IBM Security QRadar

# *Master Console*

*Version 0.9.1*

**Note**

Before using this information and the product that it supports, read the information in “Notices” on page 15.

# Contents

# Introduction to Master Console

IBM® Security QRadar® administrators use Master Console to view health and other information about deployments and hosts.

## Intended audience

This guide is intended for all QRadar users who are responsible for investigating and managing network security. To use this information, you must have QRadar access and a knowledge of your corporate network and networking technologies.

## Technical documentation

To find IBM Security QRadar product documentation on the web, including all translated documentation, access the IBM Knowledge Center (http://www.ibm.com/support/knowledgecenter/SS42VS/welcome).

For information about how to access more technical documentation in the QRadar products library, see Accessing IBM Security Documentation Technical Note (www.ibm.com/support/docview.wss?rs=0&uid=swg21614644).

## Contacting customer support

For information about contacting customer support, see the Support and Download Technical Note (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861).

## Statement of good security practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

**Please Note:**

Use of this Program may implicate various laws or regulations, including those related to privacy, data protection, employment, and electronic communications and storage. IBM Security QRadar may be used only for lawful purposes and in a lawful manner. Customer agrees to use this Program pursuant to, and assumes all responsibility for complying with, applicable laws, regulations and policies. Licensee represents that it will obtain or has obtained any consents, permissions, or licenses required to enable its lawful use of IBM Security QRadar.

# Master Console

Use Master Console to monitor IBM Security QRadar deployments.

Master Console is useful in a Managed Security Service Providers (MSSP) environment. By using the dashboard, you can simultaneously monitor multiple deployments.

The visual representation of operational data, such as CPU usage, network and disk activity, memory usage, and event and flow rates, makes it easy to monitor the health of your deployments.

The centralized offense management view shows offenses from all deployments by order of magnitude. You drill down on the information and then log in to a specific QRadar deployment to get more information about the offense.

## What's new for administrators in Master Console

Learn about the new features in each Master Console release.

### What's new in Master Console V0.9.1

Master Console V0.9.1 includes updates to fix the Deployment window refresh rate, and to ensure that Master Console works with newer versions of IBM Security QRadar.

### What's new in Master Console V0.9.0

Master Console V0.9.0 introduced searching and filtering offenses and removed support for Microsoft Internet Explorer 10.

#### Search and filter offenses

Using the new search bar, you can build text and field-based queries to filter the offenses that appear on the consolidated offense list. ⓘ Learn more...

#### Supported browser update

Browser support for Microsoft Internet Explorer 10 was dropped in this release. ⓘ Learn more...

### What's new in Master Console V0.8.1

Master Console V0.8.1 introduced local user management and support for your Active Directory and LDAP security providers.

#### User management

You can grant and control access for local users to the Master Console. After you upgrade to Master Console V0.8.1 or later, all existing QRadar users are migrated to Master Console as local users. You manage users, including adding users and changing passwords, in Master Console. ⓘ Learn more....

### Security provider integration

You can use your existing Active Directory or LDAP security infrastructure to configure user authentication. Learn more...

# Getting started with Master Console

Install Master Console to monitor the health and system of all QRadar hosts in your IBM Security QRadar deployment.

## Supported environments

Before you install and use Master Console, verify that you have the supported hardware and software in your environment.

### Hardware requirements

Master Console runs on the QRadar 3105 appliance.

Before you install Master Console, confirm that the virtual or physical appliance meets the following hardware specifications:

*Table 1. QRadar 3105 appliance overview*

| Description | Value |
|---|---|
| Processors | 8 |
| Interfaces | Two 10/100/1000 Base-T network monitoring interfaces<br>One 10/100/1000 Base-T QRadar management interface<br>One 10/100 Base-T Integrated Management Module interface<br>Two 10 Gbps SFP+ ports |
| Memory | 64 GB 8x 8 GB 1600 MHz RDIMM |
| Storage | 9 x 3.5 inch 1 TB 7.2 K rpm NL SAS, 9 TB total, 6.2 TB usable (Raid 5) |
| Power supply | Dual redundant 750W AC power supply |
| Dimensions | 29.5 inches deep x 17.7 inches wide x 2.4 inches high |

### Software requirements

To host Master Console, you must install IBM Security QRadar with the 8500 activation key (3L0C3S-2M0F3Q-6B1N0W-5N737F). You do not require a separate license key.

