# ExtraHop Explore Post-deployment Checklist

Published: 2017-11-15

After you deploy the ExtraHop Explore appliance, log into the Explore Admin UI, and configure the following settings. Refer to the section of the Explore 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 Change password section.

**NTP**

Time is critical in the Explore appliance, 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 the System Time section.

**Time Zone**

The correct time zone is critical to run scheduled reports at the correct time. Ensure the Explore appliance has the correct time zone. For more information, see the System Time section.

**Remote Authentication**

Set up remote authentication. The Explore appliance integrates with RADIUS, TACACS, and LDAP for remote integration. For more information, see the Remote Authentication section.

**Firmware Update**

Explore appliance firmware is updated often with enhancements and resolved defects. Verify that you have the current firmware. For more information, see the Firmware section.

**Audit Logging**

The Explore appliance can send events to a remote syslog collector. Configure the Explore appliance to send audit logs. For more information, see the Audit Log section.

**SMTP**

The Explore appliance can email alerts and system-health notifications. Set up and test notifications. For more information, see the Email Server and Sender section.

**System Notifications**

The Explore appliance can send email when it detects problems. Create an email group to receive notifications. For more information, see the Notifications section.

**iDRAC**

Each physical Explore appliance has an iDRAC port, similar to iLO or KVM over Ethernet. Connect and configure the iDRAC port. For more information, see Configuring the iDRAC Remote Access Console.

**SSL Certificate**

Each Explore appliance ships with a self-signed certificate. If you have a PKI deployment, generate your own certificate and upload it to each Explore appliance. Generate and deploy an SSL certificate for each Explore appliance. For more information, see the SSL Certificate section.

**DNS A Record**

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