

Back up and restore a sensor or console


Published: 2024-04-02

After you have configured your ExtraHop console and sensor with customizations such as bundles, triggers, and dashboards or administrative changes such as adding new users, ExtraHop recommends that you periodically back up your settings to make it easier to recover from a system failure.

Daily backups are automatically saved to the local datastore, however, we recommend that you manually create a system backup prior to upgrading firmware or before making a major change in your environment (changing the data feed to the sensor, for example). Then, download the backup file and save it to a secure location.

Back up a Sensor or ECA VM

Create a system backup and store the backup file to a secure location.

 **Important:** System backups contain sensitive information, including SSL keys. When you create a system backup, make sure you store the backup file to a secure location.

The following customizations and resources are saved when you create a backup.

- User customizations such as bundles, triggers, and dashboards.
- Configurations made from Administration settings, such as locally-created users and remote imported user groups, running configuration file settings, SSL certificates, and connections to ExtraHop recordstores and packetstores.

The following customizations and resources are not saved when you create a backup or migrate to a new target.

- License information for the system. If you are restoring settings to a new target, you must manually license the new target.
- Precision packet captures. You can download saved packet captures manually by following the steps in [View and download packet captures](#).
- When restoring an ECA VM console that has a tunneled connection from a sensor, the tunnel must be reestablished after the restore is complete and any customizations on the console for that sensor must be manually recreated.
- User-uploaded SSL keys for traffic decryption.
- Secure keystore data, which contains passwords. If you are restoring a backup file to the same target that created the backup, and the keystore is intact, you do not need to re-enter credentials. However, if you are restoring a backup file to a new target or migrating to a new target, you must re-enter the following credentials:
 - Any SNMP community strings provided for SNMP polling of flow networks.
 - Any bind password provided to connect with LDAP for remote authentication purposes.
 - Any password provided to connect to an SMTP server where SMTP authentication is required.
 - Any password provided to connect to an external datastore.
 - Any password provided to access external resources through the configured global proxy.
 - Any password provided to access ExtraHop Cloud Services through the configured ExtraHop cloud proxy.
 - Any authentication credentials or keys provided to configure Open Data Stream targets.

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the System Configuration section, click **Backup and Restore**.
3. Click **Create System Backup**, and then click **OK**.
A list of user-saved and automatic backups appear.

- Click the name of the new backup file, **User saved <timestamp> (new)**. The backup file, with an .exbk file extension, is automatically saved to the default download location for your browser.

Restore a sensor or console from a system backup

You can restore the ExtraHop system from the user-saved or automatic backups stored on the system. You can perform two types of restore operations; you can restore only customizations (changes to alerts, dashboards, triggers, custom metrics, for example), or you can restore both customizations and system resources.

This procedure describes the steps required to restore a backup file to the same sensor or console that created the backup file. If you want to migrate the settings to a new sensor or console, see [Transfer settings to a new console or sensor](#).

Before you begin


The target must be running the same firmware version, matching the first and second digits of the firmware that generated the backup file. If the versions are not the same, the restore operation will fail.

The following table shows examples of supported restore operations.

Source firmware	Target firmware	Supported
7.7.0	7.7.5	Yes
7.7.0	7.8.0	No

- Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
- In the System Configuration section, click **Backup and Restore**.
- Click **View or Restore System Backups**.
- Click **Restore** next to the user backup or automatic backup that you want to restore.
- Select one of the following restore options:

Option	Description
Restore system customizations	Select this option if, for example, a dashboard was accidentally deleted or any other user setting needs to be restored. Any customizations that were made after the backup file was created are not overwritten when the customizations are restored.
Restore system customizations and resources	Select this option if you want to restore the system to the state it was in when the backup was created.

 **Warning:** Any customizations that were made after the backup file was created are overwritten when the customizations and resources are restored.

- Click **OK**.
- Optional: If you selected **Restore system customizations**, click **View import log** to see which customizations were restored.
- Restart the system.
 - Return to Administration settings.
 - In the Appliance Settings section, click **Shutdown or Restart**.


- c) In the Actions column for the System entry, click **Restart**.
- d) Click **Restart** to confirm.

Restore a sensor or console from a backup file

This procedure describes the steps required to restore a system from a backup file to the same sensor or console that created the backup file.

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the System Configuration section, click **Backup and Restore**.
3. Click **Upload Backup File to Restore System**.
4. Select one of the following restore options:

Option	Description
Restore system customizations	Select this option if, for example, a dashboard was accidentally deleted or any other user setting needs to be restored. Any customizations that were made after the backup file was created are not overwritten when the customizations are restored.
Restore system customizations and resources	Select this option if you want to restore the system to the state it was in when the backup was created.

