

EXTREME NETWORKS

Onboard VSP XIQ-SE workflow

Ludovico Stevens

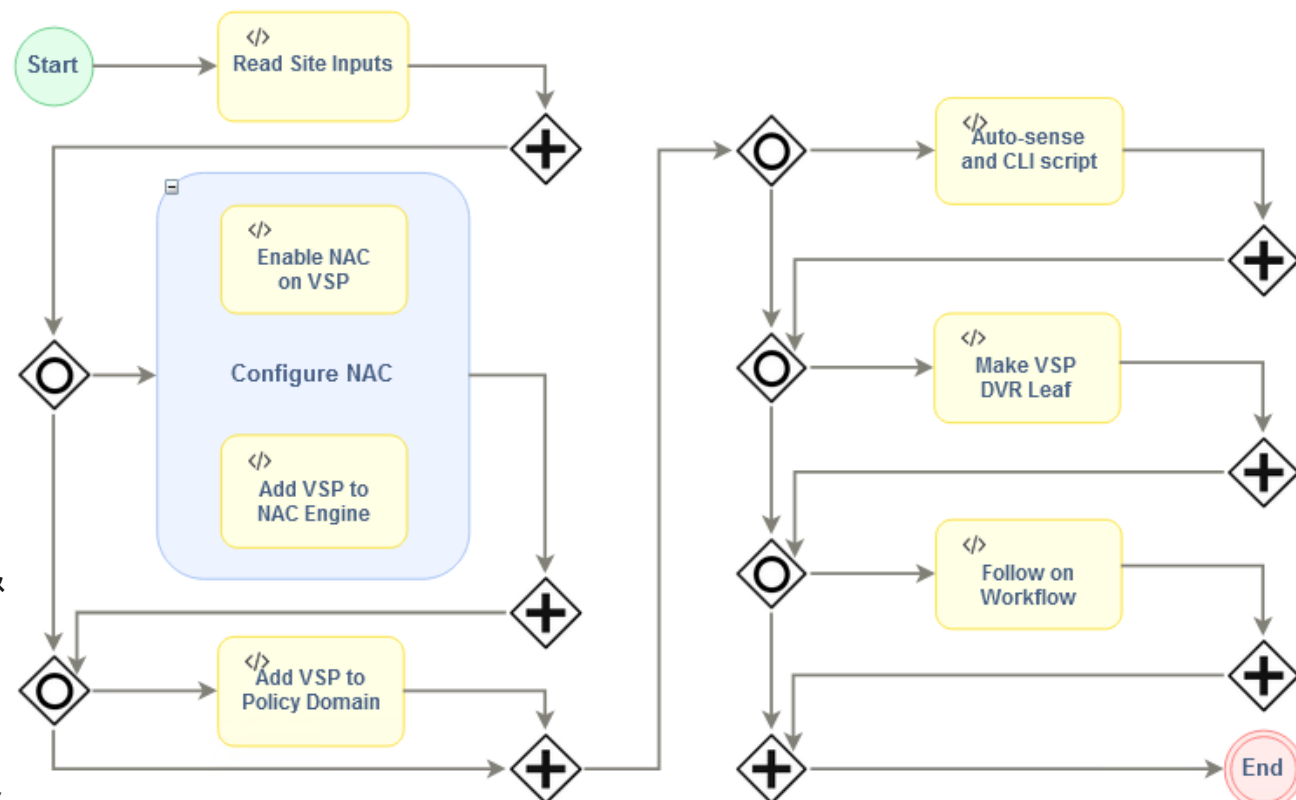
Technical Marketing Engineering

February 2025

Onboard VSP XIQ-SE workflow



- This workflow can do any of the following
- Add switch to XIQ-SE Control + configure RADIUS on switch
- Add switch to Policy domain, including to VLAN Island topology
- Configure any of the global auto-sense parameters
- Convert the switch into a DVR-Leaf
- Execute a custom CLI script with variables & logical operators
- Launch another workflow on completion
- All inputs can make use of site variables, csv variables, eval variables and emc_vars variables



Workflow manual execution



- Workflow can be manually run against 1 or many switches simultaneously

The screenshot displays the 'Devices' tab in the management console. A table lists various network devices with columns for Status, Name, Site, IP Address, and Poll Status. A context menu is open over the device list, showing options like 'FlexView', 'More Views', 'Configure...', 'Compass Search...', 'Rediscover', 'Clear Alarms...', 'Upgrade Firmware...', 'Add to Device Group...', and 'More Actions'. The 'Onboard VSP' option is highlighted in red.

