gluware
Intelligent Network Automation

APPLICATION NOTE

Performing a Network Assessment using Gluware

TABLE OF CONTENTS

OVERVIEW

Performing a network assessment is a recommended starting point for any project that involves equipment refresh planning, lifecycle management planning, network automation and many more initiatives that involve changes to the network infrastructure. It is critical to have current data regarding the inventory, configuration state and operational state before making changes.

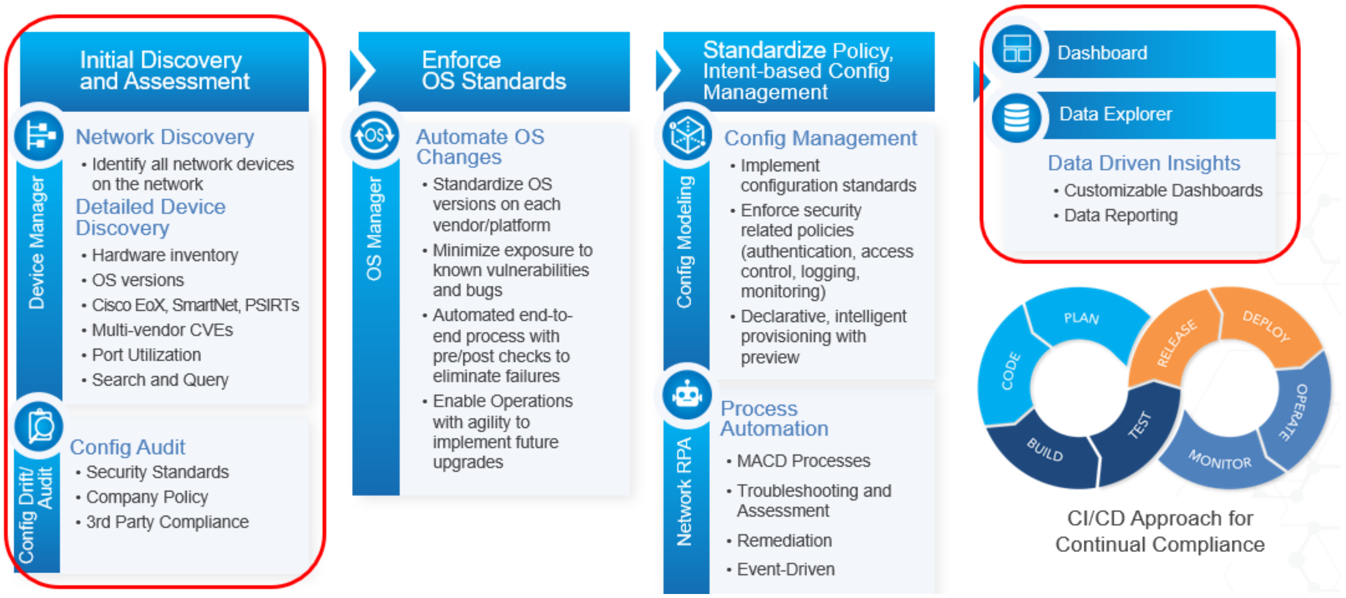

Initial Discovery and Assessment
Device Manager
Network Discovery
• Identify all network devices on the network
Detailed Device Discovery
• Hardware inventory
• OS versions
• Cisco EoX, SmartNet, PSIRTs
• Multi-vendor CVEs
• Port Utilization
• Search and Query
Config Drift/ Audit
Config Audit
• Security Standards
• Company Policy
• 3rd Party Compliance
Enforce OS Standards
OS Manager
Automate OS Changes
• Standardize OS versions on each vendor/platform
• Minimize exposure to known vulnerabilities and bugs
• Automated end-to-end process with pre/post checks to eliminate failures
• Enable Operations with agility to implement future upgrades
Standardize Policy, Intent-based Config Management
Config Modeling
Config Management
• Implement configuration standards
• Enforce security related policies (authentication, access control, logging, monitoring)
• Declarative, intelligent provisioning with preview
Network RPA
Process Automation
• MACD Processes
• Troubleshooting and Assessment
• Remediation
• Event-Driven
Dashboard
Data Explorer
Data Driven Insights
• Customizable Dashboards
• Data Reporting
PLAN
CODE
BUILD
TEST
RELEASE
DEPLOY
OPERATE
MONITOR
CI/CD Approach for Continual Compliance

Figure 1 Gluware Approach / Roadmap to Automate Your Network

Following the Gluware approach to automate your network, *Figure 1*, this application note will focus on the first phase, Initial Discovery and Assessment, along with reporting using Dashboard and Data Explorer. Gluware provides an Intelligent Network Automation solution that includes a suite of applications enabling turn-key functionality for discovery, drift detection, config audit, OS management, config management, process automation, reporting and more.

PERFORMING A NETWORK ASSESSMENT USING GLUWARE

The purpose of the assessment will create unique and specific requirements for what details are needed to be captured. For example, if the goal is a hardware refresh, then it will mostly be concerned with the age of the equipment and if it is going end-of-life (EoL) or end-of-support (EoS) either at a hardware or software level. Another example is if the purpose of the assessment is to enhance the security of the network, then the assessment will need to identify known vendor issues including Cisco PSIRTs and NIST CVEs along with specific security features and how they are configured. Since the purpose of the assessment can vary greatly, it is critical to have the capabilities and flexibility to meet the requirement of many diverse needs.

Gluware provides a solution that can accelerate the ability to perform the audit including the flexibility to capture the required data and perform an assessment of the inventory, config and operational state. The Gluware application suite provides out-of-the-box functionality with no coding required to accelerate the ability to perform initial and ongoing assessments.

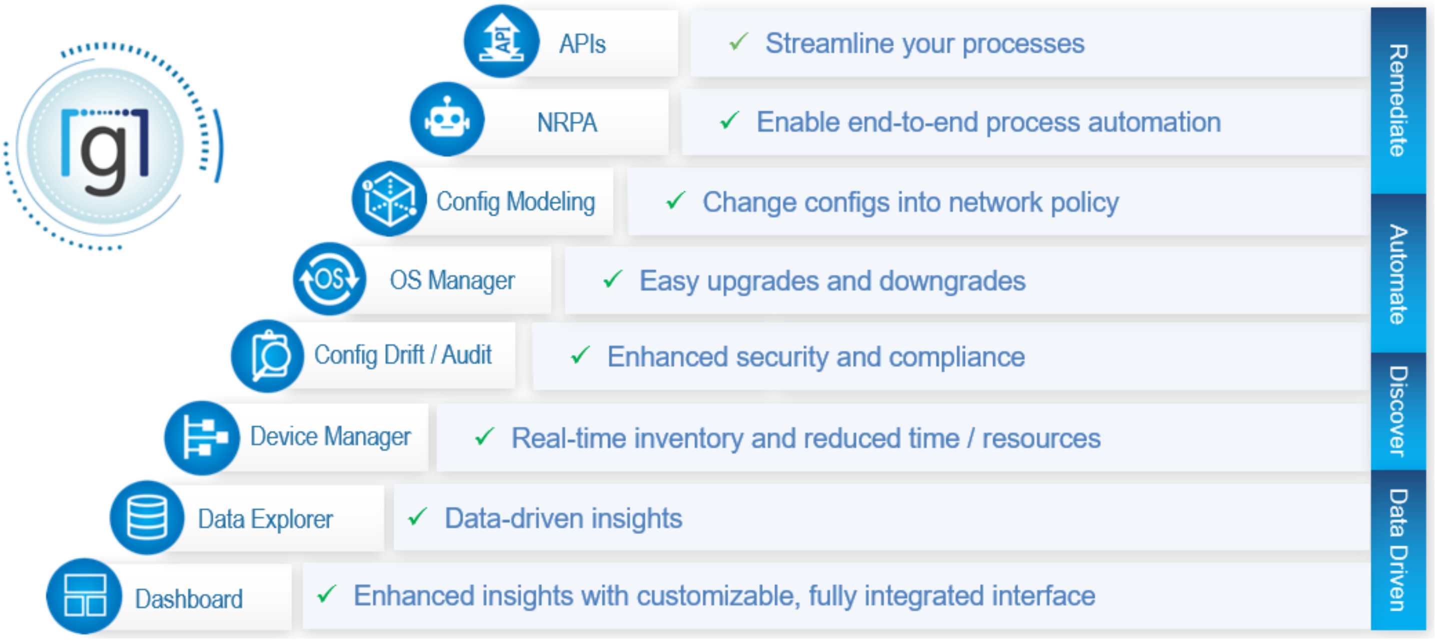

APIs
✓ Streamline your processes
NRPA
✓ Enable end-to-end process automation
Config Modeling
✓ Change configs into network policy
OS Manager
✓ Easy upgrades and downgrades
Config Drift / Audit
✓ Enhanced security and compliance
Device Manager
✓ Real-time inventory and reduced time / resources
Data Explorer
✓ Data-driven insights
Dashboard
✓ Enhanced insights with customizable, fully integrated interface
Remediate
Automate
Discover
Data Driven

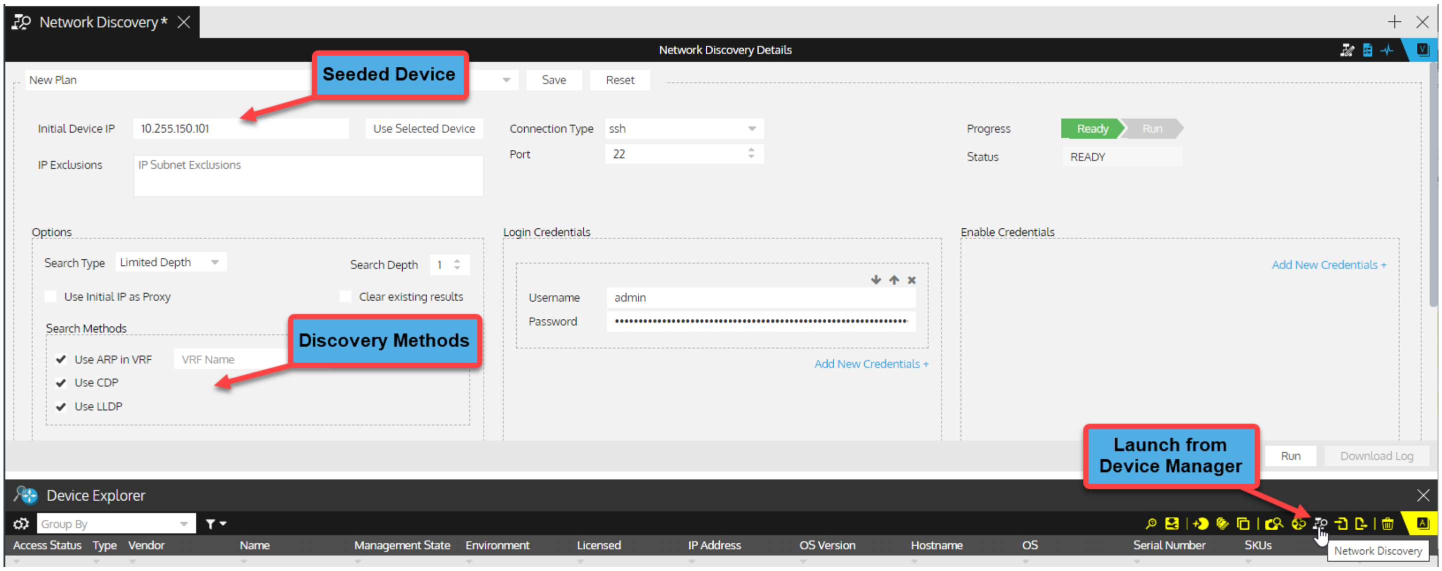
Figure 2 Gluware Intelligent Network Automation App Suite

In the Roadmap to Automate Your Network, *Figure 1*, the network assessment phase will make use of several applications in the suite including:

- Gluware Device Manager
  - Perform network discovery
  - Perform detailed device discovery
- Gluware Config and Audit
  - Perform standards-based configuration audit
  - Perform security standards audits (like CIS benchmarks)
- Gluware Topology
  - Assess visualization of the network diagram from global to site specific level
  - Generate site diagrams
- Gluware Ad-hoc Query and Config Modeling
  - Perform operational state assessment with ad-hoc query in Device Manager
  - Perform operational state assessment verification with Config Modeling
- Gluware Dashboard and Data Explorer
  - Generate dashboards to visualize data
  - Generate reports with Data Explorer

NETWORK DISCOVERY

The recommended first step in performing a network assessment is to have a detailed and accurate inventory of exactly what is connected to and running in the network. The Gluware Device Manager application provides the ability to execute a network discovery using a seeded device and network credentials. Via SSH or Telnet access, Gluware interrogates the devices ARP/CDP/LLDP tables to see the connected neighbors then crawls through the network hop-by-hop to capture all devices running in the network.



