
Site24x7
Free Online Training - Day 3

Intro about the training program

All modules of Site24x7 will be covered in 5 sessions.

We offer this training program in three time zones for your convenience.

AUS Time Zone (10:00 AEDT) | UK Time Zone (10:00 GMT) | US Time Zone (10:00 PST)

Sessions split up:

~~**Session 1 - Introduction and Deep Dive into Website Monitoring (Mon, April 17, 2023)**~~

~~**Session 2 - Infrastructure Monitoring and Custom Plugins (Tue, April 18, 2023)**~~

Session 3 - Network & Virtualization Monitoring and Log Management (Wed, April 19, 2023)

Session 4 - Application Performance Monitoring and Real User Monitoring (Thu, April 20, 2023)

Session 5 - Reports, Dashboards, Advanced Configurations, Alerting, and More (Fri, April 21, 2023)

Scope of the session

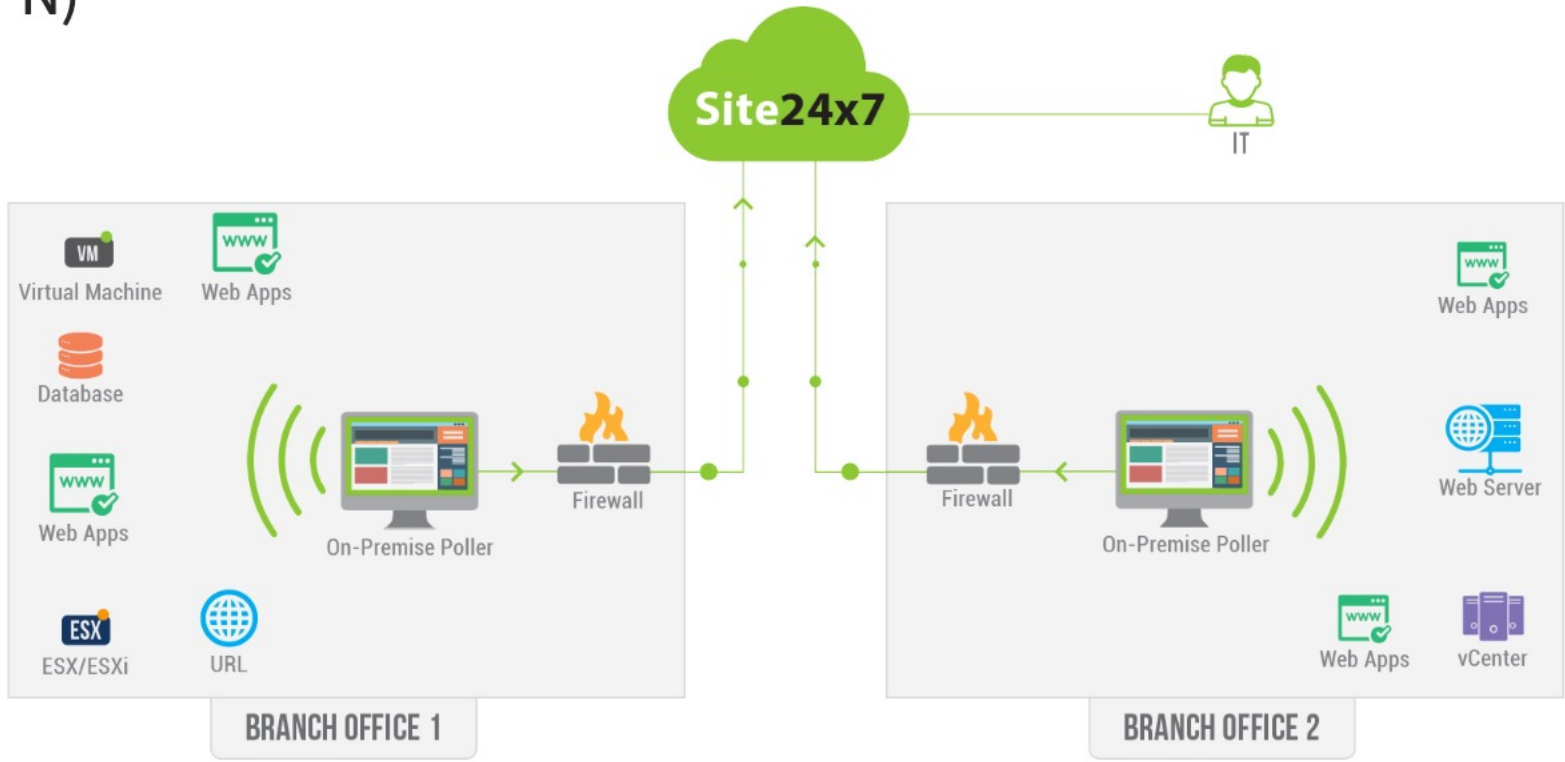
- Overview of On-Premise Poller
- Network Monitoring
- NetFlow Analyzer
- Network Configuration Manager
- VoIP Monitoring
- Cisco Meraki Monitoring
- VMware Monitoring
- Nutanix Monitoring
- VMware Horizon Monitoring
- AppLogs Monitoring

Overview of On-Premise Poller

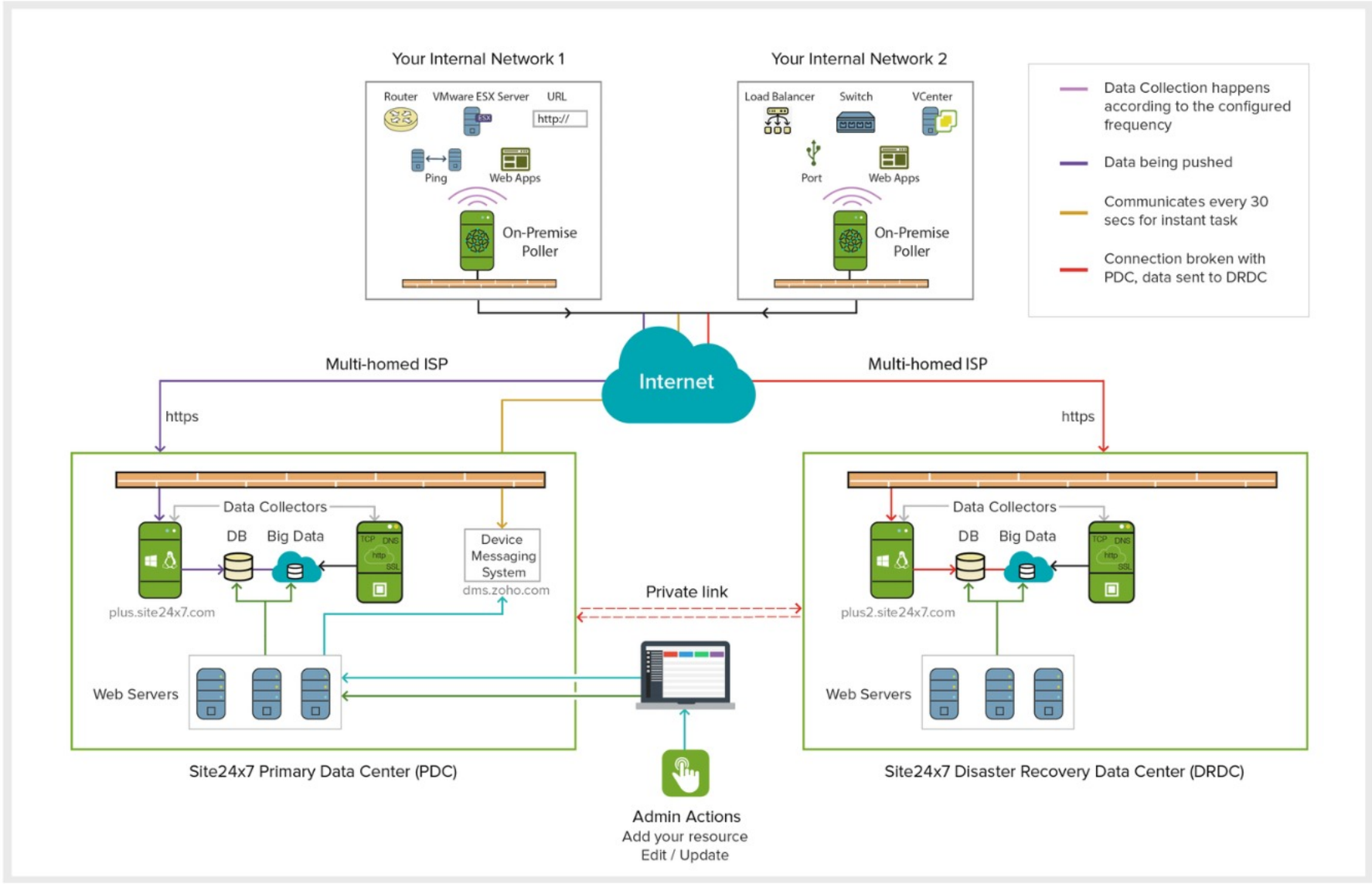
Site24x7

On-Premise Poller - Introduction

- On-Premise Poller, our lightweight agent, helps monitor your internal network and resources behind your firewall or virtual private network (VPN)



Architecture



Site24x7

Minimum Requirements

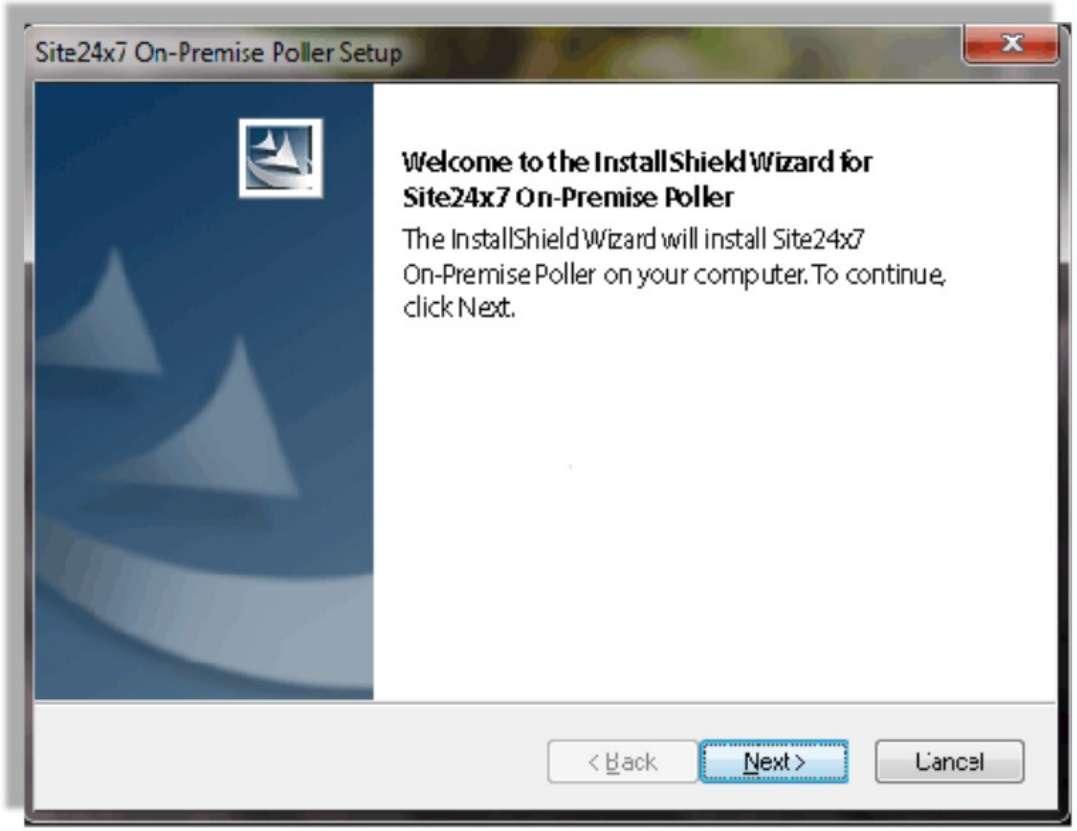
Parameters	Minimum requirements
OS	All Windows and Linux operating systems, including 32-bit and 64-bit
RAM	8 GB
Processor speed	2 GHz
Disk space	80 GB

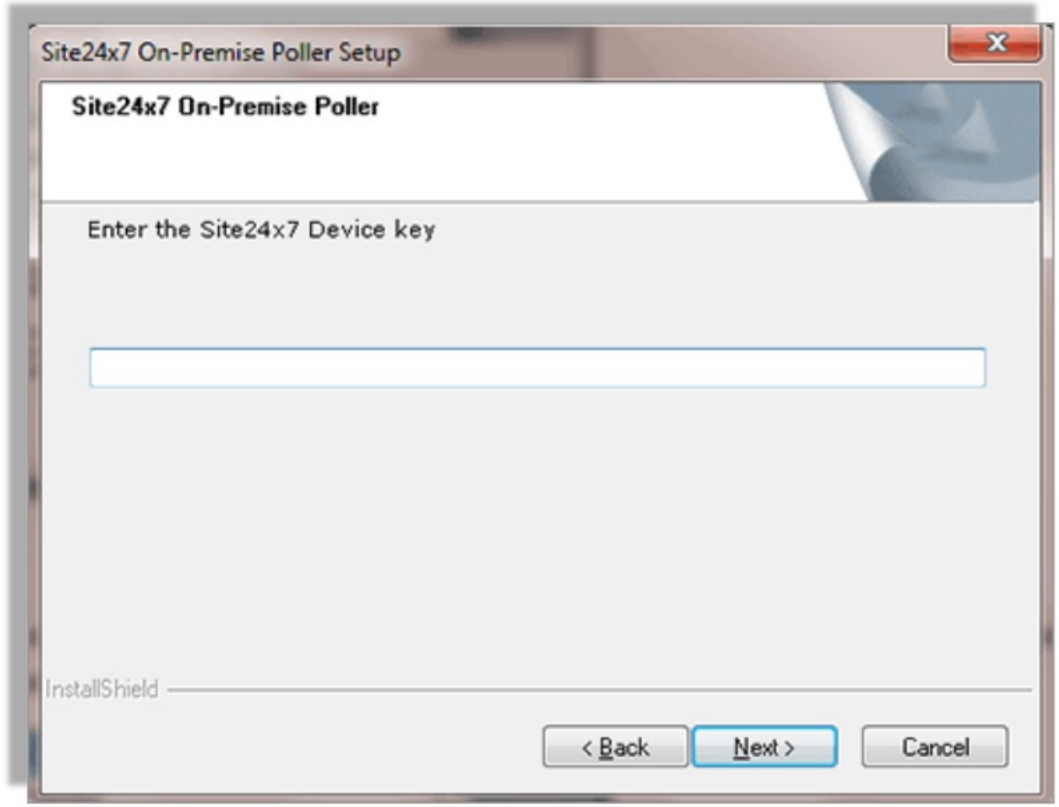
Ports and Domains to be whitelisted

- Ports
  =80
  = 443

- Domains
  > plus.site24x7.com
  > plus2.site24x7.com
  > pluspoller.site24x7.com
  > plusnetwork.site24x7.com
  > staticdownloads.site24x7.com

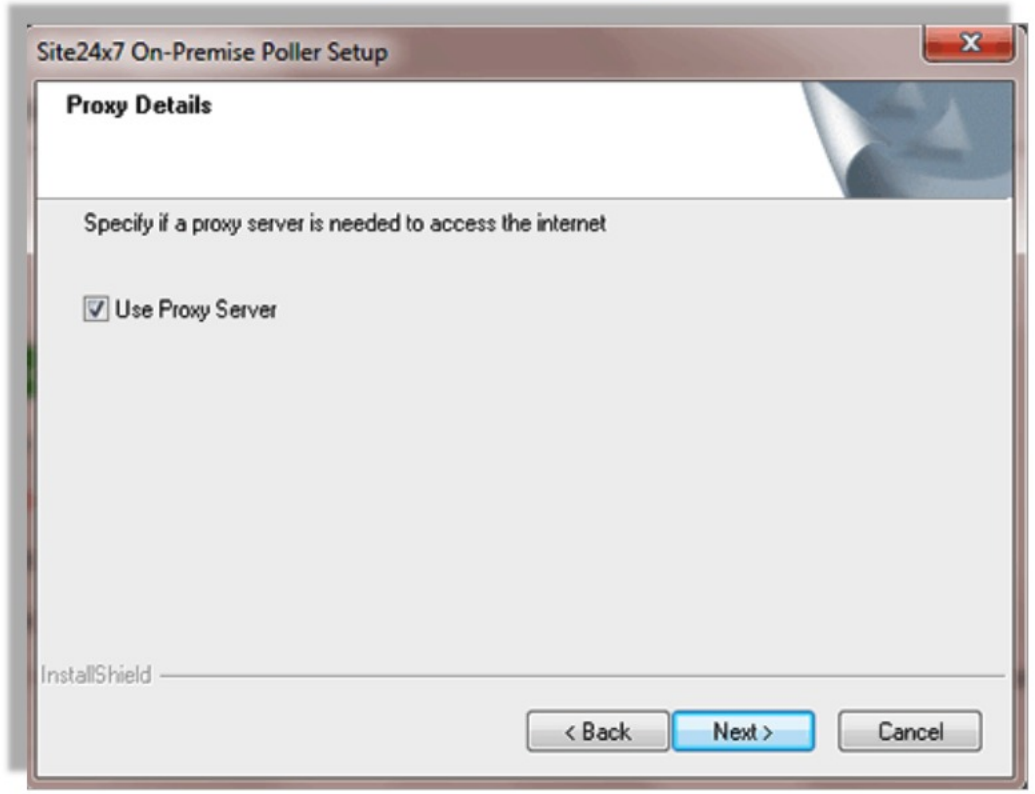
Adding On-Premise Poller for Windows

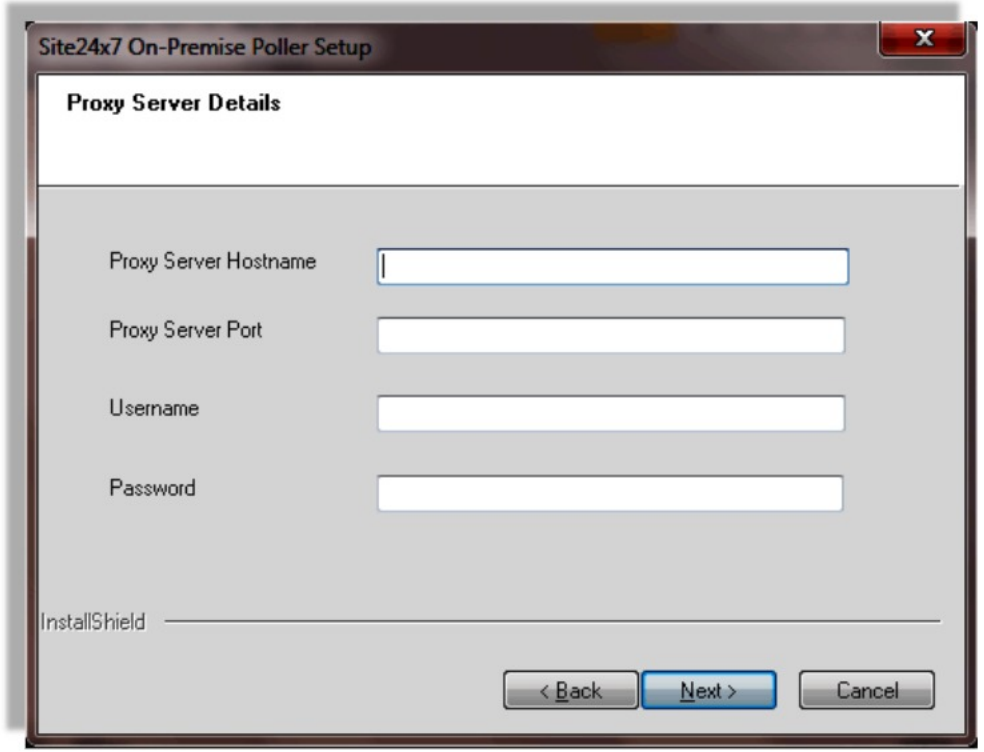




Site24x7

Configuring Proxy





Site24x7

Adding On-Premise Poller for Linux

- Execute the following commands in your terminal to install the On-Premise Poller
- 64 bit OS:
  sudo wget
  http://staticdownloads.site24x7.com/probe/Site24x7OnPremisePoller_64bit.bin
  sudo chmod 755 Site24x7OnPremisePoller_64bit.bin
  sudo ./Site24x7OnPremisePoller_64bit.bin
- 32 bit OS:
  sudo wget http://staticdownloads.site24x7.com/probe/Site24x7OnPremisePoller.bin
  sudo chmod 755 Site24x7OnPremisePoller.bin
  sudo ./Site24x7OnPremisePoller.bin
- Run the installer to install the On-Premise Poller by using your account's device key in the installation wizard

High Availability On-Premise Poller

- When an On-Premise Poller or it's Network Module goes down, the resources associated with it will not be monitored until the On-Premise Poller is backed up
- This is where Site24x7's new High Availability feature comes in handy; you can associate another On-Premise Poller to act as a standby On-Premise Poller in case of downtime
- This *failover mechanism* ensures that monitoring is never interrupted by downtime of On-Premise Pollers

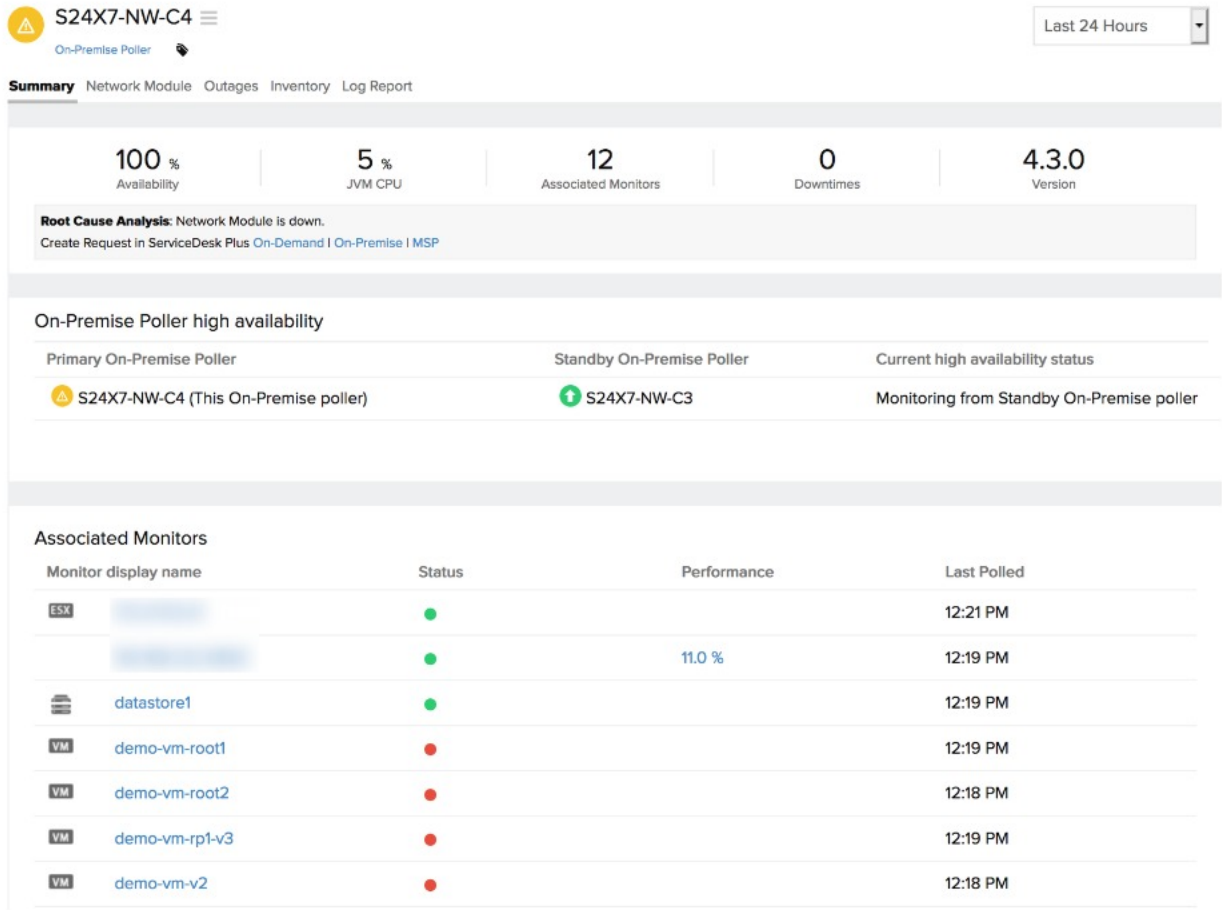
Working of HA Poller

- When there is a change in the availability status of the On-Premise Poller or the Network Module, Site24x7 initiates a status check for the next three consecutive polls
- If the status does not return to Up, the monitoring resources associated with that On-Premise Poller will then be monitored from the standby On-Premise Poller