Status	Name	Site	IP Address	Poll Status
●	5320-16P-4XE-DC-FabricEngine	/World/CTC-Readin...	10.180.48.14	Available
●	5320-24T	/World/CTC-Readin...	10.180.209.14	Available
●	5420M-2	/World/CTC-Readin...	10.180.209.10	Available
●	5420M-3	/World/CTC-Readin...	10.180.209.101	Available
●	5420M-24W-4YE-FabricEngine	/World/CTC-Readin...	180.48.11	Available
●	5520-24X		180.209.11	Available
●	5520-48T		180.209.51	Available
▶	5520-Stack		0.209.52	Available
▼	5720-2		3.2.30	Available
▶	7520E-1		180.20.76	Available
▶	7520E-2		180.20.77	Available

- FlexView
- More Views
- Configure...
- Compass Search...
- Rediscover
- Clear Alarms...
- Upgrade Firmware...
- Add to Device Group...
- More Actions

- Configure MACsec Link
- Configure SSH
- Configure SSH ctc
- Configure VOSS App-telemetry
- Delete Insight VMs
- Deploy Insight VM
- Disable Beta NVO IQagent
- Enable Beta NVO IQagent
- Enable Beta NVO IQagent v2
- Enforce Config after Onboard
- Fabric MultiArea Migrate
- Onboard Device to NAC v2
- Onboard Mgmt CLIP
- Onboard Mgmt CLIP ctc
- Onboard Mgmt OOB
- Onboard Mgmt VLAN
- Onboard Mgmt VLAN ctc
- Onboard VSP**

Workflow automatic execution during onboarding



- Workflow can be automatically run after ZTP+ onboarding, under XIQ-SE Site Actions
- In this case script will always run against 1 switch only, the onboarding switch

The screenshot displays the 'Building2' configuration page in the XIQ-SE interface. The 'Actions' tab is selected, showing various workflow settings. Below the main settings, a 'Custom Configuration' table is visible, containing one entry for 'Provisioning/Onboard VSP'.

Configuration Settings:

- ☒ Automatically Add Devices
- ☒ Add Trap Receiver
- ☒ Add Syslog Receiver
- ☒ Add to Archive
- ☒ Add to Map

Collection Mode: Historical

Collection Interval (minutes): 15

Map Name: /World/Building2/Building2

Custom Configuration Table:

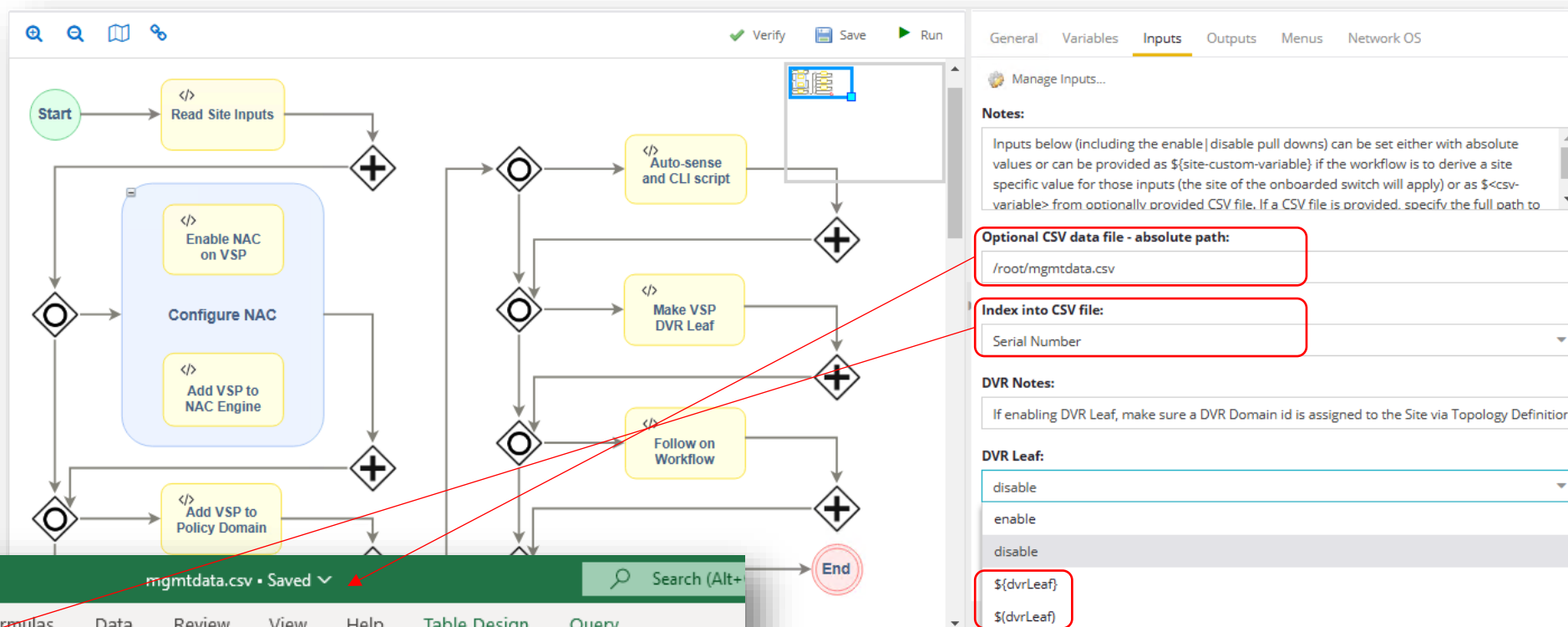
Enabled	Vendor	Family	Topology	Task
<input checked="" type="checkbox"/>	Extreme	Universal Platform F	Any	Provisioning/Onboard VSP

