ExtremeCloud IQ – Site Engine

Security Best Practices

Published: April 2022
PN: 9037479-00

Extreme Networks, Inc.

Phone / +1 408.579.2800

Toll-free / +1 888.257.3000

www.extremenetworks.com

Contents

Overview

The purpose of this document is to provide guidance for the best security practices that should be followed for ExtremeCloud IQ – Site Engine. Failure to follow these practices could leave your system vulnerable to security breaches.

Best Practices

Installation Wizard

User Running the Application

When the installation wizard prompts you to run as root, select No and run the application as a non-root user.

Figure 1: Installation wizard

SNMP profile

By default, the wizard configures the embedded SNMP. Use the most secure options, SHA and AES, instead of the default values. You should also use unique passwords.

Figure 2: SNMP configuration

Use the same values in the SNMP profile.

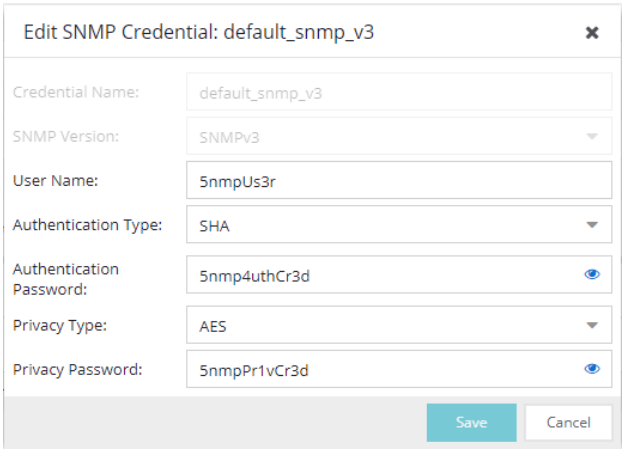

Figure 3: Site Engine SNMP configuration

Authentication to the application

Use an external authentication source for users logging into the application. See Authentication Method for additional information.

Deny SSH access to Site Engine

Deny remote root access to the operating system (OS).

Option 1: If the application is running as root, navigate to **Administration > Users > SSH Configuration** and **select Manage SSH Configuration** and **Disable Remote Root Access.**

See Network Settings for additional information.

Option 2: Modify the `/etc/ssh/sshd_config` file and change the value for `PermitRootLogin` directive from **`yes`** to **`no`**.

External access to MySQL

If external access to the internal MySQL database is not needed, drop the incoming packets using embedded iptables. Execute the following commands in the operating system:

```
iptables -A INPUT ! -i lo -p tcp --dport 4589 -j DROP
```

To make the change permanent use:

```
echo "iptables -A INPUT ! -i lo -p tcp --dport 4589 -j DROP"
>> /etc/iptables.rules
```

Site Engine - Change password to MySQL database

Admin access to the MySQL database is not permitted from external sources by default. Change the default password to the MySQL database especially if external access to MySQL is needed.

1. Select **Administration** > **Backup/Restore > Advanced**
2. Change the password and click **Save**
3. Confirm the change

4. Wait until the server restarts

Note
MySQL credentials are stored in the backup of the product. Restoring the backup will restore credentials also. To restore the backup in a fresh new system requires this procedure to be executed before the restoration. Restoring the initial database will not overwrite those credentials.

Auditing in Site Engine

The audit feature should be used. See Enable CLI Auditing for additional information.

Web Terminal Logging

Additional security can be added by auditing the actions made by users in the web terminal. To set up the audit function:

1. Select **Administration** > **Diagnostics**
2. Under **Level**, select **Advanced**
3. Select **System** > **Web Terminal**
4. Select **Eable Logging**

See Terminal for additional information.

Use trusted HTTPs Server Certificate

Use trusted CA generated HTTPS certificates. To replace the certificate:

1. Select **Administration** > **Certificates**
2. Select **Update** under **Server Configuration Information**
3. Replace the default certificate with the certificate trusted by CA.

See Certificates for additional information.

Review Ciphers used by HTTPS

Some security tools recommend reducing the Ciphers allowed for communication with the application. Review Ciphers allowed by the webserver.

Note
Changes will affect the ability of devices to ZTP+ and communication between Engines and Site Engine.

See How to Change Default Ciphers used by Extreme Management Center Web GUI for additional information.

Disable Password Auto Complete for the Web Interface

To disable Auto Complete:

1. Select **Administration** > **Options** > **Web Server**
2. Select **Disable Password Auto Complete for Web Interfaces**

See Password Auto Complete for additional information.

Managing devices

Use SSH instead of Telnet

Use the SSH protocol for scripting and CLI access to the managed devices. To configure SSH:

1. Select **Administration** > **Profiles**.
2. In the bottom half of the screen, select **CLI Credentials.**
3. Select a credential to activate **Add** or **Edit**.
4. In the pop-up window, select **SSH** for **Type** value.

