

Workflow description

XIQ Access Point import to XIQ-SE

This workflow addresses the need to use XIQ-SE Control for XIQ cloud AP's. The XIQ AP's gets imported to XIQ-SE, discovered and added to the Control.

Prerequisite

XIQ

The XIQ network policy must contain SNMP settings for the AP's to enable XIQ-SE for discovering and classifying later on the AP. Als is required to define the Radius settings for the SSID where you intend to server 802.1x authneticaion.

ExtremeCloud IQ Pilot

Network Policies > CTC-Reading > SNMP Server

1 Policy Details 2 Wireless 3 Switching/Routing 4 SR/Dell Switching 5 Branch Routing 6 Deploy Policy

POLICY DETAILS

- Policy Type
- Policy
- Policy Settings
 - DNS Server
 - NTP Server
 - SNMP Server
 - Syslog Server
 - Device Credentials
 - Device Time Zone
 - HIVE
 - Management & Native VLAN
 - IP Tracking
 - LLDP/CDP
 - Management Settings
 - Management Options
 - Traffic Filter

SNMP Server

SNMP Server ☒ ON

Re-use SNMP Server Settings (Pick existing settings)

Name * XIQ-SE

Description

SNMP Contact

☐ Disable to Send Traps over CAPWAP

SNMP Server	IP Address / Host Name	Version	Operation	Community	Admin	Auth	Encryption	Order
<input checked="" type="checkbox"/> XIQ-SE_new	10.8.255.5	V3	GET	snmpuser		MD5	DES	↑ ↓

Classification

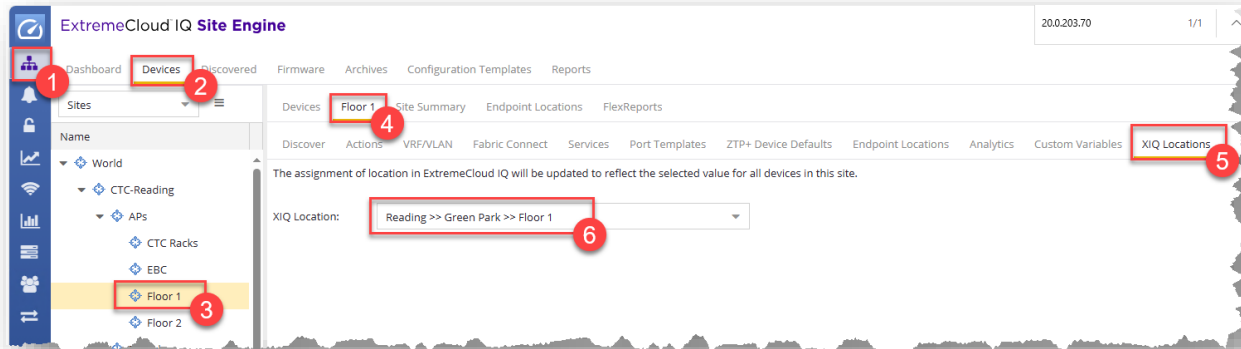
☐ Add SNMP agents to device classification

CANCEL SAVE SNMP SERVER

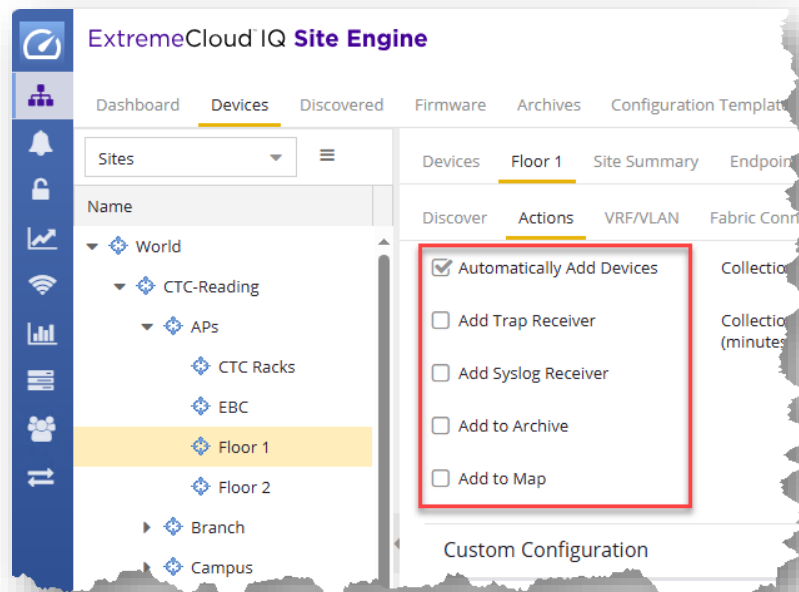
XIQ Access Point import to XIQ-SE

XIQ-SE

The XIQ location should be appropriately mapped to the XIQ-SE site paths.

