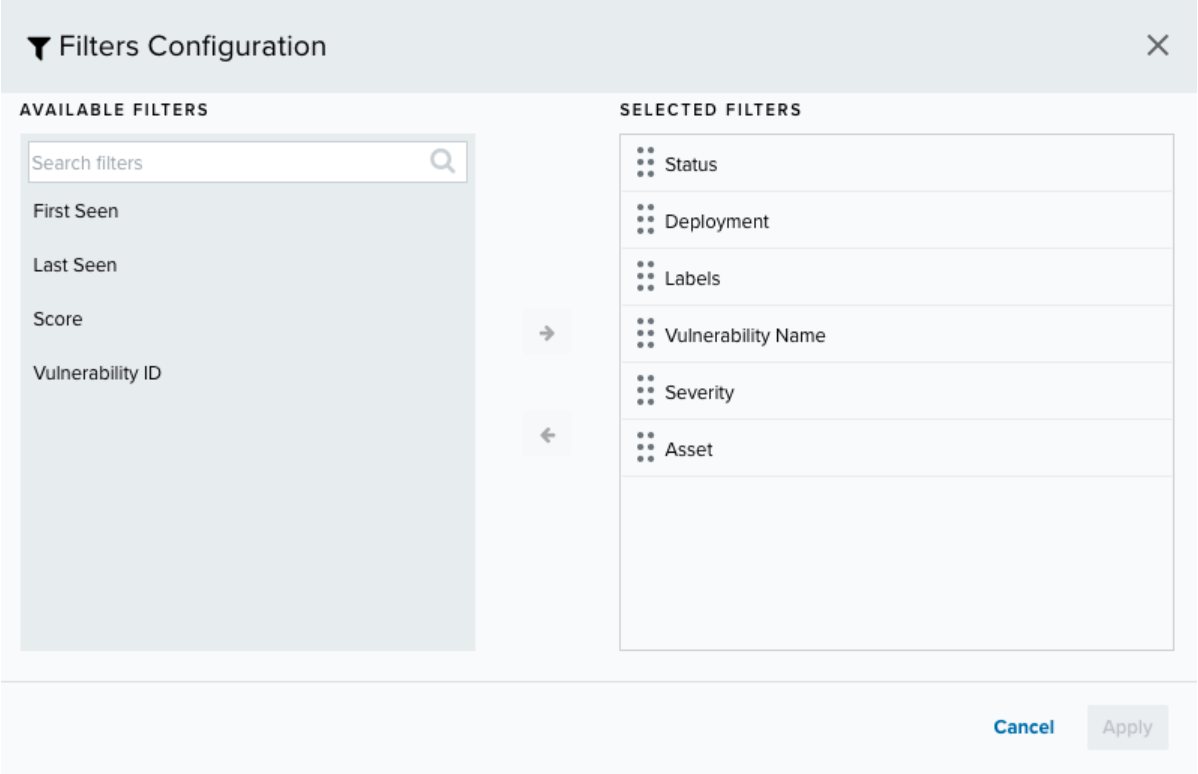


Note: If you have changed the configuration of the vulnerabilities within the List view columns, this configuration will also be saved together with the filter configuration. See Vulnerabilities Page List View for more information.

To add or delete filters from the Search & Filters area

1. Go to **Vulnerabilities**.
2. Click the **Configure Filters** link at the bottom of the Search & Filters sidebar to open the Filters Configuration window.

3. Click the arrow icons ( ) and ( ) to pass the items from the Available Filters and Selected Filters columns, and then click **Apply**.

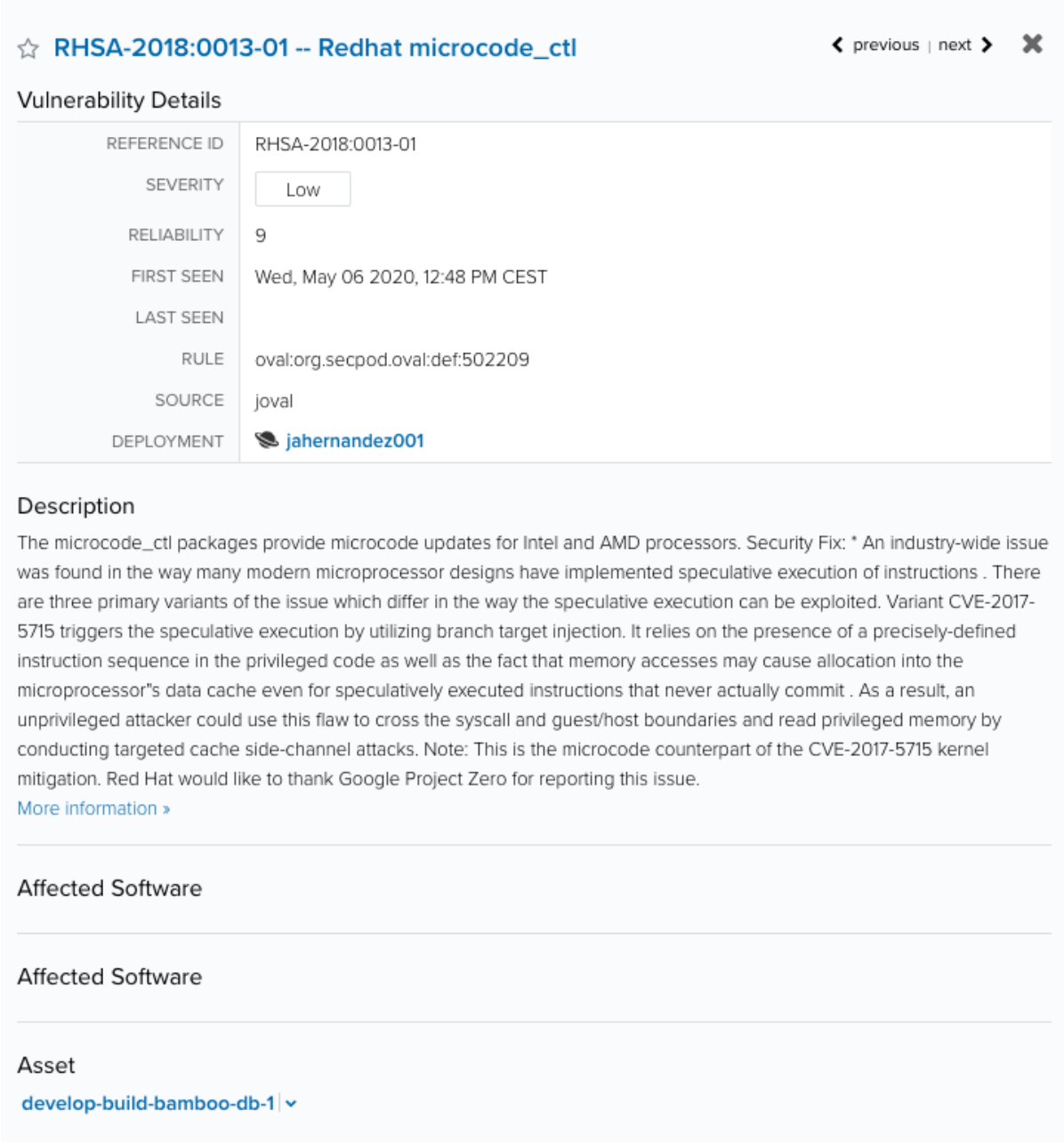


View Vulnerabilities Details

The vulnerabilities details view provides in-depth information on a vulnerability and easy access to the vulnerability within the related deployment. When you use this feature to access the vulnerability at the deployment level, you can perform further investigation, and execute actions to address it.

To view the details of a vulnerability

1. Go to **Vulnerabilities**.
2. Click the vulnerability to display a summary view, and then click the vulnerability name to open the full details of the vulnerability.



> **Note:** Click the ★ icon to bookmark an item for quick access.
>
> > **Note:** You can view your bookmarked items by going to the secondary menu and clicking the ★ icon. This will display all of your bookmarked items and provide direct links to each of them.

You can click the link in the deployment field, which opens the details of the vulnerability inside the specific deployment.

You can see the vulnerabilities details, then a description, the affected software, and the associated asset.

The ⌄ icon located next to the asset enables you to access these options:

- **Add to current filter**: Use this option to add the asset name as a search filter.
- **Look up in OTX**: This option searches the IP address of the source asset in the Open Threat Exchange page. See Using OTX in USM Anywhere for more information.
- **Full Details**: See Viewing Assets Details for more information.

3. In the upper right corner, click **Previous** and **Next** to navigate between items.
4. Click the ✖ icon to close the dialog box.

Labeling the Vulnerabilities

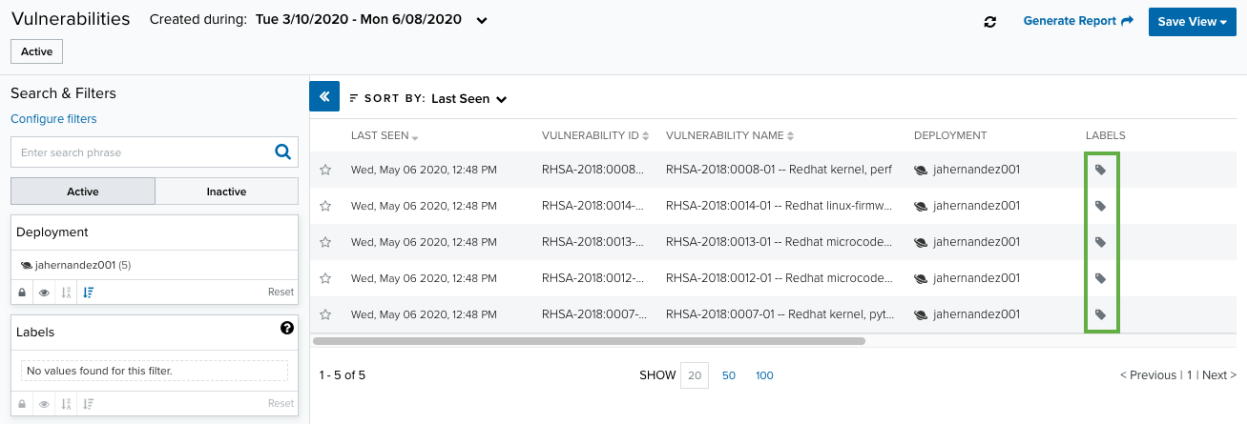
Role Availability	Read-Only	Analyst	Manager

USM Anywhere includes a set of labels that you can use to classify your vulnerabilities, to track the status of the vulnerabilities, and to search vulnerabilities using them as a filter. See Searching Vulnerabilities for more information on how to search vulnerabilities.

The Vulnerabilities page of USM Central display the labels applied from USM Anywhere.

You can't edit or delete the set of default labels:

- In Progress
- Closed
- Open
- False Positive



Create Vulnerabilities Report

You can create a PDF or CSV report of the vulnerabilities directly from the vulnerabilities page.

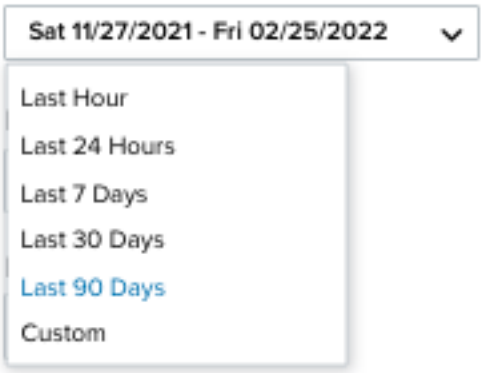
Important: LevelBlue recommends Google Chrome as the preferred browser for generating reports. The use of alternative browsers may result in poor formatting.

To create a vulnerabilities report

1. Go to **Vulnerabilities**.
2. Use filters to define the content you want to display in your report.
3. Click **Generate Report** to open the Configure Report dialog box.

   The filters selected and displayed for the page view are the ones that are populated in the report.

4. Click **Edit Filters** if you want to modify the selected filters, and then **Continue to Filters**. Do the modifications you need, and then click **Edit Report**.
5. Click the date field if you want to choose a different date range.



Choose **Last Hour**, **Last 24 Hours**, **Last 7 Days**, **Last 30 Days**, **Last 90 Days**, or **Custom Range** to set a particular date range.

6. Under the Format section, select either **CSV** or **PDF** for the format of the report.
7. Under the Repeat section, select if you want to generate the report again.

   If you want to generate the report again, choose **Never**, **Daily**, **Weekly**, **Bi-weekly**, or **Monthly**.

8. Enter an email address to send the report.
9. Select the **Send to my Email Address** option to add your email automatically.
10. Select the **Enable link expiration** option.

    This link is delivered by email and expires in 14 days.

11. Click **Next**.
12. In the Report Name field, enter a name for the report.

    This name will be displayed in the Saved Reports page.

13. (Optional.) Add a description that will be included.
14. Under the Number of records section, choose the maximum number of records to include on the report: **20**, **50**, **100**, **500**, **1000**, or **2500**.
15. If you have chosen the PDF format, you will see the Graphs section, which you can use to include additional views.

    You can add or remove graphs included in the report by clicking the → and the ← icons.

16. Select **Save & Run** if you wish to keep the report in your Saved Reports page and receive the report in the indicated email.

17. Click **Run** to run the report.

Configuration Issues

USM Anywhere assesses configuration within the system to identify the insecure use of security features, identify detailed information about configuration issues, understand operational processes, and remediate the root cause.

USM Central displays a list of configuration issues identified on your connected deployments.

Note: Configuration Issues are only available for Amazon Web Services (AWS) and Microsoft Azure Sensors.

Topics covered in this section include:

Configuration Issues List View 100

Searching Configuration Issues 103

Viewing Configuration Issues Details 105

Create Configuration Issues Report 107

Configuration Issues List View

USM Central provides a centralized view of all configuration issues identified in your connected deployments. The configuration issues main page lists configuration issues in reverse chronological order (the most recent item is displayed first). Go to **Configuration Issues**.

The Configuration Issues page displays information on configuration issues. These are the different parts of the page:

- On the left side of the page are the search and filters options. Use filters to delimit your search.
- At the top of the page, you can see any filters you have applied, and you have the option to create and select different views of the .
- The main part of the page is the list of , where each row describes an individual . Click an to open a summary view. See for more information.

If you want to analyze the data, you can maximize the screen and hide the filter pane. Click the « icon to hide the filter pane. Click the icon to expand the filter pane.

The following table displays the list of the default columns found in the List view.

List of the Default Columns in Configuration Issues

Column / Field Name	Description
Last Seen	Last date on which the configuration issue was seen in the asset. The displayed date depends on your computer's time zone
Category	Category of the configuration issue. Issues with similar impacts have the same category
Subcategory	Sub-category of the configuration issue. The sub-category explains the detail of the issue
Deployment	Name of the deployment on which the configuration issue has been identified
Asset	Asset associated with the configuration issue
Severity	Severity of the issue (values are Low, Medium, or High)

List of the Default Columns in Configuration Issues(Continued)

Column / Field Name	Description
Description	Text for identifying the configuration issue
First Seen	Date of detection of the configuration issue in the asset (the displayed date depends on your computer's time zone)

Click the icon to access these options:

- **Add to current filter**: Use this option to add the asset name as a search filter.
- **Look up in OTX**: This option searches the IP address of the asset in the LevelBlue LevelBlue Labs Open Threat Exchange® (OTX™) page. See Using OTX in USM Anywhere for more information.
- **Full Details**: See Viewing Assets Details for more information.

You can choose the number of items to display by selecting **20**, **50**, or **100** below the table. You can classify some columns by clicking the icons to the right side of the heading. You can sort the item information in ascending or descending order.

You can configure the view you want for the list of configuration issues. See Views for more information.

Click **Generate Report** to open the Configure Report dialog box. See Create Configuration Issues Report for more details.

Click the icon to bookmark an item for quick access.

Note: You can view your bookmarked items by going to the secondary menu and clicking the icon. This will display all of your bookmarked items and provide direct links to each of them.

From the list of configuration issues, you can click any individual configuration issue row to display more information on the selected configuration issue, including asset(s) that are related to the configuration issue. See Viewing Configuration Issues Details for more information.

