Sensor and console post-deployment checklist

Published: 2025-05-05

After you deploy an ExtraHop sensor or console, 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.

Required procedures

You must complete these procedures to fully deploy your ExtraHop system.

DNS

DNS enables domain name resolution. Verify that you have set DNS servers. Access the CLI interface with a terminal or go to the Admin > Connectivity page to change or set DNS IP addresses. You can set DNS IP addresses with the front panel or iDRAC iDRAC interface on physical appliances.

System hostname

Set a unique system hostname so the ExtraHop console can re-establish connectivity if the IP address changes. If the A Record is "hq-eda01.acme.org" then your hostname should be "hq-eda01."

Password

Maintain system security after the evaluation period. Change the default password. For more information, see the Default User Accounts FAQ. We recommend that you create a secondary administrator account with separate credentials as a backup in case the primary administrator credentials are lost.

NTP and time zone

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. 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 system time servers.

Apply license

You must apply a product key to activate and register your appliance.

Cloud Services

Connect to ExtraHop Cloud Services to enable Detections and Remote Access. For more information, see Connect to ExtraHop Cloud Services.

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.

Connect Appliances

Connect the console and sensors to all packetstores and recordstores. For more information, see Connect the EXA 5200 to the ExtraHop system and Connect a packetstore to RevealX Enterprise.

Recommended procedures

We recommend that you complete these procedures to optimize the performance of your ExtraHop system.

TLS 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 TLS 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.

Remote Authentication and Access

Set up remote authentication. The ExtraHop appliance integrates with SAML (preferred for the console), LDAP, RADIUS, and TACACS+. Restrict remote access from the public internet with a corporate VPN, identity-aware proxy (IAP), or other method.

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.

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.

Disk Encryption

Enable security on storage drives to provide encryption on virtual disks. For more information, see Configure self-encrypting disks (SEDs).

Network Localities

Classify non-RFC1918 IP addresses as part of your internal network. For more information, see Specify a network locality.

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 and metrics.

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.

Configure Domain Controller Decryption

The ExtraHop system can be configured to retrieve and store domain keys from one or more domain controllers. When the system observes encrypted traffic that matches the cached keys, all of the Kerberos-encrypted traffic in the domain is decrypted for supported protocols. For more information, see Decrypt domain traffic with a Windows domain controller.

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 sensor or console.

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.

Decrypt TLS Traffic with Secret Sharing

Decrypt 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. Alternatively, you can share session keys with your ExtraHop system through your existing Session key forwarding from an F5 LTM with Perfect Forward Secrecy (PFS).

Optional procedures

Consider completing these procedures if you want to further customize your ExtraHop system.

Enable Precision Packet Capture (PPCAP) disk drive

Packet capture enables you to collect, store, and retrieve data packets from your network traffic. If you have a precision packet capture disk, see Configure packet capture.

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.

Enable Precision Packet Capture (PPCAP) disk drive

Packet capture enables you to collect, store, and retrieve data packets from your network traffic. If you have a precision packet capture disk, see Configure packet capture.

Threat Intelligence

Configure threat intelligence settings to identify indicators of compromise on your network. For more information, see Threat intelligence.

Decrypt TLS Traffic with RSA Private Keys

Decrypt forwarded TLS traffic by uploading the private key and server certificate associated with that traffic. For more information, see Decrypt TLS traffic with certificates and private keys.

Configure SNMP

You can set SNMP traps and Configure SNMP settings to notify you of certain network events.