Prerequisites

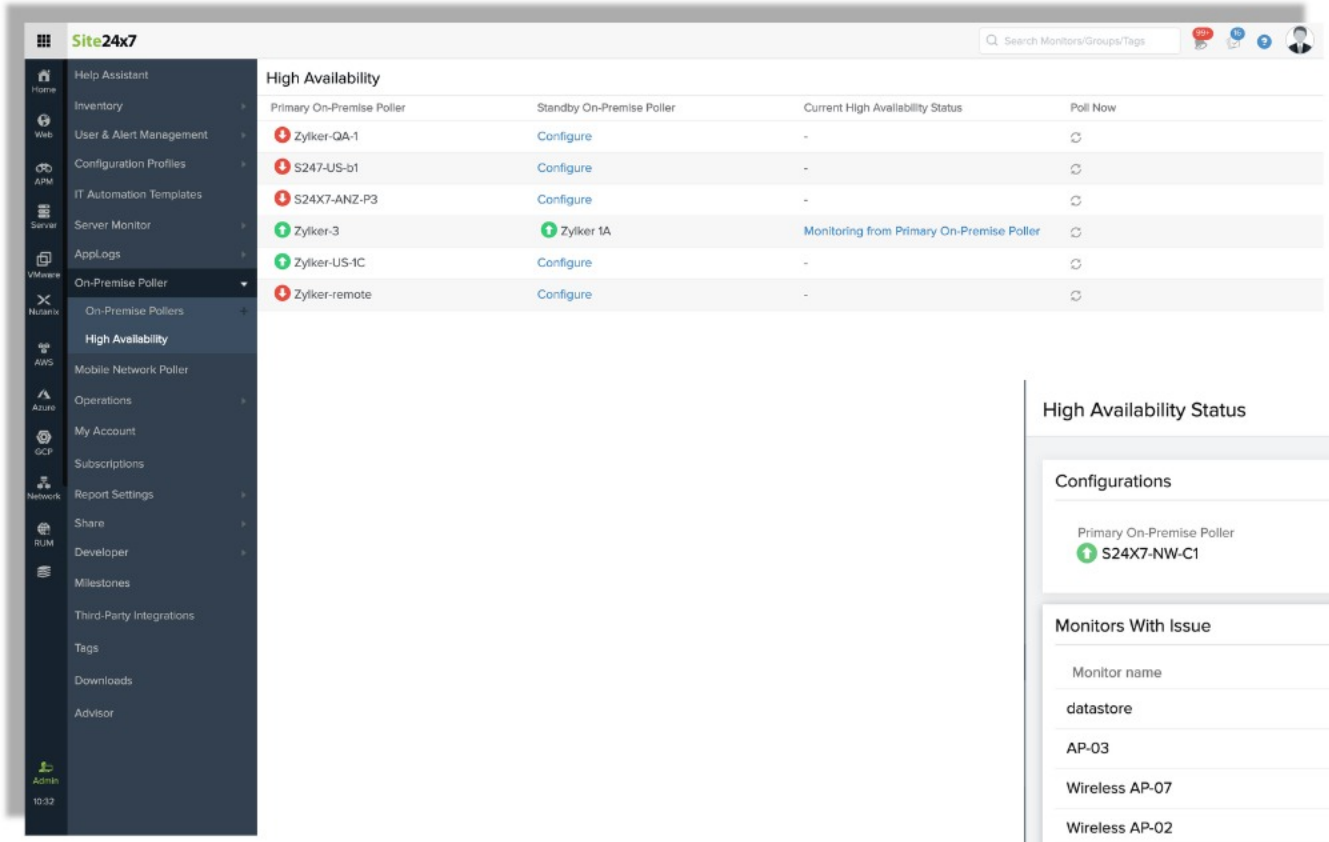
- The On-Premise Poller that is being associated as standby On-Premise Poller must not be in a down or suspended state
- The On-Premise Poller version should be 4.3.0 or above
- The On-Premise Poller should not have any monitor associated with it
- The standby On-Premise Poller must be of the same OS flavor as the primary On-Premise Poller
- The standby On-Premise Poller should not have any other On-Premise Poller associated as standby to it
- The On-Premise Poller should not be associated with another location profile (For example, the On-Premise Poller must not be associated with a location profile that contains global locations or multiple On-Premise Pollers)

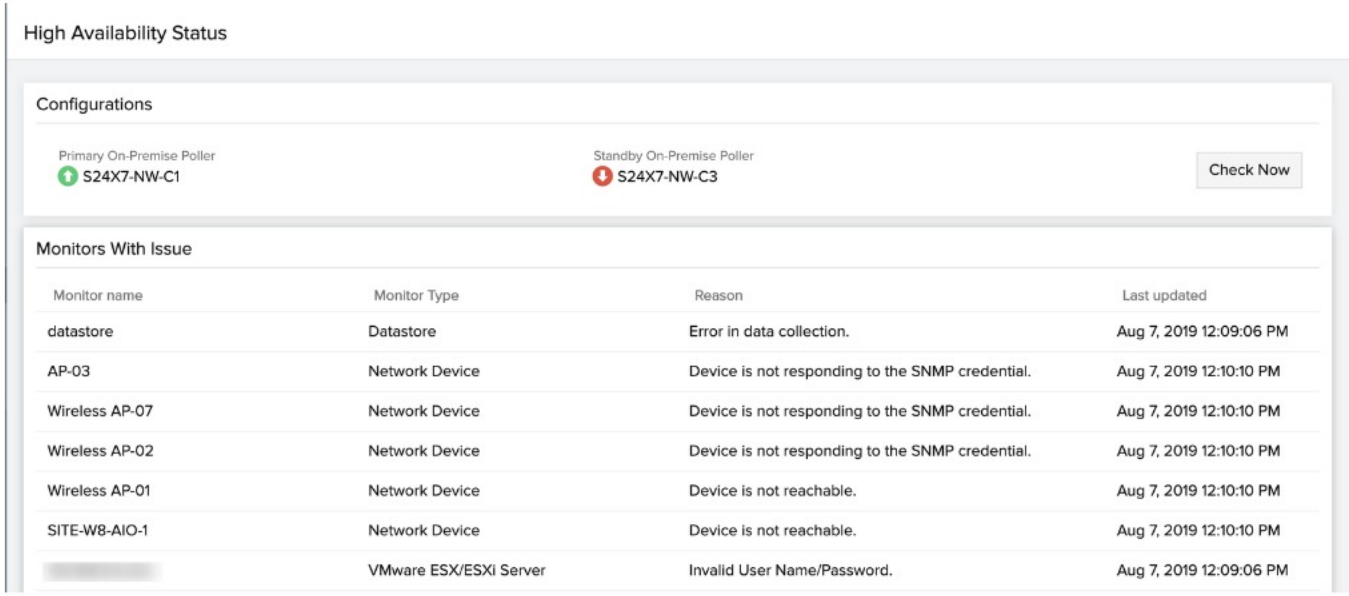
Monitoring from Standby On-Premise Poller



Site24x7

High Availability Status

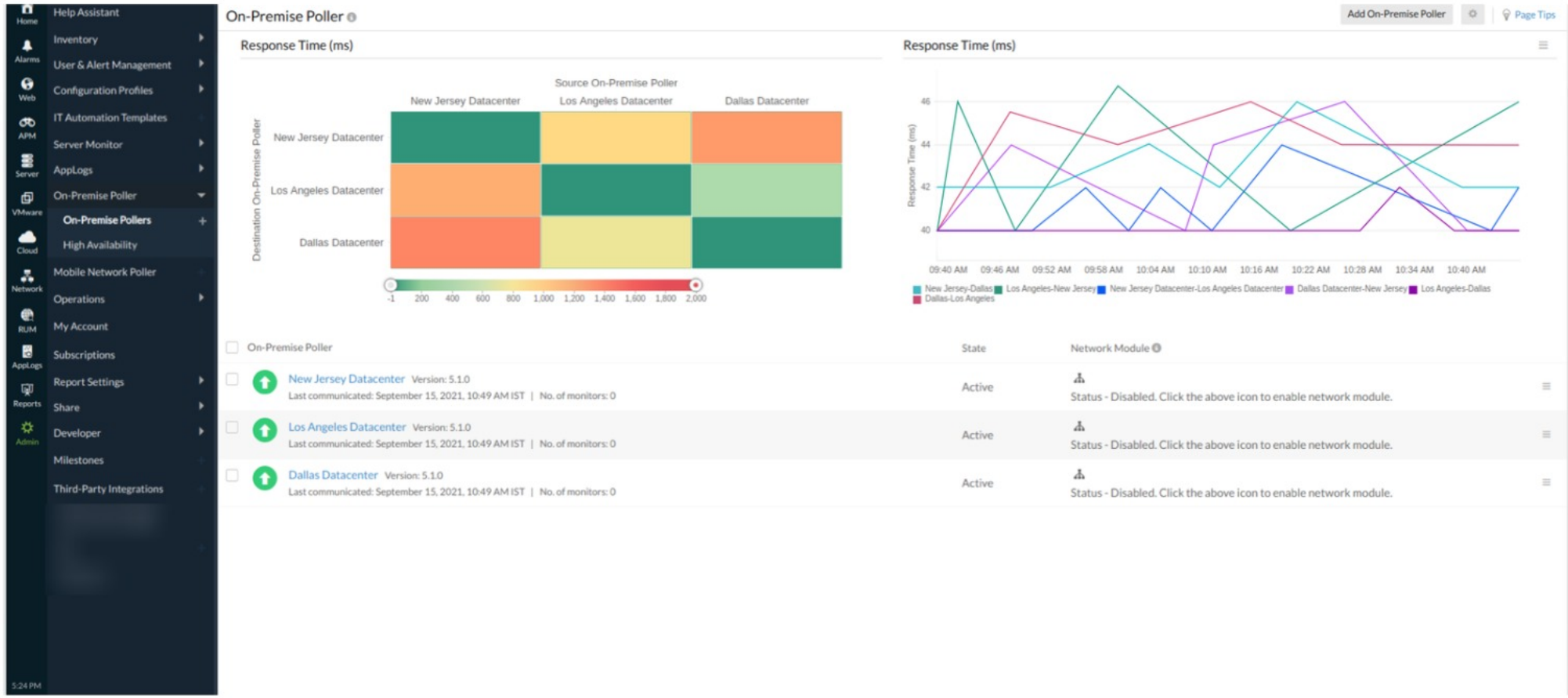




Latency Dashboard

- Understand the availability, latency, and connectivity patterns between the geographically distributed On-Premise Pollers in your account
- Polls every 5 mins and calculates the response time between the other On-Premise Pollers

Latency Dashboard



Site24x7

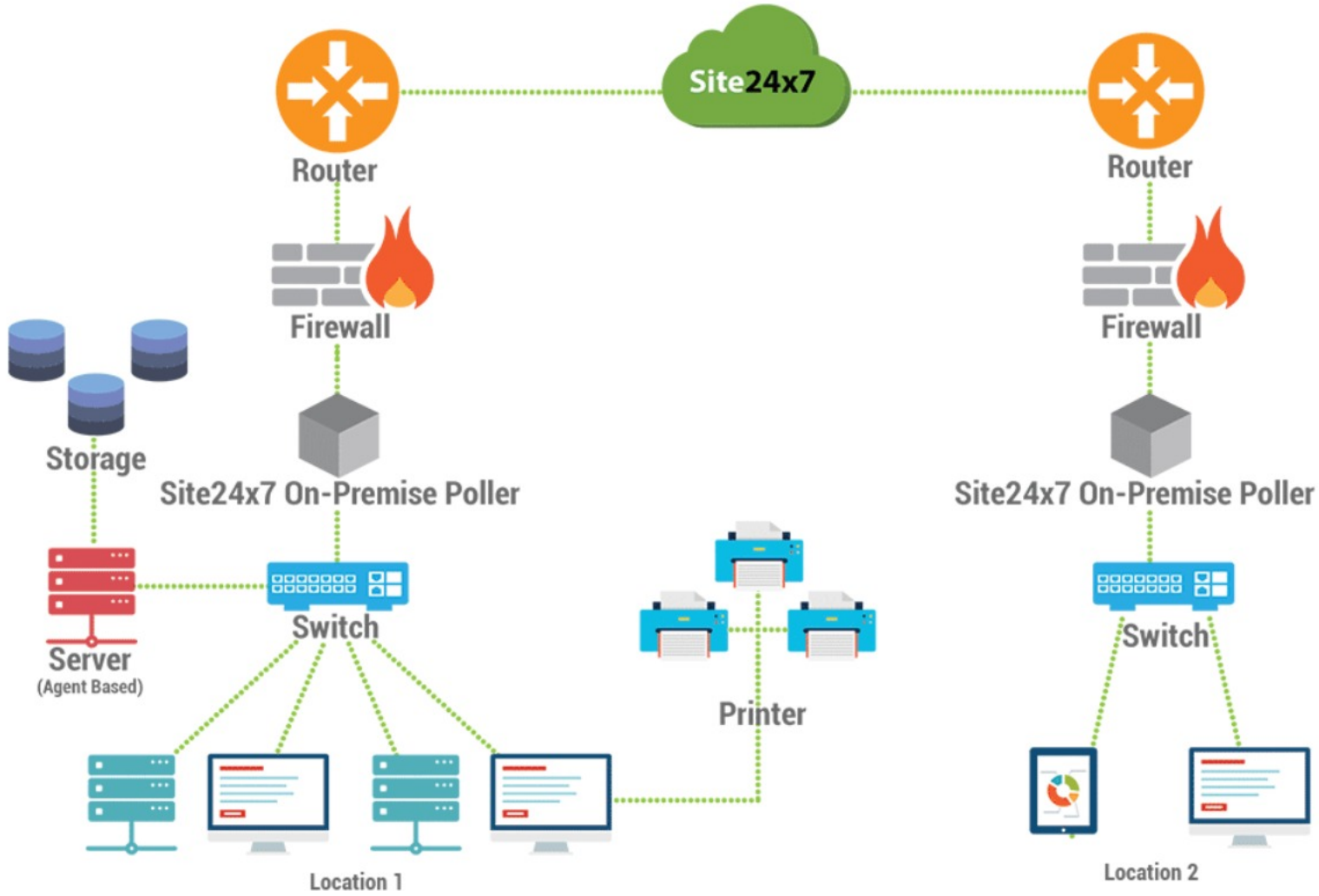
Network Monitoring

Site24x7

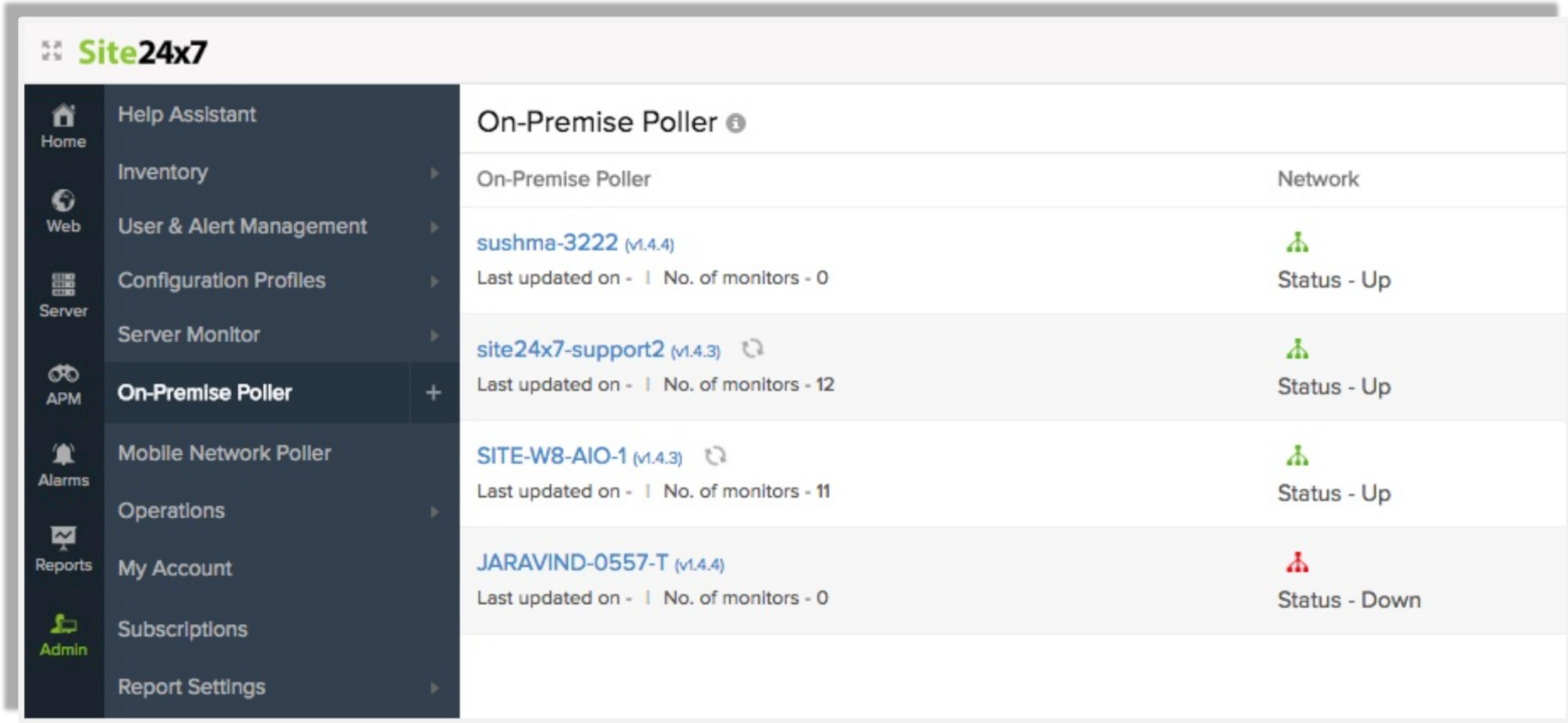
Network Monitoring - Introduction

- Built on the technical expertise of ManageEngine OpManager - with more than 15 years of experience in providing smarter, integrated network management solution
- Scalability - Monitor 1000s of Network devices
- Support for over 450 vendors and more than 10000 device types
- Automatic network discovery
- Robust monitoring for complex, distributed Networks
- Deep insights using SNMP performance counters