Views

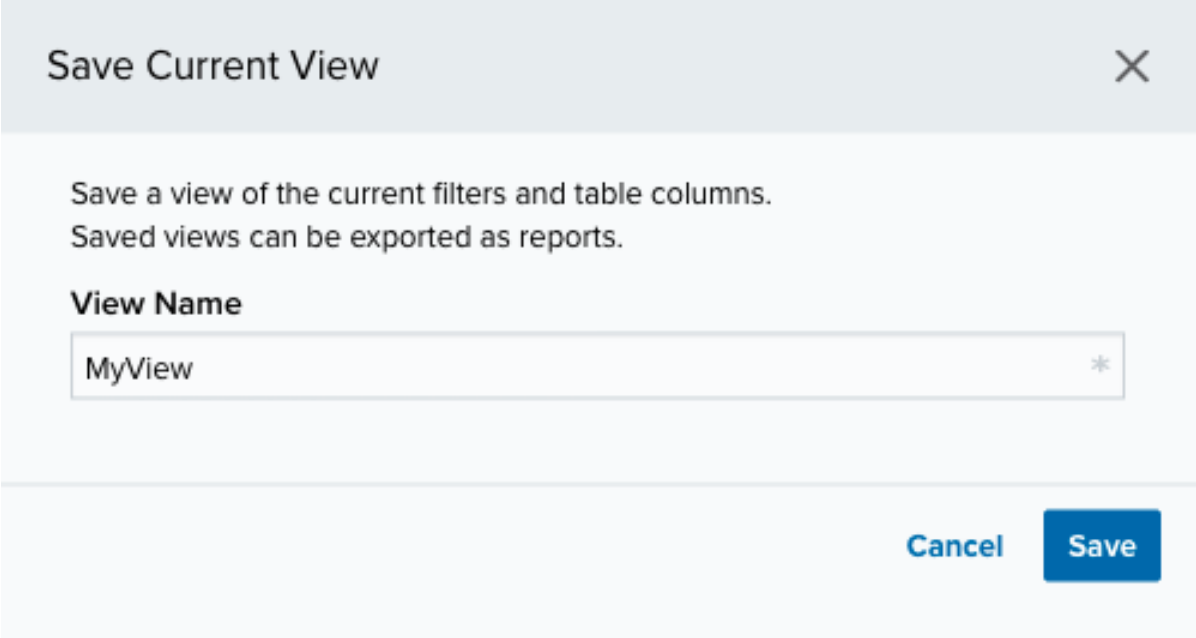
USM Central enables you to define and save a custom Configuration Issues view to have your own selected filters.

You can configure the view you want for the list of items in the page.

To create a view configuration

1. From the list view, select the filters you want to apply.
2. Go to **Save View > Save As**.

   The Save Current View dialog box opens.



3. Enter a name for the view.
4. Click **Save**.

   The created view is already selected.

To select a configured view

1. From the ist view, click **View** above the filters.
2. Click **Saved Views**, and then select the view you want to see.
3. Click **Apply**.

To delete a configured view

1. From the Configuration Issues list view, click **View** above the filters.
2. Click **Saved Views**, and then click the icon next to the saved view you want to delete.

   A Settings Delete dialog box opens to confirm the deletion.
3. Click **Accept**.

Important: The icon does not display if the view is selected.

Note: . You can only delete the views you have created .

Searching Configuration Issues

USM Central includes the option of searching items of interest on the page. There are several filters displayed by default. You can either filter your search or enter what you are looking for in the search field.

You can configure more filters and change which filters to display by clicking the **Configure Filters** link located in the upper-left side of the page. The management of filters is similar to that for assets. See Managing Filters for more information.

This table shows the filters displayed by default in the main Configuration Issues page.

Filters Displayed in the Main Configuration Issues Page

Filter Name	Meaning
Created during	Filter configuration issues triggered in the last hour, the last 24 hours, last 7 days, or last 30 days. You can also configure your own period of time by clicking the icon. This option enables you to customize a range and narrow it to delimit your search per minutes and seconds.
Active/Inactive	Filter the active or inactive configuration issues.
Deployment	Filter configuration issues by the name of the deployment on which the configuration issue has been identified.
Category	Filter configuration issues by category of the configuration issue. Issues with similar impacts have the same category.

Filters Displayed in the Main Configuration Issues Page (Continued)

Filter Name	Meaning
Subcategory	Filter configuration issues by sub-category of the configuration issue. The sub-category explains the detail of the issue.
Severity	Filter configuration issues by severity of the issue. Values are Low, Medium, or High.
Asset	Filter configuration issues by asset associated with the configuration issue.

The number between brackets displayed by each filter indicates the number of items that matches the filter. You can also use the filter controls to provide a method of organizing your search and filtered results.

The following table shows the icons displayed with each filter box.

Icons Next to the Filter Title

Icon	Meaning
A Z Z A	Sort the filters alphabetically.
	Sort the filters by number of items that matches them

In the upper-left side of the page, you can see any filters you have applied. Remove filters by clicking the ✕ icon next to the filter. Or clear all filters by clicking **Reset**.

Note: When applying filters, the search uses the logical AND operator if the used filters are different. However, when the filter is of the same type, the search uses the logical OR operator.

Those filters that have more than 10 options include a Filter Value search field for writing text and making the search easier.

To search configuration issues using a filter

1. Go to **Configuration Issues**.
2. Click a filter.

   The result of your search displays with the configuration issues identified.

Searching Configuration Issues by Using the Search Field

To search for Configuration Issues using the search field

1. Go to **Configuration Issues**.
2. Enter your query in the search field.

   If you want to search for an exact phrase having two or more words, you need to put quotation marks around the words in the phrase. This includes email addresses (for example, "bob@mycompany.com").

   Note: Wildcard characters are considered as literal characters.

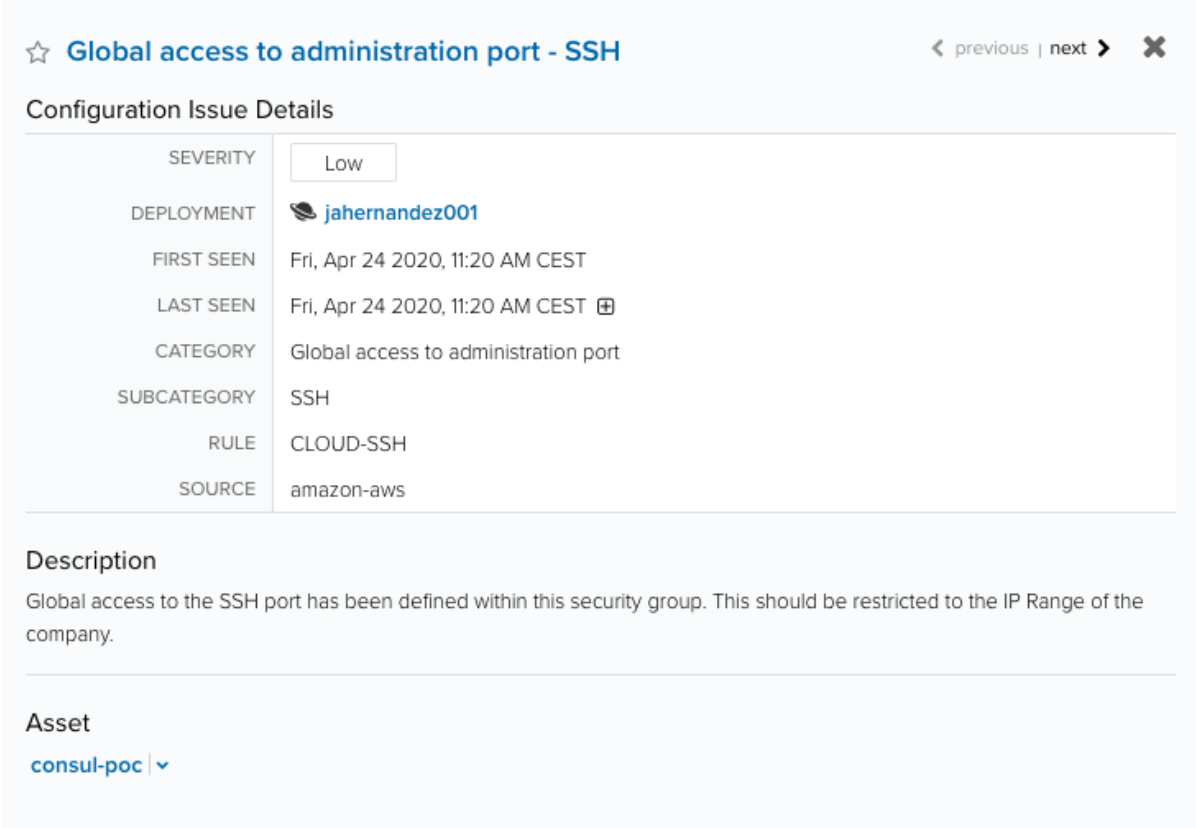
3. Click the icon.

Viewing Configuration Issues Details

The configuration issues details page provides in-depth information on a configuration issue and provides easy access to the issue within the related deployment. When you use this feature to access the configuration issue at the deployment level, you can perform further investigation, as well as execute actions to address it.

To view the details of a configuration issue

1. Go to **Configuration Issues**.
2. Click the configuration issue to display its details.



Note: Click the ★ icon to bookmark an item for quick access.

Note: You can view your bookmarked items by going to the secondary menu and clicking the ★ icon. This will display all of your bookmarked items and provide direct links to each of them.

You can click the link in the deployment field, which opens the details of the vulnerability inside the specific deployment.

It also displays the assets related to the vulnerability. You can click the icon next to the asset to go to the full details of the asset in the specific deployment.

3. In the upper right corner, click **Previous** and **Next** to navigate between items.
4. Click the icon to close the dialog box.
5. Click the configuration issue title to expand its details.
6. Click **Generate Report** to open the Configure Report dialog box.

   See Create Configuration Issues Report for more information.

Create Configuration Issues Report

You can create a PDF or CSV report of the configuration issues directly from the configuration issues page.

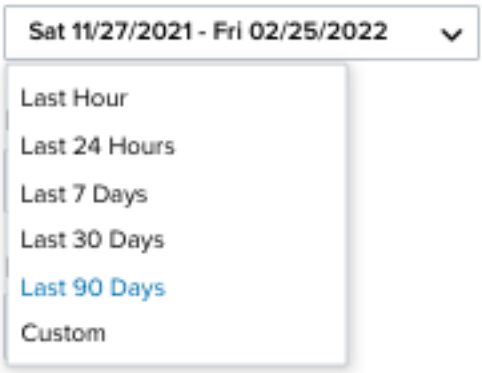
Important: LevelBlue recommends Google Chrome as the preferred browser for generating reports. The use of alternative browsers may result in poor formatting.

To create a configuration issues report

1. Go to Configuration Issues.
2. Use filters to define the content you want to display in your report.
3. Click **Generate Report** to open the Configure Report dialog box.

   The filters selected and displayed for the page view are the ones that are populated in the report.

4. Click **Edit Filters** if you want to modify the selected filters, and then **Continue to Filters**. Do the modifications you need, and then click **Edit Report**.
5. Click the date field if you want to choose a different date range.



Choose **Last Hour**, **Last 24 Hours**, **Last 7 Days**, **Last 30 Days**, **Last 90 Days**, or **Custom Range** to set a particular date range.

6. Under the Format section, select either **CSV** or **PDF** for the format of the report.
7. Under the Repeat section, select if you want to generate the report again.

   If you want to generate the report again, choose **Never**, **Daily**, **Weekly**, **Bi-weekly**, or **Monthly**.

8. Enter an email address to send the report.
9. Select the **Send to my Email Address** option to add your email automatically.
10. Select the **Enable link expiration** option.

    This link is delivered by email and expires in 14 days.

11. Click **Next**.
12. In the Report Name field, enter a name for the report.

    This name will be displayed in the Saved Reports page.

13. (Optional.) Add a description that will be included.
14. Under the Number of records section, choose the maximum number of records to include on the report: **20**, **50**, **100**, **500**, **1000**, or **2500**.
15. If you have chosen the PDF format, you will see the Graphs section, which you can use to include additional views.

    You can add or remove graphs included in the report by clicking the → and the ← icons.

16. Select **Save & Run** if you wish to keep the report in your Saved Reports page and receive the report in the indicated email.

17. Click **Run** to run the report.

Orchestration Rules Management

Every networked environment generates thousands of logs from assorted systems. USM Anywhere and USM Central enable you to manage those logs and, through the use of rules, you can prevent and frustrate attacks. The management of the different rules helps you to make the most of your environment.

Keep in mind that setting up a rule base is an iterative process. That means it happens relatively slowly and needs to be tuned over a period of time. There are always new attacks and new indicators to monitor.

USM Central enables you to create and customize these rules to add specific policies for a particular event or alarm. There are these orchestration rules:

- **Suppression rules**: Use these rules to suppress events or alarms that create noise in your system. See Suppression Rules from the Orchestration Rules Page for more information.
- **Filtering rules**: Use these rules to make the sensor drop future events that match the rule. See Filtering Rules from the Orchestration Rules Page for more information.
- **Alarm rules**: Use these rules to identify existing and emerging threats. See Alarm Rules from the Orchestration Rules Page for more information.
- **Notification rules**: Use these rules to create your own rules and receive notifications. See Notification Rules from the Orchestration Rules Page for more information.
- **Response action rules**: Use these rules to respond to an event or an alarm running an BlueApp. See Response Action Rules from the Orchestration Rules Page for more information.

Note: On the LevelBlue website, you can see the Orchestration Rules Management video, which describes how USM Central manages and shares orchestration rules between connected USM Anywhere deployments. This video includes a recorded demonstration of the steps involved in configuring, creating, filtering, disabling and enabling, and sharing rules within USM Central.

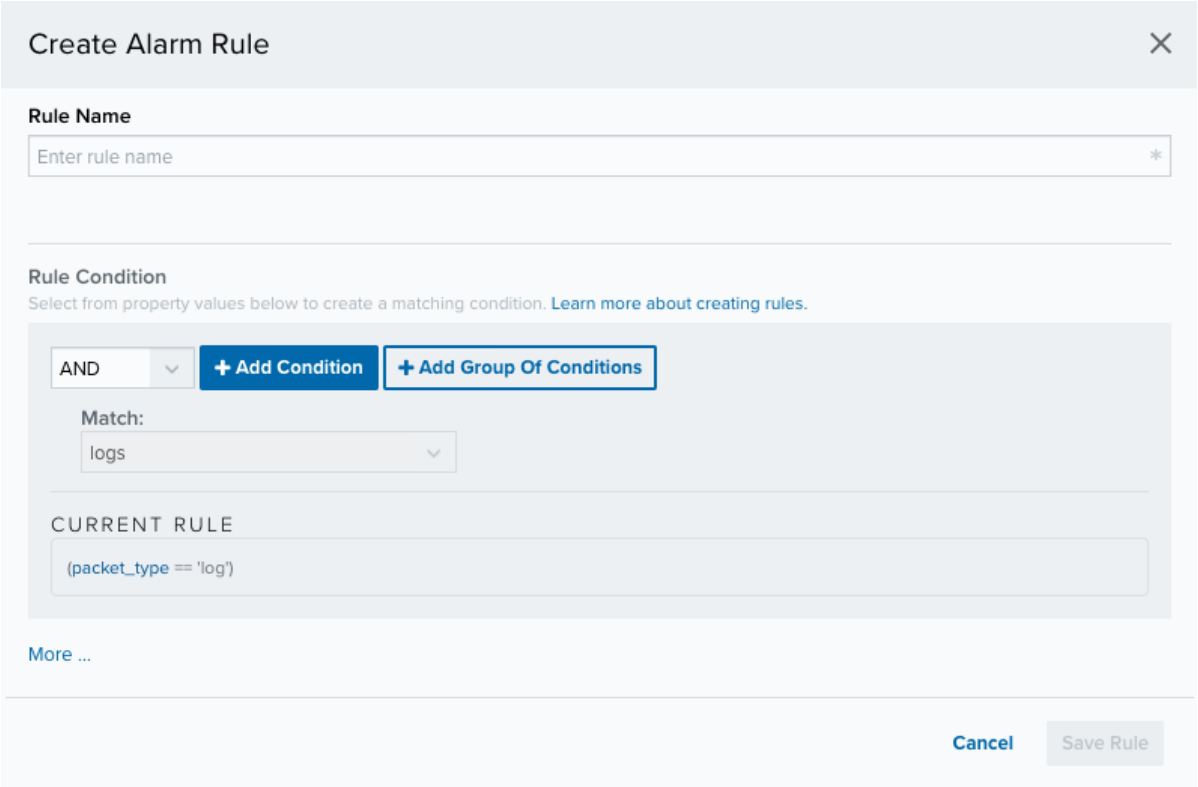
Alarm Rules from the Orchestration Rules Page

Role Availability	Read-Only	Analyst	Manager

USM Central enables you to easily identify existing and emerging threats, that are of interest. Through alarm rules, you can organize your threats and only see high-priority alarms, which can be received in email, and will help you to reduce noise and focus on important things.