See CLI Credentials Subtab for additional information.

Disable Device Terminal Automatic Login

To disable automatic login:

1. Select **Administration** > **Options** > **Device Terminal**
2. Clear **Enable Auto Login**.

See Device Terminal Options for additional information.

Use HTTPS instead of HTTP for REST calls to Managed Devices

To configure your REST calls to use HTTPS:

1. **Select Network** > **Devices**.
2. Right-click on the device
3. Select **Configure** > **Device**.
4. Clear **Use Default WebView URL**
5. In **WebView URL**, replace the default `http://%IP` with `https://%IP:443`.

The modification can also be done through Vendor Profiles. See Device for additional information.

Use SNMPv3 instead of SNMPv1

SNMPv3 is the most secure method in the device access profile for write and maximum access. Modern devices usually have enough performance to handle the most secure methods for read access also. The best security practice is to use the **AuthPriv** security level with **SHA** and **AES** methods.

To configure the access profile:

1. Select **Administration** > **Profiles**.
2. Select the device to update, right-click, and select **Edit** or select **Edit** from the toolbar. You can also setup the access profile when you add the profile.
3. Select **SNMPv3** for the **SNMP Version**

See Profiles Section for additional information.

Inventory

Use SCP instead of Trivial File Transfer Protocol (TFTP) for transferring files during backup, restore, firmware upgrade actions. To configure SCP:

1. Select **Network** > **Devices**.
2. Select the device and right-click
3. Select **Archives** > **Inventory Settings**

The default behavior for new devices can be changed through Vendor Profiles. See Inventory Settings for additional information.

Restrict Access to Scripts and Workflows

Only necessary personnel should have access to modify or create sripts and workflows. Users with access to sripts and workflows have access to the OS through Python. To restrict access:

1. Select **Administration** > **Users**.
2. In the **Authorization Groups** at the bottom of the window, select the group to modify.
3. Right-click and select **Edit** or select **Edit** from the **Authorization Groups** toolbar. You can also restrict access when you add a group.
4. In the **Edit Authorization Group** window, select **Advanced** in Category.
5. Expand **XIQ-SE OneView.**
6. Expand **Workflows/Scripts.**
7. Clear **View and Edit Workflows, Scripts and Saved Tasks**.
8. Select **Save**.
9. The capability to Edit Workflows, Scripts, and Saved Tasks has id **OV_WORKFLOW_WRITE**. See Authorization Group Capabilities for additional information.

The best security practice is to define **Authorization Groups (Roles)** for each workflow and script. See Menus for additional information.

Restrict Access to API

Only necessary personnel should have access. To restrict API access:

1. Select **Administration** > **Users**
2. In **Authorization Groups** at the bottom of the window, select the group to modify.
3. Expand **Northbound API**.
4. Clear the choices that apply.

5. Select Save.

The best security practice is to use Client API access through tokens. See Authorization Group Capabilities for additional information.

Exporting logs to SIEM or Log Manager

The best security practice is to export logs to external applications performing long-term storage of logs and Log Management.