Seeded Device

Initial Device IP: 10.255.150.101

IP Exclusions

Connection Type: ssh

Port: 22

Progress: Ready → Run

Status: READY

Options

Search Type: Limited Depth

Search Depth: 1

□ Use Initial IP as Proxy

□ Clear existing results

Search Methods

✓ Use ARP in VRF

✓ Use CDP

✓ Use LLDP

Discovery Methods

Login Credentials

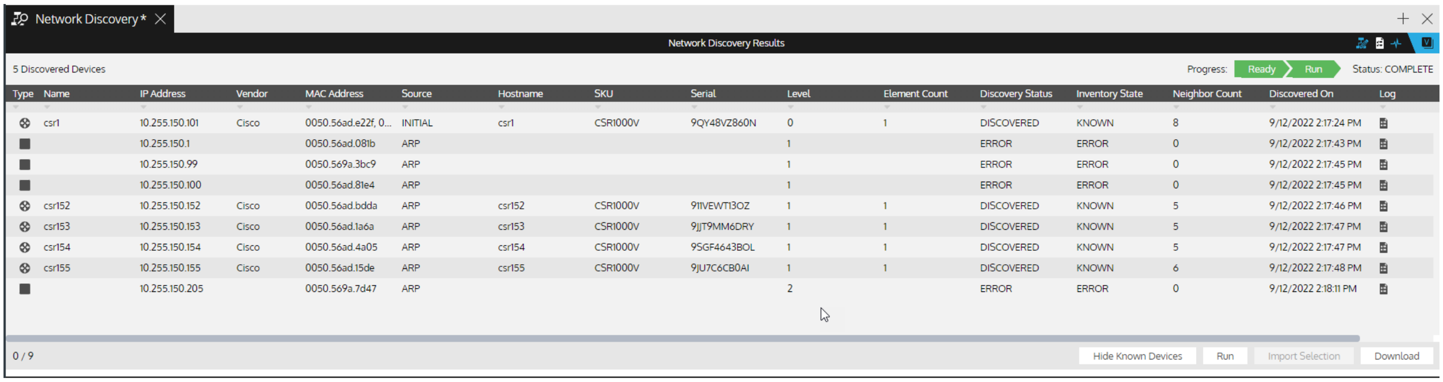
Username: admin

Password: ••

Enable Credentials

Launch from Device Manager

Figure 3 Gluware Network Discovery in Device Manager App



5 Discovered Devices

Progress: Ready → Run Status: COMPLETE

Type	Name	IP Address	Vendor	MAC Address	Source	Hostname	SKU	Serial	Level	Element Count	Discovery Status	Inventory State	Neighbor Count	Discovered On	Log
⊕	csr1	10.255.150.101	Cisco	0050.56ad.e22f, 0...	INITIAL	csr1	CSR1000V	9QY48VZ860N	0	1	DISCOVERED	KNOWN	8	9/12/2022 2:17:24 PM	▤
■		10.255.150.1		0050.56ad.081b	ARP				1		ERROR	ERROR	0	9/12/2022 2:17:43 PM	▤
■		10.255.150.99		0050.569a.3bc9	ARP				1		ERROR	ERROR	0	9/12/2022 2:17:45 PM	▤
■		10.255.150.100		0050.56ad.81e4	ARP				1		ERROR	ERROR	0	9/12/2022 2:17:45 PM	▤
⊕	csr152	10.255.150.152	Cisco	0050.56ad.bdda	ARP	csr152	CSR1000V	911VEWT13OZ	1	1	DISCOVERED	KNOWN	5	9/12/2022 2:17:46 PM	▤
⊕	csr153	10.255.150.153	Cisco	0050.56ad.1a6a	ARP	csr153	CSR1000V	9JJT9MM6DRY	1	1	DISCOVERED	KNOWN	5	9/12/2022 2:17:47 PM	▤
⊕	csr154	10.255.150.154	Cisco	0050.56ad.4a05	ARP	csr154	CSR1000V	9SGF4643BOL	1	1	DISCOVERED	KNOWN	5	9/12/2022 2:17:47 PM	▤
⊕	csr155	10.255.150.155	Cisco	0050.56ad.15de	ARP	csr155	CSR1000V	9JU7C6CB0AI	1	1	DISCOVERED	KNOWN	6	9/12/2022 2:17:48 PM	▤
■		10.255.150.205		0050.569a.7d47	ARP				2		ERROR	ERROR	0	9/12/2022 2:18:11 PM	▤

0 / 9

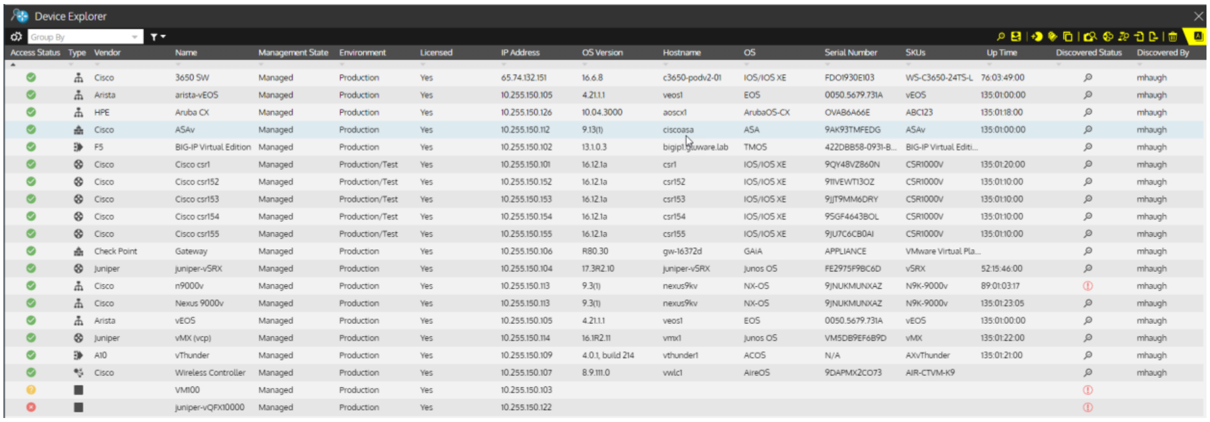
Figure 4 Gluware Network Discovery Results

Use the Network Discovery Results to:

- ✓ Identify and resolve any network reachability or credential issues.
- ✓ Compare the identified network inventory to any existing documents and identify differences.
- ✓ Download and export the list to be able to use the MAC OUI to identify endpoint vendors.
- ✓ Import all network devices into Gluware Device Manager for continued assessment.

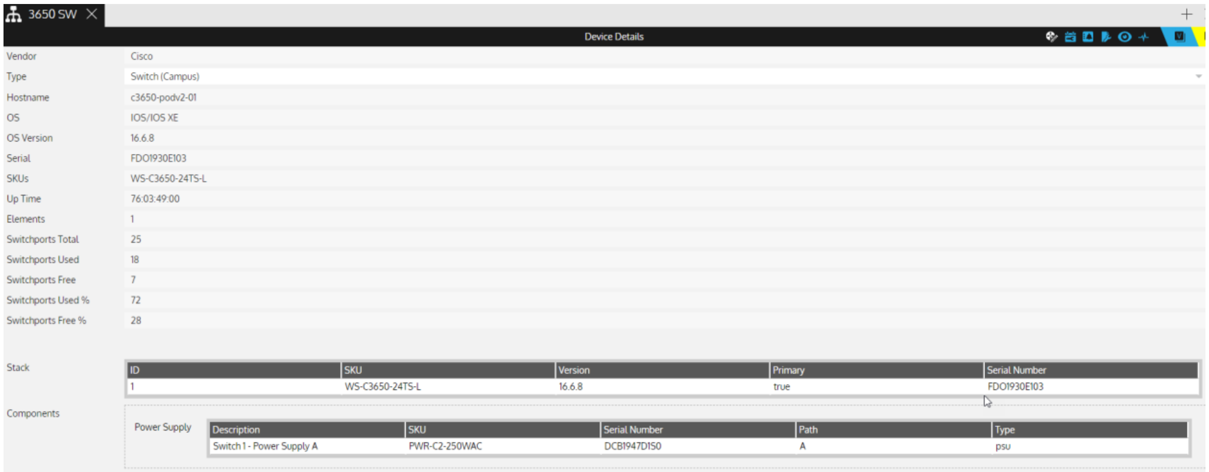
DETAILED DEVICE DISCOVERY

The next step recommended in the assessment process is to complete a detailed device inventory that captures the hardware, operating system and operational state details. The Gluware Device Manager app performs a device detect and deep discovery identifying the vendor, OS and additional details about the hardware, OS version and operating state. The device data is stored in an internal database. That data is available in several ways including the Device Explorer grid, the device details view, the Dashboard view and Data Explorer reports. The Device Explorer grid supports searching, sorting, filtering and more to help assess the data.



Access Status	Type	Vendor	Name	Management State	Environment	Licensed	IP Address	OS Version	Hostname	OS	Serial Number	SKUs	Up Time	Discovered Status	Discovered By
✓		Cisco	3650 SW	Managed	Production	Yes	65.74.132.151	16.6.8	c3650-podv2-01	IOS/IOS XE	FDO1930E103	WS-C3650-24TS-L	76:03:49:00	🔍	mhaugh
✓		Arista	arista-vEOS	Managed	Production	Yes	10.255.150.105	4.21.1.1	veos1	EOS	0050.5679.731A	vEOS	135:01:00:00	🔍	mhaugh
✓		HPE	Aruba CX	Managed	Production	Yes	10.255.150.126	10.04.3000	aoscx1	ArubaOS-CX	OVAB6A66E	ABC123	135:01:18:00	🔍	mhaugh
✓		Cisco	ASAv	Managed	Production	Yes	10.255.150.112	9.13(1)	ciscoasa	ASA	9AK93TMFEDG	ASAv	135:01:00:00	🔍	mhaugh
✓		F5	BIG-IP Virtual Edition	Managed	Production	Yes	10.255.150.102	13.1.0.3	bigip1.gluware.lab	TMOS	422DBB58-0931-B...	BIG-IP Virtual Editi...		🔍	mhaugh
✓		Cisco	Cisco csr1	Managed	Production/Test	Yes	10.255.150.101	16.12.1a	csr1	IOS/IOS XE	9QY48VZ860N	CSR1000V	135:01:20:00	🔍	mhaugh
✓		Cisco	Cisco csr152	Managed	Production/Test	Yes	10.255.150.152	16.12.1a	csr152	IOS/IOS XE	9IIVEWT13OZ	CSR1000V	135:01:10:00	🔍	mhaugh
✓		Cisco	Cisco csr153	Managed	Production/Test	Yes	10.255.150.153	16.12.1a	csr153	IOS/IOS XE	9JJT9MM6DRY	CSR1000V	135:01:10:00	🔍	mhaugh
✓		Cisco	Cisco csr154	Managed	Production/Test	Yes	10.255.150.154	16.12.1a	csr154	IOS/IOS XE	9SGF4643BOL	CSR1000V	135:01:10:00	🔍	mhaugh
✓		Cisco	Cisco csr155	Managed	Production/Test	Yes	10.255.150.155	16.12.1a	csr155	IOS/IOS XE	9JU7C6CB0AI	CSR1000V	135:01:10:00	🔍	mhaugh
✓		Check Point	Gateway	Managed	Production	Yes	10.255.150.106	R80.30	gw-16372d	GAiA	APPLIANCE	VMware Virtual Pla...		🔍	mhaugh
✓		Juniper	juniper-vSRX	Managed	Production	Yes	10.255.150.104	17.3R2.10	juniper-vSRX	Junos OS	FE2975F9BC6D	vSRX	52:15:46:00	🔍	mhaugh
✓		Cisco	n9000v	Managed	Production	Yes	10.255.150.113	9.3(1)	nexus9kv	NX-OS	9JNUKMUNXAZ	N9K-9000v	89:01:03:17	!	mhaugh
✓		Cisco	Nexus 9000v	Managed	Production	Yes	10.255.150.113	9.3(1)	nexus9kv	NX-OS	9JNUKMUNXAZ	N9K-9000v	135:01:23:05	🔍	mhaugh
✓		Arista	vEOS	Managed	Production	Yes	10.255.150.105	4.21.1.1	veos1	EOS	0050.5679.731A	vEOS	135:01:00:00	🔍	mhaugh
✓		Juniper	vMX (vcp)	Managed	Production	Yes	10.255.150.114	16.1R2.11	vmx1	Junos OS	VM5DB9EF6B9D	vMX	135:01:22:00	🔍	mhaugh
✓		A10	vThunder	Managed	Production	Yes	10.255.150.109	4.0.1, build 214	vthunder1	ACOS	N/A	AXvThunder	135:01:21:00	🔍	mhaugh
✓		Cisco	Wireless Controller	Managed	Production	Yes	10.255.150.107	8.9.111.0	vwlc1	AireOS	9DAPMX2CO73	AIR-CTVM-K9		🔍	mhaugh
?	■		VM100	Managed	Production	Yes	10.255.150.103							!	
✕	■		juniper-vQFX10000	Managed	Production	Yes	10.255.150.122							!	