To create an alarm rule

1. Go to **Settings > Rules**.
2. Select **Create Orchestration Rule > Create Alarm Rule**.



3. Enter a name for the rule.
4. Select a deployment.
5. Select the property values you want to include in the rule to create a matching condition.
6. Select an intent.

The intent describes the context of the behavior that is being observed. These intents roughly map to the stages of the intrusion kill chains but are collapsed to ensure that each is discrete. See Intent for more information about the available threat categories.

7. Enter a method.

   If known, it is the method of attack or infiltration associated with the indicator that generated the alarm.

   Note: This is a required field; if you do not complete this field, the Save button remains inactive.

8. Select a strategy.

   The strategy describes the broad-based strategy or behavior that is detected. The intention is to describe the malicious user's strategy to achieve their goal.

9. Enter a priority.

   See Priority Field for Alarms for more information.

10. Configure a mute duration set in seconds, minutes, and hours.

    You can use the mute value to set the period of time during which, once an alarm is createdUSM Anywhere will not create a new alarm based on the same conditions.

    Note: Take care to set a mute duration that is long enough to cover the span of time in which matching events will occur to maximize the efficacy of your mute.

    Important: If your USM Anywhere™ is restarted when one of your alarm mutes is active, or if there is an update or hotfix, the alarm mute will be canceled.

11. Click **Add Condition** and select the property values you want to include in the rule to create a matching condition.

    Note: If the field is related to the name of a country, you should use the country code defined by the ISO 3166.

    Note: The Sources or Destinations field needs to match the universally unique identifier (UUID) of the event or alarm. You can use the Source Name or Destination Name field instead.

12. (Optional.) Click **Add Group** to group your conditions.

Note: See Operators in the Orchestration Rules for more information.

13. (Optional.) Click the **More** link to include a multiple occurrence parameter.

    Modify these two options:

    - **Occurrences:** Specify the number of event occurrences that produce a match on the conditional expression to trigger the rule. You can enter the number of occurrences or use the arrow to scroll the value up or down. You need to enter a number between 1 and 100.
    - **Length:** Specify the length of the timespan used to identify a match for multiple occurrences. Enter the number and choose a value of seconds, minutes, or hours.

      This duration identifies the amount of time that transpires from the beginning to the end of the occurrence. If the number of occurrences is not met within this period, the rule is not a match.

      In this example, the rule applies when the configured conditions happen five times every three hours.

    These two options function together to specify the number of occurrences within a time period that will produce a match for the rule. For example, you can define a rule to trigger an alarm for an unauthorized access attempt when a failed SSH login occurs three times within a five-minute window.

14. Click **Save Rule**.

    The created rule displays in the list of rules.

Important: It takes a few minutes for an orchestration rule to become active.

To filter alarm rules by name

1. Go to **Settings > Rules**.
2. Click the box next to Filter By.
3. Enter your search.

To filter alarm rules by deployment

1. Go to **Settings > Rules**.
2. In the left navigation pane, click **Alarm Rules**.
3. Click the box **Deployment**.
4. Select **All Rules**, **Enabled**, or **Disabled**.

To filter alarm rules by rule status

1. Go to **Settings > Rules**.
2. Click the combo box next to Rule Status.
3. Select **All Rules**, **Enabled**, or **Disabled**.

To edit an alarm rule

1. Go to **Settings > Rules**.
2. On the left navigation pane, click **Alarm Rules**.
3. Click the icon of the rule you want to edit.
4. Modify the data of the items that need to be modified.
5. Click **Save Rule**.

To delete an alarm rule

1. Go to **Settings > Rules**.
2. On the left navigation pane, click **Alarm Rules**.
3. Click the icon of the rule you want to delete.
4. Confirm by clicking **Accept**.

To enable an alarm rule

1. Go to **Settings > Rules**.
2. On the left navigation pane, click **Alarm Rules**.
3. Click the icon of the rule you want to enable.

To disable an alarm rule

1. Go to **Settings > Rules**.
2. On the left navigation pane, click **Alarm Rules**.
3. Click the icon of the rule you want to disable.

To enable all alarm rules

1. Go to **Settings > Rules**.
2. On the left navigation pane, click **Alarm Rules**.
3. In the list of rules, select the first checkbox in the first column to select all the rules.
4. Click **Enable All Rules**.

To disable all alarm rules

1. Go to **Settings > Rules**.
2. On the left navigation pane, click **Alarm Rules**.
3. In the list of rules, select the first checkbox in the first column to select all the rules.
4. Click **Disable All Rules**.
5. Confirm by clicking **Accept**.

Filtering Rules from the Orchestration Rules Page

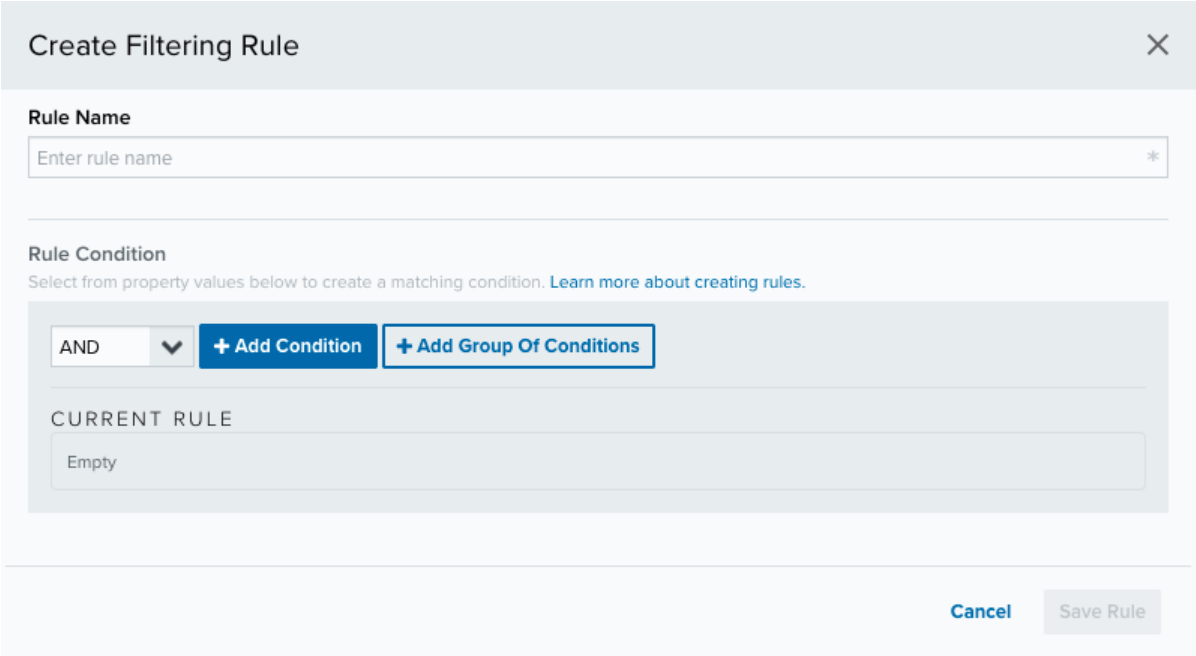
Role Availability	Read-Only	Analyst	Manager

USM Anywhere enables you to make the sensor drop future events that match the rule. These future events are neither correlated nor stored. Through these rules, you are able to define which event data you are going to store in USM Anywhere. You pay for the data you use, so discarded event information is not stored and does not count against the service-level tier of an account. This rule runs on a sensor and control node. The action of this rule has no recovery, so you must be careful when creating the rule. This action can cause a user-generated data loss environment.

Note: Filtering rules are not retroactive. The rule applies to future items, but not to previous items even if those items follow the rule.

To create a rule for filtering events

1. Go to **Settings > Rules**.
2. Select **Create Orchestration Rule > Filtering Rule**.



3. Enter a name for the rule.
4. Select a deployment.
5. Select the property values you want to include in the rule to create a matching condition.
6. Click **Add Condition** or **Add Group Of Conditions**. See Operators in the Orchestration Rules for more information.

> **Note:** If the field is related to the name of a country, you should use the country code defined by the ISO 3166.

7. Click **Save Rule**.

   The created rule displays in the list of rules.

> **Important:** It takes a few minutes for an orchestration rule to become active.

To filter filtering rules by name

1. Go to **Settings > Rules**.
2. Click the box next to Filter By.
3. Enter your search.

To filter filtering rules by deployment

1. Go to **Settings > Rules**.
2. In the left navigation pane, click **Filtering Rules**.
3. Click the box **Deployment**.
4. Select **All Rules**, **Enabled**, or **Disabled**.

To filter filtering rules by rule status

1. Go to **Settings > Rules**.
2. Click the combo box next to Rule Status.
3. Select **All Rules**, **Enabled**, or **Disabled**.

To edit a filtering rule

1. Go to **Settings > Rules**.
2. On the left navigation pane, click **Filtering Rules**.
3. Click the icon of the rule you want to edit.
4. Modify the data of the items that need to be modified.
5. Click **Save Rule**.

To delete a filtering rule

1. Go to **Settings > Rules**.
2. On the left navigation pane, click **Filtering Rules**.
3. Click the icon of the rule you want to delete.
4. Confirm by clicking **Accept**.

To enable a filtering rule

1. Go to **Settings > Rules**.
2. On the left navigation pane, click **Filtering Rules**.
3. Click the icon of the rule you want to enable.

To disable a filtering rule

1. Go to **Settings > Rules**.
2. On the left navigation pane, click **Filtering Rules**.
3. Click the icon of the rule you want to disable.

To enable all filtering rules

1. Go to **Settings > Rules**.
2. On the left navigation pane, click **Filtering Rules**.
3. In the list of rules, select the first checkbox in the first column to select all the rules.
4. Click **Enable All Rules**.

To disable all filtering rules

1. Go to **Settings > Rules**.
2. On the left navigation pane, click **Filtering Rules**.
3. In the list of rules, select the first checkbox in the first column to select all the rules.
4. Click **Disable All Rules**.
5. Confirm by clicking **Accept**.

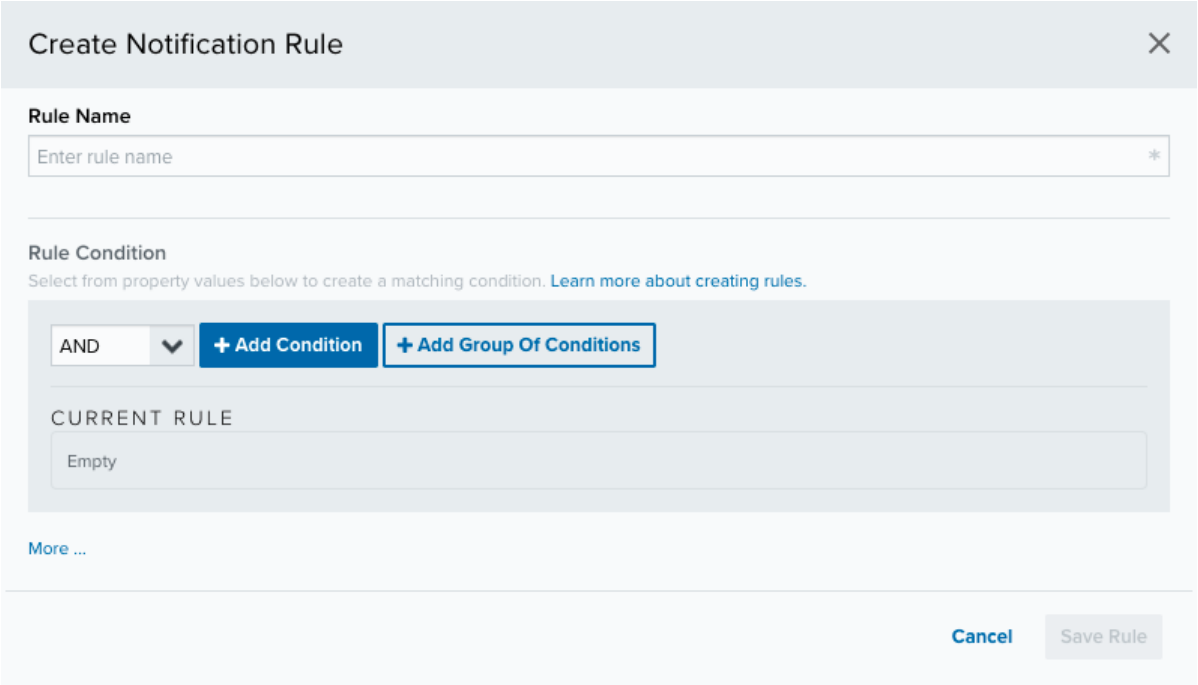
Notification Rules from the Orchestration Rules Page

Role Availability	Read-Only	Analyst	Manager

Notification rules are a mechanism to generate a specified notification method when the match criteria is met. One major difference between notification rules and other rules is that it does not have the mute operator available. These rules always generate a notification whenever the match criteria is met, and these rules never go silent.

To create a notification rule from the Orchestration Rules page

1. Go to **Settings > Rules**.
2. Select **Create Orchestration Rule > Create Notification Rule**.



3. Enter a name for the rule.
4. Select a deployment.
5. Select a notification method:
   - **Amazon SNS:** This method requires the setup of the Amazon Simple Notification Service (SNS) API call from the USM Anywhere server. There is no limit to the number of Amazon SNS endpoint notifications sent. However, this method requires having an Amazon Web Services (AWS) account for setup and use. The Amazon SNS allows the first 1000 email notifications per month to fall into the free messaging tier. See Sending Notifications Through Amazon SNS in the *USM Anywhere Deployment Guide* for more information.
   - **Datadog:** This method requires the creation of a Datadog API key and additional steps. See Sending USM Anywhere Notifications to Datadog in the *USM Anywhere Deployment Guide* for more information.
   - **Email:** This method sends the notification by email. You need to enter information for the email subject and enter a destination email address. Multiple comma-separated email addresses are possible. This method uses a built-in integration with the Amazon

Simple Email Service (SES) function and is limited to a maximum of 200 emails per rolling 24-hour period. The only user-customizable information available is the email subject line.

> **Note:** The rolling 24-hour, 200-email limit refers to all email accounts. For example, you can have a rule with multiple emails, which counts as a single email delivery. Alternately, if you have several rules with several emails, each of these counts as an individual email account. Sensor-disconnect emails do not count against this number because they are critical and are only sent to users whose role is manager.

Select the **Sanitize Email Content** checkbox to replace detailed email contents with a generic message and a link that requires user authentication to view further information.

- **PagerDuty:** This method is performed using an integration in the product, and user setup is required. See Sending USM Anywhere Notifications to PagerDuty in the *USM Anywhere Deployment Guide* for more information.
- **Slack:** This method makes use of a user-created *Slack Webhook* integration. Slack integration can also be performed using Amazon SNS. See Sending USM Anywhere Notifications to Slack in the *USM Anywhere Deployment Guide* for more information.

6. Click **Add Condition** and select the property values you want to include in the rule to create a matching condition.

   > **Note:** If the field is related to the name of a country, you should use the country code defined by the ISO 3166.

   > **Note:** The Sources or Destinations field needs to match the universally unique identifier (UUID) of the event or alarm. You can use the Source Name or Destination Name field instead.

