

Discover and Command Post-deployment Checklist

Published: 2021-10-21

After you deploy the ExtraHop Discover or Command appliance, log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin` and configure the following settings. Refer to the section of the [ExtraHop Admin UI Guide](#) specified in each action below, except where noted.

Password

Maintain system security after the evaluation period. Change the default password. For more information, see the [Default User Accounts FAQ](#).

NTP

Time is critical in the ExtraHop system, particularly when doing event correlation with time-based metrics and logs. Verify that the NTP settings are correct for your infrastructure, test settings, and sync NTP. For more information, see [Configure the system time](#).

Time Zone

The correct time zone is critical to run scheduled reports at the correct time. Ensure the ExtraHop system has the correct time zone. For more information, see [Configure the system time](#).

Remote Authentication

Set up remote authentication. The ExtraHop appliance integrates with [LDAP](#), [RADIUS](#), [SAML](#), and [TACACS+](#).

Firmware Update

The ExtraHop firmware is updated often with enhancements and resolved defects. Verify that you have the current firmware. For more information, see [Upgrade the firmware on your ExtraHop system](#).

Audit Logging

The ExtraHop system can send events to a remote syslog collector. For more information, see the [Send audit log data to a remote syslog server](#).

SMTP

The ExtraHop system can email alerts and system-health notifications. Set up and test notifications. For more information, see [Configure email settings for notifications](#).

System Notifications

The ExtraHop system can send email when it detects problems. Create an email group to receive notifications. For more information, see [Configure an email notification group](#).

iDRAC

Each physical ExtraHop appliance has an iDRAC port, similar to iLO or KVM over Ethernet. Connect and configure the iDRAC port. For more information, see [Configure the iDRAC Remote Access Console](#).

SSL Certificate

Each ExtraHop system ships with a self-signed certificate. If you have a PKI deployment, generate your own certificate and upload it to each ExtraHop system. For more information, see the [SSL Certificate](#) section.

DNS A Record

It is easier to access an ExtraHop system by hostname than by IP address. Create an A record in your DNS root ("`exa.yourdomain.local`") for each ExtraHop system in your deployment. Refer to your DNS administration manual.

Connect Appliances

Connect Command and Discover appliances to all Explore and Trace appliances. For more information, see [Connect the Discover and Command appliances to Explore appliances](#) and [Connect the Discover and Command appliances to the Trace appliance](#).

Cloud Services

Connect to ExtraHop Cloud Services to enable Detections and Remote Access. For more information, see [Connect to ExtraHop Cloud Services](#).

Threat Intelligence

Configure threat intelligence settings to identify indicators of compromise on your network. For more information, see [Threat intelligence](#).

Network Localities

Classify non-RFC1918 IP addresses as part of your internal network. For more information, see [Specify the locality for IP addresses](#).

Tuning Parameters

Help improve the quality and accuracy of rules-based detections by adding tuning parameters. For more information, see [Specify tuning parameters for detections](#).

Advanced Analysis

Target specific device groups or activity groups for Advanced Analysis as needed, based on their importance to your network. For more information, see [Analysis priorities](#).

Decrypt SSL Traffic

Decrypt forwarded SSL traffic by uploading the private key and server certificate associated with that traffic. For more information, see [Decrypt SSL traffic with certificates and private keys](#).

Configure Perfect Forward Secrecy (PFS)

Decrypt SSL/TLS traffic from your Linux and Windows servers. For more information, see [Install the ExtraHop session key forwarder on a Linux server](#) and [Install the ExtraHop session key forwarder on a Windows server](#).

Customizations and Datastore Backup

Create a system backup prior to upgrading firmware, or before making a major change in your environment. For more information, see [Back up a Discover or Command appliance](#).