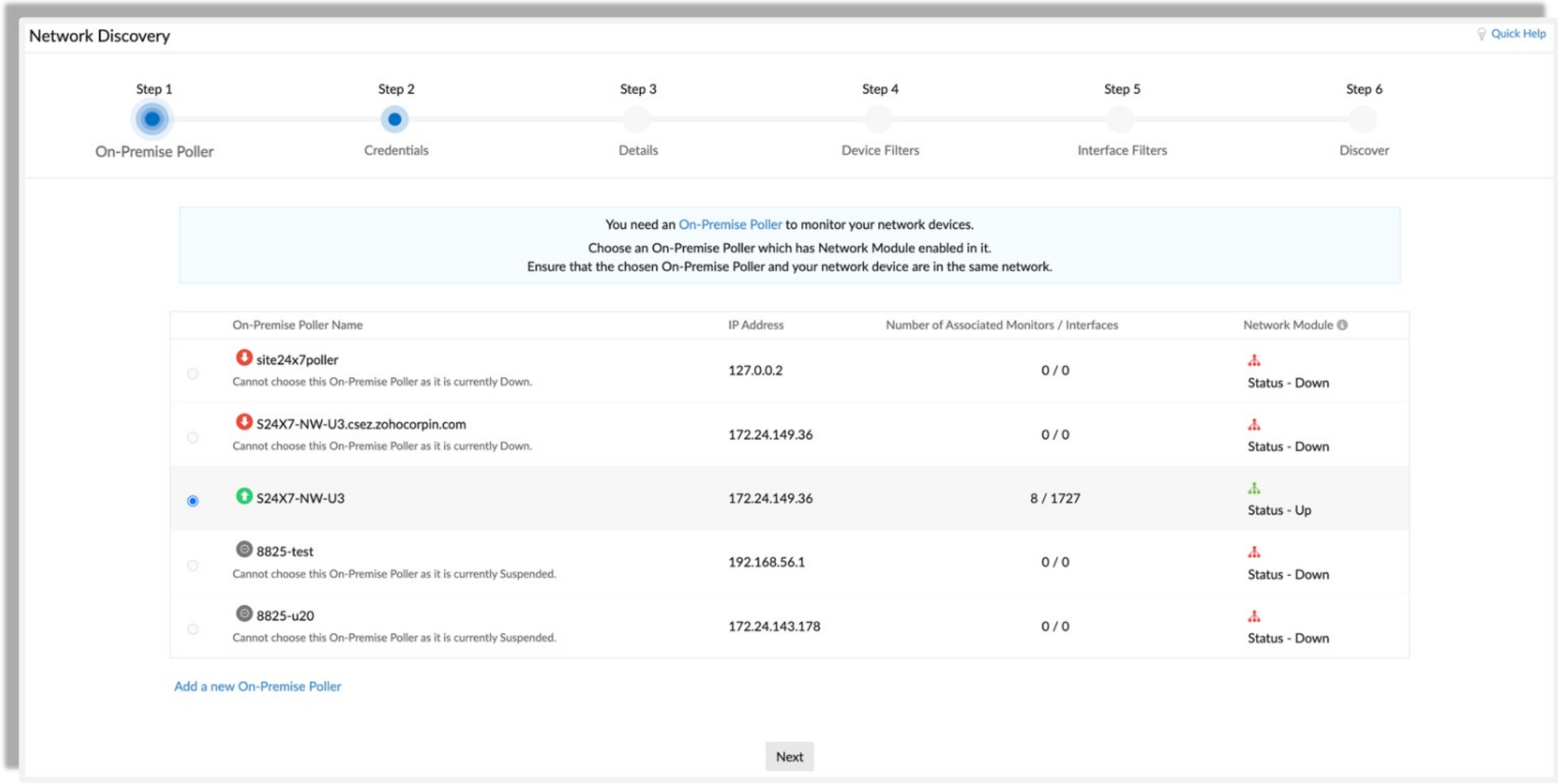
Network Monitoring Architecture



Enable Network Module

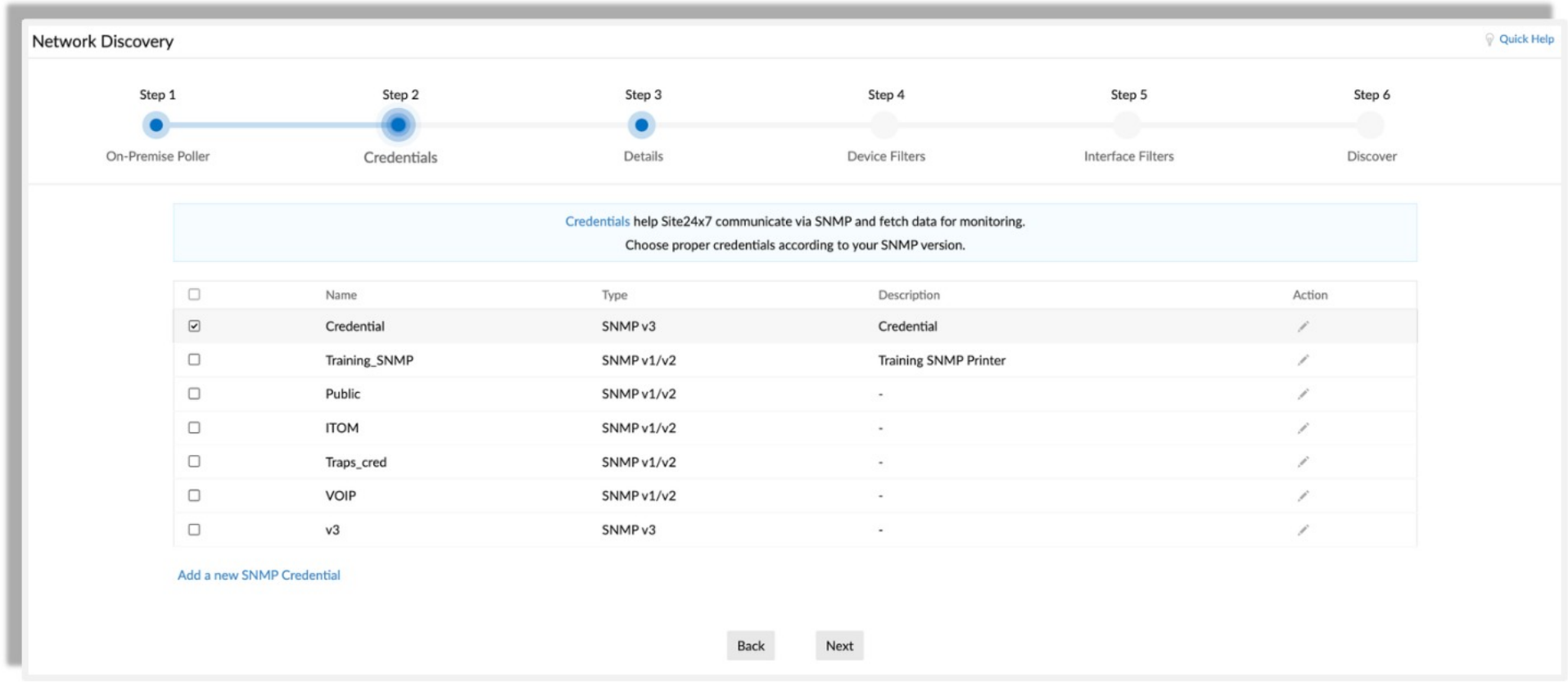


Adding a Network Monitor Step 1

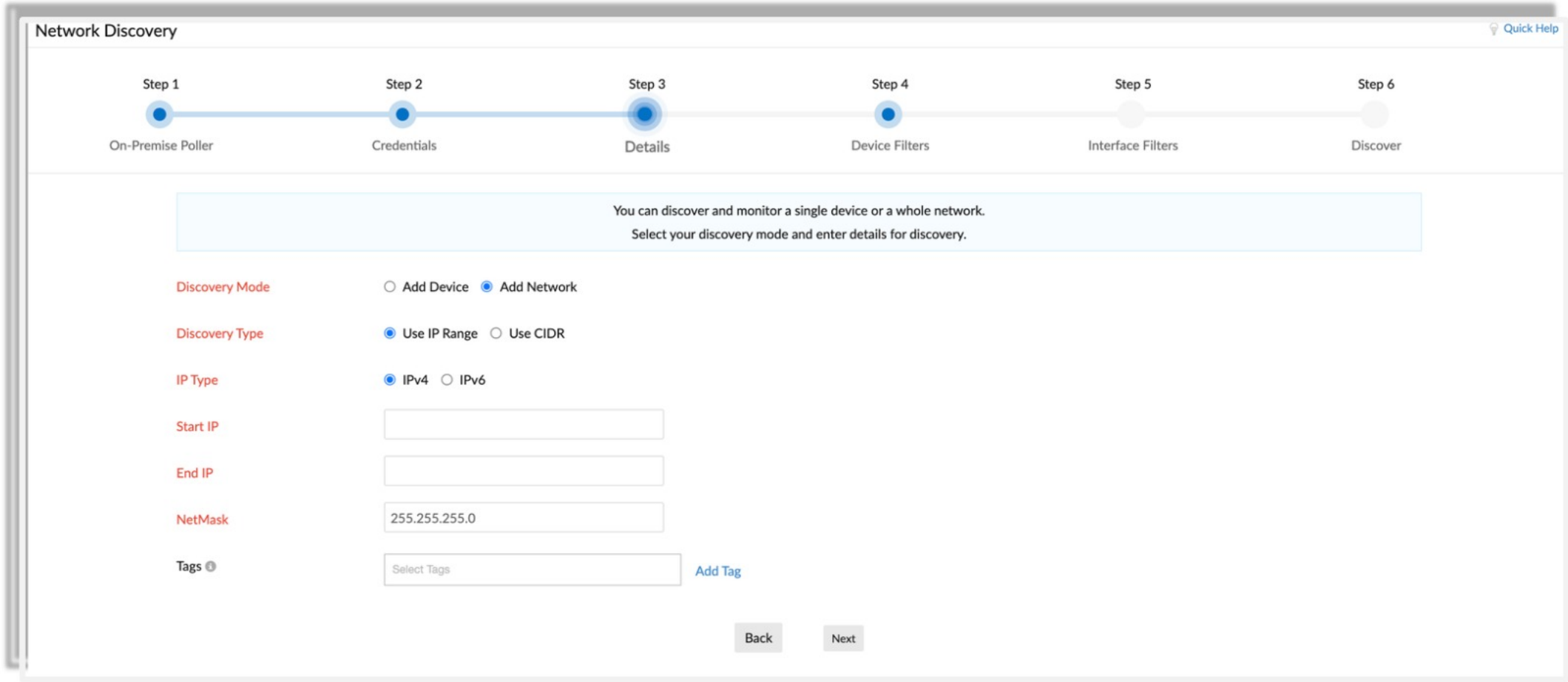


Site24x7

Adding a Network Monitor Step 2

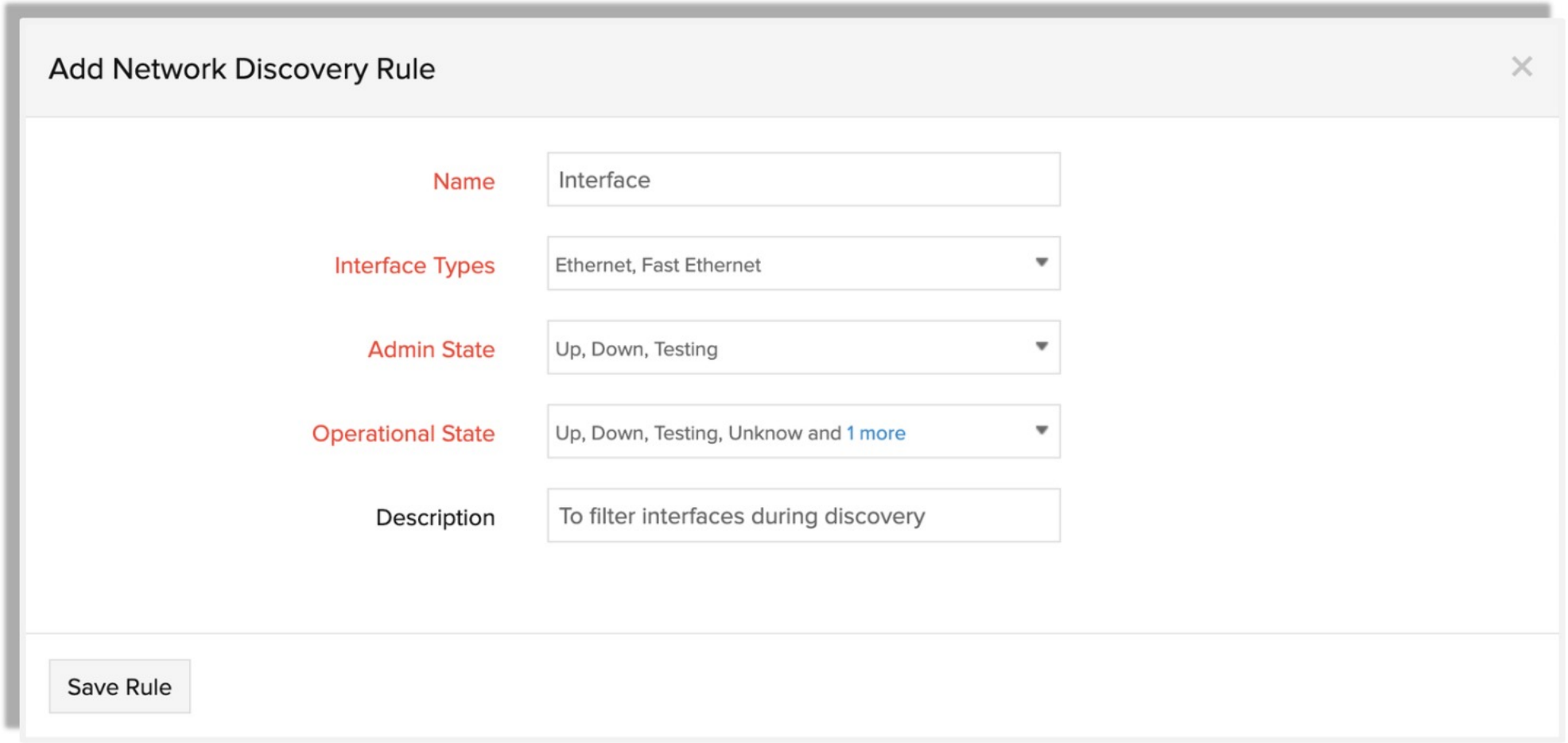


Adding a Network Monitor Step 3

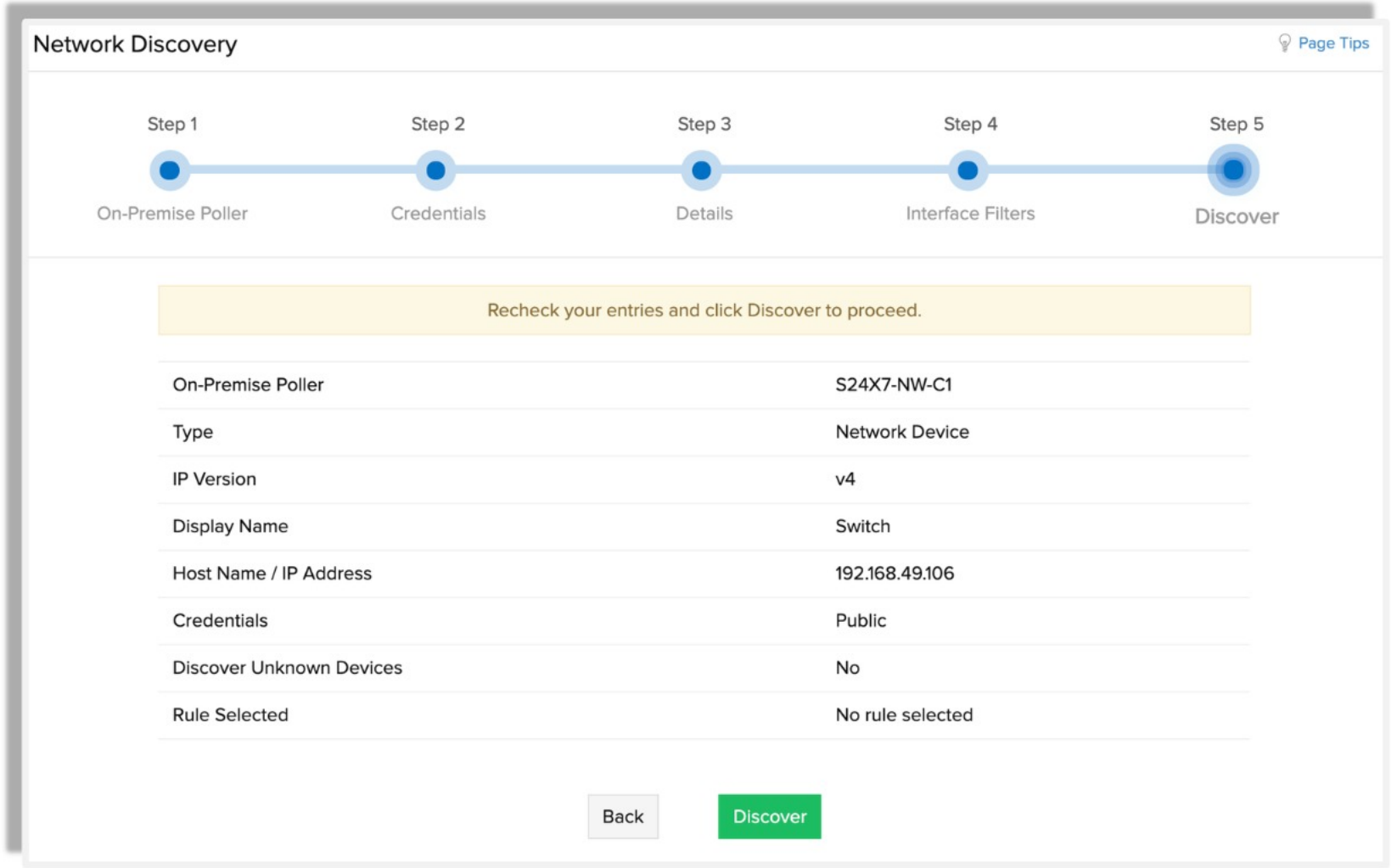


Site24x7

Adding a Network Monitor Step 4



Adding a Network Monitor Step 5



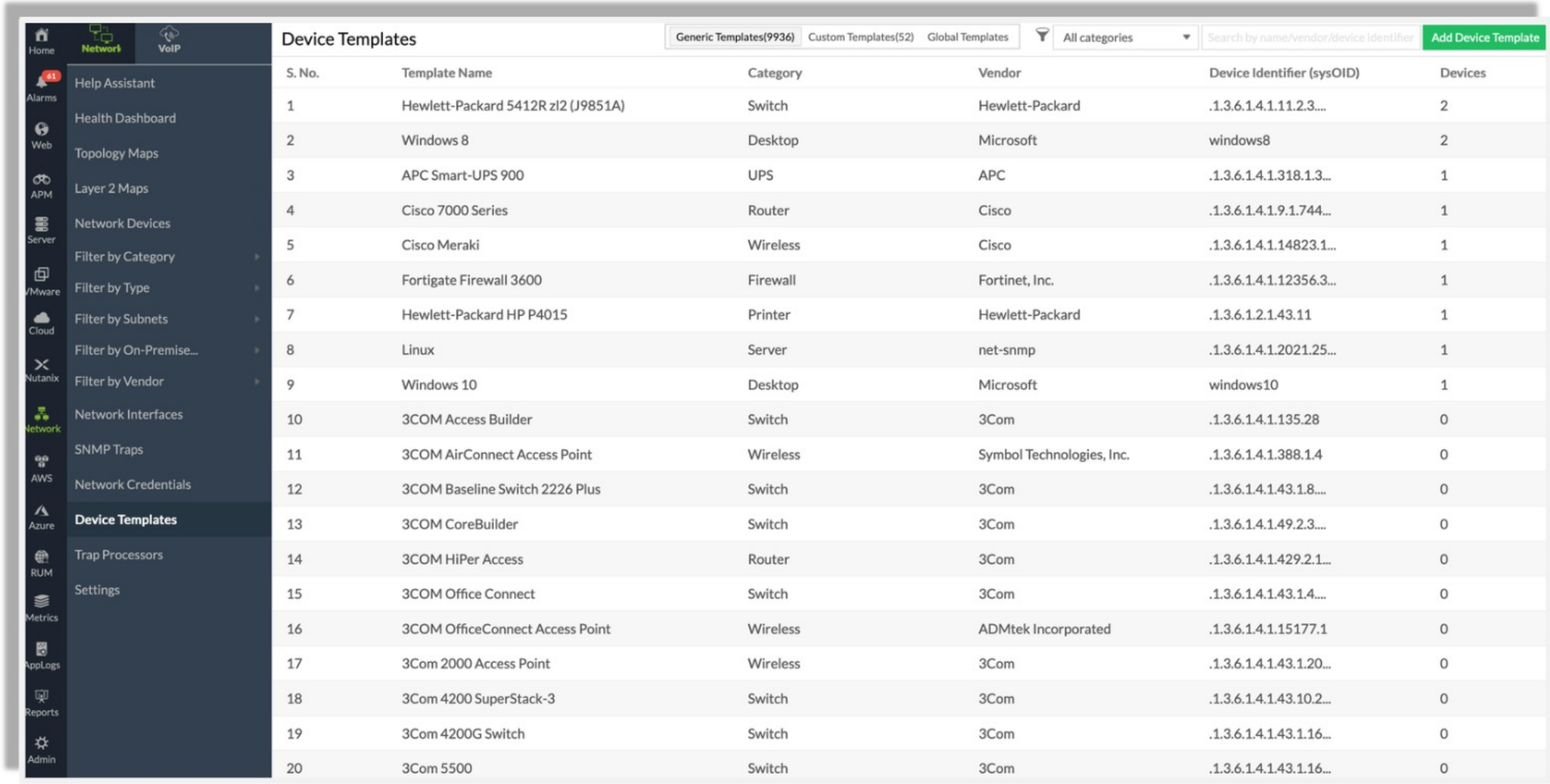
Network Monitoring Setup - Auto Discovery

- Automatically discover all the devices present within a provided IP range or within a whole network using SNMP
- Once the devices are discovered, device templates are automatically associated
- Performance metrics of the device and interface status will be immediately displayed in the web console

Supported vendors (Partial list)

- Alcatel, Barracuda Networks, Cisco, Canon Inc., Citrix Systems, Compaq, D-Link, Dell Inc., Epson, FortiGate, Hewlett Packard, Huawei, IBM, Intel Corporation, Juniper Networks, WatchGuard
- Additionally, with Site24x7 you can monitor new devices of any vendors by specifying the correct sysOID of the particular device

Device Templates for Auto Discovery



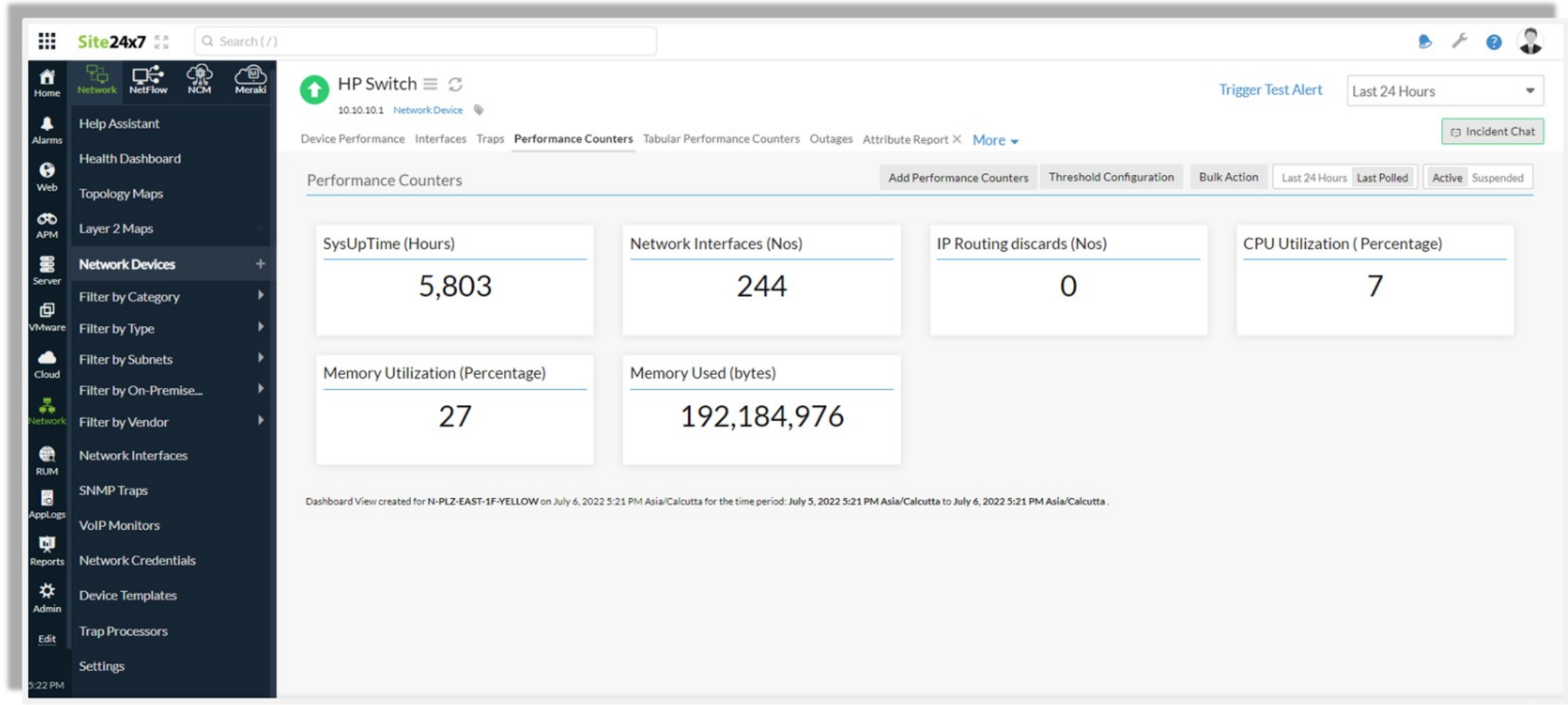
S. No.	Template Name	Category	Vendor	Device Identifier (sysOID)	Devices
1	Hewlett-Packard 5412R zl2 (J9851A)	Switch	Hewlett-Packard	.1.3.6.1.4.1.11.2.3....	2
2	Windows 8	Desktop	Microsoft	windows8	2
3	APC Smart-UPS 900	UPS	APC	.1.3.6.1.4.1.318.1.3...	1
4	Cisco 7000 Series	Router	Cisco	.1.3.6.1.4.1.9.1.744...	1
5	Cisco Meraki	Wireless	Cisco	.1.3.6.1.4.1.14823.1...	1
6	Fortigate Firewall 3600	Firewall	Fortinet, Inc.	.1.3.6.1.4.1.12356.3...	1
7	Hewlett-Packard HP P4015	Printer	Hewlett-Packard	.1.3.6.1.2.1.43.11	1
8	Linux	Server	net-snmp	.1.3.6.1.4.1.2021.25...	1
9	Windows 10	Desktop	Microsoft	windows10	1
10	3COM Access Builder	Switch	3Com	.1.3.6.1.4.1.135.28	0
11	3COM AirConnect Access Point	Wireless	Symbol Technologies, Inc.	.1.3.6.1.4.1.388.1.4	0
12	3COM Baseline Switch 2226 Plus	Switch	3Com	.1.3.6.1.4.1.43.1.8....	0
13	3COM CoreBuilder	Switch	3Com	.1.3.6.1.4.1.49.2.3....	0
14	3COM HiPer Access	Router	3Com	.1.3.6.1.4.1.429.2.1...	0
15	3COM Office Connect	Switch	3Com	.1.3.6.1.4.1.43.1.4....	0
16	3COM OfficeConnect Access Point	Wireless	ADMtek Incorporated	.1.3.6.1.4.1.15177.1	0
17	3Com 2000 Access Point	Wireless	3Com	.1.3.6.1.4.1.43.1.20...	0
18	3Com 4200 SuperStack-3	Switch	3Com	.1.3.6.1.4.1.43.10.2...	0
19	3Com 4200G Switch	Switch	3Com	.1.3.6.1.4.1.43.1.16...	0
20	3Com 5500	Switch	3Com	.1.3.6.1.4.1.43.1.16...	0