7. (Optional.) Click **Add Group** to group your conditions.

   > **Note:** See Operators in the Orchestration Rules for more information.

8. (Optional.) Click the **More** link to include a multiple occurrence parameter.

   Modify these two options:

- **Occurrences:** Specify the number of event occurrences that produce a match on the conditional expression to trigger the rule. You can enter the number of occurrences or use the arrow to scroll the value up or down. You need to enter a number between 1 and 100.
- **Length:** Specify the length of the timespan used to identify a match for multiple occurrences. Enter the number and choose a value of seconds, minutes, or hours.

  This duration identifies the amount of time that transpires from the beginning to the end of the occurrence. If the number of occurrences is not met within this period, the rule is not a match.

  In this example, the rule applies when the configured conditions happen five times every three hours.

These two options function together to specify the number of occurrences within a time period that will produce a match for the rule. For example, you can define a rule to trigger an alarm for an unauthorized access attempt when a failed SSH login occurs three times within a five-minute window.

9. Click **Save Rule**.

   The created rule displays in the list of rules.

   Important: It takes a few minutes for an orchestration rule to become active.

To filter notification rules by name

1. Go to **Settings > Rules**.
2. Click the box next to Filter By.
3. Enter your search.

To filter notification rules by deployment

1. Go to **Settings > Rules**.
2. In the left navigation pane, click **Notification Rules**.
3. Click the box **Deployment**.

4. Select **All Rules**, **Enabled**, or **Disabled**.

To filter notification rules by rule status

1. Go to **Settings > Rules**.
2. Click the combo box next to Rule Status.
3. Select **All Rules**, **Enabled**, or **Disabled**.

To edit a notification rule

1. Go to **Settings > Rules**.
2. On the left navigation pane, click **Notification Rules**.
3. Click the icon of the rule you want to edit.
4. Modify the data of the items that need to be modified.
5. Click **Save Rule**.

To delete a notification rule

1. Go to **Settings > Rules**.
2. On the left navigation pane, click **Notification Rules**.
3. Click the icon of the rule you want to delete.
4. Confirm by clicking **Accept**.

To enable a notification rule

1. Go to **Settings > Rules**.
2. On the left navigation pane, click **Notification Rules**.
3. Click the icon of the rule you want to enable.

To disable an notification rule

1. Go to **Settings > Rules**.
2. On the left navigation pane, click **Notification Rules**.
3. Click the icon of the rule you want to disable.

To enable all notification rules

1. Go to **Settings > Rules**.
2. On the left navigation pane, click **Notification Rules**.
3. In the list of rules, select the first checkbox in the first column to select all the rules.
4. Click **Enable All Rules**.

To disable all notification rules

1. Go to **Settings > Rules**.
2. On the left navigation pane, click **Notification Rules**.
3. In the list of rules, select the first checkbox in the first column to select all the rules.
4. Click **Disable All Rules**.
5. Confirm by clicking **Accept**.

Suppression Rules from the Orchestration Rules Page

Role Availability	Read-Only	Analyst	Manager

About Suppression Rules

USM Central includes suppression rules that enable you to manage false positive alarms . After you have confirmed that these issues do not pose a security threat, create a suppression rule to prevent these issues from displaying in the user interface (UI), and avoid noise in your system.

You can create a suppression rule from the details page of an alarm (View Alarm Details). This functionality works the same way, and the Create Rule dialog box is similar when you are creating a rule either from a detail page or from the system configuration window. Although it is not a rule, you can also suppress a specific alarm.

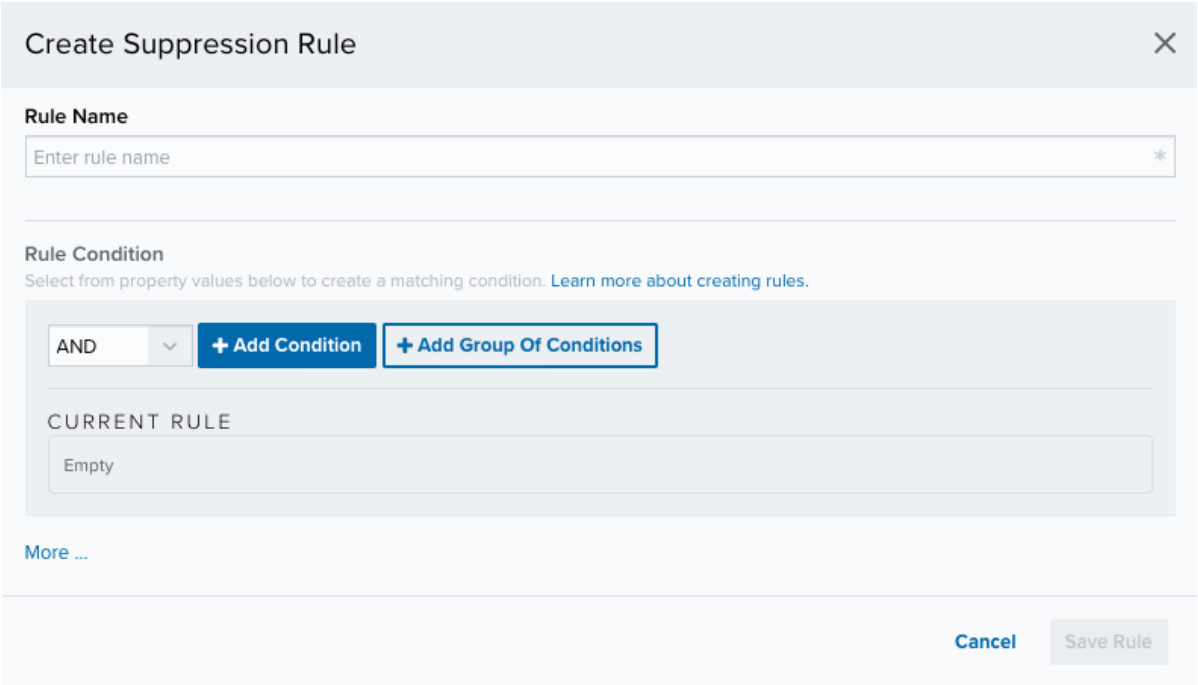
Important: The easiest way to configure a suppression rule is from the Alarms details page (see Creating Suppression Rules from the Alarms Page for more information).

Note: The suppression rule you create applies to future items. It also applies to items of the current day, up to 10 K alarms.

Managing Suppression Rules

To create a suppression rule from the orchestration rules page

1. Go to **Settings > Rules**.
2. Select **Create Orchestration Rule > Create Suppression Rule**.



3. Enter a name for the rule.
4. Select a deployment.
5. Select the property values you want to include in the rule to create a matching condition.
6. Click **Add Condition** and select the property values you want to include in the rule to create a matching condition.

> **Note:** If the field is related to the name of a country, you should use the country code defined by the ISO 3166.

> **Note:** The Sources or Destinations field needs to match the universally unique identifier (UUID) of the event or alarm. You can use the Source Name or Destination Name field instead.

7. (Optional.) Click **Add Group** to group your conditions.

Note: See Operators in the Orchestration Rules for more information.

8. (Optional.) Click the **More** link to include a multiple occurrence parameter.

   Modify these two options:

   - **Occurrences:** Specify the number of event occurrences that produce a match on the conditional expression to trigger the rule. You can enter the number of occurrences or use the arrow to scroll the value up or down. You need to enter a number between 1 and 100.
   - **Length:** Specify the length of the timespan used to identify a match for multiple occurrences. Enter the number and choose a value of seconds, minutes, or hours.

     This duration identifies the amount of time that transpires from the beginning to the end of the occurrence. If the number of occurrences is not met within this period, the rule is not a match.

     In this example, the rule applies when the configured conditions happen five times every three hours.

   These two options function together to specify the number of occurrences within a time period that will produce a match for the rule. For example, you can define a rule to trigger an alarm for an unauthorized access attempt when a failed SSH login occurs three times within a five-minute window.

9. Click **Save Rule**.

   The created rule displays in the list of rules.

Important: It takes a few minutes for an orchestration rule to become active.

To filter suppression rules by name

1. Go to **Settings > Rules**.
2. Click the box next to Filter By.
3. Enter your search.

To filter suppression rules by deployment

1. Go to **Settings > Rules**.
2. In the left navigation pane, click **Suppression Rules**.
3. Click the box **Deployment**.
4. Select **All Rules**, **Enabled**, or **Disabled**.

To filter suppression rules by rule status

1. Go to **Settings > Rules**.
2. Click the combo box next to Rule Status.
3. Select **All Rules**, **Enabled**, or **Disabled**.

To edit a suppression rule

1. Go to **Settings > Rules**.
2. On the left navigation pane, click **Suppression Rules**.
3. Click the icon of the rule you want to edit.
4. Modify the data of the items that need to be modified.
5. Click **Save Rule**.

To delete a suppression rule

1. Go to **Settings > Rules**.
2. On the left navigation pane, click **Suppression Rules**.
3. Click the icon of the rule you want to delete.
4. Confirm by clicking **Accept**.

To enable a suppression rule

1. Go to **Settings > Rules**.
2. On the left navigation pane, click **Suppression Rules**.
3. Click the icon of the rule you want to enable.

To disable a suppression rule

1. Go to **Settings > Rules**.
2. On the left navigation pane, click **Suppression Rules**.
3. Click the icon of the rule you want to disable.

To enable all suppression rules

1. Go to **Settings > Rules**.
2. On the left navigation pane, click **Suppression Rules**.
3. In the list of rules, select the first checkbox in the first column to select all the rules.
4. Click **Enable All Rules**.

To disable all suppression rules

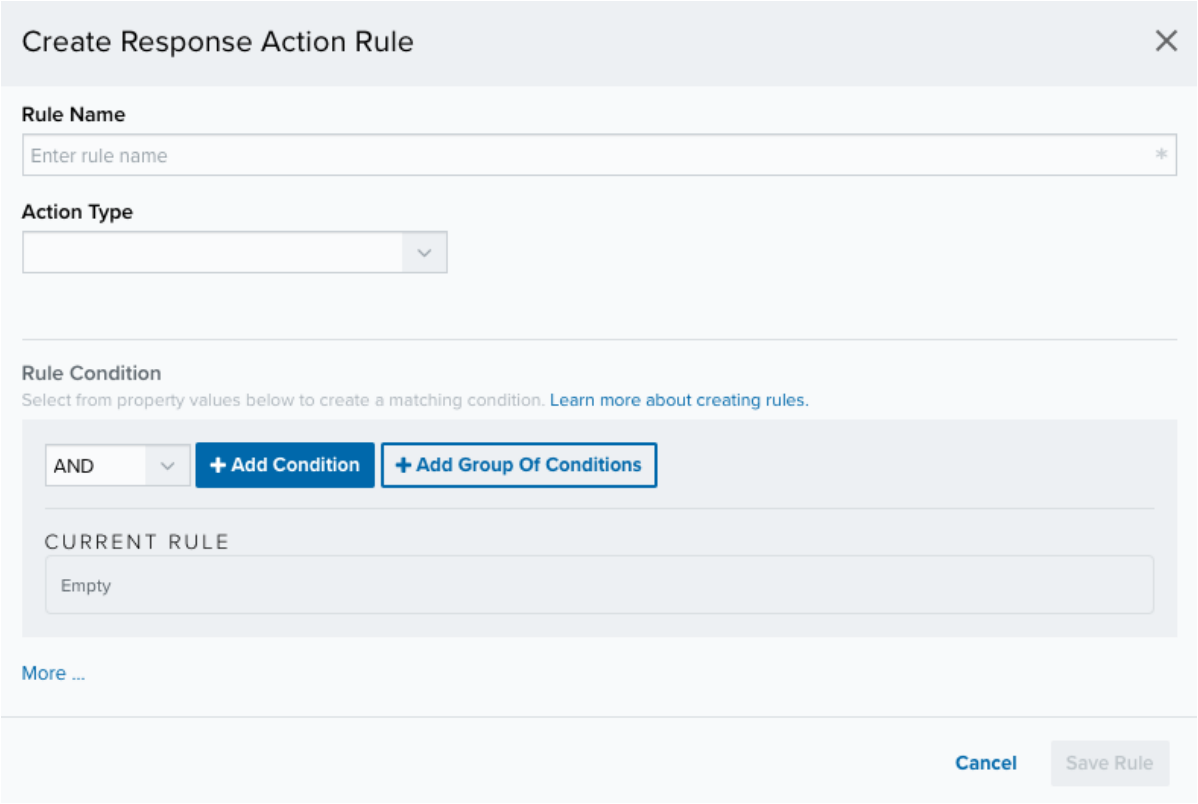
1. Go to **Settings > Rules**.
2. On the left navigation pane, click **Suppression Rules**.
3. In the list of rules, select the first checkbox in the first column to select all the rules.
4. Click **Disable All Rules**.
5. Confirm by clicking **Accept**.

Response Action Rules from the Orchestration Rules Page

Role Availability	Read-Only	Analyst	Manager

To create a response action rule

1. Go to **Settings > Rules**.
2. Select **Create Orchestration Rule > Create Response Action Rule**.



3. Enter a name for the rule.
4. Select a deployment.
5. Select an Action Type:
   - **Agent Query**: You can run a user-initiated agent query. There are several ad-hoc queries, which are in your environment by default. These queries generate events that can be used for a forensic investigation, so you can focus on fast response and remediation. See LevelBlue Agent Events and Queries for more information.
   - **Authenticated Asset Scanner**: See Performing Vulnerability Scans for more information.

- **Cisco Umbrella**: This is used to stop current and emergent threats over all ports and protocols. See BlueApp for Cisco Umbrella Actions in the *USM Anywhere AlienApps Guide* for more information.

  Note: This option displays if your environment has Cisco Umbrella Events.

- **LevelBlue Forensics and Response App**: See Collecting Forensics and Response Data in the *USM Anywhere Deployment Guide* for more information.

6. Click **Add Condition** and select the property values you want to include in the rule to create a matching condition.

   Note: If the field is related to the name of a country, you should use the country code defined by the ISO 3166.

   Note: The Sources or Destinations field needs to match the universally unique identifier (UUID) of the event or alarm. You can use the Source Name or Destination Name field instead.

7. (Optional.) Click **Add Group** to group your conditions.

   Note: See Operators in the Orchestration Rules for more information.

8. (Optional.) Click the **More** link to include a multiple occurrence parameter.

   Modify these two options:

   - **Occurrences:** Specify the number of event occurrences that produce a match on the conditional expression to trigger the rule. You can enter the number of occurrences or use the arrow to scroll the value up or down. You need to enter a number between 1 and 100.
   - **Length:** Specify the length of the timespan used to identify a match for multiple occurrences. Enter the number and choose a value of seconds, minutes, or hours.

     This duration identifies the amount of time that transpires from the beginning to the end of the occurrence. If the number of occurrences is not met within this period, the rule is not a match.

In this example, the rule applies when the configured conditions happen five times every three hours.

These two options function together to specify the number of occurrences within a time period that will produce a match for the rule. For example, you can define a rule to trigger an alarm for an unauthorized access attempt when a failed SSH login occurs three times within a five-minute window.

9. Click **Save Rule**.

   The created rule displays in the list of rules.

   Important: It takes a few minutes for an orchestration rule to become active.

To filter response action rules by name

1. Go to **Settings > Rules**.
2. Click the box next to Filter By.
3. Enter your search.

To filter response action rules by deployment

1. Go to **Settings > Rules**.
2. In the left navigation pane, click **Response Action Rules**.
3. Click the box **Deployment**.
4. Select **All Rules**, **Enabled**, or **Disabled**.

To filter response action rules by rule status

1. Go to **Settings > Rules**.
2. Click the combo box next to Rule Status.
3. Select **All Rules**, **Enabled**, or **Disabled**.

To edit a response action rule

1. Go to **Settings > Rules**.
2. On the left navigation pane, click **Response Action Rules**.
3. Click the icon of the rule you want to edit.
4. Modify the data of the items that need to be modified.
5. Click **Save Rule**.

To delete a response action rule

1. Go to **Settings > Rules**.
2. On the left navigation pane, click **Response Action Rules**.
3. Click the icon of the rule you want to delete.
4. Confirm by clicking **Accept**.