Figure 5 Gluware Device Explorer in Device Manager App



Vendor	Cisco
Type	Switch (Campus)
Hostname	c3650-podv2-01
OS	IOS/IOS XE
OS Version	16.6.8
Serial	FDO1930E103
SKUs	WS-C3650-24TS-L
Up Time	76:03:49:00
Elements	1
Switchports Total	25
Switchports Used	18
Switchports Free	7
Switchports Used %	72
Switchports Free %	28

Stack

ID	SKU	Version	Primary	Serial Number
1	WS-C3650-24TS-L	16.6.8	true	FDO1930E103

Components

Power Supply

Description	SKU	Serial Number	Path	Type
Switch 1 - Power Supply A	PWR-C2-250WAC	DCB1947D1S0	A	psu

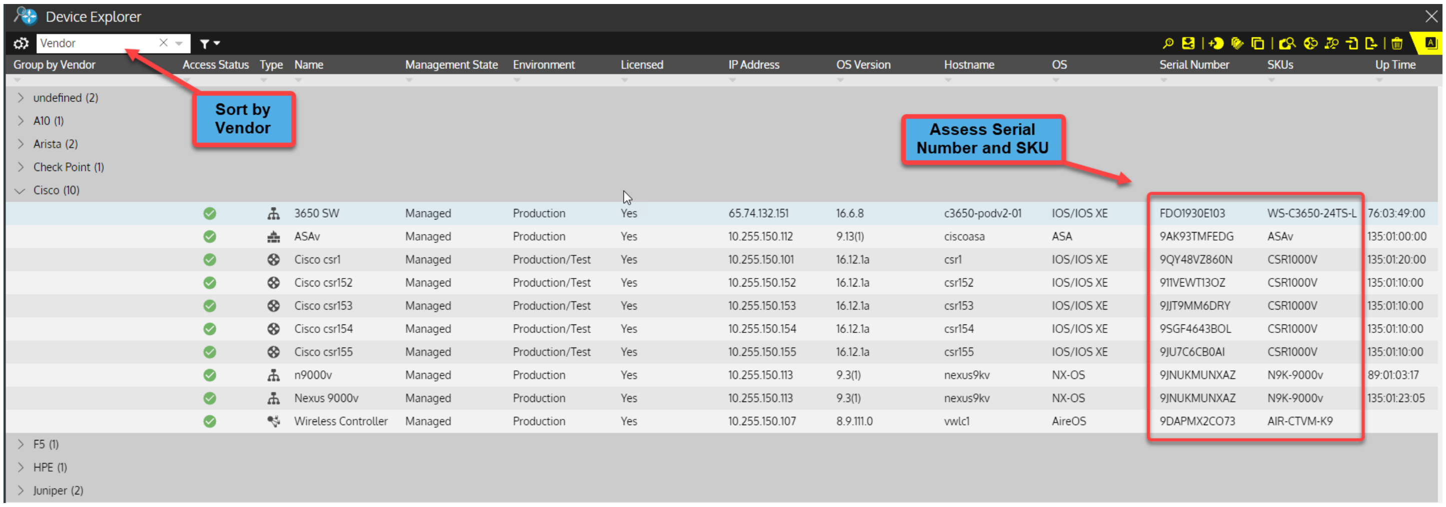
Figure 6 Detailed Device View in the Device Manager App

Use the Device Discovery Results to:

- ✓ Assess the hardware inventory including vendor, model, SKUs, and components
- ✓ Assess the OS versions running in the network
- ✓ Leverage the Cisco API integration to assess SmartNet status, EoX, and PSIRTs (security vulnerabilites)
- ✓ Leverage the NIST API integration to assess multi-vendor CVEs (security vulnerabilities)

Hardware Inventory

Use Device Manager to assess each vendor and understand exactly what platforms are running in your network. Dive deeper into the platform components like line cards, power supplies and more.

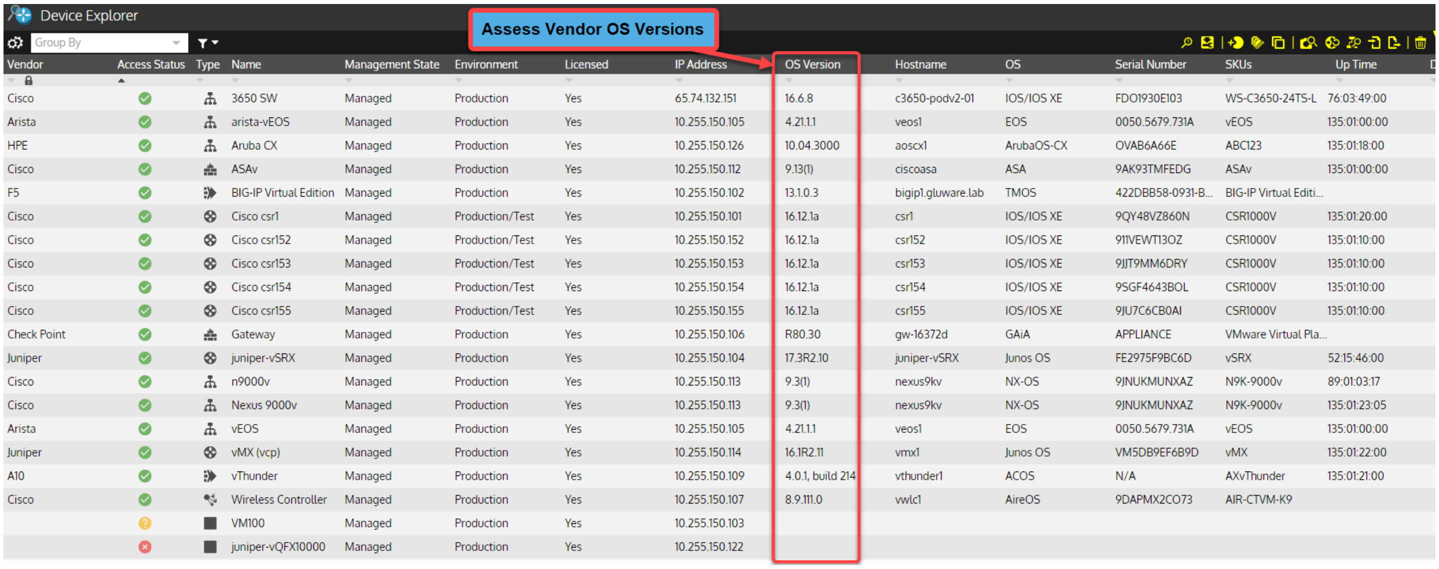


Group by Vendor	Access Status	Type	Name	Management State	Environment	Licensed	IP Address	OS Version	Hostname	OS	Serial Number	SKUs	Up Time
undefined (2)													
A10 (1)													
Arista (2)													
Check Point (1)													
Cisco (10)													
	✓		3650 SW	Managed	Production	Yes	65.74.132.151	16.6.8	c3650-podv2-01	IOS/IOS XE	FDO1930E103	WS-C3650-24TS-L	76:03:49:00
	✓		ASAv	Managed	Production	Yes	10.255.150.112	9.13(1)	ciscoasa	ASA	9AK93TMFEDG	ASAv	135:01:00:00
	✓		Cisco csr1	Managed	Production/Test	Yes	10.255.150.101	16.12.1a	csr1	IOS/IOS XE	9QY48VZ860N	CSR1000V	135:01:20:00
	✓		Cisco csr152	Managed	Production/Test	Yes	10.255.150.152	16.12.1a	csr152	IOS/IOS XE	91IVEWT13OZ	CSR1000V	135:01:10:00
	✓		Cisco csr153	Managed	Production/Test	Yes	10.255.150.153	16.12.1a	csr153	IOS/IOS XE	9JJT9MM6DRY	CSR1000V	135:01:10:00
	✓		Cisco csr154	Managed	Production/Test	Yes	10.255.150.154	16.12.1a	csr154	IOS/IOS XE	9SGF4643BOL	CSR1000V	135:01:10:00
	✓		Cisco csr155	Managed	Production/Test	Yes	10.255.150.155	16.12.1a	csr155	IOS/IOS XE	9JU7C6CB0AI	CSR1000V	135:01:10:00
	✓		n9000v	Managed	Production	Yes	10.255.150.113	9.3(1)	nexus9kv	NX-OS	9JNUKMUNXAZ	N9K-9000v	89:01:03:17
	✓		Nexus 9000v	Managed	Production	Yes	10.255.150.113	9.3(1)	nexus9kv	NX-OS	9JNUKMUNXAZ	N9K-9000v	135:01:23:05
	✓		Wireless Controller	Managed	Production	Yes	10.255.150.107	8.9.111.0	vwlc1	AireOS	9DAPMX2CO73	AIR-CTVM-K9	
F5 (1)													
HPE (1)													
Juniper (2)													

Figure 7 Use Device Explorer Sort, Search and Filter to Assess Hardware

Operating System

Use Device Manager to assess each vendor operating system (OS) and assess if standards have been implemented and enforced. Non-standard operating systems will result in security vulnerabilities and inconsistencies in features and performance.