Site24x7

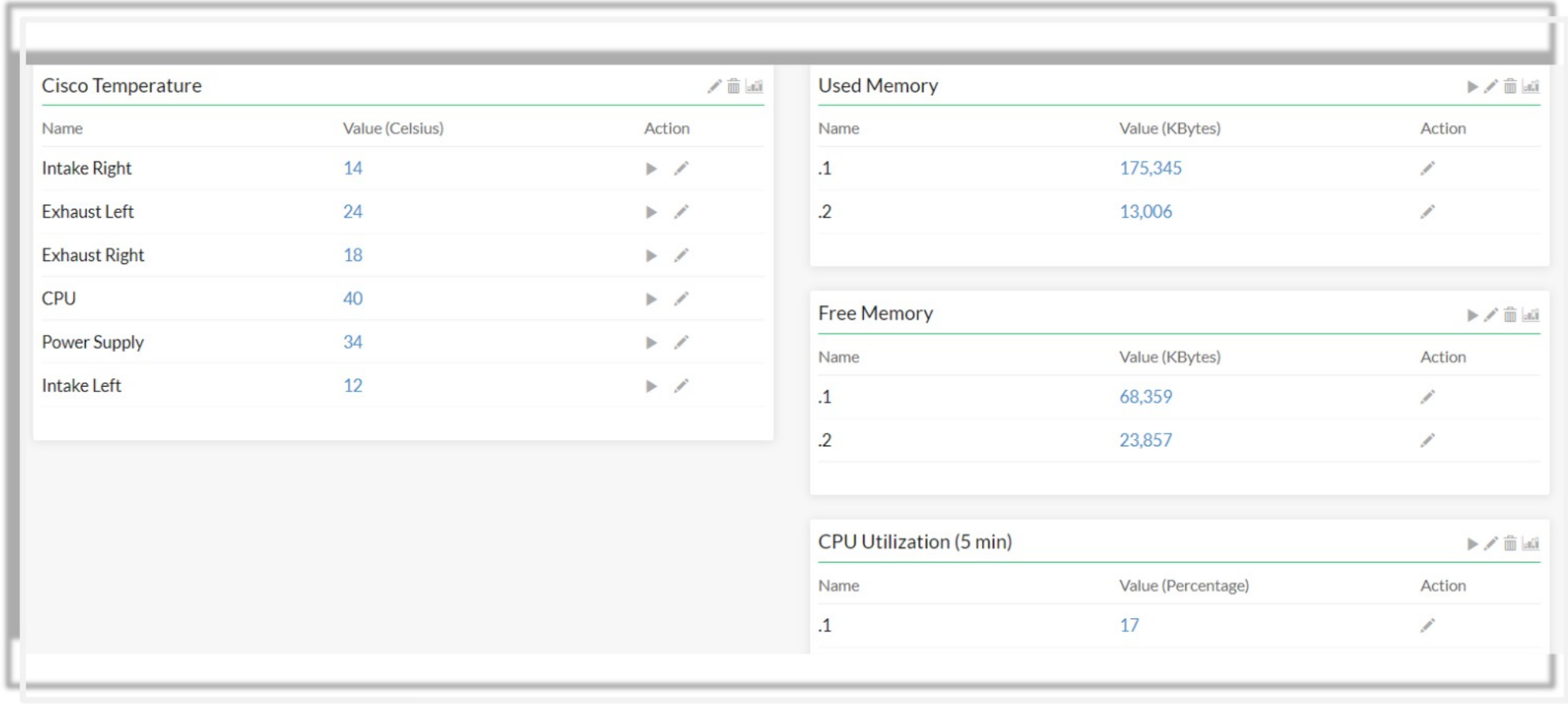
Performance Counters

- View Performance Counters associated with the device like temperature stats, memory, CPU Utilization, etc
- Add Tabular Performance Counters manually or by using the in-built MIB browser
- Create a *Table View* by including two or more performance counters to view together in a table format and add alerts to see which tabular performance counter generates alerts
- For monitoring special attributes apart from the basic performance counters provided by the vendor, add Custom Performance Counters from generic MIBs or Custom MIBs

Performance Counters



Tabular Performance Counters



Cisco Temperature

Name	Value (Celsius)	Action
Intake Right	14	
Exhaust Left	24	
Exhaust Right	18	
CPU	40	
Power Supply	34	
Intake Left	12	

Used Memory

Name	Value (KBytes)	Action
.1	175,345	
.2	13,006	

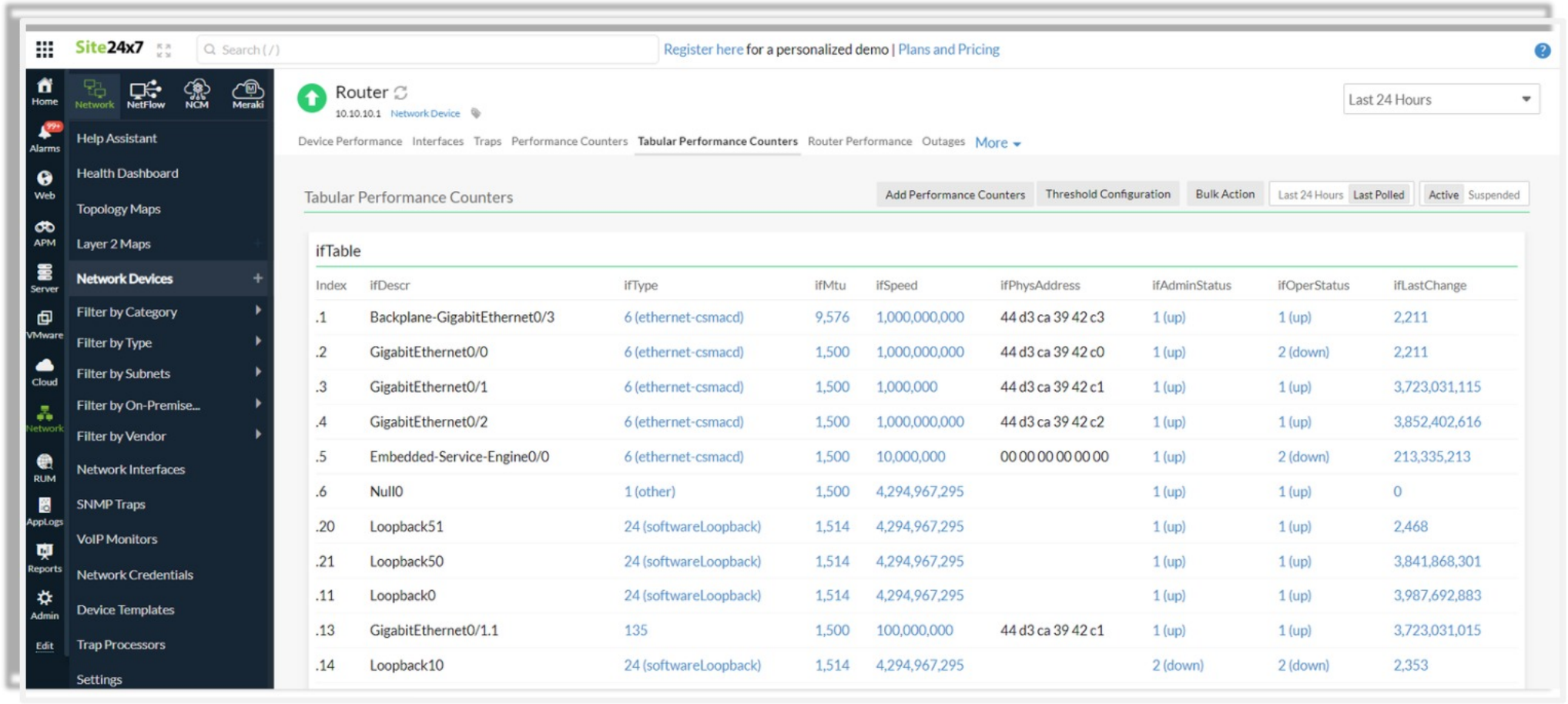
Free Memory

Name	Value (KBytes)	Action
.1	68,359	
.2	23,857	

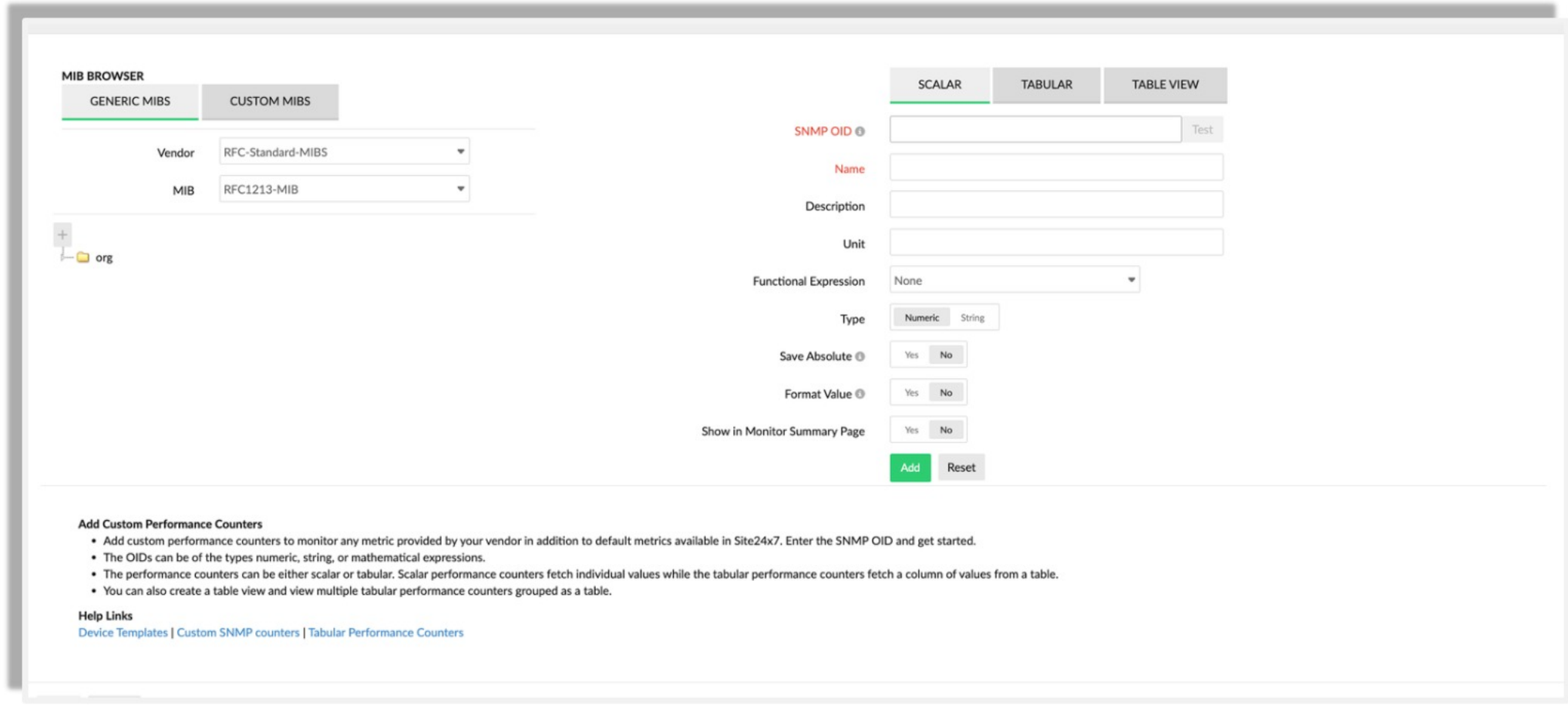
CPU Utilization (5 min)

Name	Value (Percentage)	Action
.1	17	

Table View for Performance Counters

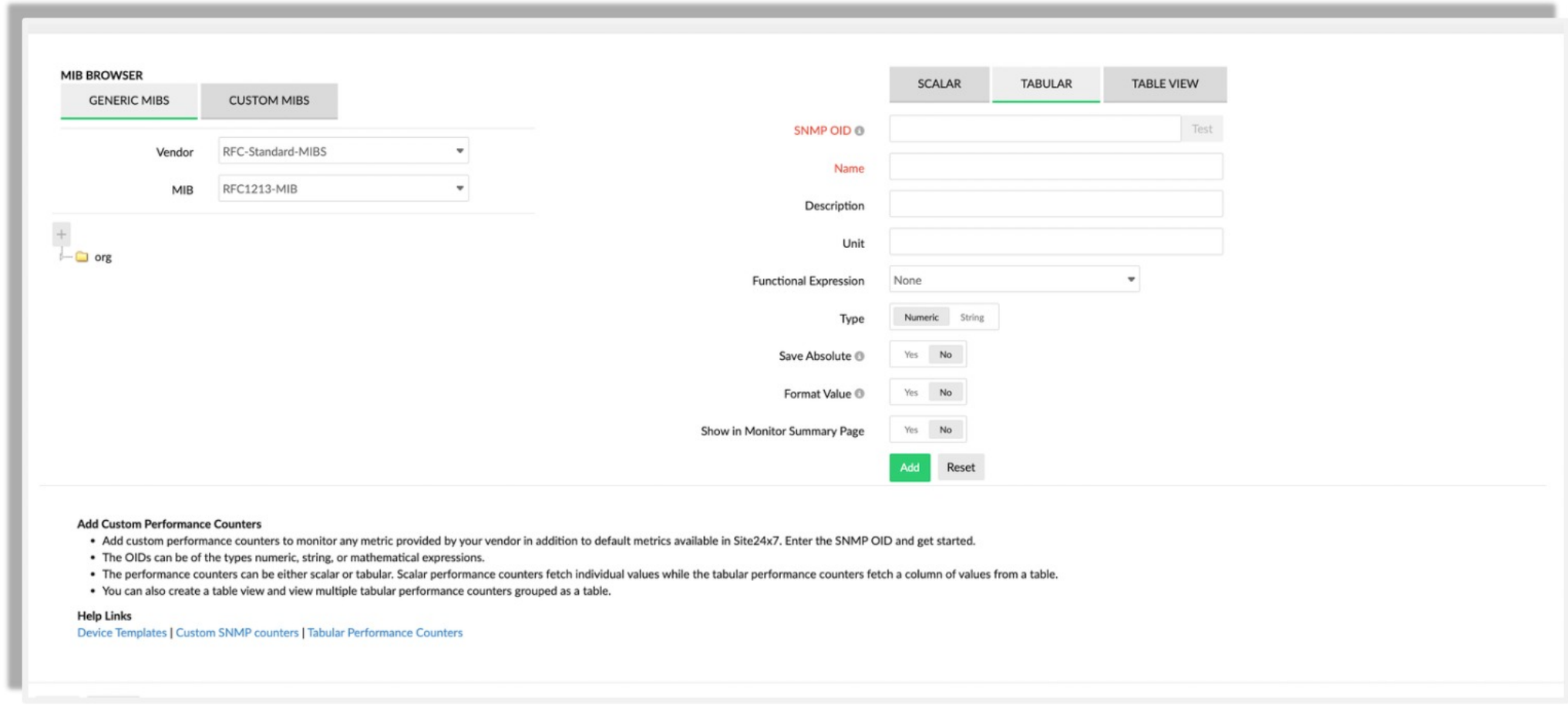


Adding Custom Performance Counters - Scalar



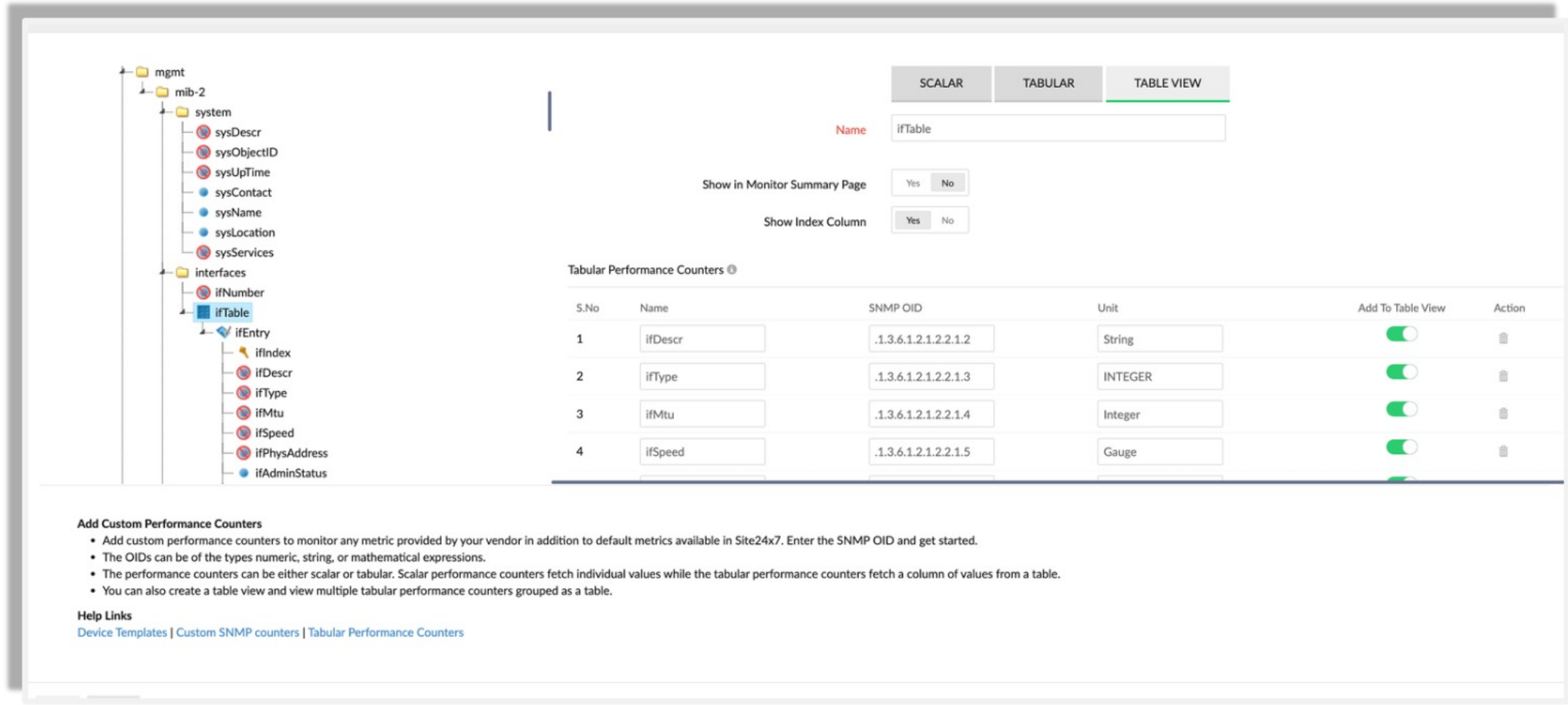
Site24x7

Adding Custom Performance Counters - Tabular



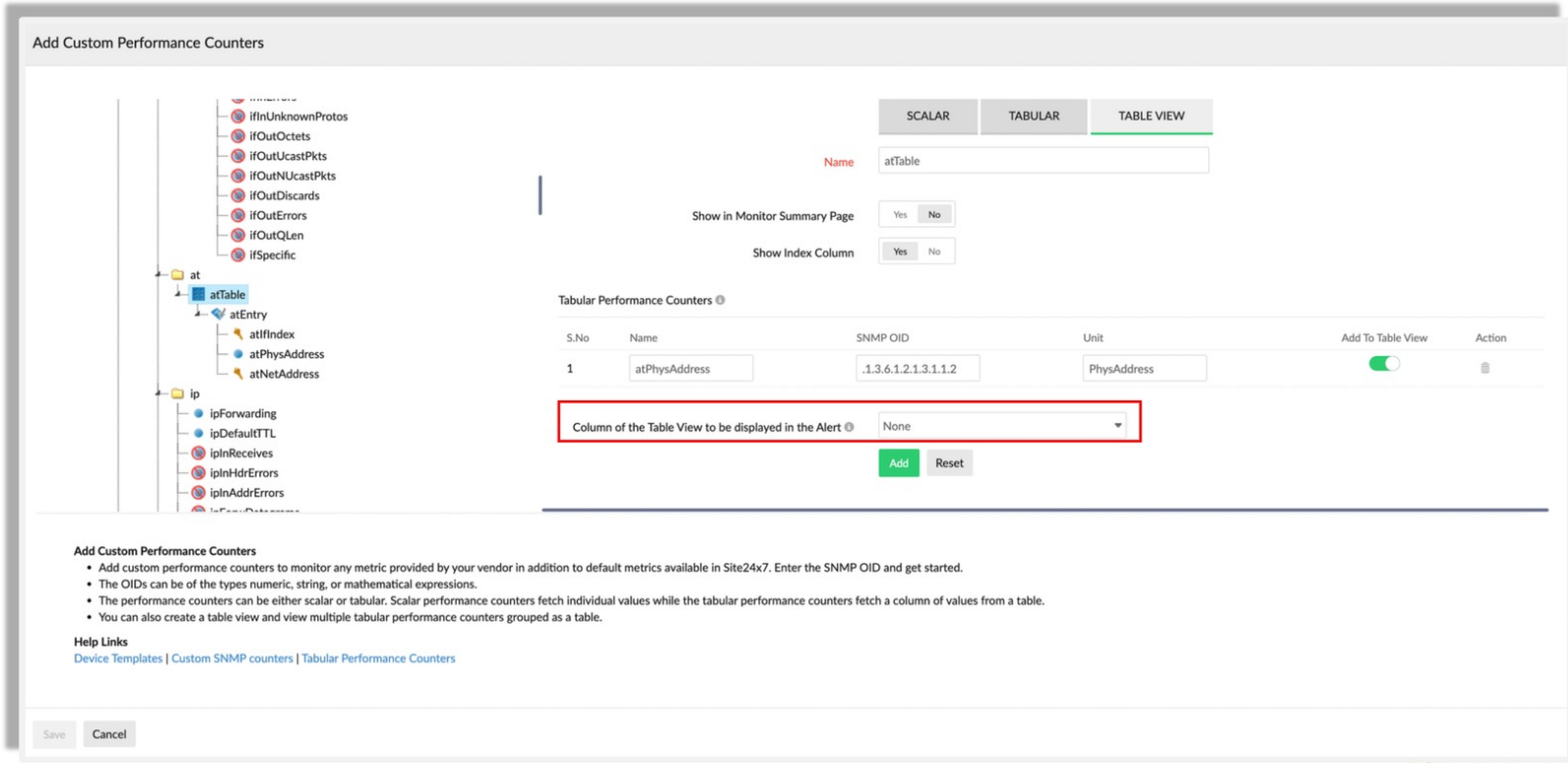
Site24x7

Adding Custom Performance Counters - Table View



Site24x7

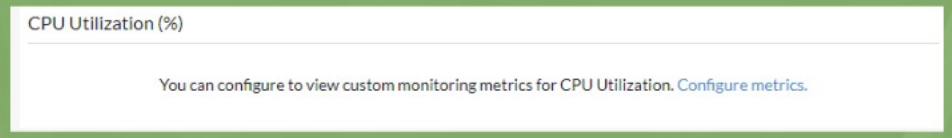
Adding Custom Performance Counters - Table View (Cont..)