You can use Master Console to monitor a QRadar Log Manager deployment, but the centralized offense management view is empty. The centralized offense management view shows offenses only for systems that monitor offenses, such as QRadar SIEM.

The QRadar version that is required to host Master Console might be different than the QRadar versions that Master Console can monitor. Before you install Master Console, review the software requirements in the following table.

*Table 2. Software requirements for Master Console*

| Master Console version | Install on | Monitors | Supported browsers |
|---|---|---|---|
| Master Console v0.9.1[*] | QRadar V7.2.6 or later | QRadar V7.2.6 or later | Microsoft Internet Explorer 11<br>Mozilla Firefox 38 Extended Support Release<br>Google Chrome (most recent version) |
| Master Console v0.9.0 | QRadar V7.2.6 | QRadar V7.2.6 or later | Microsoft Internet Explorer 11<br>Mozilla Firefox 38 Extended Support Release<br>Google Chrome (most recent version) |
| Master Console v0.8.1 | QRadar V7.2.5 or V7.2.6 | QRadar V7.2.5 or V7.2.6 | Microsoft Internet Explorer 11<br>Microsoft Internet Explorer 10<br>Mozilla Firefox 38 Extended Support Release<br>Google Chrome (most recent version) |
| [*] Product support is limited to the last version of Master Console that was released. | | | |

For more information about installing QRadar, see the *IBM Security QRadar Installation Guide*.

# Installing Master Console

Master Console is automatically installed when IBM Security QRadar V7.2.5 or later is installed with the 8500 activation key (3L0C3S-2M0F3Q-6B1N0W-5N737F). It does not require a separate license key. For more information about installing QRadar, see the *IBM Security QRadar Installation Guide*.

You can download the most recent Master Console features and enhancements from IBM Fix Central.

## Before you begin

Ensure that the appliance that you are installing on meets the minimum required hardware specifications. For more information, see “Supported environments” on page 2.

You must have a file copying software program, such as WinSCP, to copy the Master Console fix pack file from your local system to the QRadar appliance.

### About this task

The first time that you update to Master Console V0.8.1 or later, the update process imports users from the QRadar console. The import overwrites the passwords for all existing Master Console users, including the administrator, and sets them to the same password that is set on the QRadar console. The import process happens only once. Subsequent updates to Master Console do not import users or overwrite passwords.

### Procedure

1. Download the Master Console fix pack from Fix Central (http://www.ibm.com/support/fixcentral).
2. Use a software program, such as WinSCP, to copy the Master Console fix pack to the QRadar host where you installed Master Console.
3. Use SSH to log in as the root user to the QRadar host where you copied the Master Console software fix.
4. Stop the Tomcat service by typing the following command:

   ```
   service tomcat stop
   ```
5. In the console window for the QRadar appliance, install Master Console by typing the following command:

   ```
    rpm -Uvh masterconsole-<version#>.rpm
   ```
6. Restart the Tomcat service by typing the following command:

   ```
   service tomcat start
   ```

### Results

Master Console is installed and the services on the QRadar appliance are restarted.

## Opening Master Console

When Master Console is installed, use the IP address of the QRadar console to open Master Console.

### Before you begin

Ensure that QRadar is installed with the 8500 activation key (3L0C3S-2M0F3Q-6B1N0W-5N737F).

### About this task

The first time that you update to Master Console V0.8.1 or later, the update process imports users from the QRadar console. The import overwrites the passwords for all existing Master Console users, including the administrator, and sets them to the same password that is set on the QRadar console. The import process happens only once. Subsequent updates to Master Console do not import users or overwrite passwords.

### Procedure

1. Open a web browser and type the following URL:

   ```
   https://IP_address
   ```

   where *IP_address* is the IP address of the QRadar host where you installed Master Console.
2. Log in to Master Console.

If you are logging in to Master Console for the first time, use the admin account and the root password on the system.

### What to do next

To add the QRadar deployments that you want to monitor, see "Adding deployments to Master Console."

## Creating an authorization token for Master Console

You must create an authorization token so that Master Console can connect to your IBM Security QRadar deployments.

### Procedure

1. On the **Admin** tab, under **System Configuration**, click **Authorized Services**.
2. Click **Add Authorized Service** and configure the parameters.
   a. In the **Service Name** field, type a name for the service. The name can be up to 255 characters in length.
   b. In the **User Role** menu, select **Admin**.