Assess Vendor OS Versions

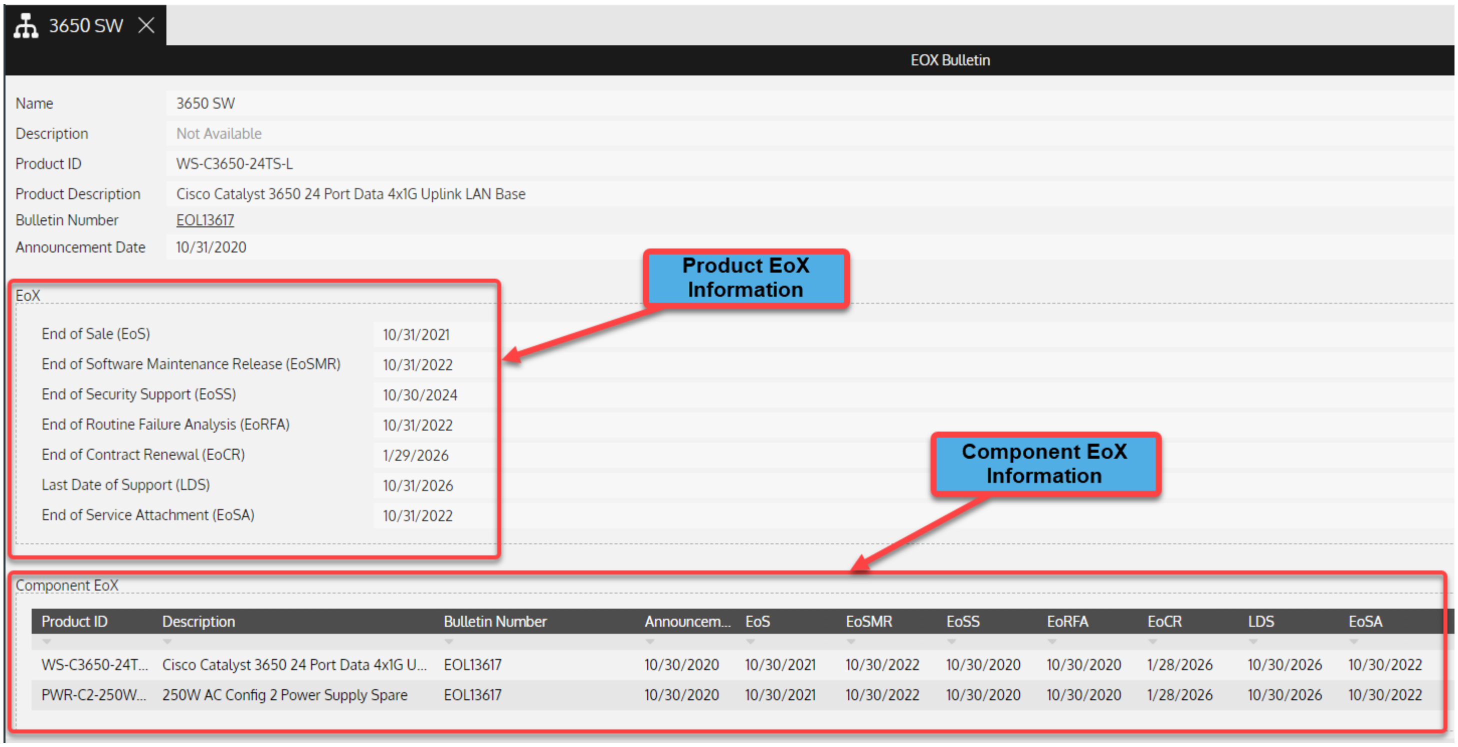
Vendor	Access Status	Type	Name	Management State	Environment	Licensed	IP Address	OS Version	Hostname	OS	Serial Number	SKUs	Up Time	D
Cisco	✓		3650 SW	Managed	Production	Yes	65.74.132.151	16.6.8	c3650-podv2-01	IOS/IOS XE	FDO1930E103	WS-C3650-24TS-L	76:03:49:00	
Arista	✓		arista-vEOS	Managed	Production	Yes	10.255.150.105	4.21.1.1	veos1	EOS	0050.5679.731A	vEOS	135:01:00:00	
HPE	✓		Aruba CX	Managed	Production	Yes	10.255.150.126	10.04.3000	aoscx1	ArubaOS-CX	OVAB6A66E	ABC123	135:01:18:00	
Cisco	✓		ASAv	Managed	Production	Yes	10.255.150.112	9.13(1)	ciscoasa	ASA	9AK93TMFEDG	ASAv	135:01:00:00	
F5	✓		BIG-IP Virtual Edition	Managed	Production	Yes	10.255.150.102	13.1.0.3	bigip1.gluware.lab	TMOS	422DBB58-0931-B...	BIG-IP Virtual Editi...		
Cisco	✓		Cisco csr1	Managed	Production/Test	Yes	10.255.150.101	16.12.1a	csr1	IOS/IOS XE	9QY48VZ860N	CSR1000V	135:01:20:00	
Cisco	✓		Cisco csr152	Managed	Production/Test	Yes	10.255.150.152	16.12.1a	csr152	IOS/IOS XE	911VEWT13OZ	CSR1000V	135:01:10:00	
Cisco	✓		Cisco csr153	Managed	Production/Test	Yes	10.255.150.153	16.12.1a	csr153	IOS/IOS XE	9JJT9MM6DRY	CSR1000V	135:01:10:00	
Cisco	✓		Cisco csr154	Managed	Production/Test	Yes	10.255.150.154	16.12.1a	csr154	IOS/IOS XE	9SGF4643BOL	CSR1000V	135:01:10:00	
Cisco	✓		Cisco csr155	Managed	Production/Test	Yes	10.255.150.155	16.12.1a	csr155	IOS/IOS XE	9JU7C6CB0AI	CSR1000V	135:01:10:00	
Check Point	✓		Gateway	Managed	Production	Yes	10.255.150.106	R80.30	gw-16372d	GAiA	APPLIANCE	VMware Virtual Pla...		
Juniper	✓		juniper-vSRX	Managed	Production	Yes	10.255.150.104	17.3R2.10	juniper-vSRX	Junos OS	FE2975F9BC6D	vSRX	52:15:46:00	
Cisco	✓		n9000v	Managed	Production	Yes	10.255.150.113	9.3(1)	nexus9kv	NX-OS	9JNUKMUNXAZ	N9K-9000v	89:01:03:17	
Cisco	✓		Nexus 9000v	Managed	Production	Yes	10.255.150.113	9.3(1)	nexus9kv	NX-OS	9JNUKMUNXAZ	N9K-9000v	135:01:23:05	
Arista	✓		vEOS	Managed	Production	Yes	10.255.150.105	4.21.1.1	veos1	EOS	0050.5679.731A	vEOS	135:01:00:00	
Juniper	✓		vMX (vcp)	Managed	Production	Yes	10.255.150.114	16.1R2.11	vmx1	Junos OS	VM5DB9EF6B9D	vMX	135:01:22:00	
A10	✓		vThunder	Managed	Production	Yes	10.255.150.109	4.0.1, build 214	vthunder1	ACOS	N/A	AXvThunder	135:01:21:00	
Cisco	✓		Wireless Controller	Managed	Production	Yes	10.255.150.107	8.9.111.0	vwlc1	AireOS	9DAPMX2CO73	AIR-CTVM-K9		
	?	■	VM100	Managed	Production	Yes	10.255.150.103							
	✗	■	juniper-vQFX10000	Managed	Production	Yes	10.255.150.122							

Figure 8 Use Device Explorer to Assess the Vendor Operating Systems

Cisco Support API Integration

Gluware provides integration with the Cisco Support API to provide value added assessments that include end-of-life/end-of-sales (EoX), SmartNet status, PSIRT information and more. The seven API calls Gluware integrates with include:

1. Hello API
2. EOX V5 API
3. Product info API 1.0
4. Serial Number to Information API Version 2
5. Automated Software Distribution
6. Software Suggestion API V2
7. Cisco PSIRT openVuln API



EOX Bulletin

Name	3650 SW
Description	Not Available
Product ID	WS-C3650-24TS-L
Product Description	Cisco Catalyst 3650 24 Port Data 4x1G Uplink LAN Base
Bulletin Number	EOL13617
Announcement Date	10/31/2020

Product EoX Information

EoX

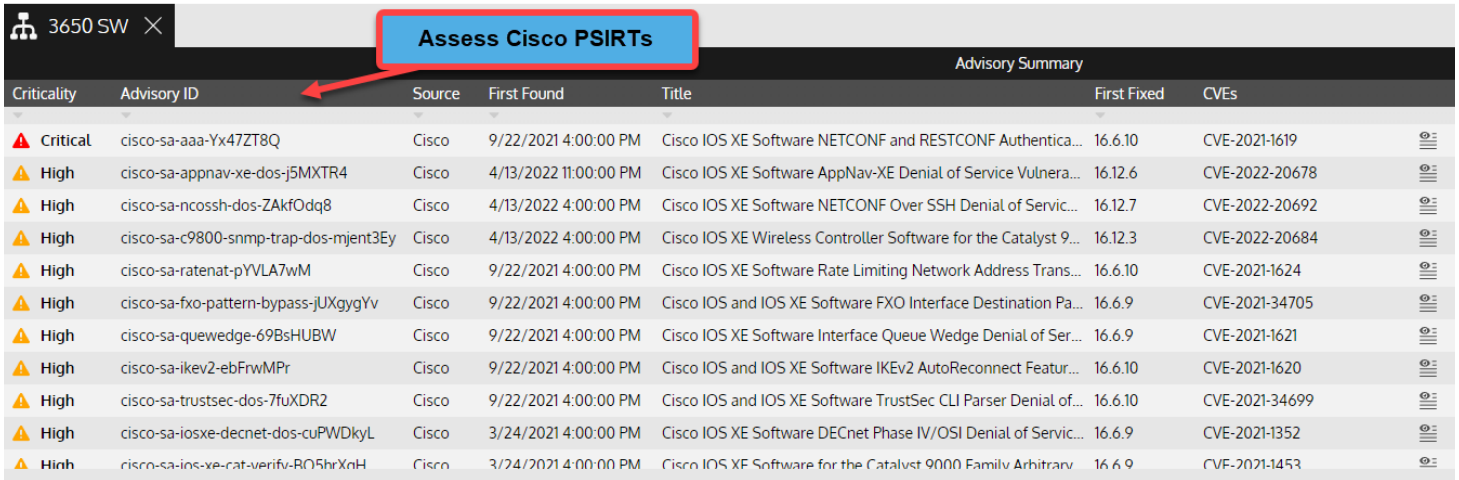
End of Sale (EoS)	10/31/2021
End of Software Maintenance Release (EoSMR)	10/31/2022
End of Security Support (EoSS)	10/30/2024
End of Routine Failure Analysis (EoRFA)	10/31/2022
End of Contract Renewal (EoCR)	1/29/2026
Last Date of Support (LDS)	10/31/2026
End of Service Attachment (EoSA)	10/31/2022

Component EoX Information

Component EoX

Product ID	Description	Bulletin Number	Announcem...	EoS	EoSMR	EoSS	EoRFA	EoCR	LDS	EoSA
WS-C3650-24T...	Cisco Catalyst 3650 24 Port Data 4x1G U...	EOL13617	10/30/2020	10/30/2021	10/30/2022	10/30/2020	10/30/2020	1/28/2026	10/30/2026	10/30/2022
PWR-C2-250W...	250W AC Config 2 Power Supply Spare	EOL13617	10/30/2020	10/30/2021	10/30/2022	10/30/2020	10/30/2020	1/28/2026	10/30/2026	10/30/2022