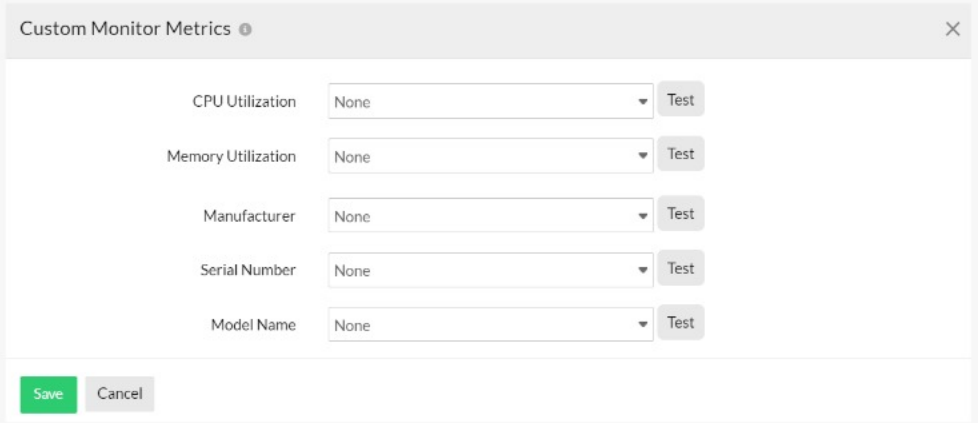
Site24x7

Adding Custom Monitor Metrics

If the Performance Counter value is not fetched with the default OIDs -

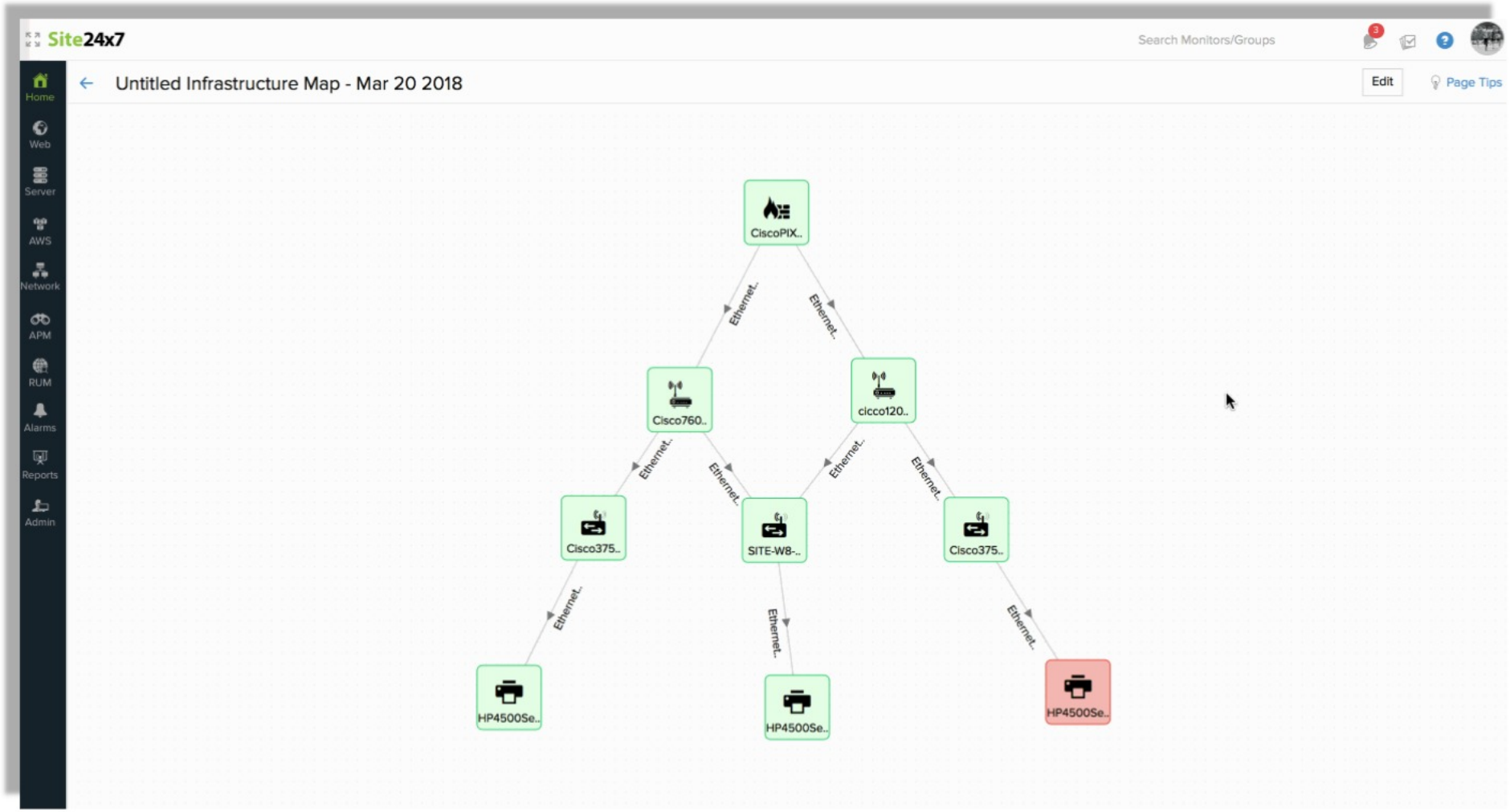


Add Custom Monitor Metrics



Site24x7

Viewing Details from Layer 2 Maps



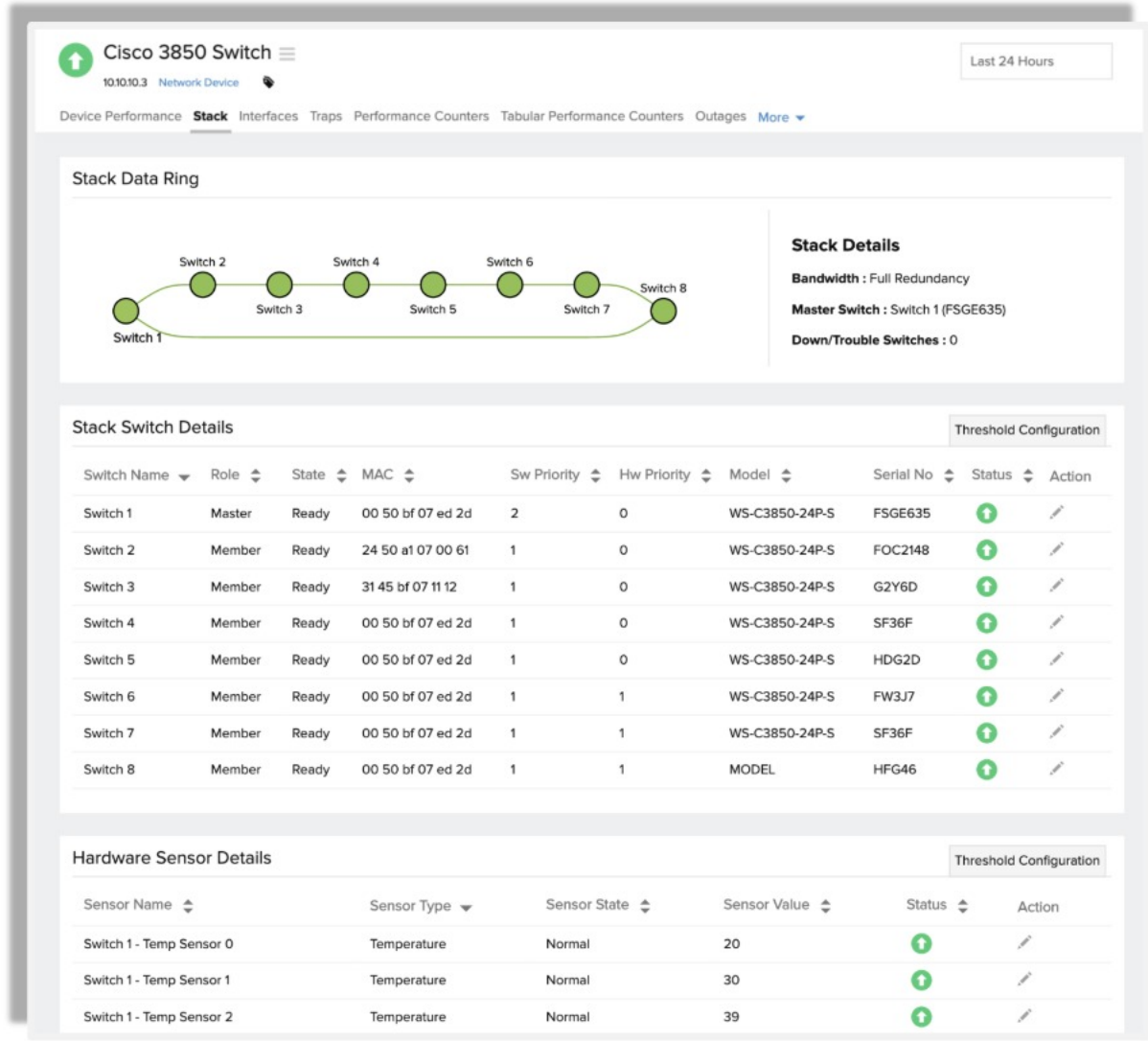
SNMP Traps

- Get instant notifications on detection of hardware and network issues using traps
- Site24x7 On-Premise Poller listens to traps from network devices via port UDP 162
- Set the trap destination host address as the IP address or the host name of the respective On-Premise Poller
- Set the trap destination port to be 162
- Save the configuration

Switch Stack Monitoring

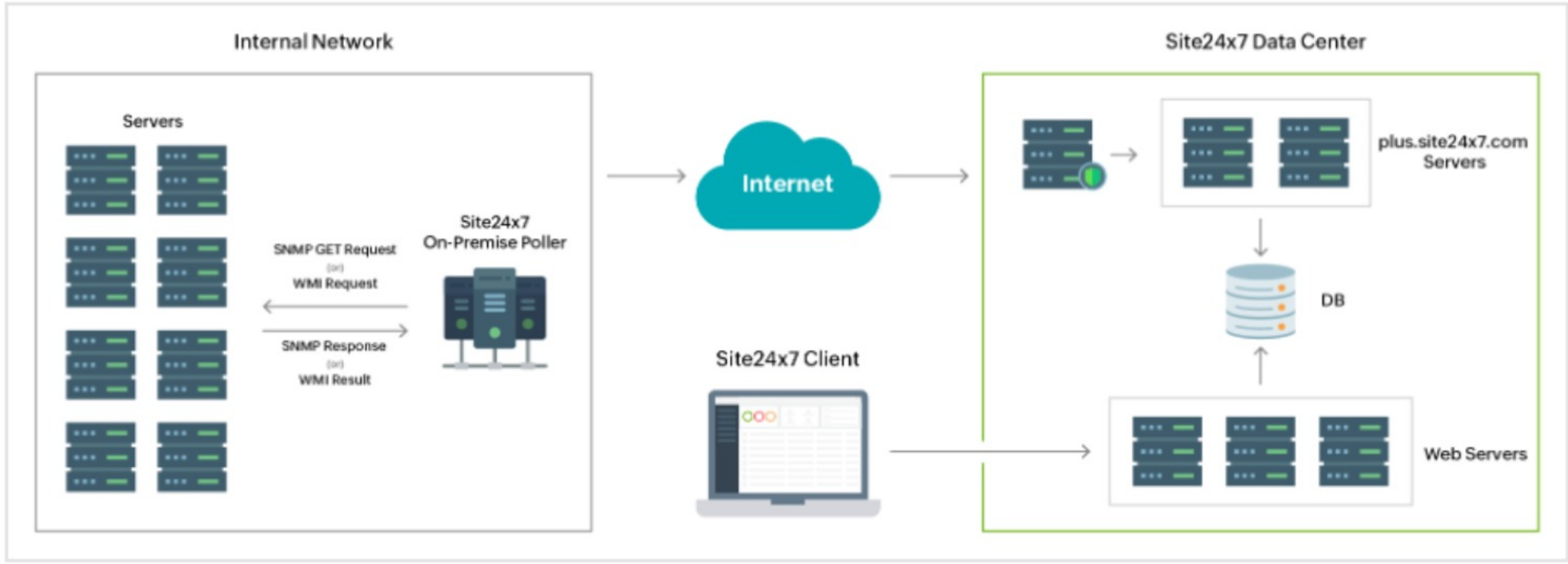
- Monitor your switch stacks and the switches connected to them with switch stack monitoring
- Drilled down monitoring at switch-level to check its health, performance, and status
- Visualize the status of every switch and its connection on the data ring

Switch Stack Monitoring Metrics Collected



Site24x7

SNMP and WMI based Agentless Server Monitoring



SNMP and WMI Server Monitoring Architecture

NetFlow Analyzer

Site24x7

NetFlow Analyzer - Introduction

- Obtain complete visibility into your network traffic and bandwidth performance in real time
- Identify traffic peaks, top applications, and conversations using different flow technologies so that you can analyze for what and by whom your bandwidth is being used

Prerequisites

- To perform network traffic analysis using Site24x7, you must install an On-Premise Poller (version: 4.6.0 or above) in the network being monitored
- The devices should be able to export flows to Site24x7

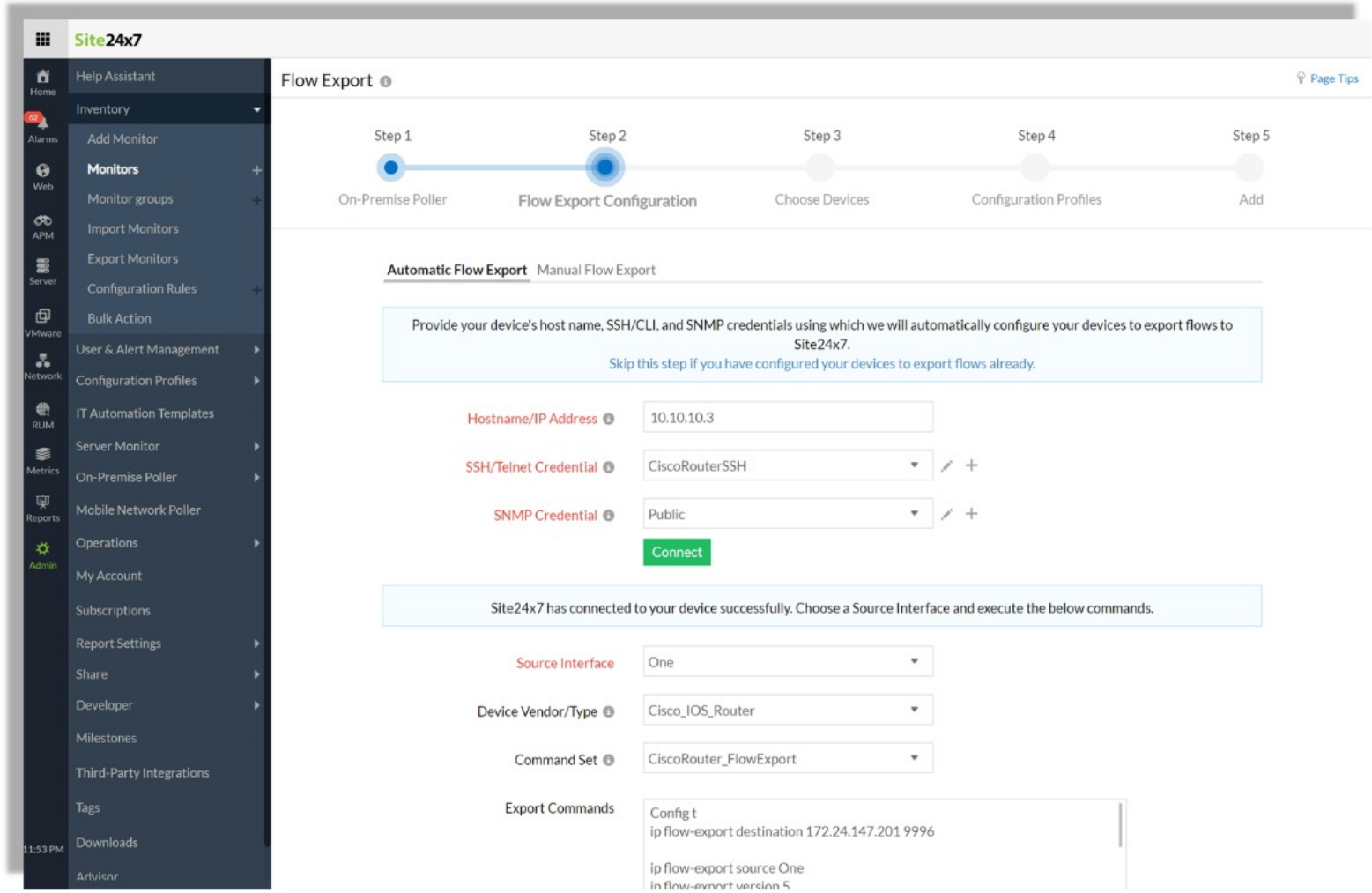
Supported Flows

- NetFlow
- J-Flow
- SFlow
- IPFIX
- NetStream
- AppFlow
- CFlow

Adding a device to monitor NetFlow

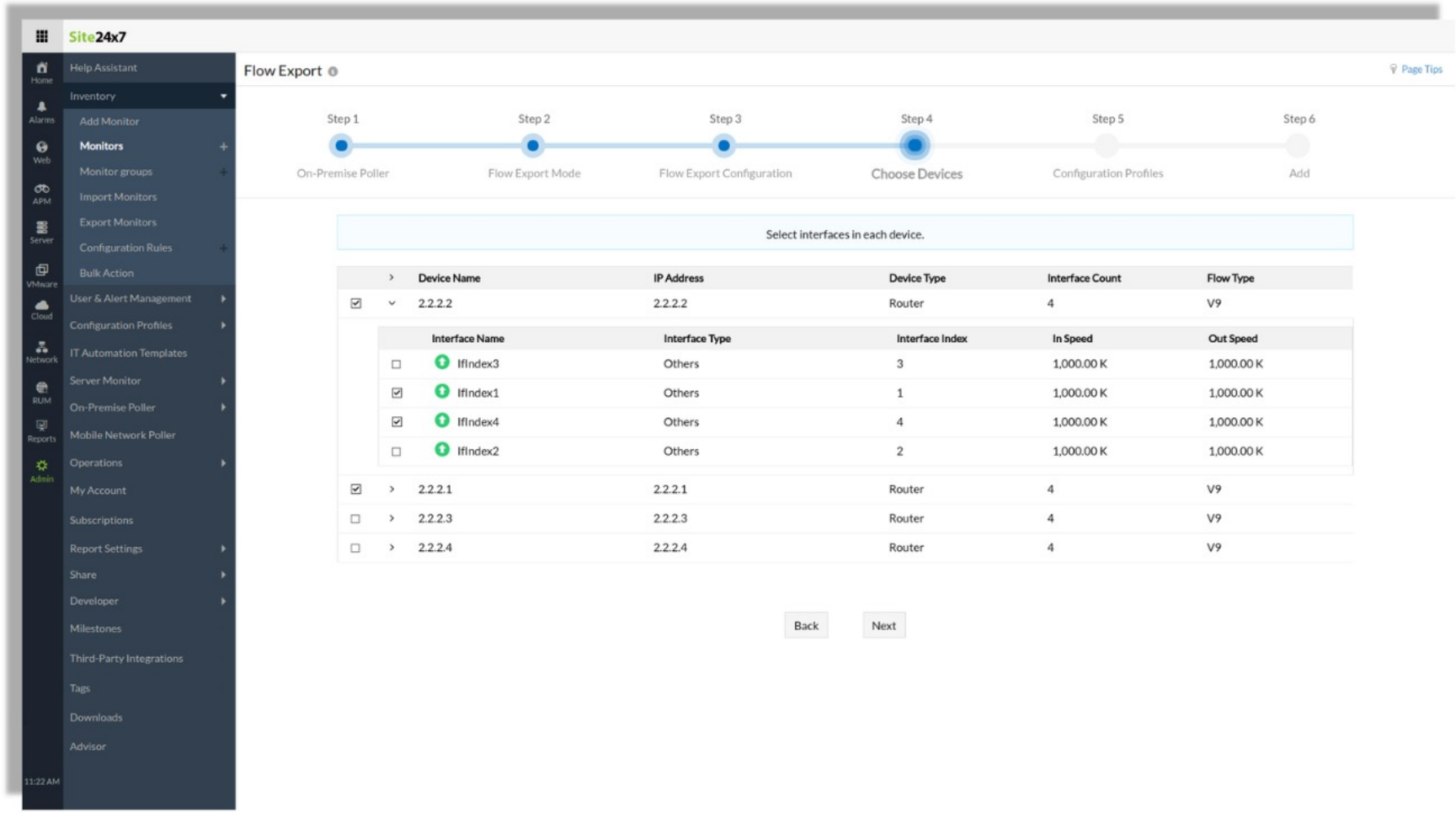
- Choose an On-Premise Poller
- Configure the devices to export flows
  (Flow export configuration - Automatic/Manual)
- Choose devices and interfaces
- Organize your monitors and configure profiles
- Verify your entries and export flows for monitoring