      The user roles that are assigned to an authorized service determine the functions that the service can access in QRadar. The authorization token for Master Console must have the **Admin** user role.
   c. In the **Security Profile** menu, select **Admin**.

      The security profile determines the networks and log sources that this service can access in QRadar. The authorization token for Master Console must have the **Admin** security profile.
   d. In the **Expiry Date** field, select a date that you want the token to expire or click the **No Expiry** check box.
3. Click **Create Service** and record the token value.

## Adding deployments to Master Console

A Master Console administrator must add the IBM Security QRadar deployments that you want to monitor.

### Before you begin

- You must have an authorization token. For more information, see "Creating an authorization token for Master Console."
- If your organization requires secure SSL, ensure that the untrusted SSL certificate is replaced with either a self-signed or trusted certificate on all QRadar deployments that you want to monitor in Master Console.
- Only QRadar administrators can add, edit, or remove QRadar deployments to Master Console.

### Procedure

1. To add a deployment, click the add (+) icon in the upper right corner of the screen.
2. Type a name for the deployment.
3. Type the console IP address or host name.
4. Type the authorization token.
5. Click **Add Deployment**.

6. If you are adding a deployment with insecure SSL, and your organization does not require secure SSL, select the **Ignore insecure SSL** check box, and click **Submit**.

## Deployment monitoring

Master Console shows a graphical representation, referred to as a *deployment card*, of the health and operational data for each IBM Security QRadar deployment that is connected to Master Console.

You can view the deployment cards on the Deployments by Severity page. To help you quickly determine which deployments require attention, the deployments cards are sorted into three groups: **Critical**, **Warning**, and **Healthy**.

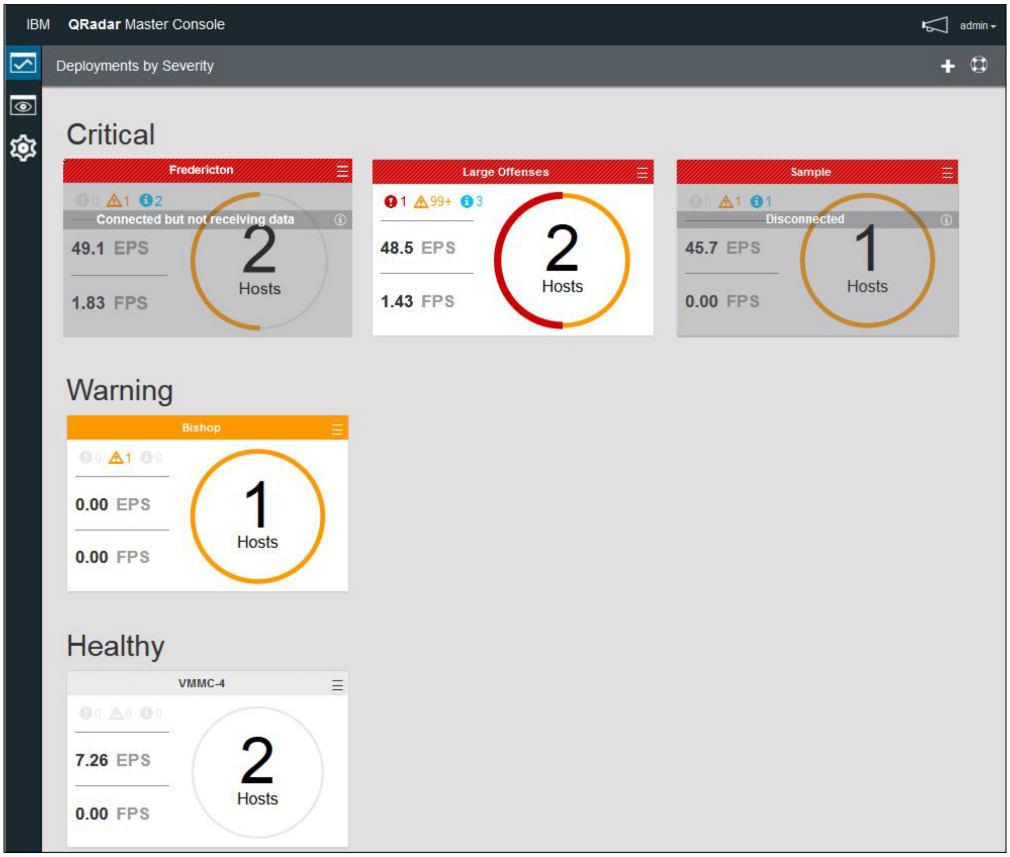


*Figure 1. Deployment cards in Master Console*

Each deployment card shows the following information:

- The number of managed hosts in the deployment.
- The status of the deployment, as represented by the colors around the circle. For example, if your deployment has two managed hosts, and 1 has a critical status, half of the circle around the number 2 is red.
- The number of critical, warning, and informational system notifications within the last 15 minutes.
- The event and flow rates, which are measured as an average over the last 15 minutes.

When Master Console cannot connect to a deployment, the deployment card shows **Disconnected**. This status might mean that the deployment is powered off. When a deployment appears as **Connected but not receiving data**, the authorization token might be revoked or expired.

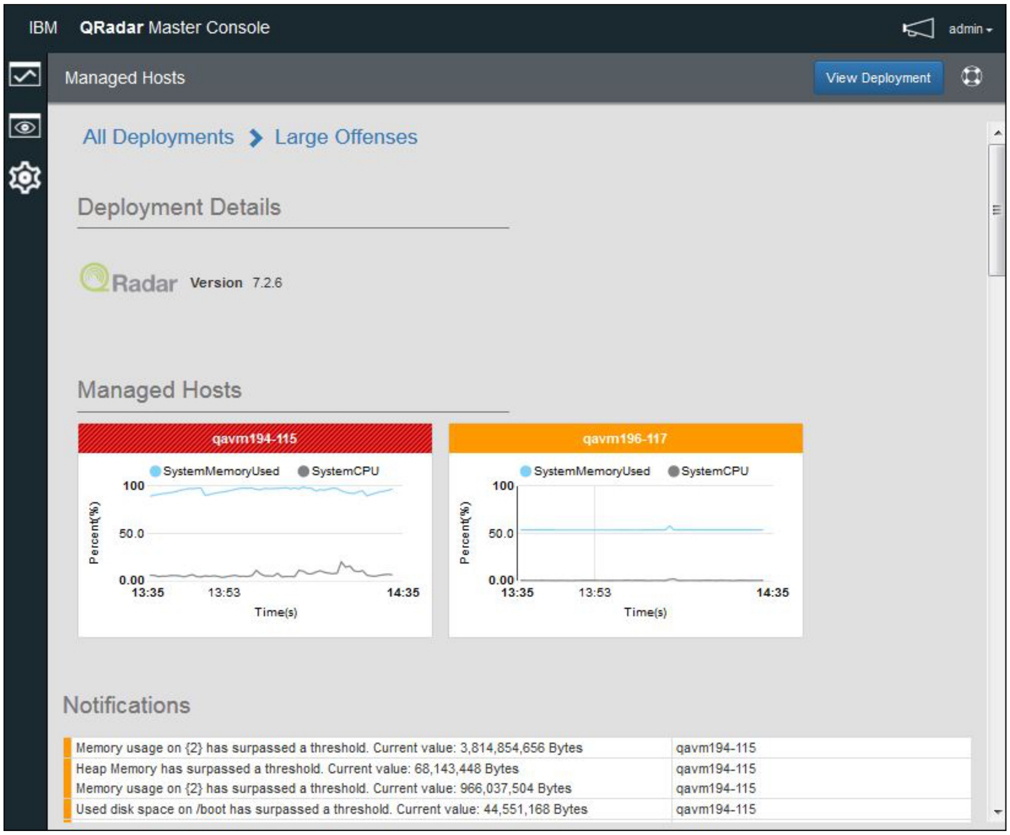
You can do the following actions on the deployment card:

- Click the deployment card to open the **Managed Hosts** view.
- Click the 'hamburger' menu ☰ icon to edit the deployment details or to disconnect the deployment from Master Console.
- When a deployment is **Disconnected** or **Connected but not receiving data**, click the information icon on the deployment card to see when data was last received.

## Monitoring managed hosts

Use the Managed Hosts page to see system notifications and the system memory and CPU usage statistics for all the managed hosts that are connected to a single deployment.