Figure 9 Device Manager Cisco API Integration for EoX Information

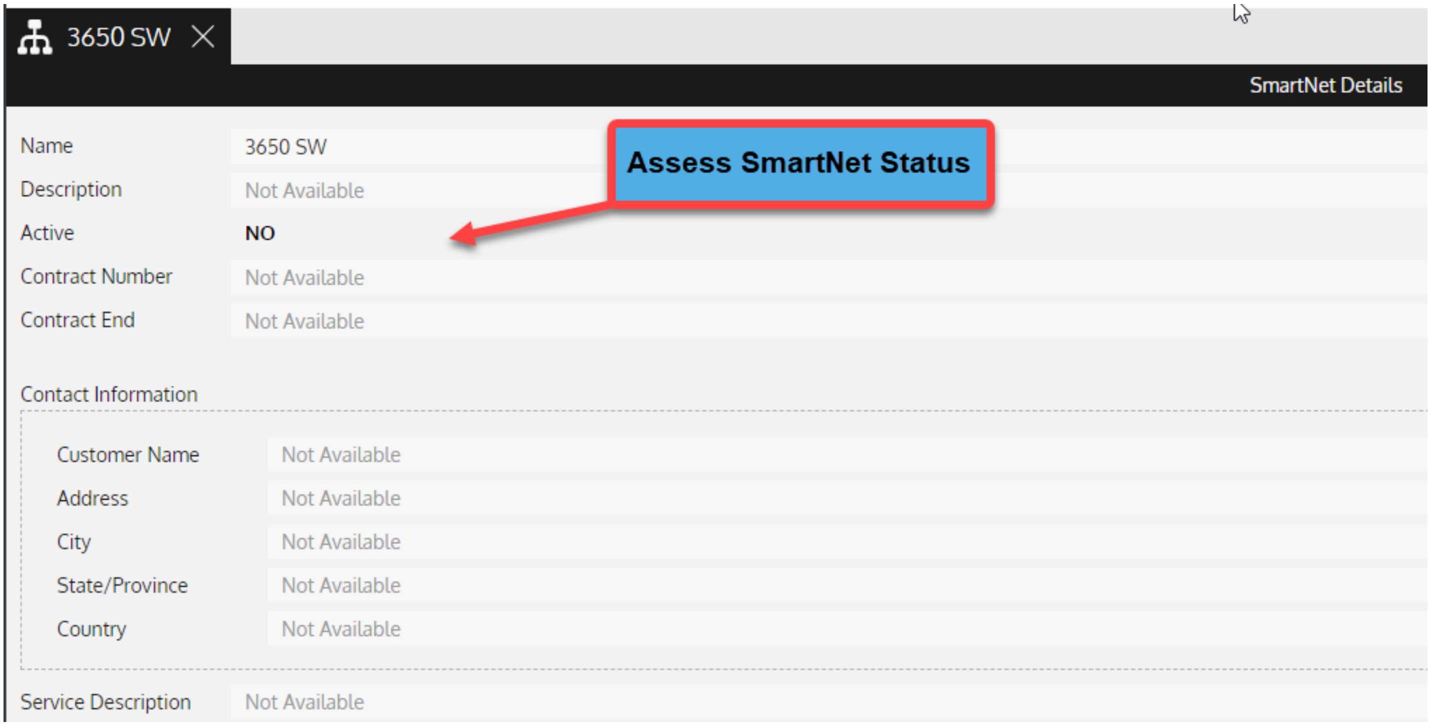


Assess Cisco PSIRTs

Advisory Summary

Criticality	Advisory ID	Source	First Found	Title	First Fixed	CVEs
Critical	cisco-sa-aaa-Yx47ZT8Q	Cisco	9/22/2021 4:00:00 PM	Cisco IOS XE Software NETCONF and RESTCONF Authentica...	16.6.10	CVE-2021-1619
High	cisco-sa-appnav-xe-dos-j5MXTR4	Cisco	4/13/2022 11:00:00 PM	Cisco IOS XE Software AppNav-XE Denial of Service Vulnera...	16.12.6	CVE-2022-20678
High	cisco-sa-ncossh-dos-ZAkfOdq8	Cisco	4/13/2022 4:00:00 PM	Cisco IOS XE Software NETCONF Over SSH Denial of Servic...	16.12.7	CVE-2022-20692
High	cisco-sa-c9800-snmp-trap-dos-mjent3Ey	Cisco	4/13/2022 4:00:00 PM	Cisco IOS XE Wireless Controller Software for the Catalyst 9...	16.12.3	CVE-2022-20684
High	cisco-sa-ratenat-pYVLA7wM	Cisco	9/22/2021 4:00:00 PM	Cisco IOS XE Software Rate Limiting Network Address Trans...	16.6.10	CVE-2021-1624
High	cisco-sa-fxo-pattern-bypass-jUXgygYv	Cisco	9/22/2021 4:00:00 PM	Cisco IOS and IOS XE Software FXO Interface Destination Pa...	16.6.9	CVE-2021-34705
High	cisco-sa-quewedge-69BsHUBW	Cisco	9/22/2021 4:00:00 PM	Cisco IOS XE Software Interface Queue Wedge Denial of Ser...	16.6.9	CVE-2021-1621
High	cisco-sa-ikev2-ebFrwMPr	Cisco	9/22/2021 4:00:00 PM	Cisco IOS and IOS XE Software IKEv2 AutoReconnect Featur...	16.6.10	CVE-2021-1620
High	cisco-sa-trustsec-dos-7fuXDR2	Cisco	9/22/2021 4:00:00 PM	Cisco IOS and IOS XE Software TrustSec CLI Parser Denial of...	16.6.10	CVE-2021-34699
High	cisco-sa-iosxe-decnet-dos-cuPWDkyL	Cisco	3/24/2021 4:00:00 PM	Cisco IOS XE Software DECnet Phase IV/OSI Denial of Servic...	16.6.9	CVE-2021-1352
High	cisco-sa-ios-xe-cat-verify-BQ5hrXgH	Cisco	3/24/2021 4:00:00 PM	Cisco IOS XE Software for the Catalyst 9000 Family Arbitrary	16.6.9	CVE-2021-1453

Figure 10 Use Device Manager to Assess Cisco PSIRTs (Security Vulnerabilities)



Name	3650 SW
Description	Not Available
Active	**NO**
Contract Number	Not Available
Contract End	Not Available

Contact Information

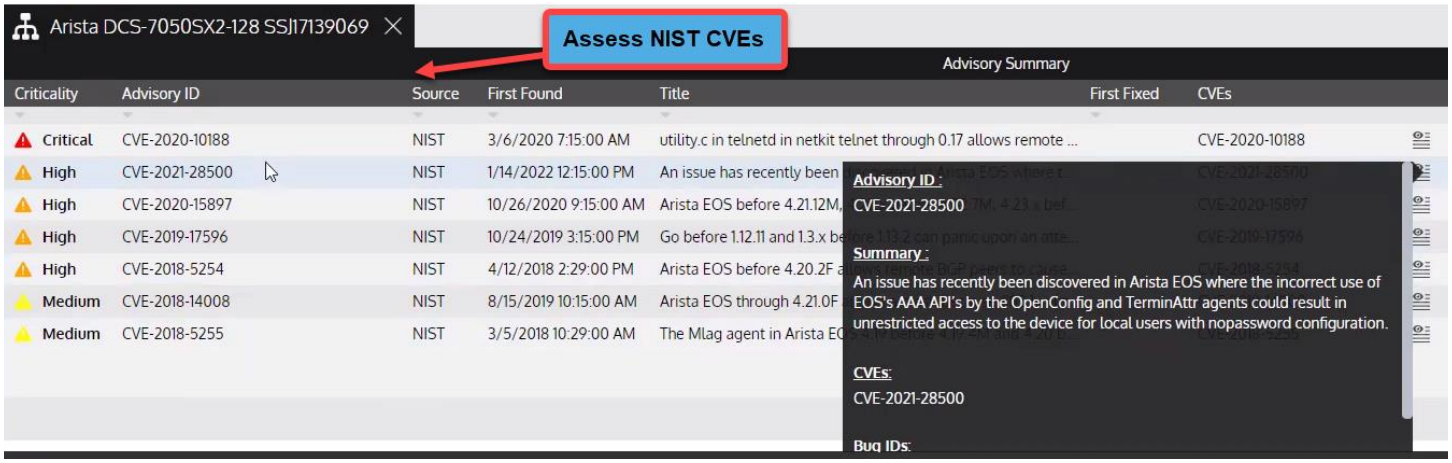
Customer Name	Not Available
Address	Not Available
City	Not Available
State/Province	Not Available
Country	Not Available

Service Description	Not Available

Figure 11 Use Device Manager to Assess Cisco SmartNet Status

NIST API Integration

Gluware provides integration with NIST National Vulnerability Database via APIs to capture multi-vendor Common Vulnerabilites and Exposures (CVEs). This information can help in the assessment of the running operating system and if a configuration work-around or upgrade is required to eliminate exposure to a known vendor vulnerability.



Criticality	Advisory ID	Source	First Found	Title	First Fixed	CVEs
▲ Critical	CVE-2020-10188	NIST	3/6/2020 7:15:00 AM	utility.c in telnetd in netkit telnet through 0.17 allows remote ...		CVE-2020-10188
▲ High	CVE-2021-28500	NIST	1/14/2022 12:15:00 PM	An issue has recently been discovered in Arista EOS where t...		CVE-2021-28500
▲ High	CVE-2020-15897	NIST	10/26/2020 9:15:00 AM	Arista EOS before 4.21.12M, [illegible] 7M, 4.23.x bef...		CVE-2020-15897
▲ High	CVE-2019-17596	NIST	10/24/2019 3:15:00 PM	Go before 1.12.11 and 1.3.x before 1.13.2 can panic upon an atte...		CVE-2019-17596
▲ High	CVE-2018-5254	NIST	4/12/2018 2:29:00 PM	Arista EOS before 4.20.2F allows remote BGP peers to cause...		CVE-2018-5254
▲ Medium	CVE-2018-14008	NIST	8/15/2019 10:15:00 AM	Arista EOS through 4.21.0F [illegible]		[illegible]
▲ Medium	CVE-2018-5255	NIST	3/5/2018 10:29:00 AM	The Mlag agent in Arista EOS 4.19 before 4.19.4M and 4.20 b...		CVE-2018-5255

Advisory ID :
CVE-2021-28500

Summary :
An issue has recently been discovered in Arista EOS where the incorrect use of EOS's AAA API's by the OpenConfig and TerminAttr agents could result in unrestricted access to the device for local users with nopassword configuration.

CVEs:
CVE-2021-28500

Bug IDs:

Figure 12 Use Device Manager to Assess NIST Multi-Vendor CVEs

CONFIGURATION AUDIT

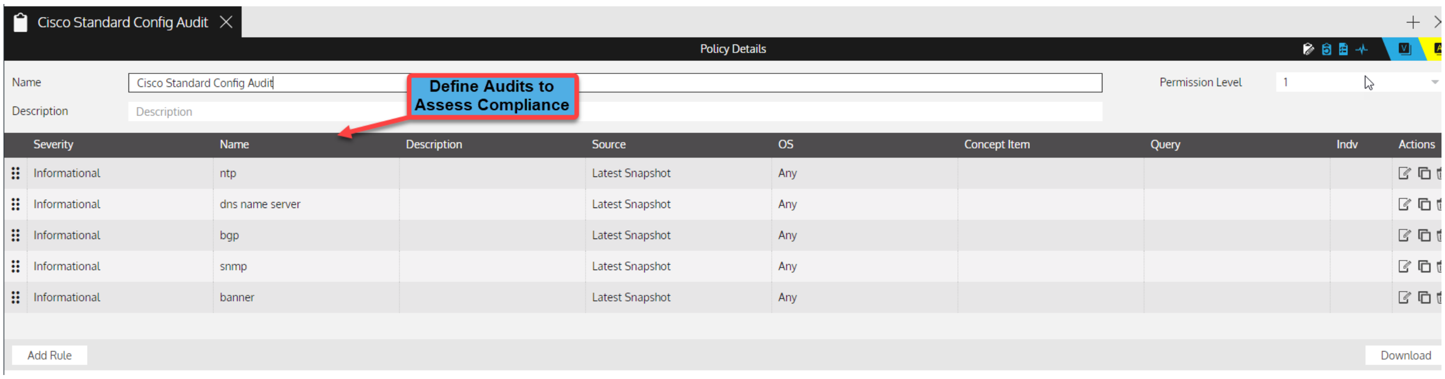
The third major phase recommended in an assessment is to evaluate device configurations for company standards, external compliance and security standards. The Gluware Config Drift and Audit app enables users to execute multi-vendor, multi-platform audits without any coding required. Users can easily define audits for company policy, ad-hoc policy and standards-based policies. Audit policies can be comprised of multiple rules defining required or forbidden configuration statements. Audit rules are built using native vendor CLI along with RegEx supported for configuration policy. Audits can be run network-wide, or on a specific set of devices and can be manually run, triggered, or scheduled. Results are available in the UI and can be downloaded in csv format.

Use Audits to assess configurations for:

- ✓ Standard company policies
- ✓ 3rd party compliance audits
- ✓ Security standard audits

Audit for Standard Configs

Enterprise IT typically has “gold standard” configurations, or at least configuration standard snippets for specific configuration components like banner, AAA, DNS, NTP, Routing, QoS and more. Gluware users can easily build audit policies to assess the device configurations and highlight any violations.