Adding a device to monitor NetFlow



Site24x7

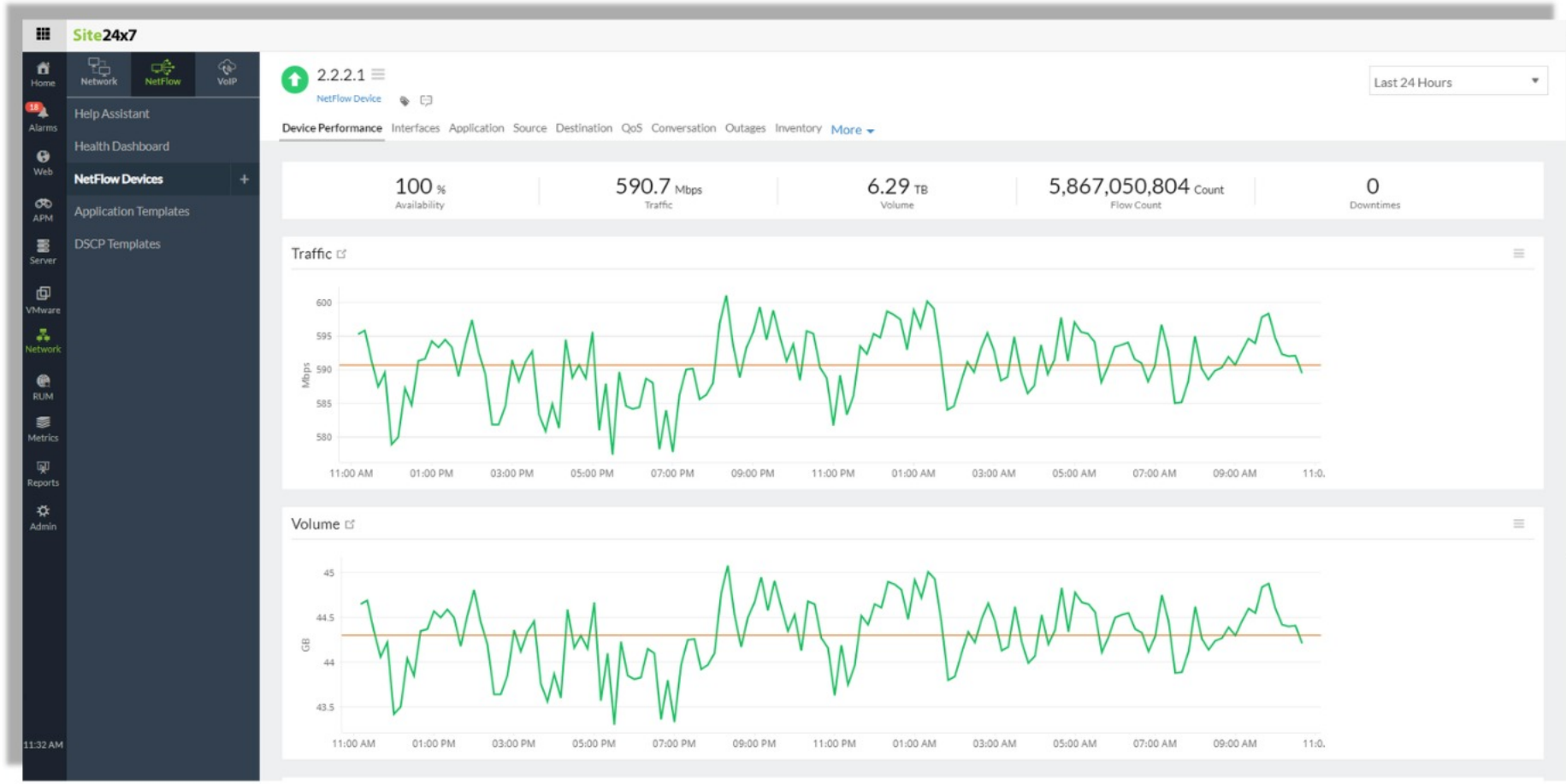
Adding a device to monitor NetFlow



Supported Templates

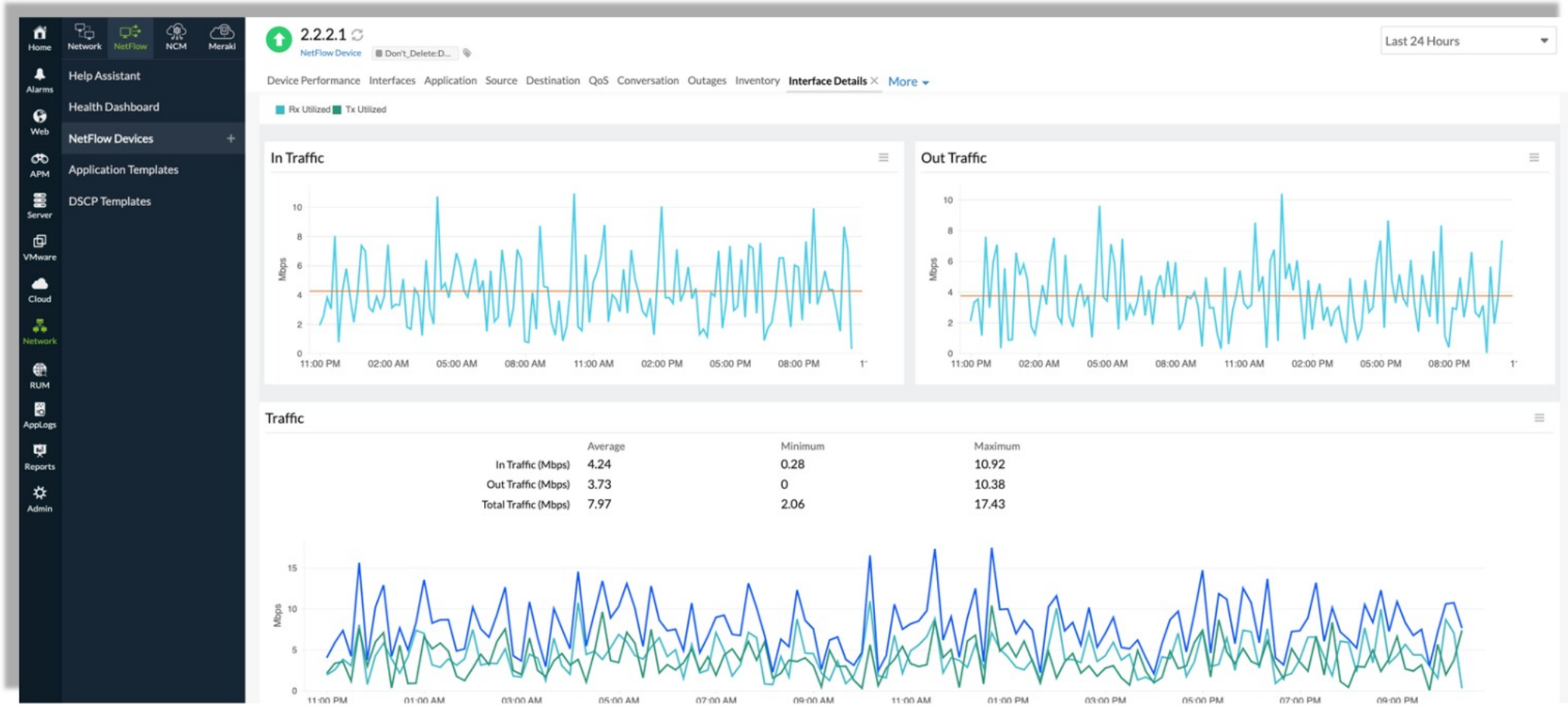
- Application Templates
- DSCP Templates

NetFlow: Device Metrics



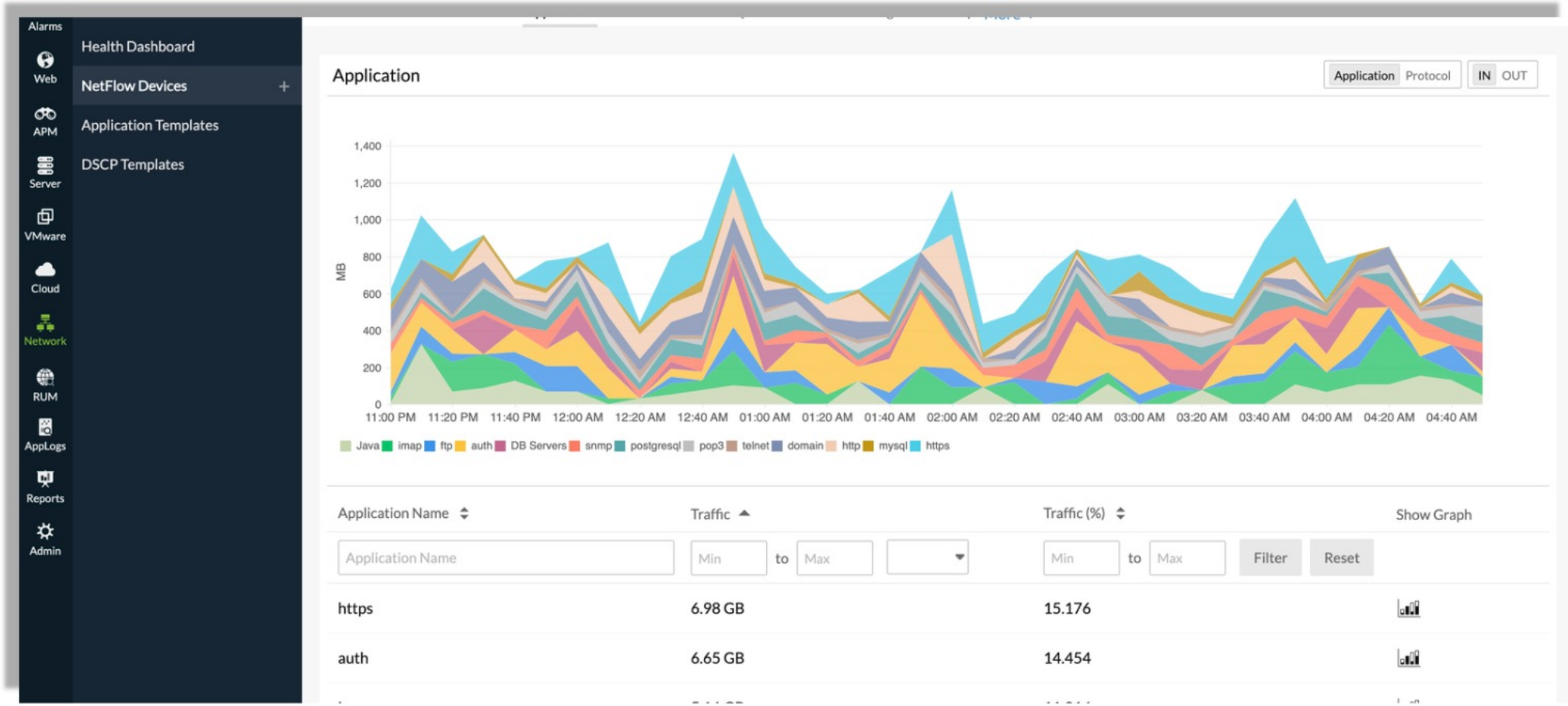
Site24x7

NetFlow: Interface Metrics



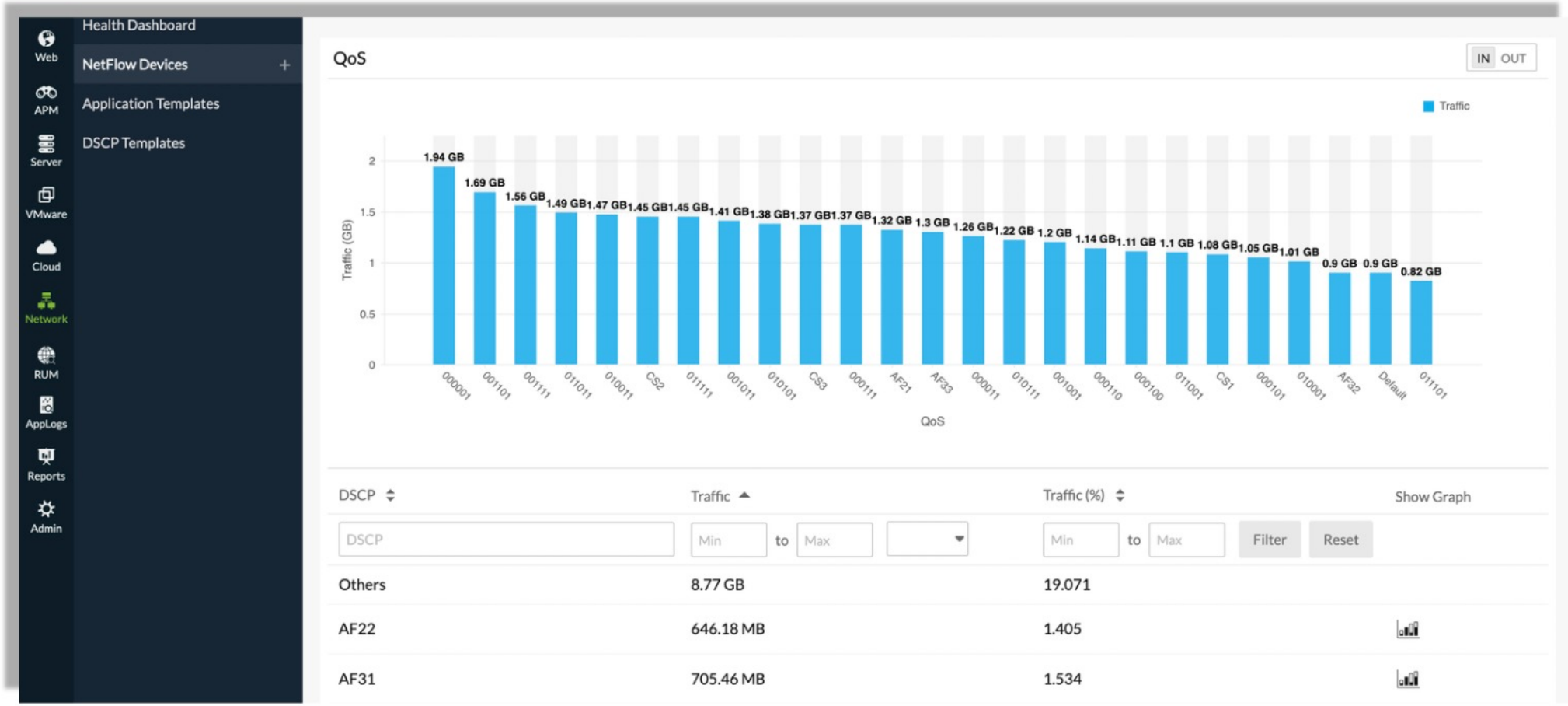
Site24x7

NetFlow: Application Metrics



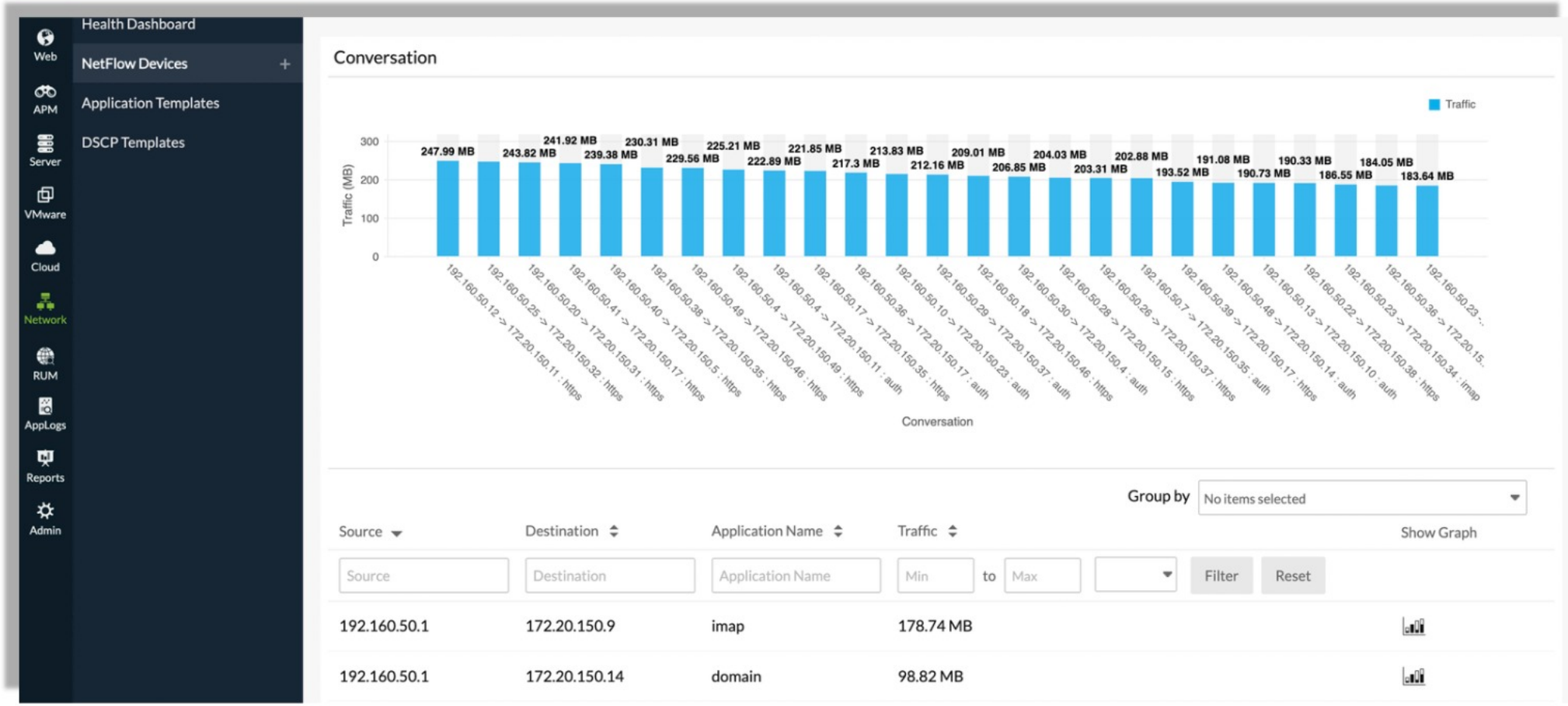
Site24x7

NetFlow: QoS Metrics



Site24x7

NetFlow: Conversation Metrics



Site24x7

Network Configuration Manager

Site24x7

Network Configuration Manager - Introduction

- Multi-vendor network device change and configuration management tool
- Allows you to
  - Continuously track and alert on the configuration changes
  - Compare configuration versions
  - Perform audits
  - Restore configurations
  - Automate device configuration backups

Prerequisites

- On-Premise Poller version 5.2.0 or above

System Requirements

Maximum no. of devices per On-Premise Poller	Processor	RAM	Disk space for aggregate data
100	4 processors	8 GB	100 GB or higher
500	8 processors	16 GB	100 GB or higher

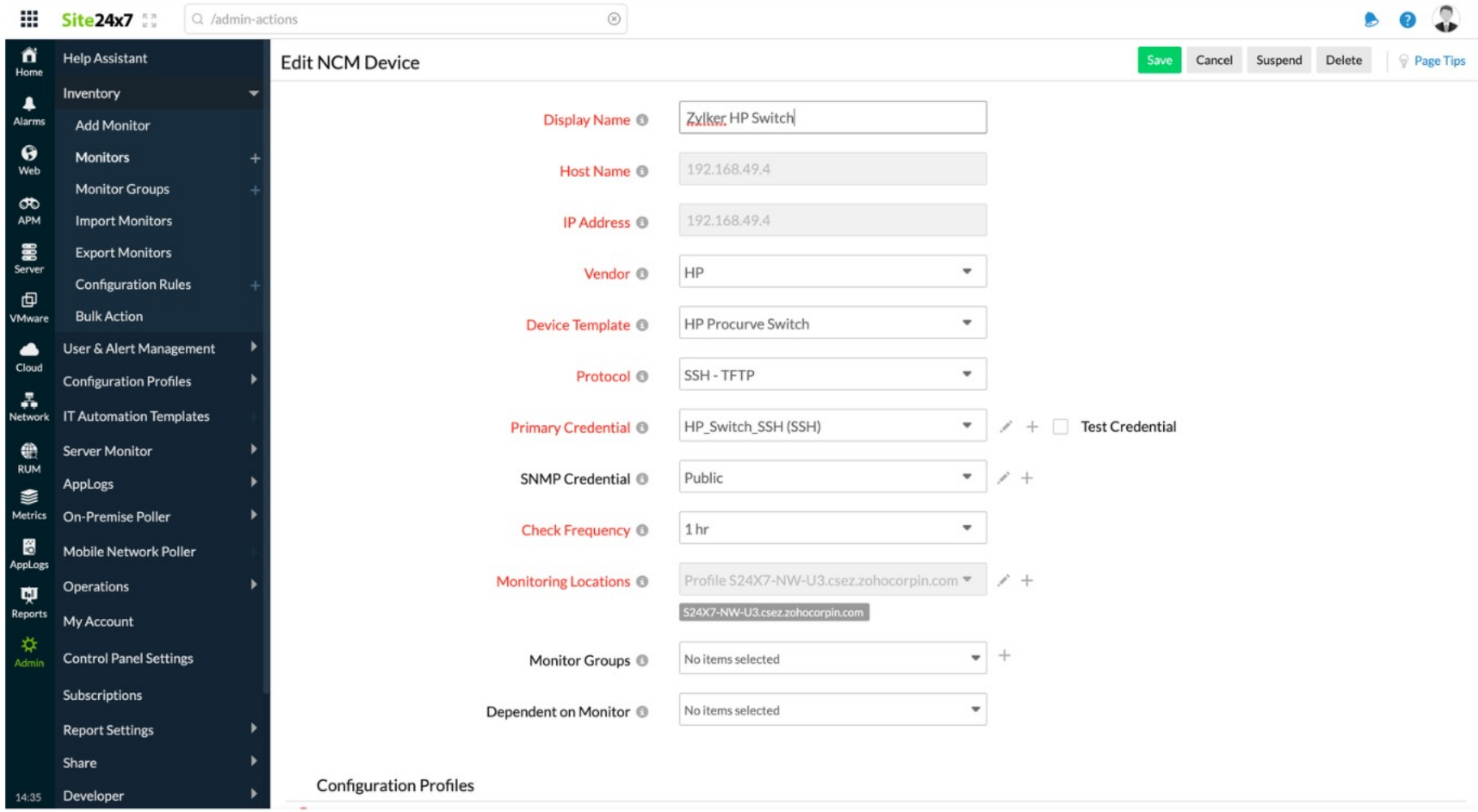
Port Requirements

Port health	Default port number
TFTP port	69
SSHD port	22
Telnet port	23
Syslog server	514

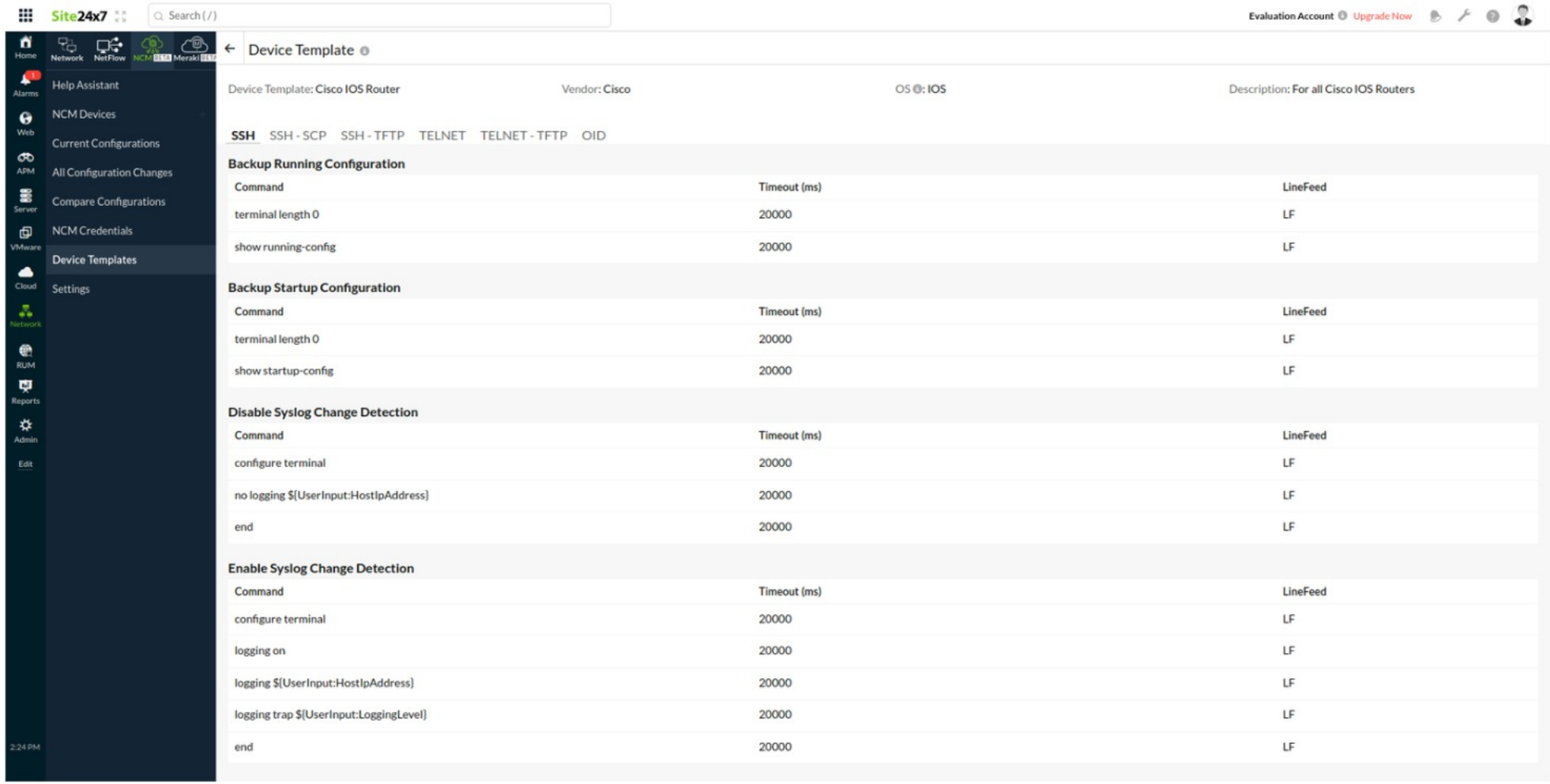
Enable Network Configuration Manager

- Log in to your Site24x7 account
- Navigate to Network > NCM > Settings
- Once the Manage NCM page pops up, choose an On-Premise Poller from the drop-down
- Toggle to Enable
- Wait 5-10 minutes
- Navigate to Admin > On-Premise Poller and ensure that the On-Premise Poller and the network module are running