To help you quickly determine which managed hosts require attention, the top portion of the managed host card is color coded: Red indicates **Critical** status, yellow indicates **Warning** status, and grey indicates **Healthy** status.



| | |
|---|---|
| Memory usage on {2} has surpassed a threshold. Current value: 3,814,854,656 Bytes | qavm194-115 |
| Heap Memory has surpassed a threshold. Current value: 68,143,448 Bytes | qavm194-115 |
| Memory usage on {2} has surpassed a threshold. Current value: 966,037,504 Bytes | qavm194-115 |
| Used disk space on /boot has surpassed a threshold. Current value: 44,551,168 Bytes | qavm194-115 |

*Figure 2. Managed Hosts page in Master Console*

### Procedure

1. To view the Managed Hosts page, click the deployment card on the Deployments by Severity page.
2. On the Managed Hosts page, you can do the following actions:
   a. Click **View Deployment** to log in to a QRadar deployment.
   b. Hover the mouse over the managed host graphs to view more information about the graph metrics.
   c. To hide a metric from the managed host graph, click the colored icon for the metric. For example, to hide the **SystemCPU** metric from the graph, click the grey circle beside **System CPU**.
   d. To view operational data about the host, such as CPU and memory usage, network and disk reads and writes, and the event and flow rates, click the managed host card.

## Monitoring offenses

Use Master Console to monitor offenses from multiple IBM Security QRadar deployments. Offenses from all deployments are displayed in a single list with the most important offenses at the top.

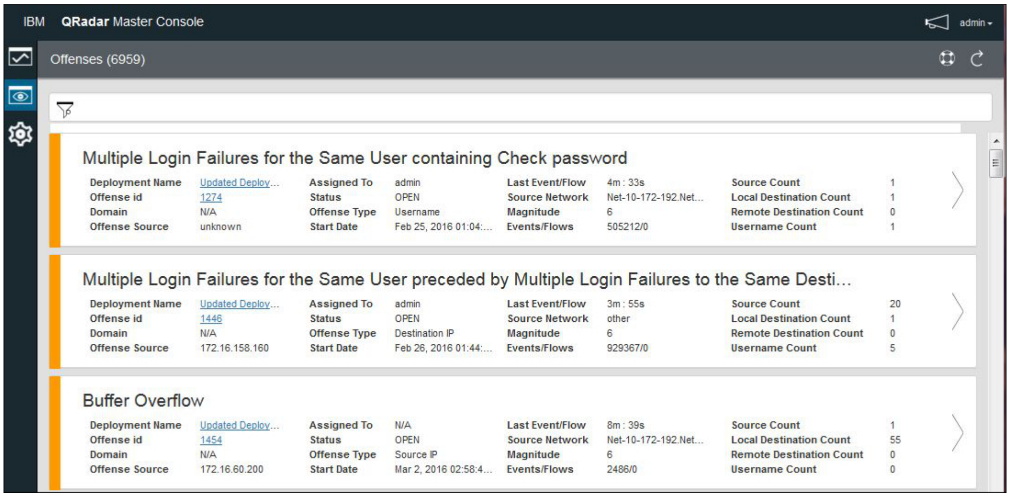
### About this task

The offense cards are sorted in the following order: magnitude, deployment, and last updated time.

*Magnitude* is an indicator of the relative importance of the offense. It is calculated based on the relevance, severity, and credibility values.

- *Relevance* determines the impact of the offense on your network. For example, if a port is open, the relevance is high.
- *Credibility* indicates the integrity of the offense as determined by the credibility rating that is configured in the log source. Credibility increases as multiple sources report the same event.
- *Severity* indicates the threat that a source poses in relation to how prepared the destination is for the attack.

Magnitude has a numeric value that determines the color of the offense card. Hover the mouse over the colored bar on the offense card to see the magnitude number.



Multiple Login Failures for the Same User containing Check password

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Deployment Name | Updated Deploy... | Assigned To | admin | Last Event/Flow | 4m : 33s | Source Count | 1 |
| Offense id | 1274 | Status | OPEN | Source Network | Net-10-172-192.Net... | Local Destination Count | 1 |
| Domain | N/A | Offense Type | Username | Magnitude | 6 | Remote Destination Count | 0 |
| Offense Source | unknown | Start Date | Feb 25, 2016 01:04:... | Events/Flows | 505212/0 | Username Count | 1 |

Multiple Login Failures for the Same User preceded by Multiple Login Failures to the Same Desti...