Buttons: Add, Edit, Delete, Update, Cancel

Onboard VSP XIQ-SE workflow inputs



- Optionally, a CSV file is uploaded to XIQ-SE beforehand
- CSV file has device data which can be device specific
- CSV data is looked up either by device initial (dhcp) IP or Serial Number or MAC Address
- CSV data can be referenced as `<name>` or `$(name)` in workflow inputs
- Site variables can still also be referenced but as `$(name)`
- The CSV variable names are case sensitive



mgmtdata.csv • Saved

	A	B	C	D	E	F	G	H
1	serial number	mgmt vlanid	mgmt isid	mgmt ip	mgmt mask	mgmt gateway	sysname	site name
2	JA092041G-01023	209	2800209	20.0.209.54	255.255.255.0	20.0.209.1	5420-bld1	/World/building1
3	TB062139K-H0210	209	2800209	20.0.209.53	255.255.255.0	20.0.209.1	5320-bld1	/World/building1
4	TB022131K-H0059	209	2800209	20.0.209.52	255.255.255.0	20.0.209.1	5320-bld2	/World/building2
5	JA102040G-00003	209	2800209	20.0.209.55	255.255.255.0	20.0.209.1	5420-bld2	/World/building2

- If your XIQ-SE was installed without “root” access, place the CSV file here instead:
`/usr/local/Extreme_Networks/NetSight/appdata/logs/scripting/NetSight_Server`

Optional CSV data file - absolute path:

```
/root/mgmtdata.csv
```

- Available path variables: **%rootDir%, %sitePath%, %siteName%**
 - %rootDir% by default is /root/; can be changed via workflow variable const_ROOT_PATH_VAR
 - %sitePath% and %siteName% are set based on site path of device; e.g. if device is in "/World/CTC-Reading/VSP Sandbox" then %sitePath% = "World/CTC-Reading" and %siteName% = "VSP Sandbox"
- Can use these to have different CSV per site