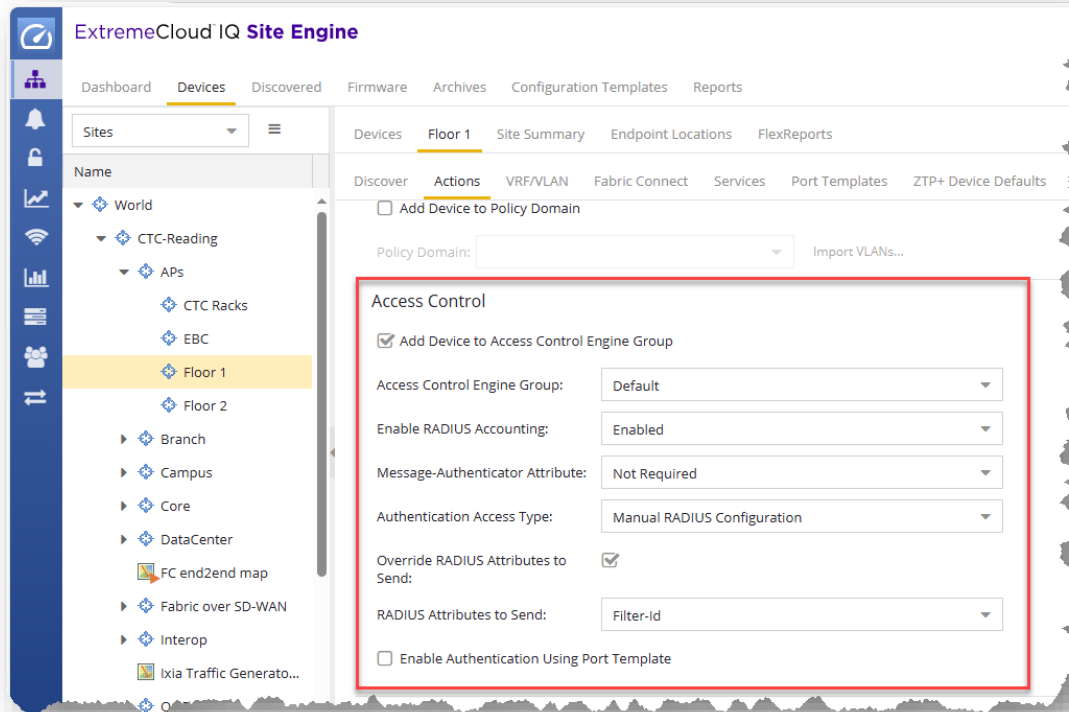


As well the Site actions



XIQ Access Point import to XIQ-SE

And Access Control settings



XIQ-SE Workflow parameter

During execution of the workflow you have to provide the parameter relevant for the success.

Run Workflow - XIQ AP import

Workflow Inputs

Timeout Properties

Timeout:

1

hr(s)

Custom Inputs

XIQ Username:

user@extremenetworks.com

XIQ Password:

.....

default Site Path:

/World/CTC-Reading/APs

Profile:

snmp_v3_profile

XIQ import filter for AP name start with:

Add AP to NAC:

true

Delete AP in XIQ-SE if not exists in XIQ:

false

Sanity check enable:

false

Next »

Cancel

4 | Page

Troubleshooting

Please note, there is no Extreme Networks GTAC for any workflow.

Before reporting an issue via GitHub or the creator of the workflow, please ensure that the workflow is configured for **DEBUG** mode. The data and debug LOG files can then be found on the XIQ-SE file system under `/dev/shm/<Execution-ID>_<Workflow-Name>/`. Note that only the last six execution debug logs will be held. The actual path can also be found in the each workflow activity log.

```

Output

Script Name: XIQ AP import_XIQ
Date and Time: 2025-03-24T16:11:49.248
XIQ-SE User: mnikulski
XIQ-SE User Domain:
IP:
16:12:06 INFO LOG file /dev/shm/2281_Workflows_CTC-Production_XIQ-AP-import/XIQ.log
16:12:08 INFO learn.AP 20.0.203.70 'CTC-410C-3/45' (up)
  
```

When SSH to XIQ-SE, the following log files should be present in the folder.

```

Using username "root".
Last login: Mon Mar 24 16:15:10 2025 from 10.8.255.158

**** Extreme Networks ****

This is the ExtremeCloud IQ - Site Engine 25.2.11.23.  Alter files with caution.

WWW Site:      http://www.extremenetworks.com
Support Email: support@extremenetworks.com
Phone:        +1 800-998-2408

*****
root@xiq-se:~# cd /dev/shm/2279_Workflows_CTC-Production_XIQ-AP-import/
root@xiq-se:/dev/shm/2279_Workflows_CTC-Production_XIQ-AP-import#
root@xiq-se:/dev/shm/2279_Workflows_CTC-Production_XIQ-AP-import# ls -l
total 104
-rw-r--r-- 1 root root 5261 Mar 24 14:56 emc_vars.json
-rw-r--r-- 1 root root 1664 Mar 24 14:56 se_aps.json
-rw-r--r-- 1 root root 719 Mar 24 14:56 se_locations.json
-rw-r--r-- 1 root root 4233 Mar 24 14:56 se_sites.json
-rw-r--r-- 1 root root 35 Mar 24 14:56 se_unknow_devices.json
-rw-r--r-- 1 root root 6744 Mar 24 14:56 update.log
-rw-r--r-- 1 root root 3856 Mar 24 14:56 xiq_aps.json
-rw-r--r-- 1 root root 10404 Mar 24 14:56 XIQ.log
-rw-r--r-- 1 root root 49666 Mar 24 14:56 XIQ-SE.log
root@xiq-se:/dev/shm/2279_Workflows_CTC-Production_XIQ-AP-import#
  
```

Please include all log files when reporting an issue.