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Deployment Name | Updated Deploy... | Assigned To | admin | Last Event/Flow | 3m : 55s | Source Count | 20 |
| Offense id | 1446 | Status | OPEN | Source Network | other | Local Destination Count | 1 |
| Domain | N/A | Offense Type | Destination IP | Magnitude | 6 | Remote Destination Count | 0 |
| Offense Source | 172.16.158.160 | Start Date | Feb 26, 2016 01:44:... | Events/Flows | 929367/0 | Username Count | 5 |

Buffer Overflow

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Deployment Name | Updated Deploy... | Assigned To | N/A | Last Event/Flow | 8m : 39s | Source Count | 1 |
| Offense id | 1454 | Status | OPEN | Source Network | Net-10-172-192.Net... | Local Destination Count | 55 |
| Domain | N/A | Offense Type | Source IP | Magnitude | 6 | Remote Destination Count | 0 |
| Offense Source | 172.16.60.200 | Start Date | Mar 2, 2016 02:58:4... | Events/Flows | 2486/0 | Username Count | 0 |

*Figure 3. Deployment cards in Master Console*

The offense card shows the following information:

*Table 3. Offense card information*

| Parameter | Description |
|---|---|
| **Offense ID** | A link to the offense summary. |
| **Offense Source** | The offense source information depends on the type of offense.<br>For example, if the **Offense Type** is Source IP, then the **Offense Source** field shows the IP address for the source of the event that created the offense. If the **Offense Type** is Destination IP, then the **Offense Source** field shows the destination IP address of the event. |
| **Assigned To** | If no user is assigned to investigate the offense, you can assign offenses to users in QRadar. For more information about assigning offenses to QRadar, see the *IBM Security QRadar Users Guide*. |
| **Status** | By default, the filter displays only the open offenses. |
| **Offense Type** | Determined by the rule that created the offense.<br>For example, if the offense type is **Log source event**, the rule that generated the offense correlates events that are based on the device that detected the event. |
| **Start Date** | Specifies the date and time of the first event or flow that is associated with the offense. |
| **Last Event/Flow** | Specifies the elapsed time since the last event or flow was observed for the offense, category, source IP address, or destination IP address. |
| **Source Network** | Specifies the network of the device that attempted to breach the security of a component on your network. |
| **Event/Flow** | Specifies the number of events or flows that are associated with the source IP address, destination IP address, event name, user name, MAC address, log source, host name, port, log source, ASN address, IPv6 address, rule, ASN, Application, network or category. |
| **Source Count** | Specifies the number of source IP addresses that are associated with offenses in the category. If a source IP address is associated with offenses in five different low-level categories, the source IP address is counted only once. |

### Procedure

1. Open Master Console and click the offenses icon.
2. Click the arrow link on the offense card to log in to the deployment and open the offense summary.
3. To view offenses that are hidden or closed, click the filter icon and select the check boxes for the offenses that you want to view.

   The number of offenses that match the applied filter is displayed in the page header.
4. Click the refresh icon to update the listed offenses.

**Related tasks**:

"Opening Master Console" on page 4
When Master Console is installed, use the IP address of the QRadar console to open Master Console.

## Filtering the list of offenses

Create a search query to filter the offense cards that appear in the consolidated offense list. For example, you can filter the offense list to show only those offenses that are assigned to one individual or you can filter to show only the offenses for a single deployment.

### About this task

You use the full-text search field on the **Offenses** view to quickly find offenses that are close or exact matches and display them in ranked order. You can create a query to find a single word, part of a word, or multiple words in exact order or in any order. You can search for data across all the data fields on the offense card, or you can narrow the search by specifying the identifier that you want to search on.

The full text search capability is based on the Apache Lucene search engine. Searches are not case-sensitive. To search by using a single character wildcard, use the ? symbol. To search by using multiple character wildcards, use the * symbol.