Define Audits to Assess Compliance

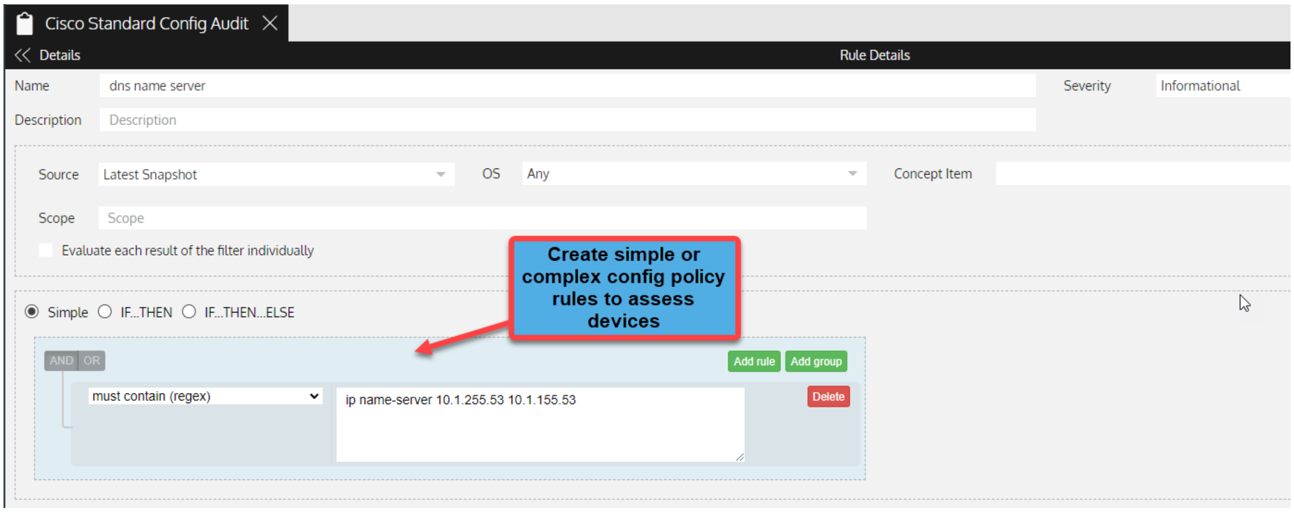
Name: Cisco Standard Config Audit

Description: Description

Permission Level: 1

Severity	Name	Description	Source	OS	Concept Item	Query	Indv	Actions
Informational	ntp		Latest Snapshot	Any				
Informational	dns name server		Latest Snapshot	Any				
Informational	bgp		Latest Snapshot	Any				
Informational	snmp		Latest Snapshot	Any				
Informational	banner		Latest Snapshot	Any				

Figure 13 Use Config Drift and Audit to Assess Configurations



Name: dns name server

Severity: Informational

Description: Description

Source: Latest Snapshot

OS: Any

Concept Item

Scope: Scope

☐ Evaluate each result of the filter individually

● Simple ○ IF...THEN ○ IF...THEN...ELSE

must contain (regex)

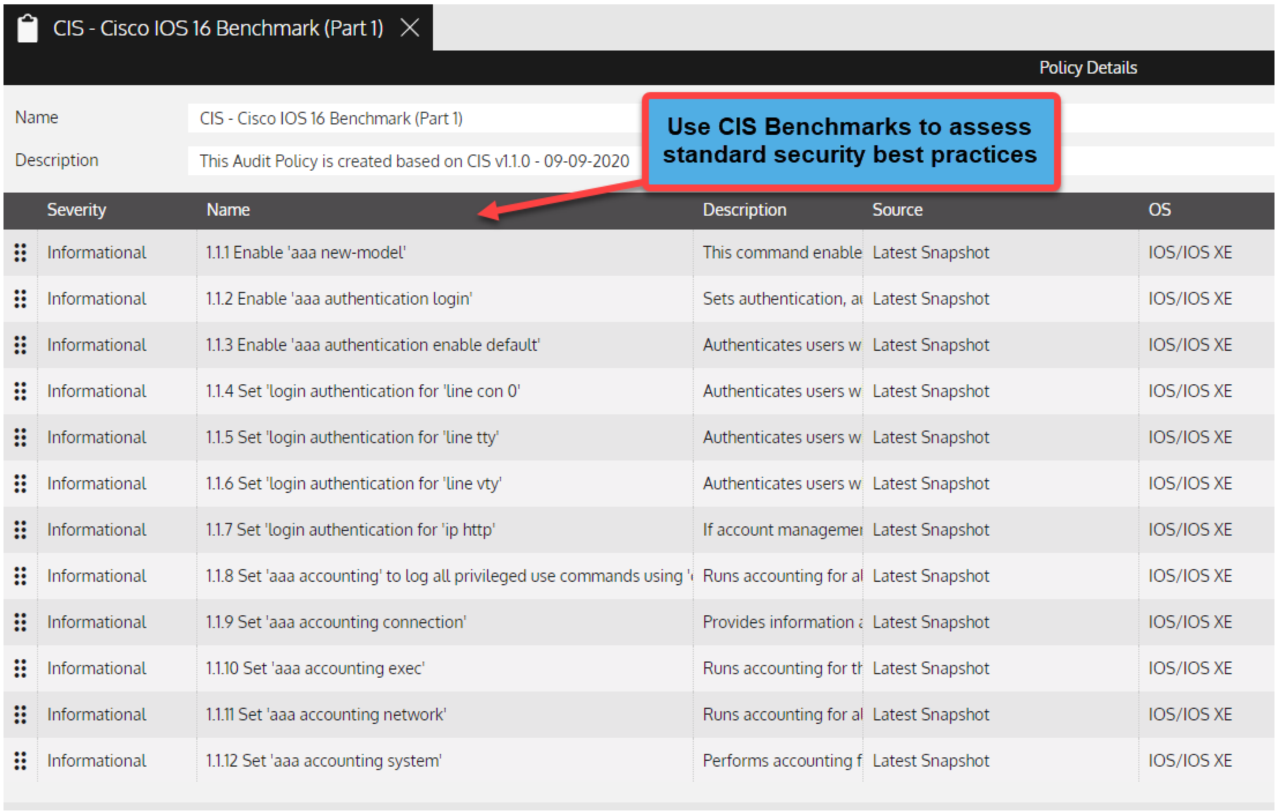
```
ip name-server 10.1.255.53 10.1.155.53
```

Create simple or complex config policy rules to assess devices

Figure 14 Create No-Code Audit Rules to Assess Device Configurations

Security Audits (CIS Benchmarks)

Improving the security posture of network infrastructure is a top priority across Enterprise IT. Leveraging standard security best practices like those defined by NIST, CIS and others are generally a good starting point. Gluware provides example audits including CIS benchmarks to help accelerate this process. Custom security audits can also easily be defined using the Config Drift and Audit app.



Name: CIS - Cisco IOS 16 Benchmark (Part 1)

Description: This Audit Policy is created based on CIS v1.1.0 - 09-09-2020

Use CIS Benchmarks to assess standard security best practices

Severity	Name	Description	Source	OS
Informational	1.1.1 Enable 'aaa new-model'	This command enable	Latest Snapshot	IOS/IOS XE
Informational	1.1.2 Enable 'aaa authentication login'	Sets authentication, a	Latest Snapshot	IOS/IOS XE
Informational	1.1.3 Enable 'aaa authentication enable default'	Authenticates users w	Latest Snapshot	IOS/IOS XE
Informational	1.1.4 Set 'login authentication for 'line con 0'	Authenticates users w	Latest Snapshot	IOS/IOS XE
Informational	1.1.5 Set 'login authentication for 'line tty'	Authenticates users w	Latest Snapshot	IOS/IOS XE
Informational	1.1.6 Set 'login authentication for 'line vty'	Authenticates users w	Latest Snapshot	IOS/IOS XE
Informational	1.1.7 Set 'login authentication for 'ip http'	If account managemei	Latest Snapshot	IOS/IOS XE
Informational	1.1.8 Set 'aaa accounting' to log all privileged use commands using '	Runs accounting for al	Latest Snapshot	IOS/IOS XE
Informational	1.1.9 Set 'aaa accounting connection'	Provides information a	Latest Snapshot	IOS/IOS XE
Informational	1.1.10 Set 'aaa accounting exec'	Runs accounting for th	Latest Snapshot	IOS/IOS XE
Informational	1.1.11 Set 'aaa accounting network'	Runs accounting for al	Latest Snapshot	IOS/IOS XE
Informational	1.1.12 Set 'aaa accounting system'	Performs accounting f	Latest Snapshot	IOS/IOS XE

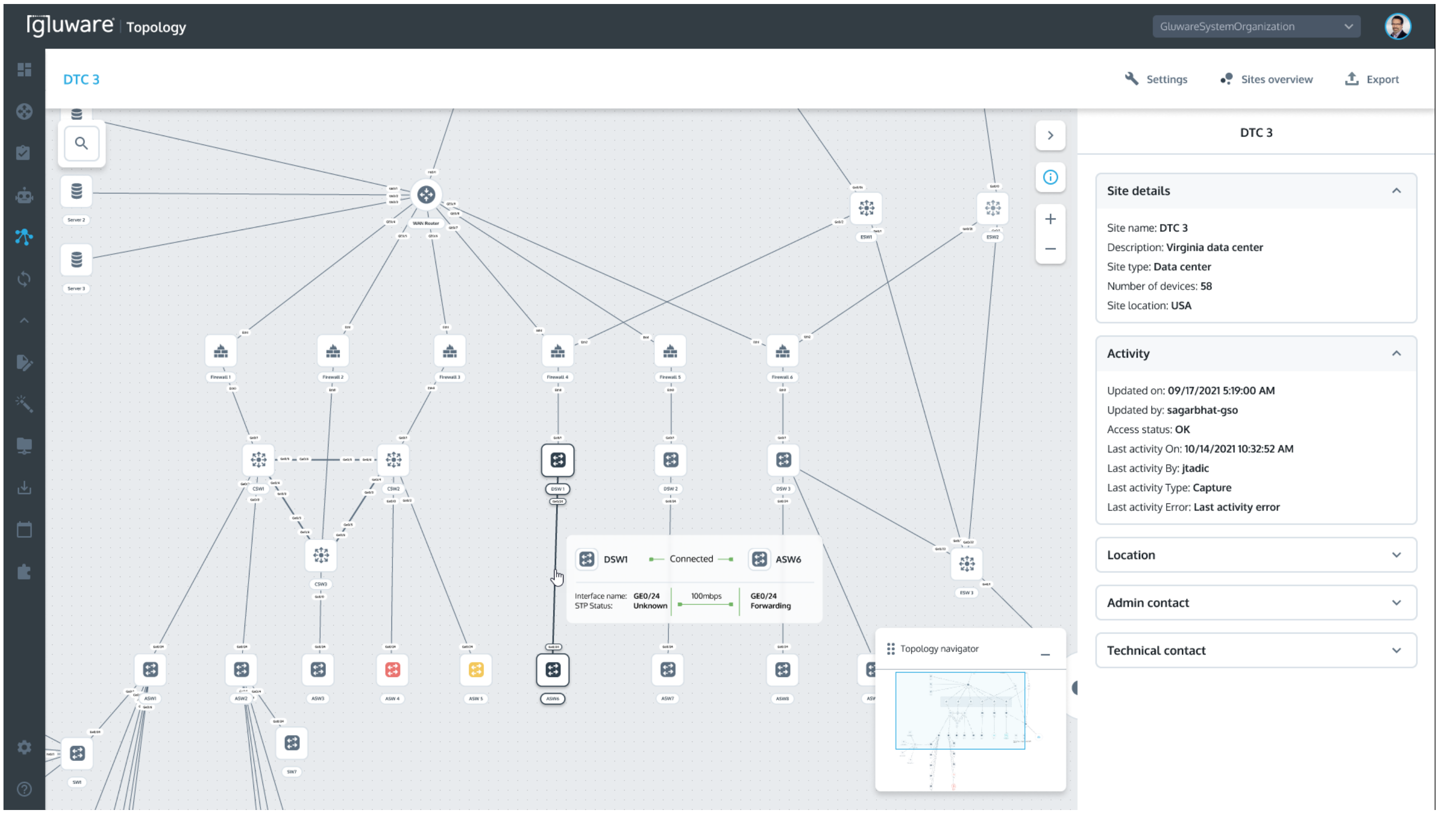
Figure 15 Use Config Drift and Audit to Run CIS Benchmarks to Assess Security

NETWORK VISUALIZATION AND SITE DIAGRAMS

The fourth phase in a typical assessment is to evaluate the topology including physical and logical relationships of network devices. Gluware Topology provides network diagramming and documentation ideal for use in assessing a network. Diagrams are automatically rendered and updated with Gluware's powerful device and network discovery capabilities previously described in the Device Manager app.