To enable a response action rule

1. Go to **Settings > Rules**.
2. On the left navigation pane, click **Response Action Rules**.
3. Click the icon of the rule you want to enable.

To disable an response action rule

1. Go to **Settings > Rules**.
2. On the left navigation pane, click **Response Action Rules**.
3. Click the icon of the rule you want to disable.

To enable all response action rules

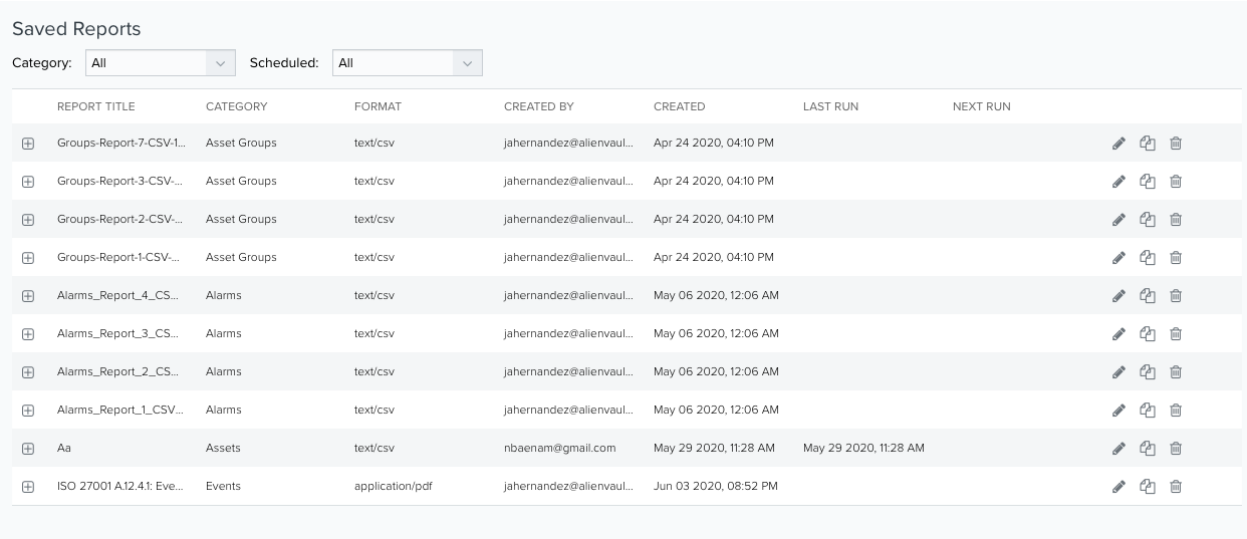
1. Go to **Settings > Rules**.
2. On the left navigation pane, click **Response Action Rules**.
3. In the list of rules, select the first checkbox in the first column to select all the rules.
4. Click **Enable All Rules**.

To disable all response action rules

1. Go to **Settings > Rules**.
2. On the left navigation pane, click **Response Action Rules**.
3. In the list of rules, select the first checkbox in the first column to select all the rules.
4. Click **Disable All Rules**.
5. Confirm by clicking **Accept**.

Saved Reports

The Saved Reports page contains a list of all the reports that have been saved in USM Anywhere and USM Central. From this page you can edit, copy, delete, or run any of the reports you have saved. Reports created in USM Anywhere can be viewed in USM Central, but can only be edited in their native USM Anywhere environment. The reports listed on the page can be filtered by category or scheduled status. You can also click the ⊞ icon next to any of the saved reports to view their export history or download a previously run report.



To edit a saved report created in USM Central

1. Click the icon to edit the report.
2. Click **Edit Filters** to add any additional filters you want to include in the report.
3. Select the date range for the information included in the report.
   You can select a predefined range of **Last Hour**, **Last 24 Hours**, **Last 7 Days**, or **Last 30 Days**, or you can set your own date range by clicking the icon.

   > **Note:** This option is not available when generating reports for assets or asset groups.

4. Under Format, select either **CSV** or **PDF**.

> **Note:** CSV reports based on filters that include timestamp columns include an additional column that displays the timestamp in a format that can be easily interpreted and sorted in a spreadsheet, labeled ISO 8601.
>
> For example, if you generate a CSV report that contains the timestamp column “Time Created” containing "Tue, Feb 15 2022, 02:48 PM", an additional column named “Time Created ISO 8601” will be included that converts the timestamp to the ISO 8601 format of "2022-02-15T14:48:43.596".

5. Under Repeat, click the drop-down list to select how often you want the scheduled report to be generated.

   If you don't want the report to be recurring, leave the selection as **Never**.

   If you have selected a time interval for recurring reports to be generated, the First Run Date, Repeat On, and Time sections show up below the Repeat section:

   - **First Run Date:** Select the day you want the first report to be generated.
   - **Schedule:** Define the frequency at which the report is generated. Options are Daily, Weekly, Bi-Weekly, Monthly, or Yearly. Select **Never** if you only want to run the report once.
   - **Time:** Select the UTC time you want the reports to run on the days they're generated.

6. In the Email Addresses section, enter the email addresses of the people to whom you want the report to be sent when it is generated. Select **Enable Link Expiration** if you want the link to the report to expire after 14 days.

   > **Note:** The subject of these emails assumes the following format:
   >
   > `$SUBDOMAIN USM Report Notification: $REPORT_NAME`
   >
   > Where $SUBDOMAIN is the subdomain of your USM Central instance and $REPORT_NAME is the name you specify for the report.

7. Click **Next** to go to the Format Output section.
8. In the Name field, enter a name for the report.
   This name displays in the Saved Reports page. You can also add a description that will be included in the generated emails.
9. For Number of Records, choose the maximum number of records to be included in the report.

10. If you have chosen the PDF format, use the Graphs section to include additional views. You can add or remove graphs included in the report by clicking the → and ← icons.

11. Select **Save & Run** to save your report and run it, or select **Run** if you don't wish to keep the report in your Saved Reports page.

To copy a saved report created in USM Central

1. Click the icon to copy a report.

   The Configure Report dialog box opens.

2. Click **Edit Filters** to add any additional filters you want to include in the report.

3. Select the date range for the information included in the report.
   You can select a predefined range of **Last Hour**, **Last 24 Hours**, **Last 7 Days**, or **Last 30 Days**, or you can set your own date range by clicking the icon.

   Note: This option is not available when generating reports for assets or asset groups.

4. Under Format, select either **CSV** or **PDF**.

   Note: CSV reports based on filters that include timestamp columns include an additional column that displays the timestamp in a format that can be easily interpreted and sorted in a spreadsheet, labeled ISO 8601.

   For example, if you generate a CSV report that contains the timestamp column “Time Created” containing "Tue, Feb 15 2022, 02:48 PM", an additional column named “Time Created ISO 8601” will be included that converts the timestamp to the ISO 8601 format of "2022-02-15T14:48:43.596".

5. Under Repeat, click the drop-down list to select how often you want the scheduled report to be generated.

   If you don't want the report to be recurring, leave the selection as **Never**.

   If you have selected a time interval for recurring reports to be generated, the First Run Date, Repeat On, and Time sections show up below the Repeat section:

- **First Run Date:** Select the day you want the first report to be generated.
- **Schedule:** Define the frequency at which the report is generated. Options are Daily, Weekly, Bi-Weekly, Monthly, or Yearly. Select **Never** if you only want to run the report once.
- **Time:** Select the UTC time you want the reports to run on the days they're generated.

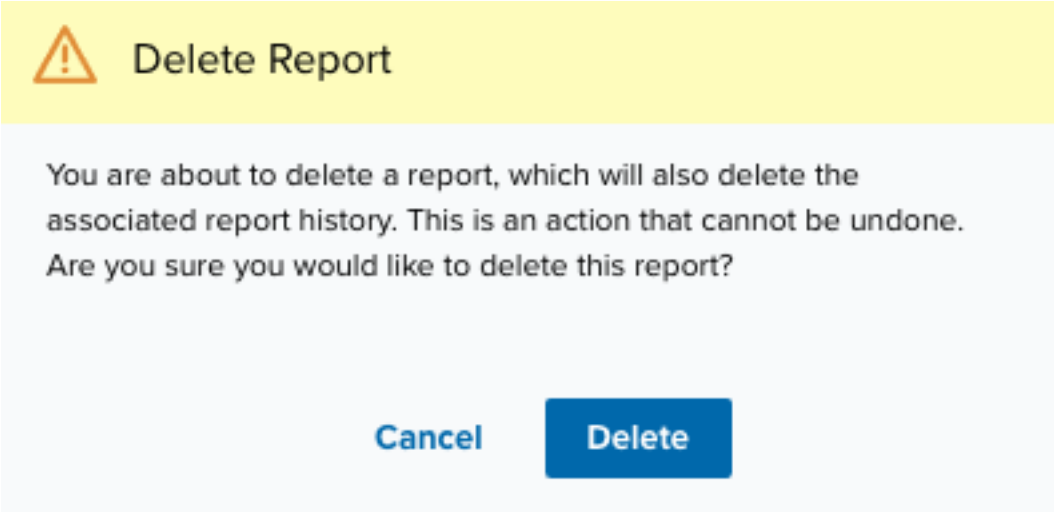
6. In the Email Addresses section, enter the email addresses of the people to whom you want the report to be sent when it is generated. Select **Enable Link Expiration** if you want the link to the report to expire after 14 days.

> **Note:** The subject of these emails assumes the following format:
>
> `$SUBDOMAIN USM Report Notification: $REPORT_NAME`
>
> Where $SUBDOMAIN is the subdomain of your USM Central instance and $REPORT_NAME is the name you specify for the report.

7. Click **Next** to go to the Format Output section.
8. In the Name field, enter a name for the report.
   This name displays in the Saved Reports page. You can also add a description that will be included in the generated emails.
9. For Number of Records, choose the maximum number of records to be included in the report.
10. If you have chosen the PDF format, use the Graphs section to include additional views. You can add or remove graphs included in the report by clicking the → and ← icons.
11. Select **Save & Run** to save your report and run it, or select **Run** if you don't wish to keep the report in your Saved Reports page.

To delete a saved report created in USM Central

1. Locate the report in the Saved Reports list.
2. In the row for the report, click the icon.



3. Click **Delete** to confirm.

System Events Management

An event is a record of activity that contains information and resides in a log file. USM Anywhere collects, normalizes, and enriches logs with additional metadata, which are called events.

USM Anywhere enables you to display system events. These events are any events generated within your environment. They are not actions associated with any of the monitored assets or networks collected by your environment. For instance, the system generates a system event when an asset, a user, or a node is created, updated, or deleted or when you modify your multifactor authentication (MFA) subscription.

This topic discusses these subtopics:

USM Central System Events List View 139

Searching System Events 140

Viewing System Event Details 142

USM Central System Events List View

Role Availability | ✗ Read-Only | ✓ Analyst | ✓ Manager

USM Central provides a centralized view of your system events. Go to **Settings > System Events**.

The system events page displays information on any events generated within your environment. On the left you can find the search and filters options. In the upper-left side of the page, you can see any filters you have applied, and you have the option to create and select different views of the system events. The main part of the page is the actual list of system events. Each row describes an individual system event.

If you want to analyze the data, you can maximize the screen and hide the filter pane. Click the « icon to hide the filter pane. Click the ▼ icon to expand the filter pane.

Note: By default, the list will display all System Events created during the last 24 hours.

The following table displays the list of the default columns found in the List view.

List of the Default Columns in the System Events Page

Column Field Name	Description
Event Name	Name of the event.
Time Created	The date and time of the creation of the event. The displayed date depends on your computer's time zone.
Source Address	IP address of the event or computer that it takes place on.
Source	Email of the user that the action is being performed on. For example, if user email@mycompany.com modifies or creates user new@mycompany.com, then the destination email is new@mycompany.com.
Affected Resource	Email of the user that performed the action. For example, when user email@mycompany.com logs in, the source email is email@mycompany.com.

List of the Default Columns in the System Events Page(Continued)

Column Field Name	Description
Event outcome	Indicates if the action was success and completed or if it failed.
Event Details	It is a small description of what was changed in the system event. It only gets populated for certain actions and indicates what is being changed. Most of these are user changes (for example, when a user is suspended, a locked status is reset, MFA is enabled or disabled, or a password is updated.

Click the ★ icon to bookmark an item for quick access.

Note: You can view your bookmarked items by going to the secondary menu and clicking the ★ icon. This will display all of your bookmarked items and provide direct links to each of them.

You can choose the number of items to display by selecting **20**, **50**, or **100** below the table. You can classify some columns by clicking the icons to the right side of the heading. You can sort the item information in ascending or descending order.

Searching System Events

Role Availability	Read-Only	Analyst	Manager

USM Central includes the option of searching items of interest on the page. There are several filters displayed by default. You can either filter your search or enter what you are looking for in the search field.

This table shows the filters displayed by default in the main System Events page.

Filters Displayed by Default in the Main System Events Page

Filter Name	Meaning
Created during	Filter system events triggered in the last hour, last 24 hours, last 7 days, last 30 days, or last 90 days. You can also configure your own period of time by clicking the **Custom Range** option. This option enables you to customize a range. When you click **Custom Range**, a calendar opens. You can choose the first and last day to delimit your search by clicking the days on the calendar or entering the days directly. Then select the hours, minutes, and seconds by clicking the specific box. Finally, select **AM** or **PM**.
Event Name	Filter system events by the short, user-readable description of the system event.
Affected Resource	Filter system events by the email of the user that performed the action. For example, when user email@alienvault.com logs in, the source email is email@alienvault.com.
Source	Filter system events by the email of the user that the action is being performed on. For example, if user email@alienvault.com modifies or creates user new@alienvault.com, then the destination email is new@alienvault.com.
Source Address	Filter system events by IP address of the event or computer that it takes place on.
Event Outcome	Filter system events by the by how the action was: success and completed or failed.

The number between brackets displayed by each filter indicates the number of items that matches the filter. You can also use the filter controls to provide a method of organizing your search and filtered results. These are the icons next to each filter title:

Icons Next to the Filter Title

A Z Z A	Sort the filters alphabetically.
	Sort the filters by the number of items that matches them.

In the upper-left side of the page, you can see any filters you have applied. Remove filters by clicking the ✖ icon next to the filter. Or clear all filters by clicking **Reset All Filters**.

> **Note:** When applying filters, the search uses the logical AND operator if the used filters are different. However, when the filter is of the same type, the search uses the logical OR.

Those filters that have more than ten options include a Filter Value search field for writing text and making the search easier.

Searching System Events by Using the Search Field

To search System Events using the search field

1. Go to **Settings > System Events**.
2. Enter your query in the search field.

   If you want to search for an exact phrase having two or more words, you need to put quotation marks around the words in the phrase. This includes email addresses (for example, "bob@mycompany.com").

   > **Note:** Wildcard characters are considered as literals.

3. Click the icon.

The result of your search displays with the items identified.

Viewing System Event Details

Role Availability	Read-Only	Analyst	Manager

The system event details page provides in-depth information on system events.

To view the details of a system event

1. Go to **Settings > System Events**.
2. Click the system event to display its details.

   Click the icon to bookmark an item for quick access.

> **Note:** You can view your bookmarked items by going to the secondary menu and clicking the ★ icon. This will display all of your bookmarked items and provide direct links to each of them.

3. In the upper right corner, click **Previous** and **Next** to navigate between items.
4. Click the ✖ icon to close the dialog box.

User Management

Role Availability	Read-Only	Analyst	Manager

In USM Central, user administration and management provides a broad range of control for security, role-based permissions, and integration with connected deployments. The system requires that all users log in with a username and a password. LevelBlue recommends that users enable Using Multi-Factor Authentication (MFA) for their account to provide extra security to their USM Central environment and all connected deployments.

USM Central collects information about when a user logs in to the system and what the user does. This information is available when you go to **Settings > System Events**. See System Events Management for more information.

Users can access settings for their own account and log out of the system by clicking the icon at the bottom of the expanded pane.

Notable user management features in USM Central include the following:

- Accounts in USM Central use role-based access control (RBAC) to assign users to pre-defined levels of access to different functions in the user interface (UI). See Role-Based Access Control (RBAC) in USM Central for more information.
- Account access can be given an extra level of security by enabling MFA to log in. See Role-Based Access Control (RBAC) in USM Central for more information.