You can narrow the search by specifying which field on the offense card that you want to search on. The following table shows the field identifiers for the fields on the offense card:

*Table 4. Field identifiers for searching data on the Offense card*

| Offense card description | Field Identifier |
|---|---|
| **Offense Description** | description |
| **Deployment name** | deployment_name |
| **Offense ID** | offense_id |
| **Domain** | domain_id |
| **Offense source** | offense_source |
| **Assigned to** | assigned_to |
| **Status** | status |

*Table 4. Field identifiers for searching data on the Offense card (continued)*

| Offense card description | Field Identifier |
|---|---|
| **Offense type** | offense_type<br>You cannot use wildcards to search on `offense_type`. You must specify exact match text in the query. |
| **Start date** | start_time |
| **Last Event/Flow** | last_updated_time |
| **Source Network** | source_network |
| **Magnitude** | magnitude |
| **Events/Flows** | event_count<br>flow_count |
| **Source Count** | source_count |
| **Local Destination Count** | local_destination_count |
| **Remote Destination Count** | remote_destination_count |
| **Username Count** | username_count |

## Procedure

1. Click the offenses 👁 icon.
2. In the search field, type the search query for the text that you want to search for.
   - To search for any data that appears on the offense card, type the text in the search box.
   - To search for data in a specific field, type the field identifier followed by a colon and then the term you are looking for.
   - To escape special characters, use \ before these characters in your search query:

     ```
     + - && || ! ( ) { } [ ] ^ " ~ * ? : \
     ```

   **Search query examples:**

   The following table shows examples of queries you can use to search data on the offense card:

*Table 5. Master Console search expressions*

| Description | Search query |
|---|---|
| Searches for offenses that have `text` or `test` in any field. | `te?t` |
| Searches for offenses that have `test`, `tests`, or `tester`. | `test*` |
| Searches for offenses that have `password` in any field. | `*password*` |
| Searches for offenses that have a magnitude rating of 2, 3 or 4. | `magnitude:[2 to 4]` |
| Searches for offenses that have a magnitude rating of either 3 or 5. | `magnitude:(3 OR 5)` |

*Table 5. Master Console search expressions (continued)*

| Description | Search query |
|---|---|
| Searches for offenses where the Offense Type is equal to `Event Name`. | `offense_type: "Event Name"` |
| Searches for offenses that were updated within the last 10 days from now. | `last_update_time:[NOW-10DAYS to NOW]` |
| Searches for offenses from the `Bishop` deployment that have a magnitude of 3. | `deployment_name:Bishop AND magnitude:3` |

3. To view offenses that are hidden or closed, click the filter icon and select to check boxes for the offenses that you want to see.

   The number of offenses that match the applied filter is displayed in the page header.

# User management

Master Console users are administered directly in Master Console.

The first time that you update to Master Console V0.8.1 or later, the update imports users from the QRadar console. The import process happens only once. Subsequent updates to Master Console do not import users. After the initial import, all user accounts are managed directly from Master Console.

## Adding a local user

After Master Console is installed and updated to the most recent version, administrators add new users directly in Master Console.

### Procedure

1. Click the settings icon.
2. Click **User Management**.
3. In the upper right corner of the User Management window, click the add (+) icon to open the Create user window.
4. Enter the information for the new user.
5. If the new user is an administrator, click the **Security Admin** check box.
6. Click **Create User**.

## Editing user settings

Change the settings, such as user passwords, of a local user in Master Console.

### About this task

Local user passwords that are changed in IBM Security QRadar are not automatically applied in Master Console. You must edit the user setting and change the password in Master Console.

You cannot change LDAP and Active Directory passwords in Master Console.

### Procedure

1. Click the settings ⚙ icon.
2. Click **User Management**.
3. On the card for the user that you want to edit, click the 'hamburger' menu ☰ icon.
4. Select **Edit User**.
5. Modify the user information on the Edit User window.
6. Click **Edit User** to save your changes.

## Removing a local user

If the user no longer requires access, remove the local user from Master Console.

### Procedure

1. Click the settings ⚙ icon.
2. Click **User Management** to view the cards for all local users.
3. On the card for the user that you want to edit, click the 'hamburger' menu ☰ icon.
4. Select **Remove User**.
5. In the confirmation window, click **Remove User**.

## Configuring Active Directory and LDAP authentication in Master Console

To configure a Microsoft Active Directory or an LDAP authentication provider in Master Console, you must manually edit the `/opt/qradar/masterconsole/conf/shiro.ini` file.

### Before you begin

Back up the `/opt/qradar/masterconsole/conf/shiro.ini` file.

