Back up and restore a Discover or Command appliance

Published: 2020-12-15

After you have configured your Command and Discover appliances with customizations such as bundles, triggers, and dashboards or administrative changes such as adding new users, ExtraHop recommends that you periodically back up your appliance 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 appliance, for example). Then, download the backup file and save it to a secure, off-appliance location.

Back up a Discover or Command appliance

Create a system backup and 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.
- Appliance configuration settings made in the Admin UI, such as locally-created users and remote imported user groups, running configuration file settings, appliance SSL certificates, and connections to Explore and Trace appliances.

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

- License information for the appliance. If you are restoring settings to a new target appliance, you must manually license the new appliance.
- Precision packet captures. You can download saved packet captures manually by following the steps in View and download packet captures.
- When restoring a Command appliance that has a tunneled connection from a Discover appliance, the tunnel must be reestablished after the restore is complete and any customizations on the Command appliance for that Discover appliance 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 appliance 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 appliance or migrating to a new appliance, 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 page 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.

4. 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 Discover or Command appliance 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 appliance that created the backup file. If you want to migrate the settings to a new appliance, see Transfer settings to a new Command or Discover appliance.

Before you begin
The target appliance must be running a firmware version that is the same major and minor version as the firmware version that generated the backup file. If the major and minor firmware versions are not the same, the restore operation will fail.

The following table shows examples of supported restore operations.

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

1. Log in to the Administration page on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the System Configuration section, click **Backup and Restore**.
3. Click **View or Restore System Backups**.
4. Click **Restore** next to the user backup or automatic backup that you want to restore.
5. 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.

6. Click **OK**.
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 the main Admin UI page.

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.

Restore a Discover or Command appliance from a backup file

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

1. Log in to the Administration page 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 the main Admin UI page.
   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 Command or Discover appliance

This procedure describes the steps required to restore a backup file to a new Command or Discover appliance. Only system settings from your existing Discover or Command appliance to a new appliance 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 appliance from the network before transferring settings. The target and source appliance cannot be active on the network at the same time.

Important: Do not disconnect any Discover appliances that are already connected to a Command appliance.

- Deploy and register the target appliance.
  - Ensure that the target appliance is the same type of appliance, physical or virtual, as the source appliance.
  - Ensure that the target appliance is the same size or larger (maximum throughput on the Discover appliance; CPU, RAM, and disk capacity on the Command appliance) as the source appliance.
  - Ensure that the target appliance is running a firmware version that is the same major and minor version as the firmware version that generated the backup file. If the major and minor firmware versions are not the same, the restore operation will fail.

    The following table shows examples of supported configurations.

Source appliance firmware	Target appliance 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 Command appliance, you must manually reconnect all Discover appliances
- When transferring settings to a target Command appliance that is configured for a tunneled connection to the Discover appliances, we recommend that you configure the target Command appliance with the same hostname and IP address as the source Command appliance.

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

   Note: If the source appliance was connected to Atlas services, you must manual connect the target appliance to Atlas.

Reconnect Discover appliances to the Command appliance

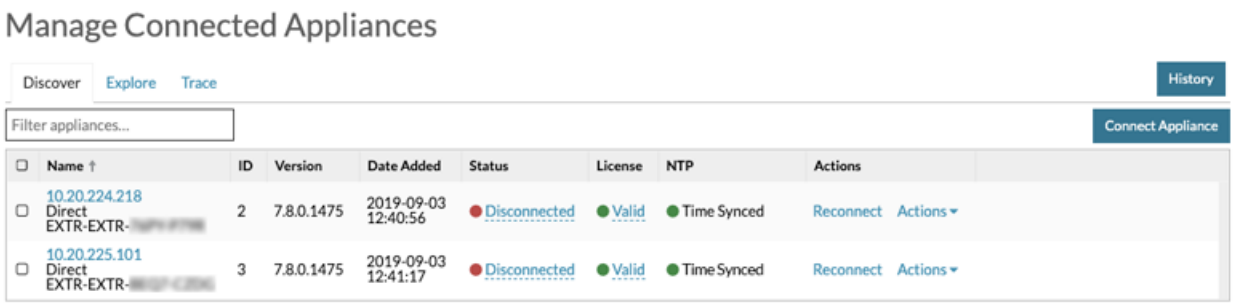
If you transferred settings to a new Command appliance, you must manually reconnect all previously connected Discover appliances.

Before you begin

Important: If your Command and Discover appliances are configured for a tunneled connection, we recommend that you configure the source and target Command appliances 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 Command appliance.

1. Log in to the Administration page on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Connected Appliance Administration section, under ExtraHop Discover Settings, click **Manage Discover Appliances**.
3. In the Actions column for the first Discover appliance, click **Reconnect**.



4. Type the password for the setup user of the Discover appliance.
5. Click **Connect**.
6. Repeat steps 3-5 for any remaining disconnected Discover appliances.
All disconnected Discover appliances are now online.