Typical Network Assessments Use Gluware Topology to:

- ✓ Visualize the network
- ✓ Assess the network from the global level to the site specific level
- ✓ Generate Site Diagrams



DSW1 — Connected — ASW6

Interface name: GE0/24 | 100mbps | GE0/24
STP Status: Unknown | | Forwarding

DTC 3

Site details

Site name: **DTC 3**
Description: **Virginia data center**
Site type: **Data center**
Number of devices: **58**
Site location: **USA**

Activity

Updated on: **09/17/2021 5:19:00 AM**
Updated by: **sagarbhat-gso**
Access status: **OK**
Last activity On: **10/14/2021 10:32:52 AM**
Last activity By: **jtadic**
Last activity Type: **Capture**
Last activity Error: **Last activity error**

Location

Admin contact

Technical contact

Figure 16 Use Gluware Topology to Visualize, Assess, and Document the Network

OPERATIONAL STATE ASSESSMENT

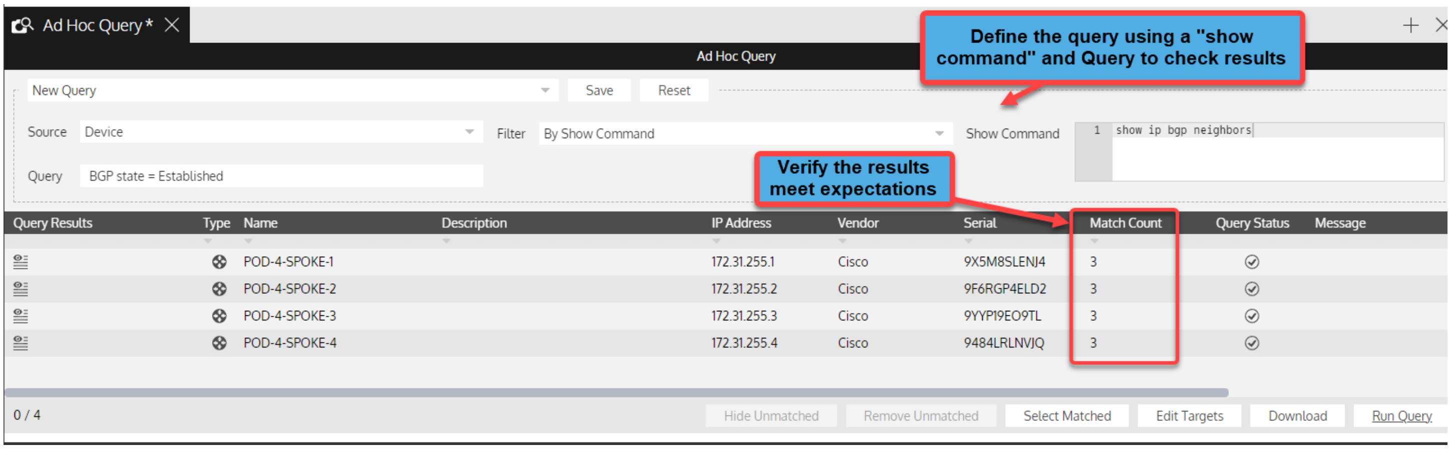
The next step in an in-depth assessment will involve examining the operational state of the network devices including the port states, protocol states and other related operational health. Gluware Device Manager captures a basic set of state related items; however, for more in-depth and custom assessments, Gluware provides the Ad-Hoc Query utility and State Assessment within the Config Modeling app.

Execute State Assessments to evaluate:

- ✓ Interface status and health
- ✓ Protocol state
- ✓ Route counts
- ✓ High-availability status
- ✓ Security parameters like ACL counts

Ad-Hoc Query

The Ad-Hoc Query utility available from the Gluware Device Explorer enables users to execute queries based on a “show command” and an assessment of the results to determine how many matches exist on each device. Detailed views of the output and matched condition are also available. This is an extremely useful tool to assess specific protocols and their operational state.



Define the query using a "show command" and Query to check results

Source: Device

Filter: By Show Command

Show Command:

```
show ip bgp neighbors
```

Query: BGP state = Established

Verify the results meet expectations

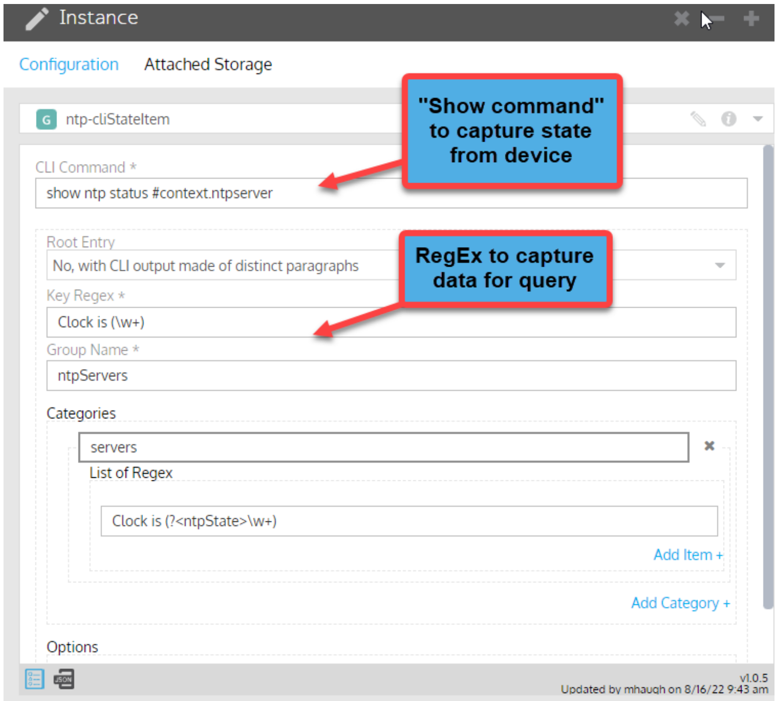
Query Results	Type	Name	Description	IP Address	Vendor	Serial	Match Count	Query Status	Message
		POD-4-SPOKE-1		172.31.255.1	Cisco	9X5M8SLENJ4	3	✓	
		POD-4-SPOKE-2		172.31.255.2	Cisco	9F6RGP4ELD2	3	✓	
		POD-4-SPOKE-3		172.31.255.3	Cisco	9YYP19EO9TL	3	✓	
		POD-4-SPOKE-4		172.31.255.4	Cisco	9484LRLNVJQ	3	✓	

0 / 4

Figure 17 Use Ad-Hoc Query to Assess the Operational State

Config Modeling State Assessment

State Assessment is a capability within the Gluware Config Modeling solution that enables users to define any operational state check along with a query to assess the results. It can be used for troubleshooting purposes and is typically used for pre/post configuration change verification. It is also a powerful capability to use when performing network assessments.


Instance
Configuration
Attached Storage
ntp-cliStateItem

CLI Command *: show ntp status #context.ntpserver

Root Entry: No, with CLI output made of distinct paragraphs

Key Regex *: Clock is (\w+)

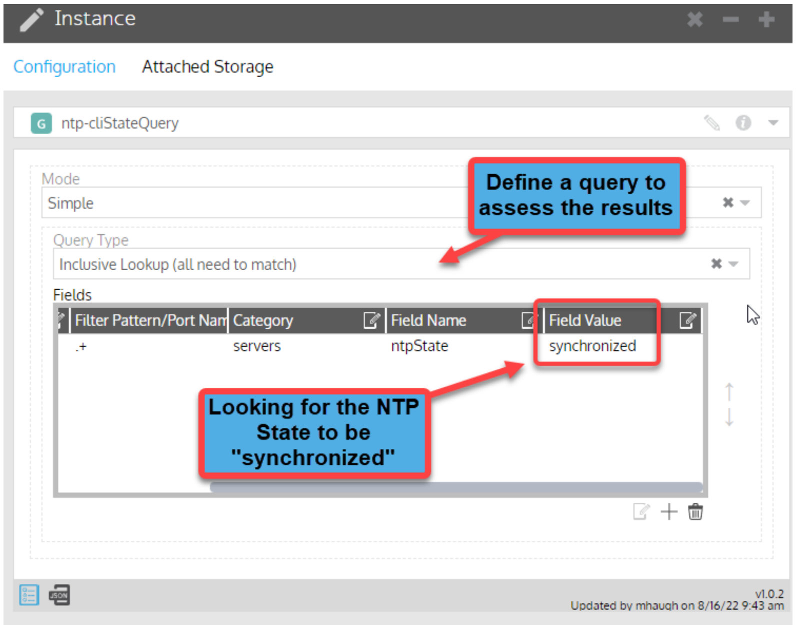
Group Name *: ntpServers

Categories: servers

List of Regex: Clock is (?<ntpState>\w+)

Add Item +
Add Category +
Options
v1.0.5
Updated by mhaugh on 8/16/22 9:43 am
"Show command" to capture state from device
RegEx to capture data for query

Figure 18 Define a State Assessment in Config Modeling using “Show Commands” and RegEx


Instance
Configuration
Attached Storage
ntp-cliStateQuery

Mode: Simple

Query Type: Inclusive Lookup (all need to match)

Fields

Filter Pattern/Port Nam	Category	Field Name	Field Value
.+	servers	ntpState	synchronized

v1.0.2
Updated by mhaugh on 8/16/22 9:43 am
Define a query to assess the results
Looking for the NTP State to be "synchronized"

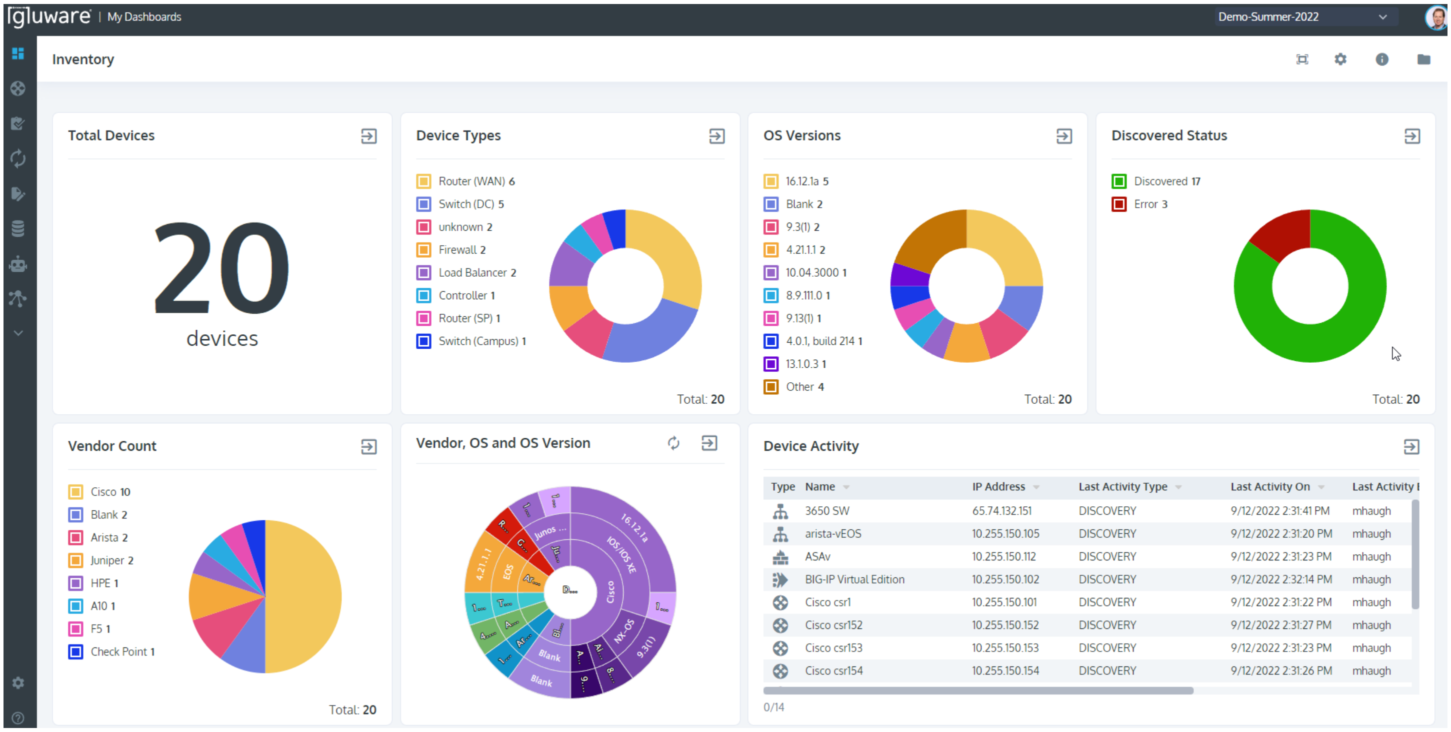
Figure 19 Define a State Assessment Query to Assess the Operational State

REPORTING

Artifacts are a key deliverable for any assessment. This includes archiving the raw data as well as processing the data to provide key insights and assessments based on that data. Gluware provides numerous ways to view, process and assess the data extracted from the network infrastructure. Beyond capabilities of the native applications mentioned, like Device Manager, Config Drift and Audit and Config Modeling, Gluware has two specific applications to provide data-driven insights.