  > **Note:** LevelBlue recommends that users enable MFA for their account. MFA adds extra security because it requires multiple factors to authenticate a user, making it more difficult for an unauthorized person to gain access to the account.

- Connected deployments can be accessed from the USM Central drop-down list at the top of the page. MFA authorization is carried over between deployments when logging into other environments from the USM Central deployments drop-down list.
- Manager accounts can regulate which connected deployments are visible in the USM Central UI for other accounts.

Because USM Central user accounts are replicated in all connected deployments, users created in USM Central will have the same role permissions in the connected deployment. These roles can be individually changed in the user management controls from the

connected deployments as well. Because of the level of customization available, this enables users to have higher or lower role-based permissions in connected deployments as well as different views of what deployment information is visible in the USM Central UI.

Topics covered in this section include:

Creating Users 146

Role-Based Access Control (RBAC) in USM Central 148

Editing Users 151

Managing Your Profile Settings 154

Deleting Users 161

Configuring Web UI Session Timeout 162

Regulated Deployment Access 163

Using Multi-Factor Authentication 165

User Account Protections 168

Creating Users

Role Availability	Read-Only	Analyst	Manager

Add a user account in your USM Central environment for each member of your team who needs access. Users created in USM Central are automatically created in the connected deployments as well. These new users share the same role access in both environments. Manager accounts can manually change the access of other user accounts in the individual environments.

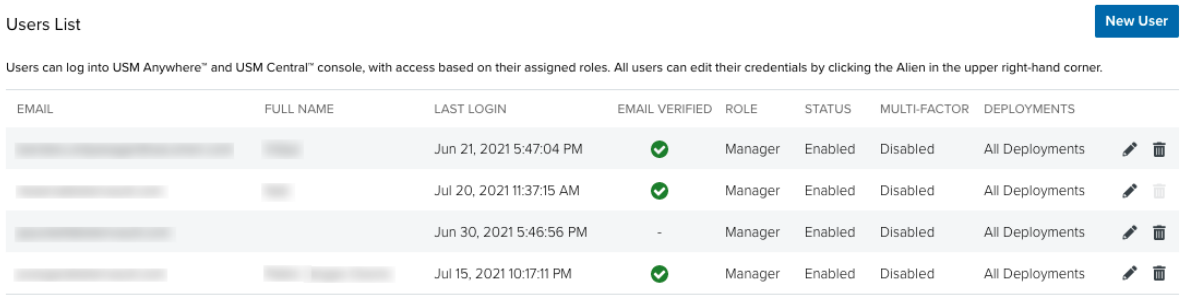
If an account is created in a connected deployment first and then added to USM Central, the account from the connected deployment will take precedence over the account in USM Central. This can cause issues with things like multifactor authentication (MFA) login for the USM Central account. LevelBlue recommends that you delete the account on the connected deployment before adding the account to USM Central.

If you are an LevelBlue Managed Security Service Provider (MSSP), managing more than one USM Central instance is common. For example, you may have an instance for each of your clients, or you may maintain a production instance and a staging instance for testing purposes. Each instance has its unique subdomain. When creating users in these instances, be aware that you cannot use the same email address even when the user is in an instance with a different subdomain. You will receive an error saying "Unable to create user" if you try.

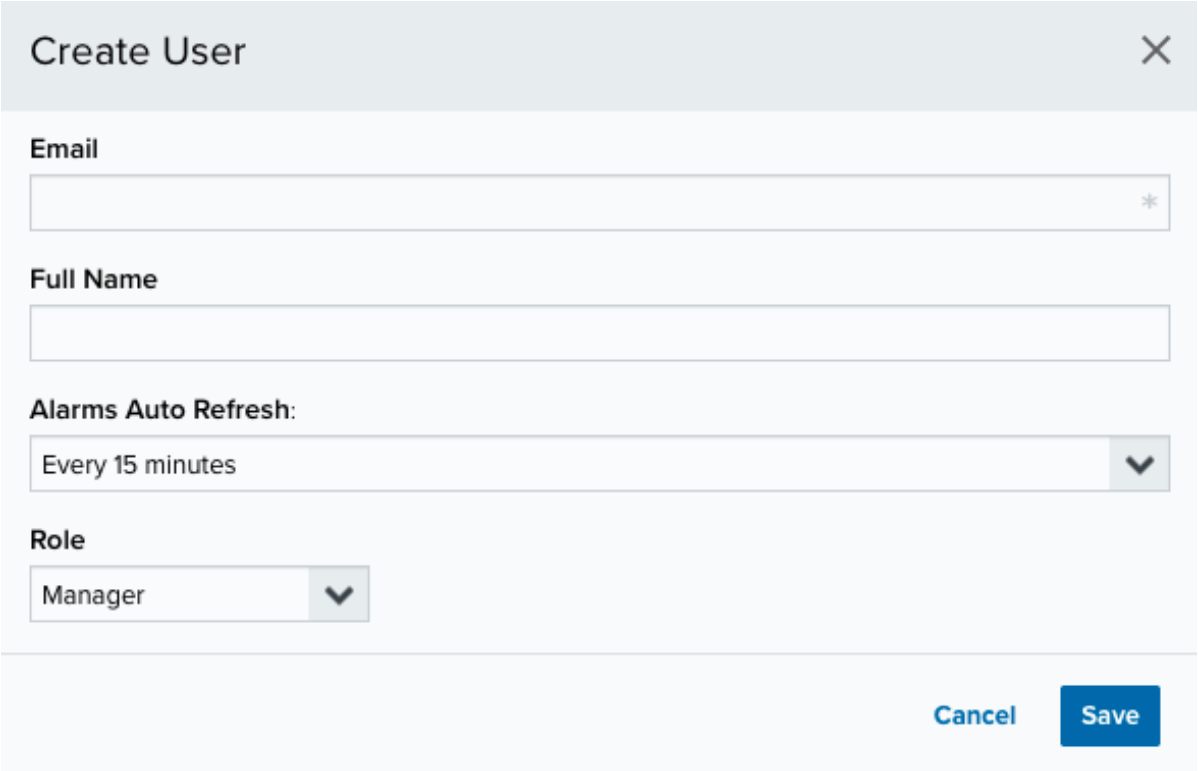
USM Central implements role-based access control (RBAC). See Role-Based Access Control (RBAC) in USM Central for more information.

To create a user

1. Go to **Settings > Users** to open the page.
2. Click **New User**.



3. Enter the user's email address and full name.



4. Each user is required to verify their account and set up their initial password, with the exception of the user whose email address is associated with the USM Central license.

   This user is indicated by a dash (-) in the Email Verified column. A green checkmark indicates an account verification email was sent and a user has set their password. Users who have not fully verified their account are indicated by a red X .

   Note: If you manage multiple USM Central instances, you cannot create users with the same email address in different subdomains.

5. (Optional.) Configure an interval for auto-refreshing the alarms page.
6. Select the role you want to assign to the user.

   See Role-Based Access Control (RBAC) in USM Central for more information.

7. Click **Save**.

   USM Central sends an email to the email address that includes a link to set a password and login.

Role-Based Access Control (RBAC) in USM Central

Role Availability	Read-Only	Analyst	Manager

USM Central implements role-based access control (RBAC), which provides users with the following:

- The ability to restrict certain users from accessing administrative capabilities like adding new users
- Predefined roles that range from read-only access to full administrative capabilities so managers can easily select the appropriate role for a new user

There are three roles in USM Central:

- **Read-Only**: You can access views and search the system but cannot make system changes that impact other users.
- **Analyst**: You can view and search the system and perform all the same tasks as the Read-Only role, and also view alarms.
- **Manager**: This role enables Analyst permissions, and also enables you to update deployments, add or configure credentials for users, and view alarms.

You can see the predefined roles in USM Central in the following table.

Predefined Roles in USM Central

Section	Action	Read-Only User	Analyst User	Manager User
Bottom Navigation	Bookmarks, help, feedback links	✔	✔	✔
	Profile Settings	✔	✔	✔

Predefined Roles in USM Central (Continued)

Section	Action	Read-Only User	Analyst User	Manager User
Alarms	View: alarms page and alarm details	✔	✔	✔
	Configure filters	✔	✔	✔
	Asset drop-down menu items: add to current filter, look up in OTX	✔	✔	✔
	Asset drop-down menu items: full details	✔	✔	✔
	Manage columns	✔	✔	✔
	Generate report	✔	✔	✔
	Save views	✔	✔	✔
	Alarm details: create rule	✘	✔	✔
	Alarm labels: apply, create, manage	✘	✔	✔
	Alarm Status: update	✘	✔	✔
Vulnerabilities	View: vulnerabilities page and vulnerabilities details	✔	✔	✔
	Generate report	✔	✔	✔
	Save views	✔	✔	✔
	Asset drop-down menu items: add to current filter, look up in OTX, full details	✔	✔	✔

Predefined Roles in USM Central (Continued)

Section	Action	Read-Only User	Analyst User	Manager User
Configuration Issues	View: configuration issues page and configuration issues details	✔	✔	✔
	Configure filters	✔	✔	✔
	Generate report	✔	✔	✔
	Save view	✔	✔	✔
	Asset drop-down menu items: add to current filter, look up in OTX, full details	✔	✔	✔
Settings > Deployments	View the deployments page	✔	✔	✔
	Connect to an existing deployment	✘	✔	✔
	Create a new deployment	✘	✘	✔
	Disconnect a deployment	✘	✘	✔
	Configure a deployment	✘	✘	✔
	Access a connected deployment	✘	✔	✔
Settings > Users	View the user page	✔	✔	✔
	Edit a user	✘	✘	✔
	Delete a user	✘	✘	✔
	Create a user	✘	✘	✔

Predefined Roles in USM Central (Continued)

Section	Action	Read-Only User	Analyst User	Manager User
Settings > System Events	View the system events page	✔	✔	✔
Settings > System Settings	Modify the session timeout	✖	✔	✔
Settings > Rules	View the rules page	✔	✔	✔
	Create an orchestration rule	✖	✔	✔
Reports > Saved Reports	Edit a report	✖	✔	✔
	Copy a report	✖	✔	✔
	Delete a report	✖	✔	✔

Note: On LevelBlue website, you can see the Role Based Access Control video which describes how USM Central implements role-based access control. This video includes a recorded demonstration of the steps involved in configuring Role-Based Access Control within USM Central.

Editing Users

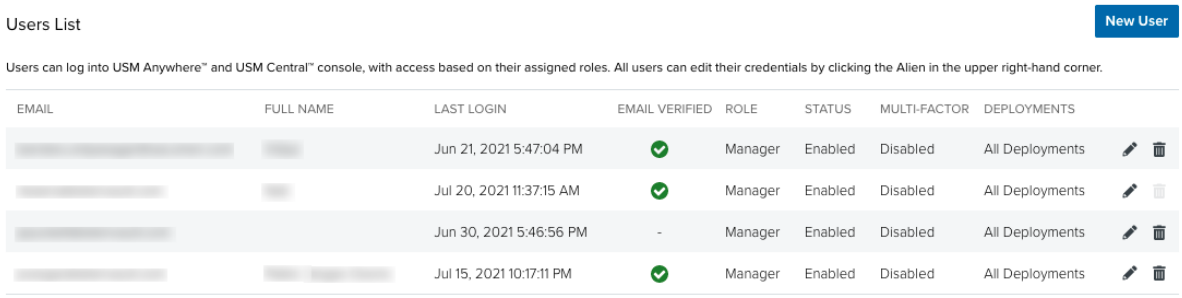
Role Availability ✖ Read-Only ✖ Analyst ✔ **Manager**

Assuming the Manager role, you can modify several items for the account of another user. For example, if users are unable to log in because they forgot their password or no longer have an authentication mobile device, you can perform a reset for their account.

Note: Only users having a role of Manager can edit users.

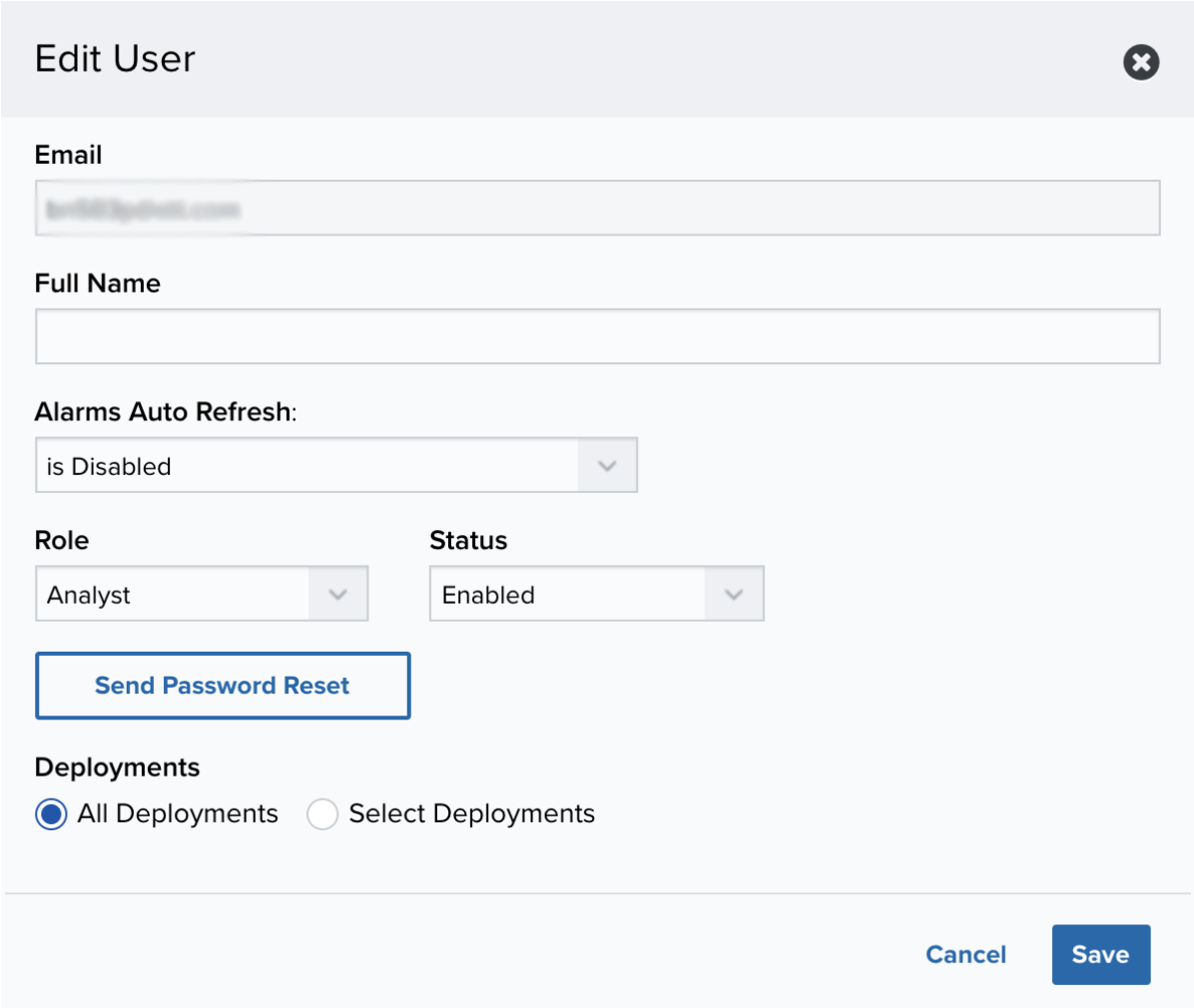
To edit a user account

1. Go to **Settings > Users** to open the page that displays the list of user accounts in your USM Central environment.



2. In the row for the user account, click the icon.

3. Make changes to the account parameters as needed:



Note: If you click the ✎ of your own user, the Profile page displays. See Managing Your Profile Settings for more information.

- Change the email address for the account.
- Change the full name for the account.
- Change the time of the alarm auto refreshing page.
- Change the role for the account. See Role-Based Access Control (RBAC) in USM Anywhere for more information.