Review the configuration on your authentication server. Depending on the type of authentication provider that you configure, you might need to provide the following parameter values:

*Table 6. Authentication parameter descriptions*

| **Parameter** | **Description** |
|---|---|
| `searchBase` | The root of the Active Directory or LDAP directory where users are organized. |
| `searchFilter` | Used to find the context of the Active Directory or LDAP user. Account is a default object class that is used by most servers, but this entry varies based on the specific Active Directory or LDAP server configuration. |
| `groupAttribute` | Identifies the user groups that the Active Directory or LDAP user belongs to. |
| `groupRolesMap` | A map of Active Directory or LDAP groups to Apache Shiro roles. |

*Table 6. Authentication parameter descriptions (continued)*

| Parameter | Description |
|---|---|
| `userDnTemplate` | The DN template that retrieves a user from the Active Directory or LDAP server. |
| `contextFactory.url` | The Active Directory or LDAP server IP address and port number. |
| `principalSuffix` | Specify a principal suffix to simplify the logon information that users must specify.<br>For example, instead of `username@this.is.my.long.domain.name.in.canada.com`, you can create a user principal suffix that is called `canada`, and users can type `username@canada`. |

## Procedure

1. Open the `/opt/qradar/masterconsole/conf/shiro.ini` file.
2. To configure Microsoft Active Directory, do these steps:
   a. Find the following section and replace the example values with the values for your authentication environment:

```
# -----------------------------------------------------------------------------
# following section is for configuring ActiveDirectory realm. Replace example
# values before add to securityManager.realm
# -----------------------------------------------------------------------------
adRealm = org.apache.shiro.realm.activedirectory.ActiveDirectoryRealm
adRealm.url = ldap://{ad_server}:389
adRealm.groupRolesMap = "CN=the_users,CN=Users,DC=department,DC=company,DC=com":"admin"
adRealm.searchBase = "DC=department,DC=company,DC=com"
adRealm.systemUsername= user_name
adRealm.systemPassword= password
adRealm.principalSuffix= @company.com
```

   b. Add `$adRealm` to the `securityManager.realms` entry:

```
securityManager.realms = $localRealm, $adRealm
```

3. To configure LDAP, do these steps:
   a. Find the following section and replace the example values with the values for your authentication environment:

```
#-----------------------------------------------------------------------------
# following section is for configuring OpenLdap realm. Replace example
# values before add to securityManager.realm
#-----------------------------------------------------------------------------
ldapRealm = com.ibm.si.mc.security.shiro.realm.LdapRealm
ldapRealm.searchBase = "dc=company,dc=com"
ldapRealm.searchFilter = (&(objectClass=account)(uid={0}))
ldapRealm.groupAttribute = ou
ldapRealm.groupRolesMap = "Manager":"admin"
ldapRealm.userDnTemplate = uid={0},dc=company,dc=com
ldapRealm.contextFactory.url = ldap://{ldap_server}:389
```

   b. Add `$ldapRealm` to the `securityManager.realms` entry:

```
securityManager.realms = $localRealm, $ldapRealm
```

4. Save the `/opt/qradar/masterconsole/configurations/shiro.ini` file.
5. Restart the tomcat server by using the following command:

```
service tomcat restart
```

# Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions..

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

## Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

## Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

### Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

### Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

### Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

### Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

## IBM Online Privacy Statement

IBM Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

Depending upon the configurations deployed, this Software Offering may use session cookies that collect each user's session id for purposes of session management and authentication. These cookies can be disabled, but disabling them will also eliminate the functionality they enable.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, See IBM's Privacy Policy at http://www.ibm.com/privacy and IBM's Online Privacy Statement at http://www.ibm.com/privacy/details the section entitled "Cookies, Web Beacons and Other Technologies" and the "IBM Software Products and Software-as-a-Service Privacy Statement" at http://www.ibm.com/software/info/product-privacy.

## Privacy policy considerations

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering's use of cookies is set forth below.

Depending upon the configurations deployed, this Software Offering may use session cookies that collect each user's session id for purposes of session management and authentication. These cookies can be disabled, but disabling them will also eliminate the functionality they enable.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, See IBM's Privacy Policy at http://www.ibm.com/privacy and IBM's Online Privacy Statement at http://www.ibm.com/privacy/details the section entitled "Cookies, Web Beacons and Other Technologies" and the "IBM Software Products and Software-as-a-Service Privacy Statement" at http://www.ibm.com/software/info/product-privacy.

Printed in USA