Workflow execution



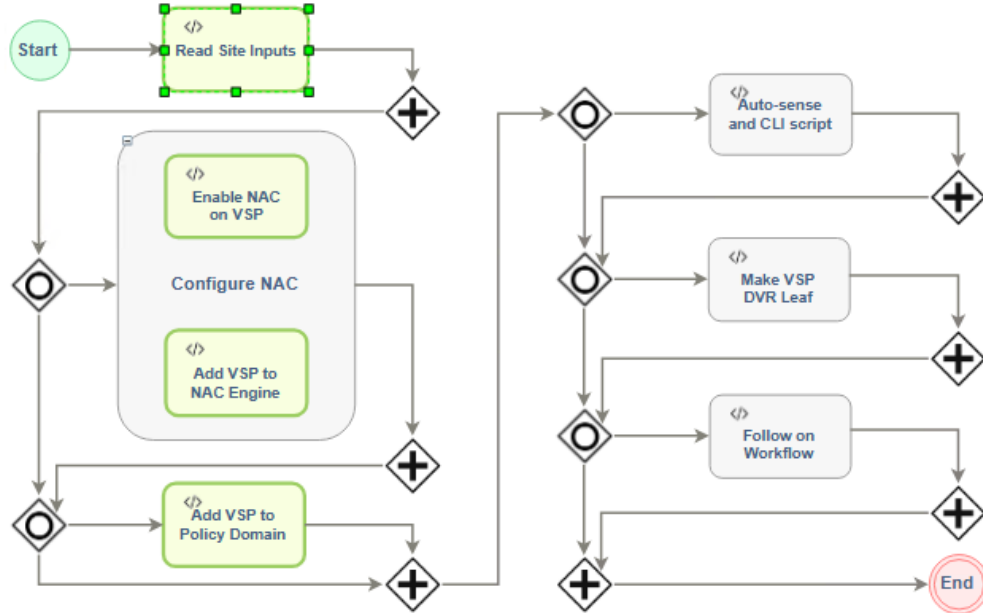
Summary

Status	Start Date/Time	Name	Version	Source	# Devices	Started By	End Date/Time	Message	Path
✓	2/7/2025 4:14:26 PM	Onboard VSP	155	Northbound Interfa...	1	NetSight Server	2/7/2025 4:15:01 PM	Added device 10.9.193.133 to Policy Domain...	/Workflows/Onboard VSP

Graph View Table View



Stop Workflow Show Output Show Variables



Devices Grid

Show Output

Status	Device IP	Output Path	Start Date/Time	End Date/Time	Message
SUCCESS	10.9.193.133		2/7/2025 4:14:...	2/7/2025 4:14:...	Validated i...

Output - 10.9.193.133

Activity: ReadSiteInputs_01
Input Data:

- VSP switch IP = 10.9.193.133
- Selected Switch Serial Number = SB012050G-00079
- Selected Switch MAC Address = F0:64:26:A8:E4:00
- Input CSV file =
- Key to CSV data =
- DVR Leaf = disable
- DVR Domain Id = None
- Network Access Control (NAC) = enable
- NAC Engine Group name = Default
- NAC Load Balancer enabled = 0
- NAC Load Balancer IP list = []
- NAC Engine IP list = [u'10.9.203.6']
- RADIUS Server ordered IP list = [u'10.9.203.6']
- RADIUS Client unordered IP list = [u'10.9.203.6']
- RADIUS Attributes template name = Extreme VOSS - Per-User ACL Org
- RADIUS Shared Secret = radius
- Create RADIUS Server for = eapol
- Location Group name =
- Add to Policy = enable
- Policy Domain = Default Policy Domain
- Policy VLAN Island Topology = Building1
- Auto-sense Voice I-SID =
- Auto-sense Voice VLAN-id =

Close

ALL RIGHTS RESERVED.

Additional CLI commands input / sample →

Additional CLI commands:

```
#No need to start with enable, config term; commented lines are ignored
#clock time-zone US Eastern
#snmp-server location ${location}
#snmp-server contact "Master of Disaster!"
```

- The additional CLI commands input can make use of the following variables:
 - Site variables **\${var}**: Useful to apply same values to all devices in same XIQ-SE Site. Or to apply same values to all devices in same sub-Sites
 - **Emc_vars** \${deviceIP}: Useful to feed some of these values into the same space as Site variables
 - CSV variables **\$<var>**: Useful to provide device specific values
 - Eval variables **\${var}**: Useful to compute new values within the template file and be able to store and re-use these values via a variable
- The additional CLI commands input can make use of the following pragmas
 - **#if/#elseif/#else/#end, #error fail|stop|continue, #eval / #eval <varname>=(), #sleep, #last**
 - but not: #block start|execute
- Please refer to documentation of the Apply Config Template workflow here:
 - https://github.com/extremenetworks/ExtremeScripting/blob/master/XMC_XIQ-SE/oneview_workflows/xwf/Apply_Config_Template_Workflow.pdf

```
#No need to start with enable, config term; commented lines are ignored
clock time-zone US Eastern
snmp-server location ${location}
snmp-server contact "Master of Disaster!"
no snmp-server community-by-index first
no snmp-server community-by-index second
router isis; spbm 1 multicast enable; exit
auto-sense eapol voice lldp-auth
ip dhcp-snooping enable
web-server password ro user // password // password
web-server password rwa admin // password // password
#if ("5520-24" in ${deviceType} or "5420-24" in ${deviceType})
    interface gigabitEthernet 1/1-1/24
        no snmp trap link-status
        slpp-guard enable timeout 0
        spanning-tree bpduguard enable timeout 0
        eapol re-authentication enable re-authentication-period 36000
    exit
#elseif("5520-48" in ${deviceType} or "5420-48" in ${deviceType})
    interface gigabitEthernet 1/1-1/48
        no snmp trap link-status
        slpp-guard enable timeout 0
        spanning-tree bpduguard enable timeout 0
        eapol re-authentication enable re-authentication-period 36000
    exit
#end
```