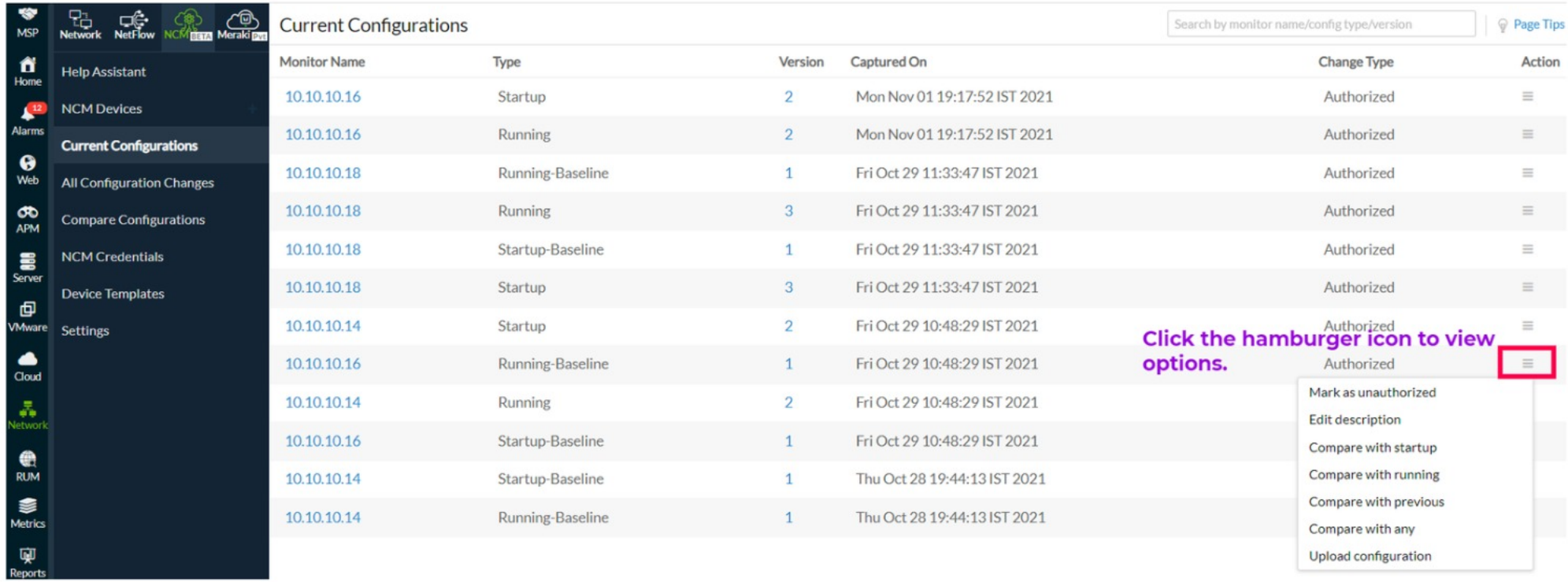
Add devices


Site24x7
/admin-actions
Home
Alarms
Web
APM
Server
VMware
Cloud
Network
RUM
Metrics
AppLogs
Reports
Admin
Help Assistant
Inventory
Add Monitor
Monitors
Monitor Groups
Import Monitors
Export Monitors
Configuration Rules
Bulk Action
User & Alert Management
Configuration Profiles
IT Automation Templates
Server Monitor
AppLogs
On-Premise Poller
Mobile Network Poller
Operations
My Account
Control Panel Settings
Subscriptions
Report Settings
Share
Developer
14:35
Edit NCM Device
Save
Cancel
Suspend
Delete
Page Tips
Display Name
Zylker HP Switch
Host Name
192.168.49.4
IP Address
192.168.49.4
Vendor
HP
Device Template
HP Procurve Switch
Protocol
SSH - TFTP
Primary Credential
HP_Switch_SSH (SSH)
Test Credential
SNMP Credential
Public
Check Frequency
1 hr
Monitoring Locations
Profile S24X7-NW-U3.csez.zohocorpin.com
S24X7-NW-U3.csez.zohocorpin.com
Monitor Groups
No items selected
Dependent on Monitor
No items selected
Configuration Profiles

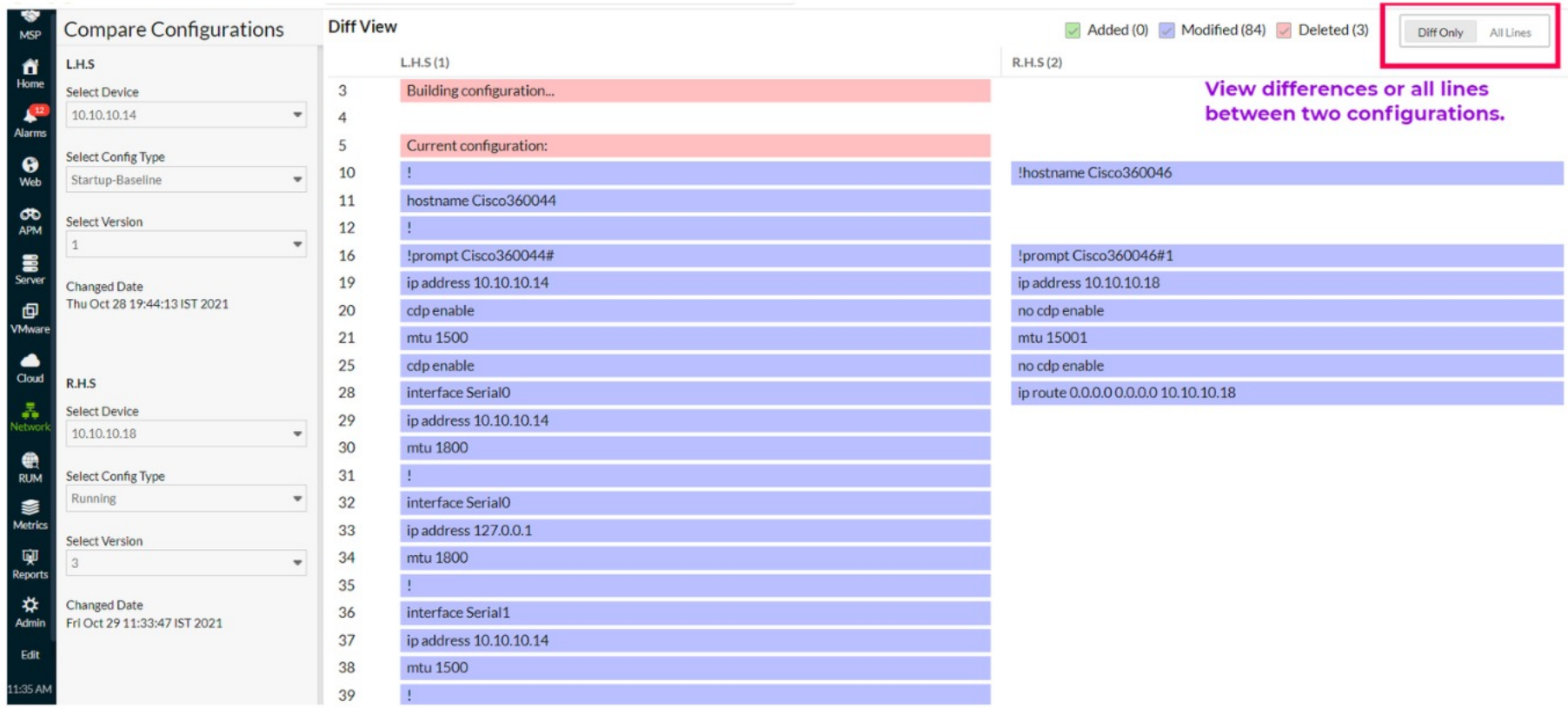
Device templates



Current configurations



Compare configurations



Site24x7

VoIP Monitoring

Site24x7

VoIP Monitoring

- With Site24x7, you can assess the quality of VoIP call services through out the call path using Cisco Internet Protocol Service Level Agreement (IPSLA)
- Analyzing the network and the call transmission across the call path will help to troubleshoot and rectify issues

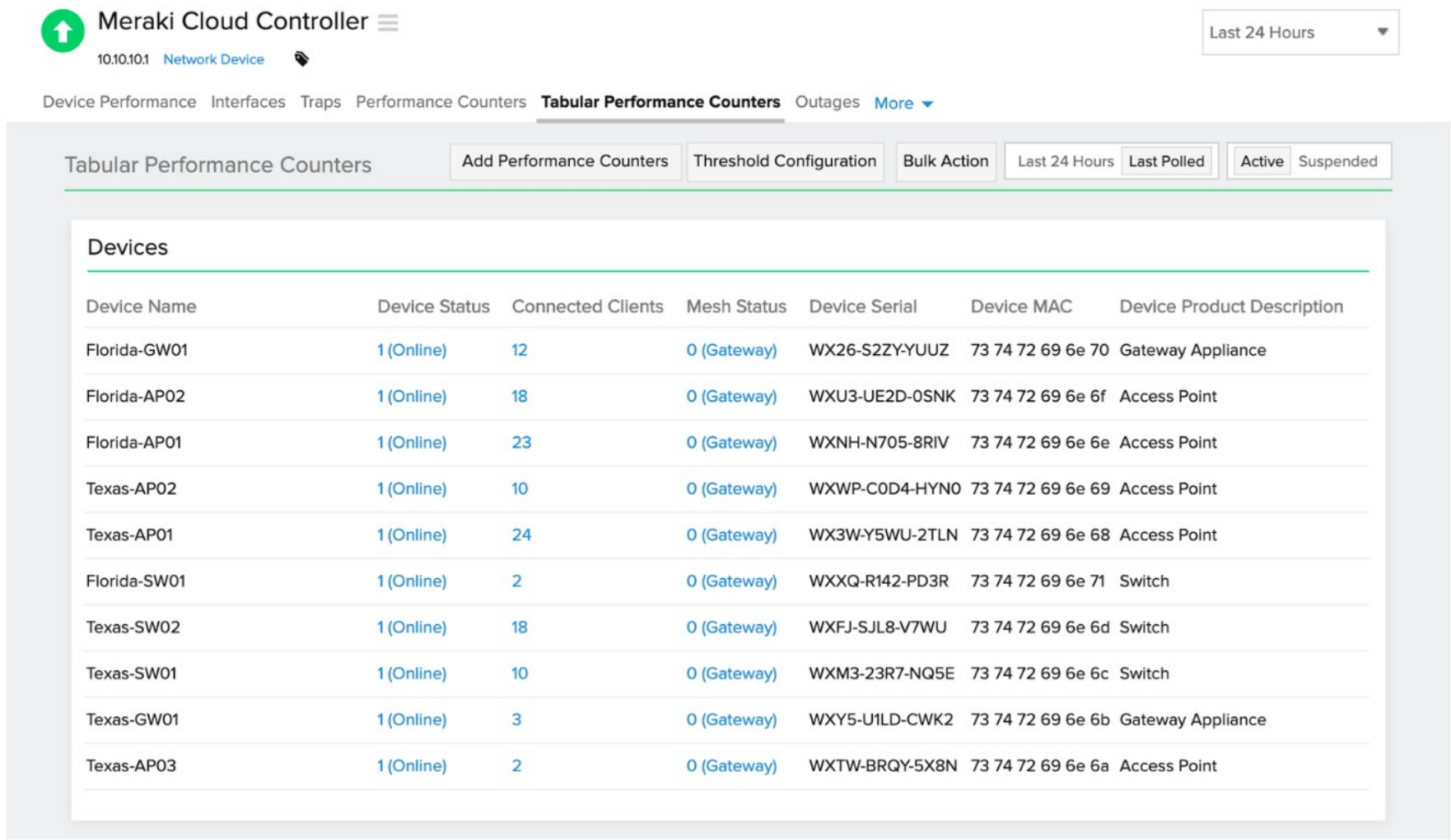
Prerequisites

- Install Site24x7 On-Premise Poller
- Both the source and the destination devices should be a Cisco switch, firewall, or router
- The Cisco Internetwork Operating System (IOS) version should be 12.4 or later
- Enable IPSLA in the destination device
- The source device and the interface should be monitored by Site24x7 with SNMP read-write community credentials

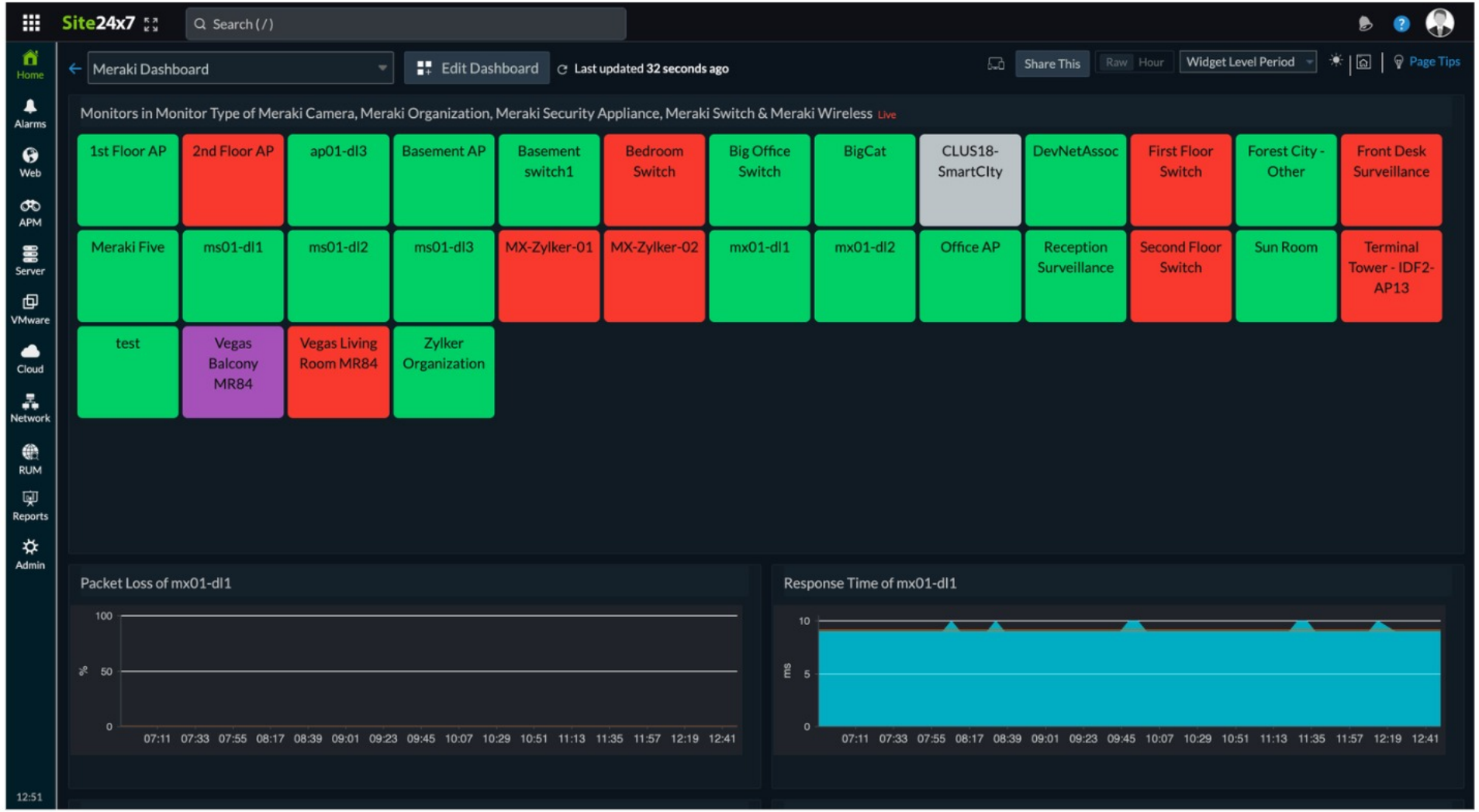
Cisco Meraki Monitoring

Site24x7

SNMP-based


Meraki Cloud Controller
10.10.10.1 Network Device
Last 24 Hours
Device Performance Interfaces Traps Performance Counters Tabular Performance Counters Outages More
Tabular Performance Counters
Add Performance Counters
Threshold Configuration
Bulk Action
Last 24 Hours Last Polled
Active Suspended
Devices
Device Name | Device Status | Connected Clients | Mesh Status | Device Serial | Device MAC | Device Product Description
Florida-GW01 | 1 (Online) | 12 | 0 (Gateway) | WX26-S2ZY-YUUZ | 73 74 72 69 6e 70 | Gateway Appliance
Florida-AP02 | 1 (Online) | 18 | 0 (Gateway) | WXU3-UE2D-0SNK | 73 74 72 69 6e 6f | Access Point
Florida-AP01 | 1 (Online) | 23 | 0 (Gateway) | WXNH-N705-8RIV | 73 74 72 69 6e 6e | Access Point
Texas-AP02 | 1 (Online) | 10 | 0 (Gateway) | WXWP-C0D4-HYN0 | 73 74 72 69 6e 69 | Access Point
Texas-AP01 | 1 (Online) | 24 | 0 (Gateway) | WX3W-Y5WU-2TLN | 73 74 72 69 6e 68 | Access Point
Florida-SW01 | 1 (Online) | 2 | 0 (Gateway) | WXXQ-R142-PD3R | 73 74 72 69 6e 71 | Switch
Texas-SW02 | 1 (Online) | 18 | 0 (Gateway) | WXFJ-SJL8-V7WU | 73 74 72 69 6e 6d | Switch
Texas-SW01 | 1 (Online) | 10 | 0 (Gateway) | WXM3-23R7-NQ5E | 73 74 72 69 6e 6c | Switch
Texas-GW01 | 1 (Online) | 3 | 0 (Gateway) | WXY5-U1LD-CWK2 | 73 74 72 69 6e 6b | Gateway Appliance
Texas-AP03 | 1 (Online) | 2 | 0 (Gateway) | WXTW-BRQY-5X8N | 73 74 72 69 6e 6a | Access Point

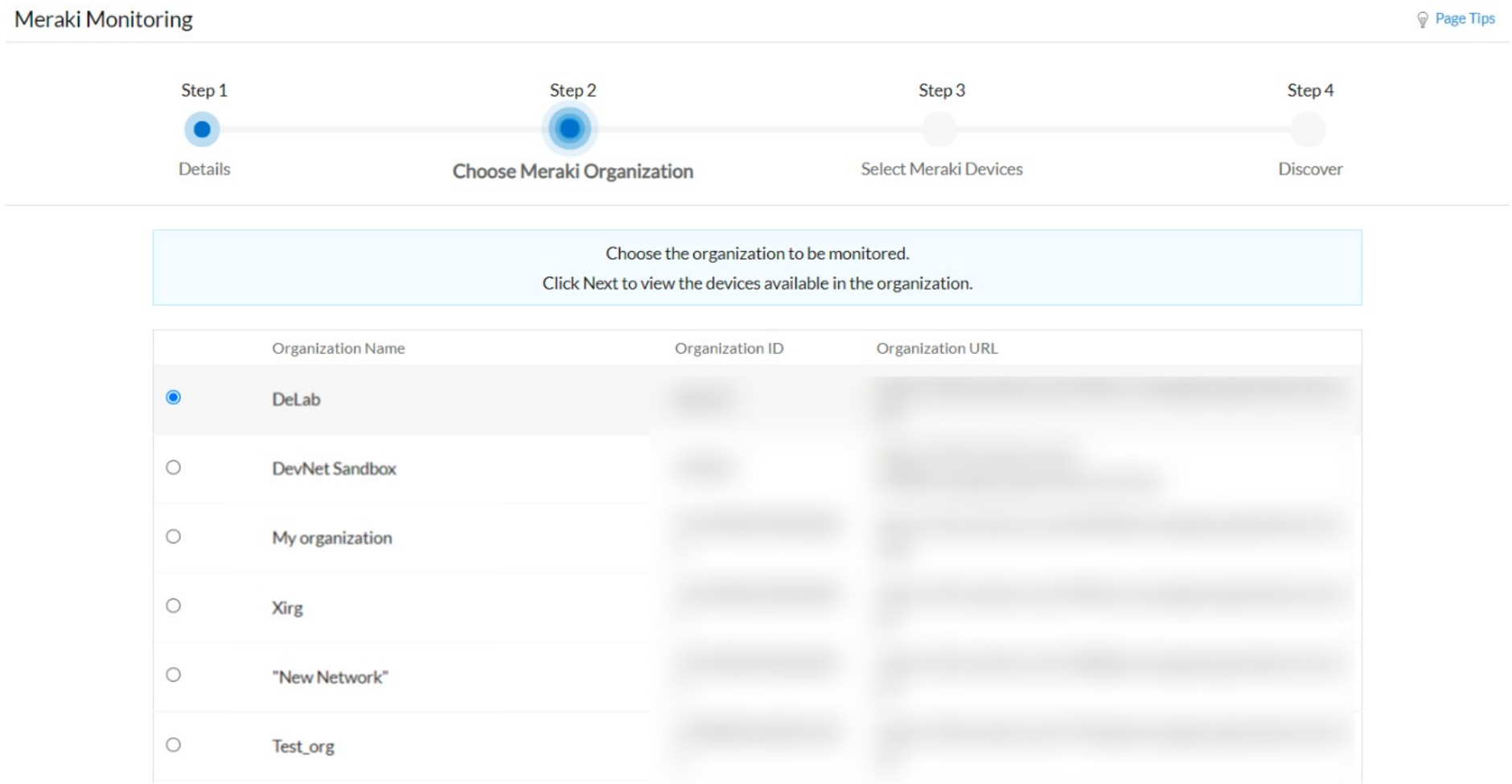
REST API-based



Prerequisites

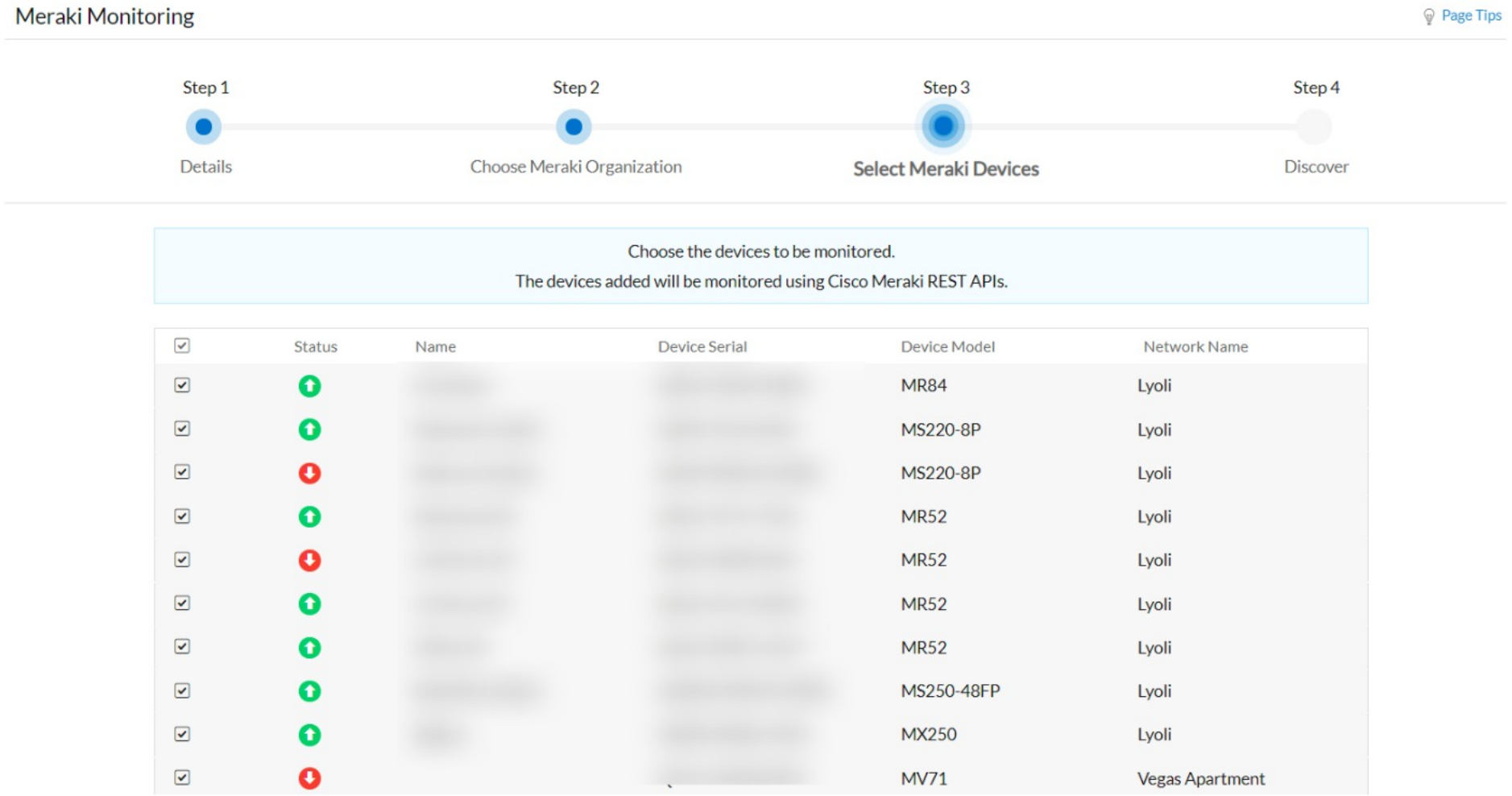
- The Meraki REST API key generated in your Cisco Meraki dashboard needs to be granted read-only access to Site24x7.