1. Create file `/etc/rsyslog.d/10-remote.conf` with the following content. Adjust the destination (target):

```
module(load="imfile" PollingInterval="1" mode="inotify")
input(type="imfile"
file="/usr/local/Extreme_Networks/NetSight/appdata/logs/adm
in.log" tag="admin" severity="info" facility="local6"
PersistStateInterval="10")
input(type="imfile"
file="/usr/local/Extreme_Networks/NetSight/appdata/logs/app
id.log" tag="appid" severity="info" facility="local6"
PersistStateInterval="10")
input(type="imfile"
file="/usr/local/Extreme_Networks/NetSight/appdata/logs/con
sole.log" tag="console" severity="info" facility="local6"
PersistStateInterval="10")
input(type="imfile"
file="/usr/local/Extreme_Networks/NetSight/appdata/logs/fab
ricManager.log" tag="fabricManager" severity="info"
facility="local6" PersistStateInterval="10")
input(type="imfile"
file="/usr/local/Extreme_Networks/NetSight/appdata/logs/Gov
ernance.log" tag="Governance" severity="info"
facility="local6" PersistStateInterval="10")
input(type="imfile"
file="/usr/local/Extreme_Networks/NetSight/appdata/logs/inv
entory.log" tag="inventory" severity="info"
facility="local6" PersistStateInterval="10")
input(type="imfile"
file="/usr/local/Extreme_Networks/NetSight/appdata/logs/nac
ApplianceEvent.log" tag="nacApplianceEvent" severity="info"
facility="local6" PersistStateInterval="1$
input(type="imfile"
file="/usr/local/Extreme_Networks/NetSight/appdata/logs/nss
chedule.log" tag="nsschedule" severity="info"
facility="local6" PersistStateInterval="10")
input(type="imfile"
file="/usr/local/Extreme_Networks/NetSight/appdata/logs/Pol
icy.log" tag="Policy" severity="info" facility="local6"
PersistStateInterval="10")
input(type="imfile"
file="/usr/local/Extreme_Networks/NetSight/appdata/logs/tam
Audit.log" tag="tamAudit" severity="info" facility="local6"
PersistStateInterval="10")
input(type="imfile"
file="/usr/local/Extreme_Networks/NetSight/appdata/logs/tam
```

```
.log" tag="tam" severity="info" facility="local6"
PersistStateInterval="10")
input(type="imfile"
file="/usr/local/Extreme_Networks/NetSight/appdata/logs/wir
eless.log" tag="wireless" severity="info" facility="local6"
PersistStateInterval="10")
input(type="imfile"
file="/usr/local/Extreme_Networks/NetSight/appdata/logs/wir
elessAudit.log" tag="wirelessAudit" severity="info"
facility="local6" PersistStateInterval="10")
input(type="imfile"
file="/usr/local/Extreme_Networks/NetSight/appdata/logs/wir
elessEvent.log" tag="wirelessEvent" severity="info"
facility="local6" PersistStateInterval="10")

local6.* action(type="omfwd"
target="<ExternalSyslogServer>" port="514" protocol="UDP")
& stop
```

2. Restart the rsyslog service
   `systemctl restart rsyslog`

Securing SMTP connection

Use TLS or SSL on SMTP communication. See How to Configure Extreme Management Center SMTP for Gmail, Microsoft SMTP, Exchange, Office 365, and Other Services for additional information.

ExtremeControl

Default credentials

Admin Web Page Credentials

To change the Access Control Engine default credentials for WebView:

1. Select **Control** > **Access Control** > **Configuration** > **Global & Engine Settings** > **Default** > **Credentials** > **Admin Web Page Credentials**
2. Enter a new username and password
3. Select **Save**

See Admin Web Page Credentials for additional information.

Assessment Adapter

To change the Assessment Adapter default credentials even if Assessment Adapter is not being used:

1. Select **Administration** > **Options** > **Access Control** > **Assessment Server** > **Assessment Agent Adapter Credentials**
2. Enter a new username and password
3. Select **Save**

See Assessment Server for additional information.

Shared Secret

Change the Shared Secret default radius:

1. Select **Control** > **Access Control** > **Configuration** > **Global & Engine Settings** > **Engine Settings** > **Default** > **Credentials**
2. Under **Switch Configuration**, enter a new **Shared Secret**
3. Select **Save**

See Switch Configuration for additional information.

Secure Communication

Secure communication should be configured between Access Control Engine and ExtremeCloud IQ – Site Engine. See ExtremeCloud IQ - Site Engine and ExtremeControl Secure Communication for additional information.

Auditing

Enable the auditing feature:

1. Select **Control** > **Access Control** > **Configuration** > **Global & Engine Settings** > **Engine Settings** > **Default** > **Auditing** > **Enable Auditing**
2. Select **Enable Auditing**
3. Enter the auditing rules
4. Select **Save**

See Auditing for additional information.

SSH access to the Operating System

Deny remote root access to the OS:

1. Select **Control** > **Access Control** > **Configuration** > **Global & Engine Settings** > **Engine Settings** > **Default** > **Network Settings**
2. Select **Manage SSH Configuration** and **Disable Remote Root Access**
3. Click **Save**

Note
Firmware upgrade of AccessControl Engine requires root privileges.

See Manage SSH Configuration for additional information.

ExtremeAnalytics

Default credentials to WebView

Change the Analytics Engine default credentials for WebView.

1. Select **Analytics** > **Configuration** > **Engines**
2. Select one engine > **Configuration** > **Web Credentials**

3. Enter a new username and password
4. Select **Save**

See Web Credentials for additional information.

Auditing

Enable the auditing feature.

1. Select **Analytics** > **Configuration** > **Engines**
2. Select one engine > **Configuration** > **Auditing**
3. Select **Enable Auditing**
5. Enter the auditing rules
6. Select **Save**

See Auditing for additional information.

SSH access to the Operating System

Deny remote root access to the OS:

1. Select **Analytics** > **Configuration** > **Engines**
2. Select one engine > **Configuration** > **Network Settings**
3. Select **Manage SSH Configuration** and **Disable Remote Root Access**
4. Select **Save**

Note
Firmware upgrade of ApplicationAnalytics Engine requires root privileges.

See SSH for additional information.