Dashboard

The Gluware Dashboard app provides a rich graphical view of the underlying data captured from the network infrastructure. Numerous example dashboards are provided for administrative and app-specific views. Dashboards are fully customizable using a drag-and-drop editor and library of widgets. These include rich text notes, web pages, RSS feed, counts, tables schedules, user activity, and more.



Inventory

Total Devices

20
devices

Device Types

- 🟨 Router (WAN) 6
- 🟦 Switch (DC) 5
- 🟥 unknown 2
- 🟧 Firewall 2
- 🟪 Load Balancer 2
- 🟦 Controller 1
- 🟥 Router (SP) 1
- 🟦 Switch (Campus) 1

Total: 20

OS Versions

- 🟨 16.12.1a 5
- 🟦 Blank 2
- 🟥 9.3(1) 2
- 🟧 4.21.1.1 2
- 🟪 10.04.3000 1
- 🟦 8.9.111.0 1
- 🟥 9.13(1) 1
- 🟦 4.0.1, build 214 1
- 🟪 13.1.0.3 1
- 🟧 Other 4

Total: 20

Discovered Status

- 🟩 Discovered 17
- 🟥 Error 3

Total: 20

Vendor Count

- 🟨 Cisco 10
- 🟦 Blank 2
- 🟥 Arista 2
- 🟧 Juniper 2
- 🟪 HPE 1
- 🟦 A10 1
- 🟥 F5 1
- 🟦 Check Point 1

Total: 20

Vendor, OS and OS Version

Device Activity

Type	Name	IP Address	Last Activity Type	Last Activity On	Last Activity I
	3650 SW	65.74.132.151	DISCOVERY	9/12/2022 2:31:41 PM	mhaugh
	arista-vEOS	10.255.150.105	DISCOVERY	9/12/2022 2:31:20 PM	mhaugh
	ASAv	10.255.150.112	DISCOVERY	9/12/2022 2:31:23 PM	mhaugh
	BIG-IP Virtual Edition	10.255.150.102	DISCOVERY	9/12/2022 2:32:14 PM	mhaugh
	Cisco csr1	10.255.150.101	DISCOVERY	9/12/2022 2:31:22 PM	mhaugh
	Cisco csr152	10.255.150.152	DISCOVERY	9/12/2022 2:31:27 PM	mhaugh
	Cisco csr153	10.255.150.153	DISCOVERY	9/12/2022 2:31:23 PM	mhaugh
	Cisco csr154	10.255.150.154	DISCOVERY	9/12/2022 2:31:26 PM	mhaugh

0/14

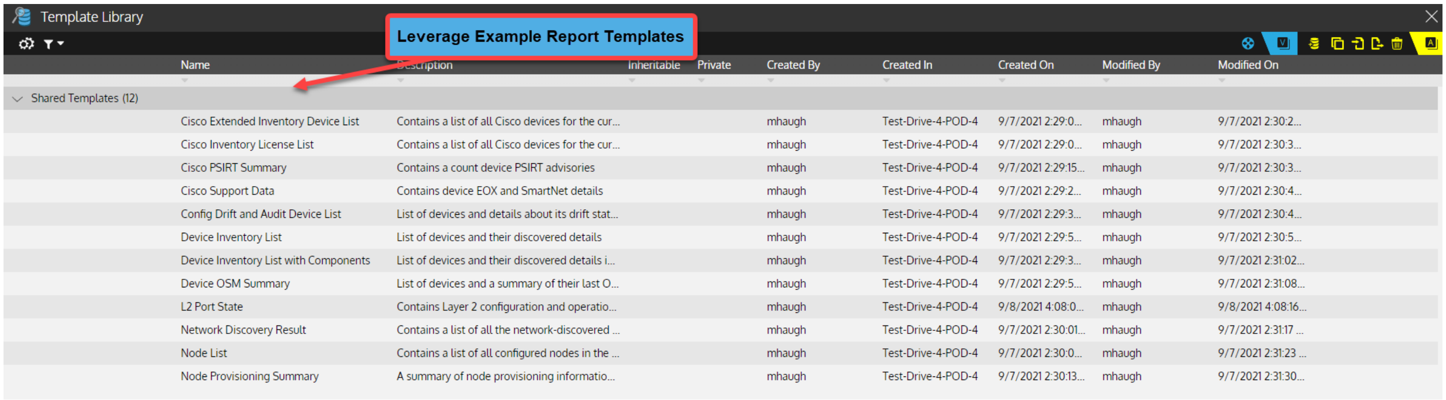
Figure 20 Use Gluware Dashboard to Visualize the Data from the Network Infrastructure

Data Explorer

Data Explorer offers unparalleled visibility into network data that enables NetOps teams to automate networks based on actionable, data-driven insights to enhance agility, performance, and security. The Data Explorer solution is powered by direct access to the underlying databases within the user's Gluware instance enabling the ability to assess network information faster.

Use Data Explorer to:

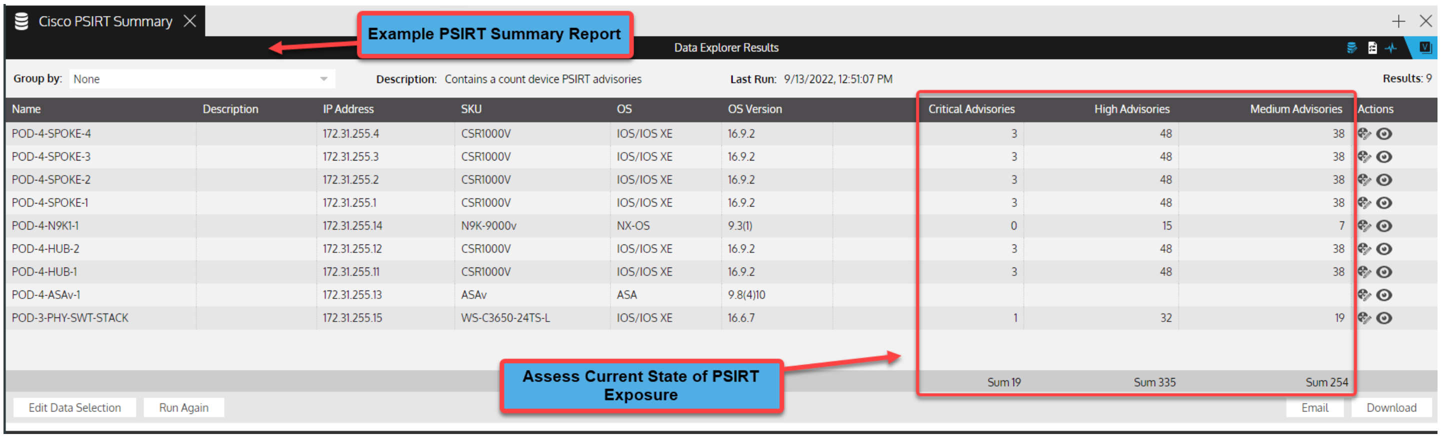
- ✓ Access to the data from each Gluware app
- ✓ Access platform, configuration and operational state data
- ✓ Create custom default reports for each app
- ✓ Leverage the created report templates from each app once created



Shared Templates (12)

Name	Description	Inheritable	Private	Created By	Created In	Created On	Modified By	Modified On
Cisco Extended Inventory Device List	Contains a list of all Cisco devices for the cur...			mhaugh	Test-Drive-4-POD-4	9/7/2021 2:29:0...	mhaugh	9/7/2021 2:30:2...
Cisco Inventory License List	Contains a list of all Cisco devices for the cur...			mhaugh	Test-Drive-4-POD-4	9/7/2021 2:29:0...	mhaugh	9/7/2021 2:30:3...
Cisco PSIRT Summary	Contains a count device PSIRT advisories			mhaugh	Test-Drive-4-POD-4	9/7/2021 2:29:15...	mhaugh	9/7/2021 2:30:3...
Cisco Support Data	Contains device EOX and SmartNet details			mhaugh	Test-Drive-4-POD-4	9/7/2021 2:29:2...	mhaugh	9/7/2021 2:30:4...
Config Drift and Audit Device List	List of devices and details about its drift stat...			mhaugh	Test-Drive-4-POD-4	9/7/2021 2:29:3...	mhaugh	9/7/2021 2:30:4...
Device Inventory List	List of devices and their discovered details			mhaugh	Test-Drive-4-POD-4	9/7/2021 2:29:5...	mhaugh	9/7/2021 2:30:5...
Device Inventory List with Components	List of devices and their discovered details i...			mhaugh	Test-Drive-4-POD-4	9/7/2021 2:29:3...	mhaugh	9/7/2021 2:31:02...
Device OSM Summary	List of devices and a summary of their last O...			mhaugh	Test-Drive-4-POD-4	9/7/2021 2:29:5...	mhaugh	9/7/2021 2:31:08...
L2 Port State	Contains Layer 2 configuration and operatio...			mhaugh	Test-Drive-4-POD-4	9/8/2021 4:08:0...	mhaugh	9/8/2021 4:08:16...
Network Discovery Result	Contains a list of all the network-discovered ...			mhaugh	Test-Drive-4-POD-4	9/7/2021 2:30:01...	mhaugh	9/7/2021 2:31:17 ...
Node List	Contains a list of all configured nodes in the ...			mhaugh	Test-Drive-4-POD-4	9/7/2021 2:30:0...	mhaugh	9/7/2021 2:31:23 ...
Node Provisioning Summary	A summary of node provisioning informatio...			mhaugh	Test-Drive-4-POD-4	9/7/2021 2:30:13...	mhaugh	9/7/2021 2:31:30...

Figure 21 Use Gluware Data Explorer to Generate Reports Leveraging Example Templates



Group by: None

Description: Contains a count device PSIRT advisories

Last Run: 9/13/2022, 12:51:07 PM

Results: 9

Name	Description	IP Address	SKU	OS	OS Version	Critical Advisories	High Advisories	Medium Advisories	Actions
POD-4-SPOKE-4		172.31.255.4	CSR1000V	IOS/IOS XE	16.9.2	3	48	38	
POD-4-SPOKE-3		172.31.255.3	CSR1000V	IOS/IOS XE	16.9.2	3	48	38	
POD-4-SPOKE-2		172.31.255.2	CSR1000V	IOS/IOS XE	16.9.2	3	48	38	
POD-4-SPOKE-1		172.31.255.1	CSR1000V	IOS/IOS XE	16.9.2	3	48	38	
POD-4-N9K1-1		172.31.255.14	N9K-9000v	NX-OS	9.3(1)	0	15	7	
POD-4-HUB-2		172.31.255.12	CSR1000V	IOS/IOS XE	16.9.2	3	48	38	
POD-4-HUB-1		172.31.255.11	CSR1000V	IOS/IOS XE	16.9.2	3	48	38	
POD-4-ASAv-1		172.31.255.13	ASAv	ASA	9.8(4)10				
POD-3-PHY-SWT-STACK		172.31.255.15	WS-C3650-24TS-L	IOS/IOS XE	16.6.7	1	32	19	
						Sum 19	Sum 335	Sum 254	

Figure 22 Gluware Data Explorer Example PSIRT Summary Report

CONCLUSION

Network assessments are the first step in any process related to projects that affect the infrastructure. Decisions need to be data-driven, and having the ability to get that data and execute a timely assessment is critical to a successful project. The Gluware Intelligent Network Automation solution provides out-of-the-box capabilities through the suite of applications to accelerate and execute a comprehensive assessment. Gluware amplifies the power and skill set of the user to execute the assessment at any scale.

Additional Gluware Resources

Watch a demo of Network Discovery

Watch a demo of Device Manager

Watch a demo of Config Audit

Watch a demo of Ad-Hoc Query

Watch a demo of Config Modeling State Assessment

Watch a demo of Dashboard

Watch a demo of Data Explorer

Cisco Support API

NIST

gluware®
Intelligent Network
Automation