- Change the status for the account. If you need to temporarily disable a user account, you can set the status to **Disabled**. This is a best practice for revoking access and usually a better alternative to deleting a user account.
- Click **Send Password Reset** to reset the password for the user. When you do a password reset, the user receives an email with a link to set a new password for the account.
- Change the deployments if needed.
- In the Deployments section, click the button related to the settings you want to apply:
  - Click **All Deployments** if you want the user to have visibility over all connected deployments.
  - Click **Select Deployments** if you want to designate specific deployments.
- If you click the **Select Deployments** button, the connected deployments will display below. Select the checkbox for each of the deployments to which you want the user to have access.

4. Click **Save**.

To reset a password account

1. Go to **Settings > Users** to open the users list page.
2. Click the icon next to the user account you want to reset the password.

   Note: You are not allowed to change the email address for the account.

3. Change the **Full Name** for the account.
4. Click **Send Password Reset**.

   The user receives an email with a link that enables him to change the password.

5. Click **Save**.

Managing Your Profile Settings

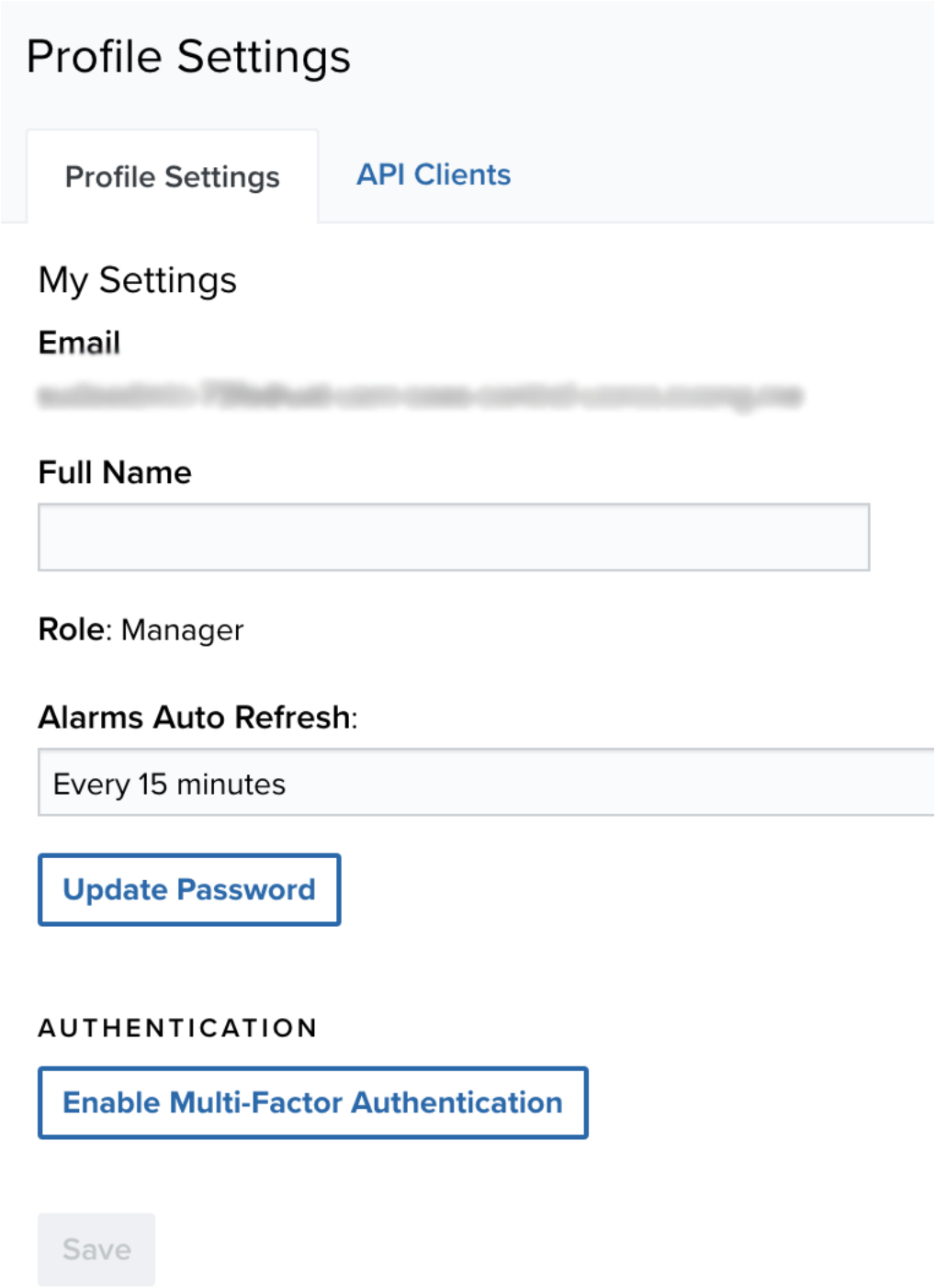
Role Availability	Read-Only	Analyst	Manager

You can manage your own user account, which enables you to do the following:

- Change your full name and password
- Enable multi-factor authentication (MFA) for the account
- Configure an interval for auto-refreshing the alarms pages

To manage your profile settings

1. At the bottom of the expanded pane of the USM Central web user interface (UI), hover over the profile settings options, and select **Profile**.



2. Modify the data of the items that can be modified.

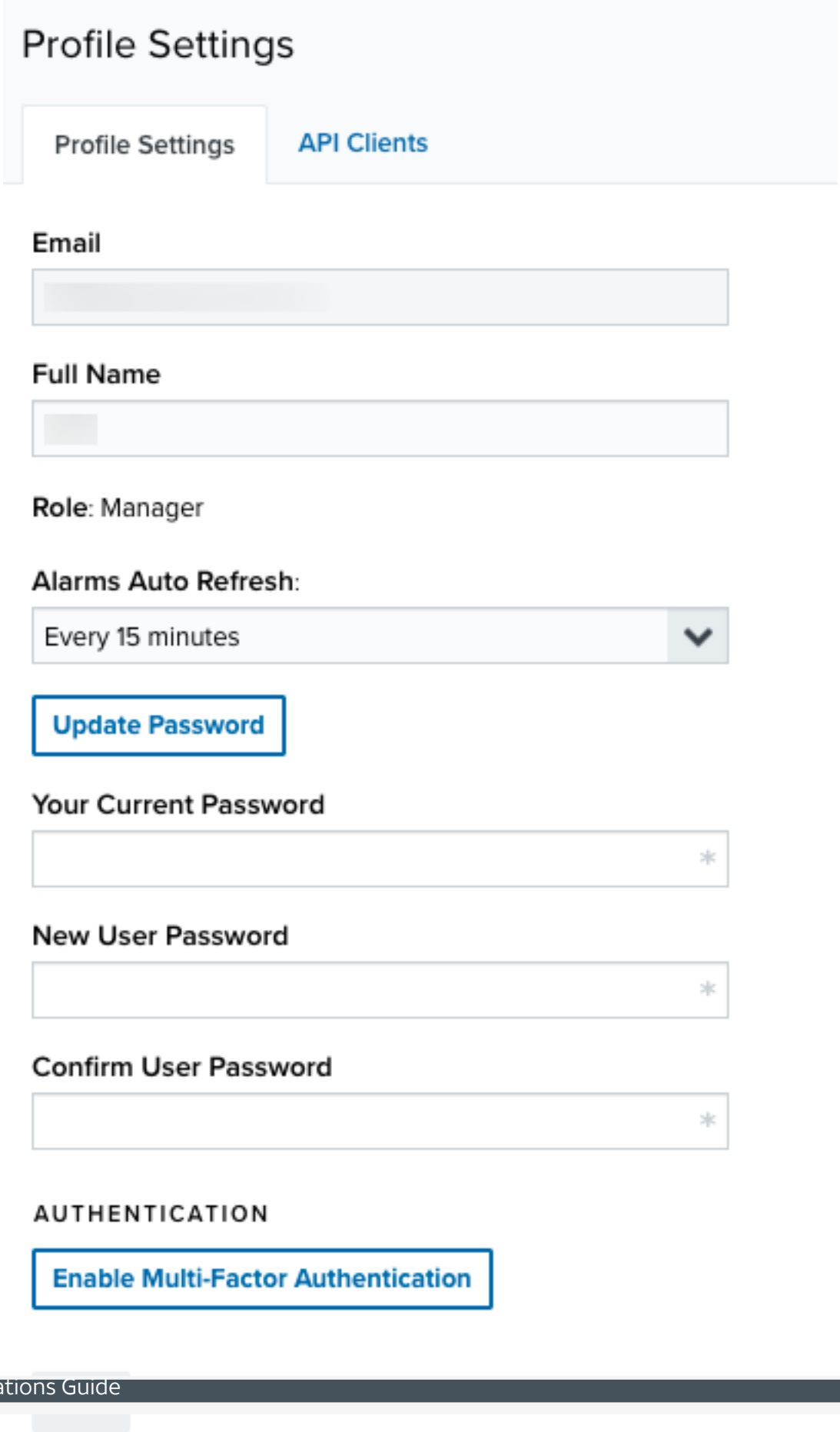
Change Your Full Name, and Password

USM Anywhere helps you meet the Payment Card Industry (PCI) standard by enforcing password complexity, password expiration, and forbidding password reuse. See the USM Anywhere Password Policy for details.

To set a new password

1. Open the Profile Settings page.
2. You have two options to choose from based on your role:
   - **General user**: At the bottom of the expanded pane of the USM Central web user interface (UI), hover over the profile settings options, and select **Profile**.
   - **Manager**: Go to **Settings > Users** and click the icon of your user.

   Both actions open the profile page.
3. Click **Update Password** to display the password fields.


Profile Settings
Profile Settings
API Clients
Email
Full Name
Role: Manager
Alarms Auto Refresh:
Every 15 minutes
Update Password
Your Current Password
New User Password
Confirm User Password
AUTHENTICATION
Enable Multi-Factor Authentication

> **Note:** The date of the last update displays in front of the Update Password button.

4. Enter your current password and the new password.
5. Click **Save**.

Enable MFA

If you want to protect your account, enable MFA for your user account. When this feature is activated, USM Central displays the multifactor authentication page for you to complete your MFA configuration. The displayed page provides a unique QR code that is used by the Authenticator app to retrieve a verification code. See Using Multifactor Authentication for more information about this security configuration.

> **Note:** LevelBlue recommends that users enable MFA for their account. MFA adds extra security because it requires multiple factors to authenticate a user, making it more difficult for an unauthorized person to gain access to the account.

To enable MFA

1. Open the Profile Settings page.
2. You have two options to choose from based on whether your role is as the general user or as the manager:
   - **General user**: At the bottom of the expanded pane of the USM Central web user interface (UI), hover over the profile settings options, and select **Profile**.
   - **Manager**: Go to **Settings > Users** and click the icon of your user.

   Both actions open the Profile Settings page.
3. Select **Enable Multi-Factor Authentication**.
4. Download the Google Authenticator app on your mobile device and scan the QR code.
5. Enter the verification code.
6. Click **Save**.

Select the Time for Auto-Refreshing the Alarms Page

If you want to configure the time that the alarms page refreshes its information, you can set an interval. These are the options:

- **Is Disabled**: The page works as usual and displays the icon for manually updating the page.
- **Every 15 min**: The page is reloaded every 15 minutes.
- **Every 30 min**: The page is reloaded every 30 minutes.
- **Every hour**: The page is reloaded every hour.
- **Every 2 hours**: The page is reloaded every 2 hours.

To log out of the system

1. At the bottom of the expanded pane of the USM Central web user interface (UI), hover over the profile settings options.
2. Select **Logout**.

API Clients

Role Availability	Read-Only	Analyst	Manager

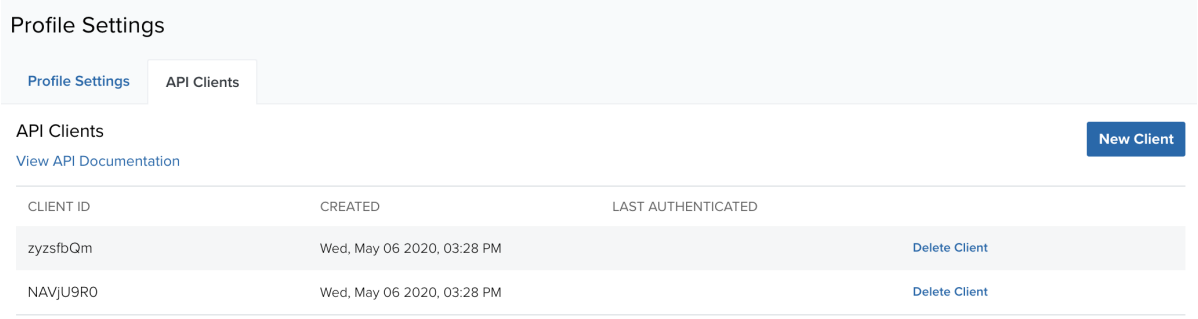
USM Central offers a Representational State Transfer (REST) API framework that enables you to customize elements of data in your environment. The APIs return JSON responses with errors that use HTTP response codes. To access the API, you need to create a client identification (ID) and secret code in the USM Central interface, and use that information to create a token. USM Central uses Open Authorization (OAuth) 2.0 to authenticate against the REST APIs.

Edition: The API is available in the Standard and Premium editions of USM Anywhere.

See the Affordable pricing to fit every budget page for more information about the features and support provided by each of the USM Anywhere editions.

To open the API Clients page

1. At the bottom of the expanded pane of the USM Central web user interface (UI), hover over the icon and select **Profile Settings > API Clients**.



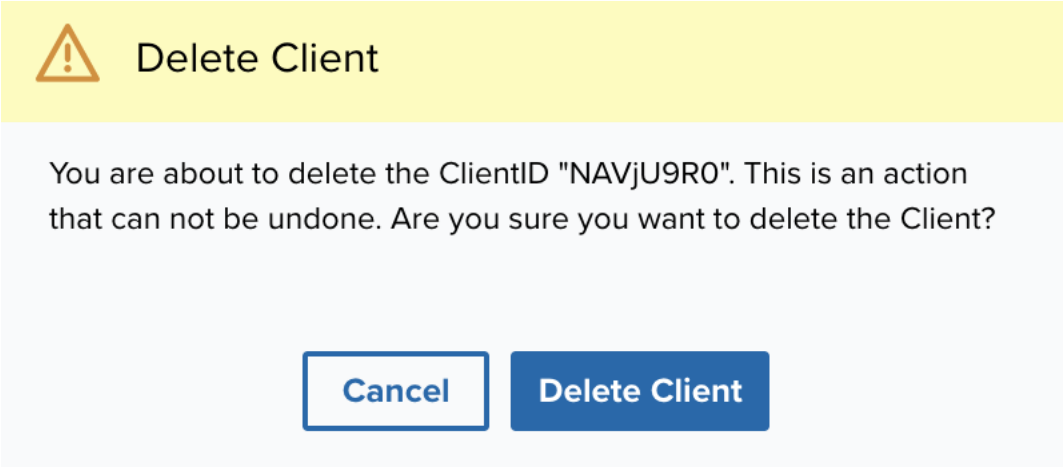
2. Click **New Client** to create a new client. See the LevelBlue APIs for more information.

To delete an API Client

1. At the bottom of the expanded pane of the USM Central web user interface (UI), hover over the icon and select **Profile Settings > API Clients**.

2. Locate the API client that you want to delete and click **Delete Client**.

   The delete client dialog box opens.