 **Warning:** Any customizations that were made after the backup file was created are overwritten when the customizations and resources are restored.

5. Click Choose File and navigate to a backup file that you saved previously.
6. Click **Restore**.
7. Optional: If you selected **Restore system customizations**, click **View import log** to see which customizations were restored.
8. Restart the system.
 - a) Return to Administration settings.
 - b) In the Appliance Settings section, click **Shutdown or Restart**.
 - c) In the Actions column for the System entry, click **Restart**.
 - d) Click **Restart** to confirm.

Transfer settings to a new console or sensor

This procedure describes the steps required to restore a backup file to a new console or sensor. Only system settings from your existing console or sensor are transferred. Metrics on the local datastore are not transferred.

Before you begin

- Create a system backup and save the backup file to a secure location.
- Remove the source sensor or console from the network before transferring settings. The target and source cannot be active on the network at the same time.


 **Important:** Do not disconnect any sensors that are already connected to a console.

- [Deploy](#) and [register](#) the target sensor or console.
 - Ensure that the target is the same type of sensor or console (physical or virtual) as the source.
 - Ensure that the target is the same size or larger (maximum throughput on the sensor; CPU, RAM, and disk capacity on the console) as the source.
 - Ensure that the target has a firmware version that matches the firmware version that generated the backup file. If the first two digits of the firmware versions are not the same, the restore operation will fail.

The following table shows examples of supported configurations.


Source firmware	Target firmware	Supported
7.7.0	7.7.0	Yes
7.7.0	7.7.5	Yes
7.7.5	7.7.0	No
7.7.0	7.6.0	No
7.7.0	7.8.0	No

- After transferring settings to a target console, you must manually reconnect all sensors.
 - When transferring settings to a target console that is configured for a tunneled connection to the sensors, we recommend that you configure the target console with the same hostname and IP address as the source console.
1. Log in to the Administration settings on the target system through `https://<extrahop-hostname-or-IP-address>/admin`.
 2. In the System Configuration section, click **Backup and Restore**.
 3. Click **Upload Backup File to Restore System**.
 4. Select **Restore system customizations and resources**.
 5. Click **Choose File**, navigate to the stored backup file, and then click **Open**.
 6. Click **Restore**.

 **Warning:** If the backup file is incompatible with the local datastore, the datastore must be reset.

After the restore is complete, you are logged out of the system.


7. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin` and verify that your customizations were correctly restored on the target sensor or console.

 **Note:** If the source sensor or console was connected to ExtraHop Cloud Services, you must manually connect the target to ExtraHop Cloud Services.

Reconnect sensors to the console

If you transferred settings to a new console, you must manually reconnect all previously connected sensors.

Before you begin

 **Important:** If your console and sensors are configured for a tunneled connection, we recommend that you configure the source and target consoles with the same IP address and hostname. If you cannot set the same IP address and hostname, skip this procedure and create a new tunneled connection to the new IP address or hostname of the console.

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.

- In the Connected Appliance Administration section, under ExtraHop Discover Settings, click **Manage Discover Appliances**.
- In the Actions column for the first sensor, click **Reconnect**.

Manage Connected Appliances

Discover								Explore	Trace	History
Filter appliances...										Connect Appliance
<input type="checkbox"/>	Name ↑	ID	Version	Date Added	Status	License	NTP	Actions		
<input type="checkbox"/>	10.20.224.218 Direct EXTR-EXTR- <small>XXXXXXXXXX</small>	2	7.8.0.1475	2019-09-03 12:40:56	● Disconnected	● Valid	● Time Synced	Reconnect	Actions ▾	
<input type="checkbox"/>	10.20.225.101 Direct EXTR-EXTR- <small>XXXXXXXXXX</small>	3	7.8.0.1475	2019-09-03 12:41:17	● Disconnected	● Valid	● Time Synced	Reconnect	Actions ▾	

- Type the password for the setup user of the sensor.
- Click **Connect**.
- Repeat steps 3-5 for any remaining disconnected sensors.
All disconnected sensors are now online.

Manage Connected Appliances

Discover								Explore	Trace	History
Filter appliances...										Connect Appliance
<input type="checkbox"/>	Name ↑	ID	Version	Date Added	Status	License	NTP	Actions		
<input type="checkbox"/>	10.20.224.218 Direct EXTR-EXTR- <small>XXXXXXXXXX</small>	2	7.8.0.1475	2019-09-03 12:40:56	● Online	● Valid	● Time Synced	Actions ▾		
<input type="checkbox"/>	10.20.225.101 Direct EXTR-EXTR- <small>XXXXXXXXXX</small>	3	7.8.0.1475	2019-09-03 12:41:17	● Online	● Valid	● Time Synced	Actions ▾		