3. Click **Delete Client**.

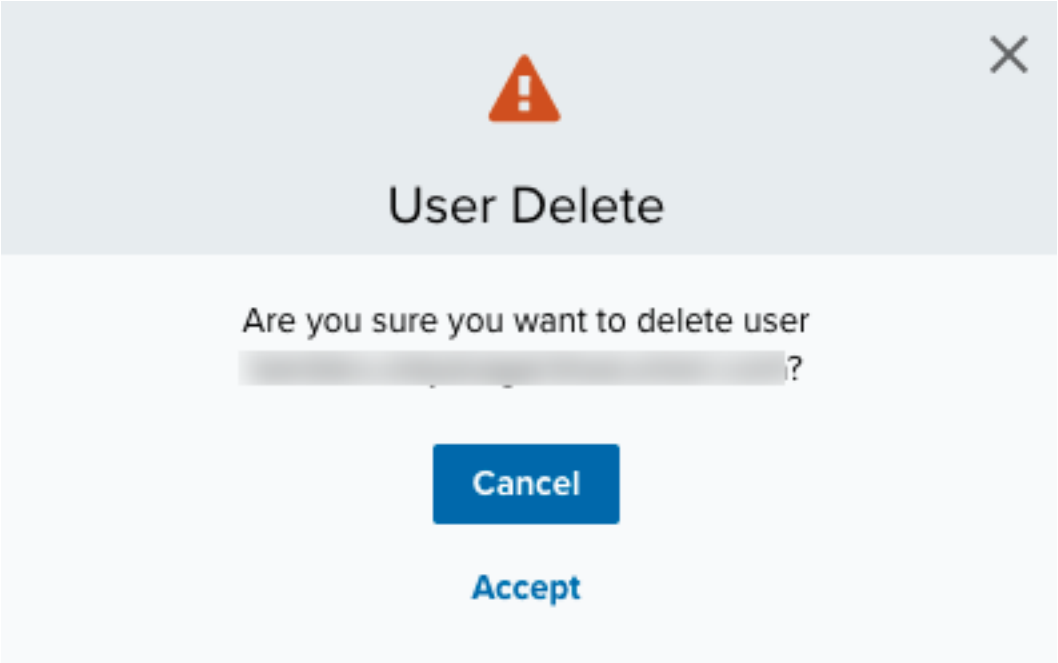
Deleting Users

Role Availability	Read-Only	Analyst	Manager

You can delete a user account in your USM Central whenever you need to.

To delete a user account

1. Go to **Settings > Users** to open the page that displays the list of user accounts in your USM Central environment.
2. In the row for the user account, click the icon.



3. Click **Accept** to confirm the process or click **Cancel** to exit.

Note: Only users having a role of Manager can delete users. See Role-Based Access Control (RBAC) in USM Central for more information.

Configuring Web UI Session Timeout

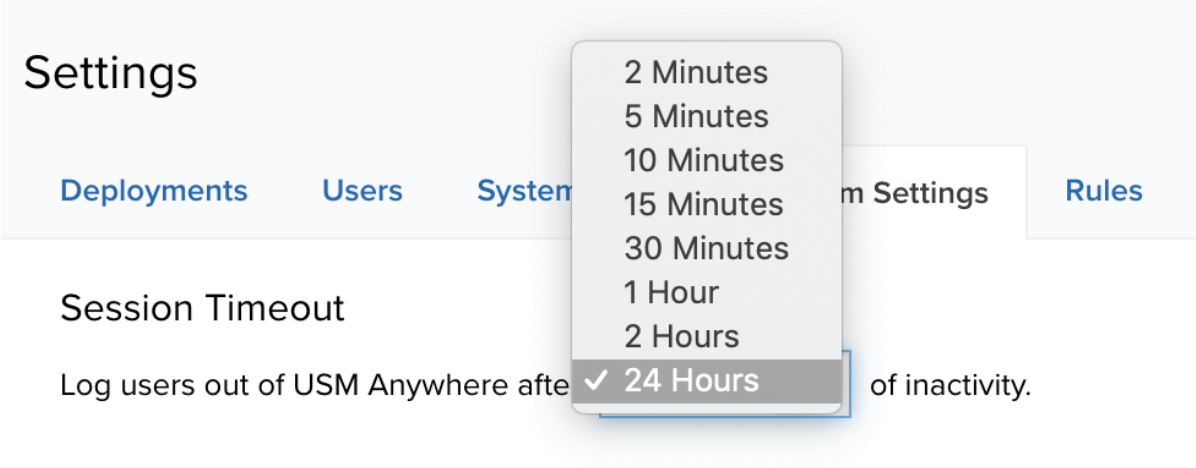
Role Availability	Read-Only	Analyst	Manager

USM Central supports up to 20 concurrent sessions per user, including both USM Central and USM Anywhere sessions. You can configure the length of time a session is inactive before the system automatically logs you out of USM Central. Concurrent API sessions are not limited.

Important: GovCloud users are limited to two concurrent sessions for each user, including USM Central, USM Anywhere, and API sessions.

To configure your web user interface (UI) session timeout

1. Go to **Settings > System Settings**.
2. Use the drop-down list to set the session timeout.



A notification bar displays to confirm the change.

Note: The new configuration applies after you log in.

Regulated Deployment Access

Role Availability	Read-Only	Analyst	Manager
	✗	✗	✓

With USM Central, users with a Manager role can assign Analyst and Read-Only users access to specified connected deployments. Giving an Analyst or Read-Only user access to a designated set of specific deployments will limit the view to only those deployments for which they have been assigned, and hide any details related to other deployments.

Existing Analyst and Read-Only users have access to all deployments by default, but a Manager can change access at any time by editing a user's account settings. When you create a new Read-Only or Analyst user, you can choose to assign select deployments or allow access to all deployments at that time. Deployments that are added at a later time will be

accessible to users with **All Deployments** access, while users with **Select Deployment** access will not be able to view the newly added deployment until access is specifically granted to their account.

Analysts with **Select Deployments** access can create labels in USM Central, but they are unable to edit or delete any USM Central labels. Read-Only and Analyst users can view the list of the deployments they have access to by clicking on the icon and selecting **Profile**. For more information on role permissions, see Role-Based Access Control (RBAC) in USM Central.

Note: Changes to deployment access that are made during the Analyst or Read-Only user's session will not be effective until they log out and log back into the system or are issued a new Using Multi-Factor Authentication after 24 hours.

Add or Edit Deployment Access

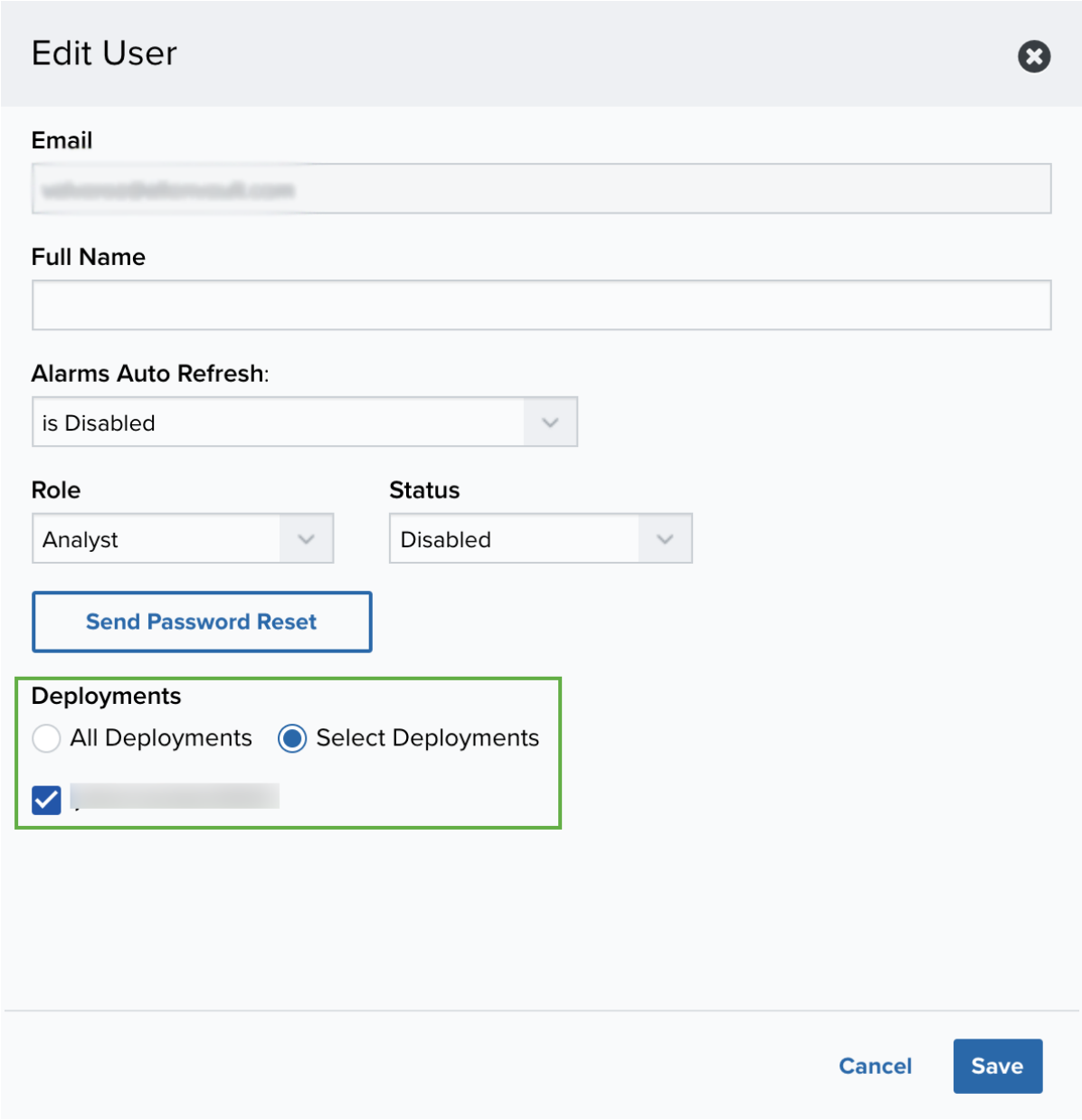
You can define a user's access to deployments in the user's account settings. Deployment access can also be defined for a user when you Creating Users.

To edit a user's deployment access

1. Go to **Settings > Users**.
2. Click the icon next to the user whose access you want to edit.
3. In the Deployment section of the Edit User window, click the button related to the settings you want to apply:
   - Click **All Deployments** if you want the user to have visibility over all connected deployments.
   - Click **Select Deployments** if you want to designate specific deployments.
4. If you click the **Select Deployments** button, the connected deployments display below.

Check the box for each of the deployments you want the user to have access to.

5. Click **Save**.



Using Multi-Factor Authentication

Role Availability	Read-Only	Analyst	Manager

To protect your USM Central account, enable multi-factor authentication (MFA). MFA adds extra security because it requires multiple factors to authenticate a user, making it more difficult for an unauthorized person to gain access to the account. In USM Central, MFA provides a layered defense of two independent credentials: what you know (your user account name and password) and what you have (security token on your personal device).

To use MFA in USM Central, you must have a mobile device that supports an Authenticator app. LevelBlue recommends the Google Authenticator app, which is available for iOS and Android devices. Google Authenticator implements two-step verification services using the Time-based One-Time Password (TOTP) algorithm and HMAC-based One-time Password Algorithm (HOTP) for authentication.

Configure MFA for Your Account

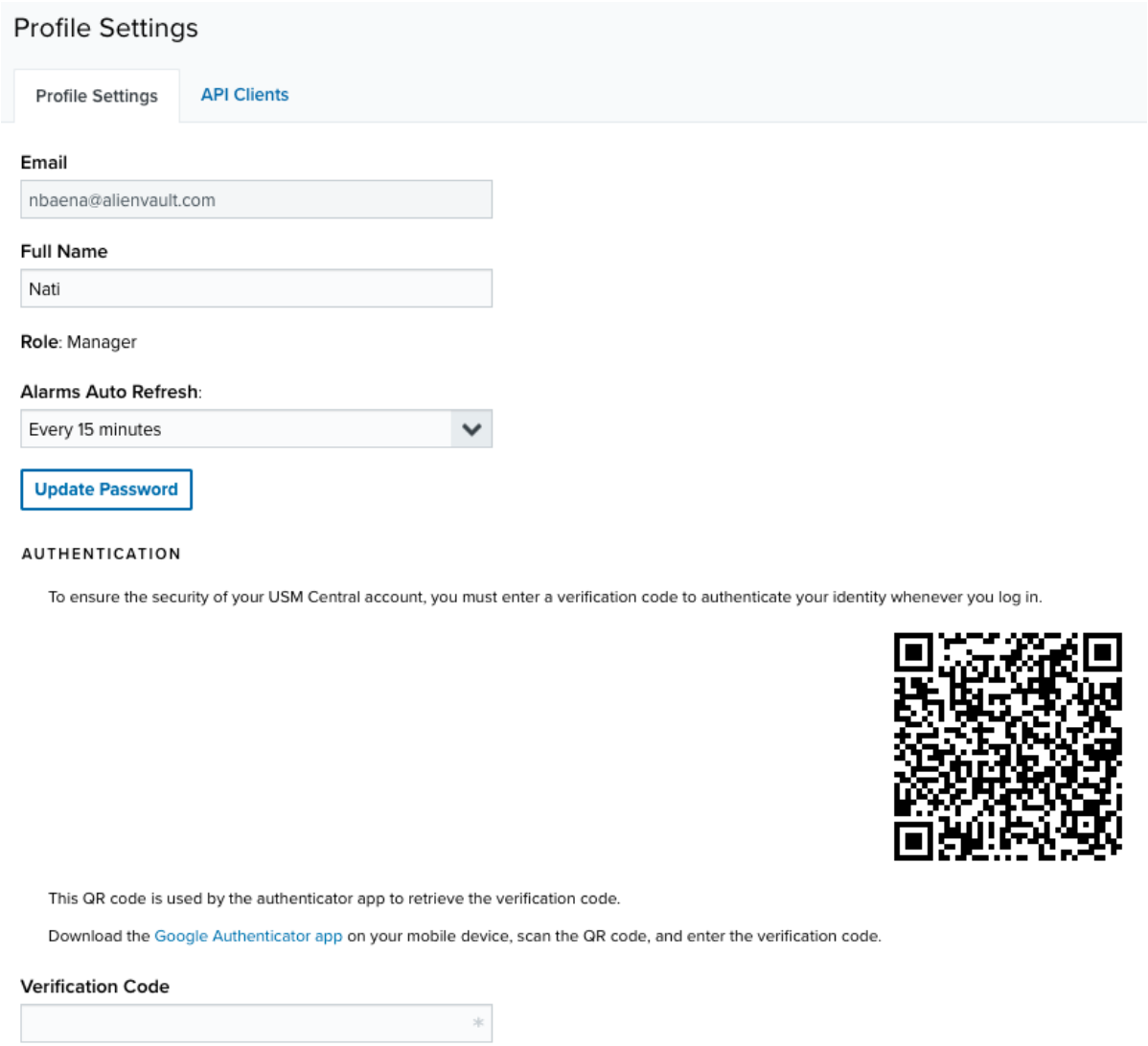
Before you set up MFA for your account, you must install the Authenticator app on your device.

To configure MFA for your account

1. At the bottom of the expanded pane of the USM Central web user interface (UI), hover over the icon and select **Profile**.

2. Click **Enable Multi-Factor Authentication**.

   The pane expands to provide a unique QR code that is used by the Authenticator app to retrieve a verification code. The code is emailed to you as well.



3. Open the Authenticator app on your device.
4. Scan the QR code using the Authenticator app.
5. Click **Save**.
6. Hover over the icon and select **Logout**.
7. Click **Login**.
8. On the login page, enter your user account and password, and click **Login**.
9. Enter the one-time passcode in the text box of USM Central, and then click **Login**.

Change Your Authentication Device

If you lose or change your mobile device or need to have your MFA reset, please contact LevelBlue Technical Support.

User Account Protections

Role Availability	Read-Only	Analyst	Manager

45-Day Inactivity Lock

Inactive users are locked out after 45 days of inactivity. Managers can unlock the users in the system if they're locked out, or users can contact LevelBlue support to have their account unlocked. Once an account has been unlocked, the user needs to log back in the same day for the system to save their unlocked status.

To unlock an account

1. Go to **Settings > Users**.
2. Click the button.

Note: This complies with the Payment Card Industry (PCI) Standard 8.5.5.

Brute Force IP Block

After six failed login attempts on an account, the system automatically locks the account. Once a user account is locked out, it remains locked for a minimum of 30 minutes or until a system administrator resets the account.

Note: This complies with the PCI Standard 8.5.13.