Add Meraki organization & Devices to be monitored



Site24x7

Add Meraki organization & Devices to be monitored



Site24x7

VMware Monitoring

Site24x7

VMware Monitoring - Introduction

- Automatically discover and map your entire vSphere environment, from data centers to VMs, in real time
- Monitor different CPU, memory, disk, and network metrics from time to time to understand how each component is performing
- Obtain performance metrics at the host level, VM level, and guest OS level, and correlate them for complete VMware performance monitoring
- Avoid resource contention and optimize resource allocation so you can ensure your capacity planning is also accurate

VMware vCenter Monitoring

- Auto-discover your entire virtual infrastructure through VMware vCenter and visualize critical metrics in one view

- Prerequisites:
  > Site24x7 On-Premise Poller
  > Access to Managed Object Browser
  > VMware Read-only or Administrator roles to monitor vCenter

VMware resources	Privilege	Reason
vCenter	No additional privileges are required	
ESX/ESXi host	No additional privileges are required	
Virtual machine (VM)	*Interact.PowerOff*, *Interact.PowerOn*, and *Interact.Reset* for the connected ESX/ESXi host	To stop, start, and reset VMs for the Site24x7 console
Datastore	*Browse* and *Config* for all connected ESX/ESXi hosts	To perform basic monitoring
Resource pool	No additional privileges are required	
All types	*System.Read*, *System.View*, and *System.Anonymous*	Default privileges for **Read Only** role.

- Reference:https://support.site24x7.com/portal/en/kb/articles/vmware-privileges-required

Different types of polling for VMware resources

- **VMware vCenter-based polling :** Here, you can provide your vCenter credentials, and Site24x7 use the same to monitor all the associated ESX/ESXi host, VMs, datastores, Snapshots, hardware, and resource pools
- vCenter-based polling works from On-Premise Poller version 4.6.4. Hence, upgrade your On-Premise Poller to this version or the latest

- **VMware ESX/ESXi-based polling :** In this case, you need to create user credentials at each ESX/ESXi host level and enable the required privileges
- This has to be done at the individual ESX/ESXi host level to monitor the ESX/ESXi host and its associated VMs, datastores, Snapshots, hardware, and resource pools
- You can choose the type of polling while adding the ESX/ESXi host monitors

VMware ESX/ESXi Monitoring

- Gain in-depth insights on critical performance metrics of CPU, memory, disk, datastore, and network of your ESX/ESXi servers
- You can also add your VMware datastores and resource pools for monitoring while adding ESX/ESXi hosts
- Prerequisites:
  > Site24x7 On-Premise Poller
  > Access to Managed Object Browser
  > VMware Read-only or Administrator roles to monitor ESX/ESXi servers

VMware VM Monitoring

- Track the performance of your virtual environment and gain exhaustive reports on disk I/O, datastore, network and memory of virtual servers
- You will need to add an ESX/ESXi host first, and this will in turn discover the VMs mapped to it
- Prerequisites:
  > Site24x7 On-Premise Poller
  > VMware Read Only or Administrator roles along with Interact.PowerOff, Interact.PowerOn, and Interact.Reset privileges for the connected ESX/ESXi host

VMware VM Monitor and Server Monitor Integration

- If you're monitoring your VMware virtual machines (VMs) via both Site24x7 VMware Monitoring and the server agent, you can integrate both for a unified view of VM metrics, as well as guest OS metrics

- **Benefits**

  By integrating your VM and server monitors, you'll be able to view the following additional metrics for your VMware VM monitor:

  > CPU, memory, thread count, and handle count of all your Windows services

  > CPU and memory use, number of instances, thread count, and handle count of all your processes

  > Additional guest OS network-level metrics like data sent, data received, packets sent, packets received, and bandwidth

  > You can also perform URL checks, port checks, file checks, directory checks, and NFS checks

  > From the Tools tab, you can execute commands and WMI queries

  > You will also receive support for Site24x7 AppLogs

How to integrate?

- To integrate, your VM should be monitored both via the server agent and Site24x7 VMware Monitoring

  1. Go to the VMware tab
  2. Click on the desired VM monitor name
  3. Go to the Processes tab
  4. Click Integrate

- If your VM isn't monitored using the server agent, you need to download the server agent and add a server monitor

- Once installed, your server monitor will automatically integrate with the VMware VM monitor

VMware Datastore Monitoring

- View the virtual machines that use your datastore the most in terms of key metrics like latencies, operations per second, occupied space, allocated space, and disk space management
- Prerequisites:
  > Site24x7 On-Premise Poller
  > VMware Read Only or Administrator roles along with Browse and Config privileges for that particular VMware ESX/ESXi host

VMware Resource Pool Monitoring

- Optimize and manage the resources allocated to virtual machines (VMs) with VMware Resource Pool monitoring. Avoid resource contention in your CPU and RAM by monitoring all your critical resource pool metrics

- Prerequisites:
  > Site24x7 On-Premise Poller
  > VMware Read Only or Administrator roles for that particular VMware ESX/ESXi host

VMware Snapshot Monitoring

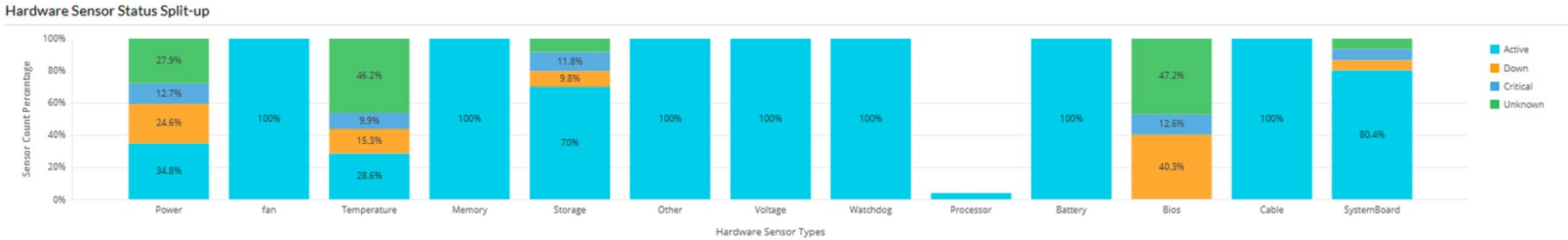
- Add all the snapshots associated with your datastore for monitoring so that you can effectively manage your space requirements
- Using Site24x7's Snapshot Monitoring feature, you can monitor the snapshots that belong to the virtual machines that are a part of that datastore
- It also allows you to monitor the performance at each snapshot-level and configure thresholds for each of them
- Prerequisites:
  > Site24x7 On-Premise Poller version 4.6.4. or above
  > VMware Datastore.Browse privileges required for datastore monitoring

VMware Hardware Monitoring

- Monitor your ESX/ESXi hardware sensors like cables, systemboards, and Bios and get detailed analysis including the status and count of all the hardware sensors

- Prerequisites:
  > Site24x7 On-Premise Poller version 5.1.1 and above
  > VMware Read Only or Administrator role for that particular VMware ESX/ESXi host

VMware Hardware Monitoring



Nutanix Monitoring

Site24x7

Nutanix Monitoring - Introduction

- Nutanix is a hyper-converged infrastructure solution that combines compute, virtualization, storage, networking, and security
- It can host and store virtual machines (VMs)
- A Nutanix Controller VM runs on each node, enabling the pooling of local storage from all nodes in the cluster
- Each node runs a standard hypervisor and contains processors, memory, and local storage (solid state drives and hard disks)
- It's important to monitor Nutanix clusters, hosts, and virtual machines
- Site24x7 monitors all of these from a single console
- Prerequisites: Site24x7 On-Premise Poller version 4.4.4 or above

Nutanix Cluster Monitoring

- A Nutanix Virtual Computing Platform is a scale-out hyper-converged storage and compute platform
- Nutanix nodes collectively form a Nutanix cluster; each node contains CPU, memory, RAM, and storage, and they also run hypervisors. On each of these nodes runs a controller VM
- Gain in-depth insights on all key performance metrics of CPUs, memory, disks, content cache, and storage controllers
- You can monitor your Nutanix hosts and virtual machines by simply enabling auto-discovery while adding Nutanix clusters for monitoring

Nutanix Host Monitoring

- Monitor Nutanix hosts and obtain metric-level data on all components like CPU, memory, storage, input-output operations, bandwidth, and latency
- You can also set thresholds and receive alerts when any of the thresholds are breached

Nutanix VM Monitoring

- Monitor Nutanix virtual machines (VMs) and obtain metric-level data on all components like CPU ready time, storage, memory, storage containers, virtual disks, and virtual NICs
- You can also set thresholds and receive alerts when any of the thresholds are breached

VMware Horizon Monitoring

Site24x7

VMware Horizon Monitoring - Introduction

- VMware Horizon is a solution that simplifies the management and delivery of virtual desktops and apps on-premises, in the cloud, or in a hybrid or multi-cloud configuration through a single platform to end users
- Add VMware Horizon monitor to discover all the instances of View Connection Server, and monitor the performance of various resources associated with your virtual desktop infrastructure (VDI)

Prerequisites

- Site24x7 On-Premise Poller with version 4.4.6 and above
- Enable VMware PowerCLI Module

Interpret VMware Horizon Performance

- Analyze the performance of a VMware Horizon by viewing the connections in machines, servers, and event databases
- Summary: A glimpse of the number of associated resources and sessions
- Machines: Shows the number of machines connected
- Servers: Shows the View Connection Server details and vCenter Server details
- Events database: The details of the events database
- Settings: Lists the global settings

AppLogs Monitoring

Site24x7

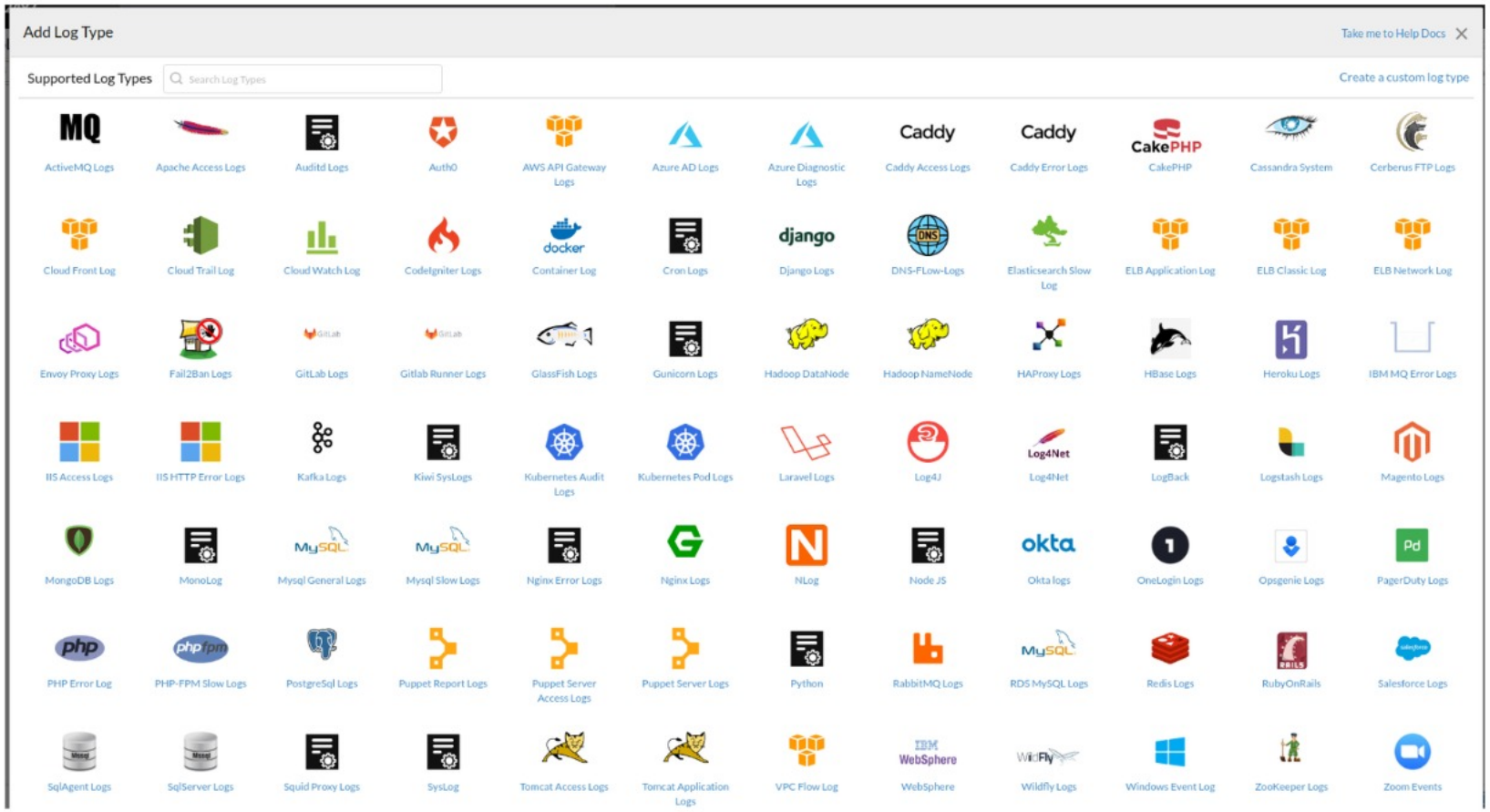
View Unstructured Log Data in a Structured Way

Highlights

- Consolidate logs across servers
- Out-of-the-box support for common application, server, network device logs
- Provision to add any custom logs
- Alerting based on configured threshold
- Query language style - ease of use
- Different report types for different query types
- Dedicated dashboard of each log types

Out-of-the-box Support for Common Applications

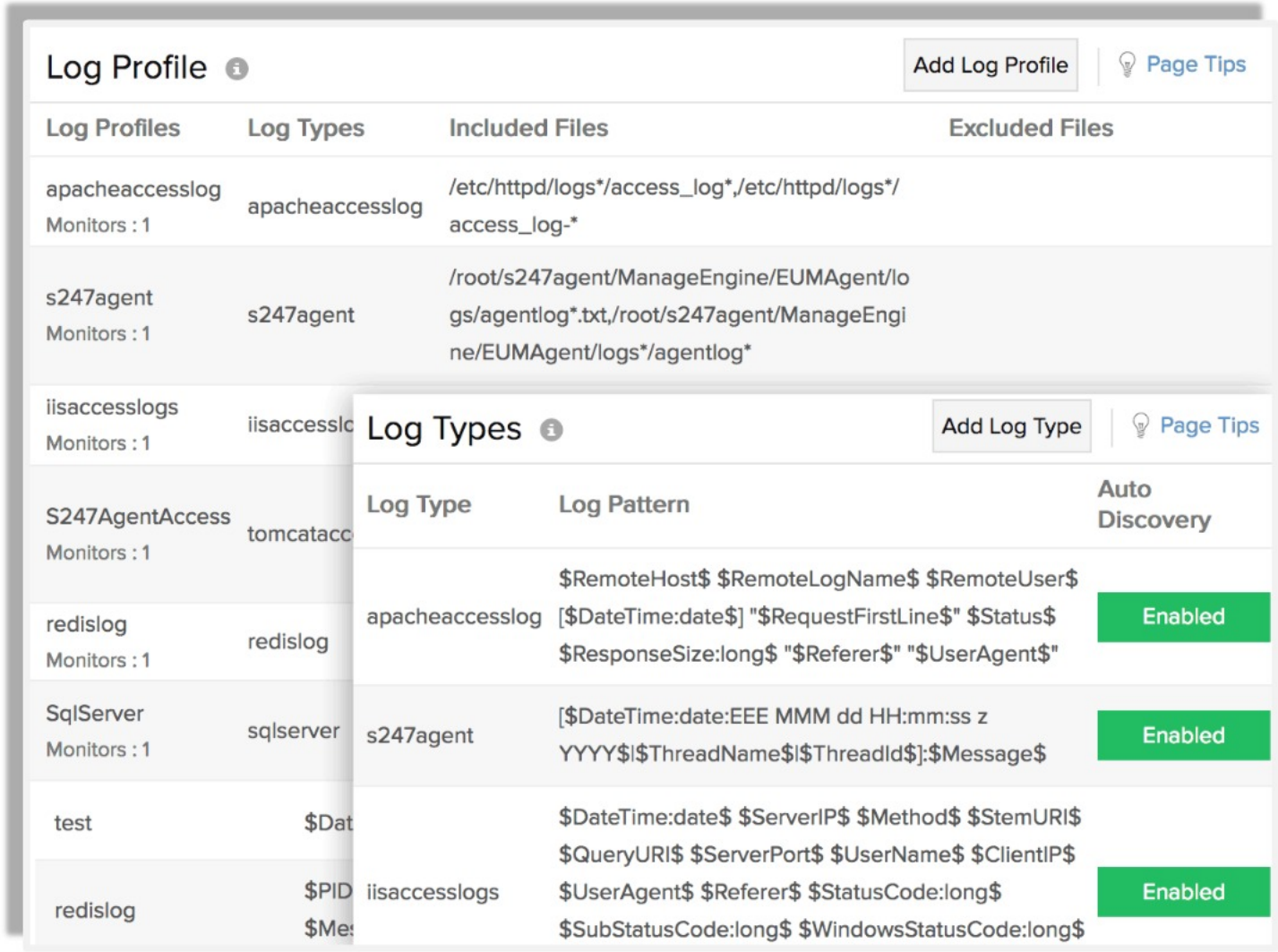
Supported Log Types



> AppLogs supports over 100 log types by default including AWS & AZURE

Site24x7

Log Profile



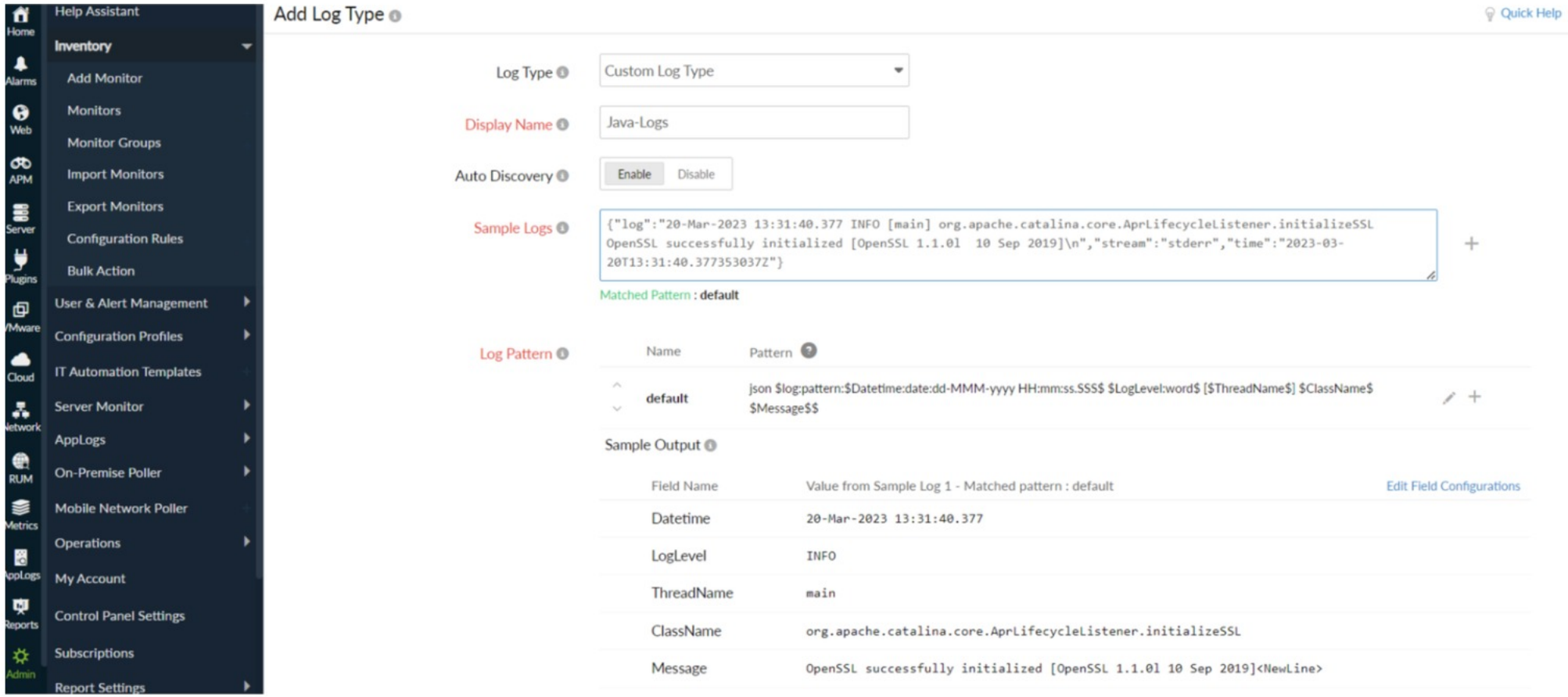
Site24x7

Types of Log Sources

- Local File
- Remote File
- Windows Event Logs
- Amazon Lambda
- Azure Functions
- Log Collectors - Logstash | Fluentd

Collect Logs from Network Devices

Custom Log type



Site24x7

Multiple Log Pattern

Combining different patterns of logs under a single log type

Site24x7

Multiple Patterns

Multiple Patterns...

Derived Fields

To extract meaningful information from the message fields

Site24x7

Derived Field Configuration

[Thu Aug 12 14:52:23 IST 2022|DEBUG|39]:SSL Handshake Time https://zylker.com :42

[Thu May 12 14:37:51 IST 2022|DEBUG|30]: Object.wait break after up notification received...

[Thu May 12 14:37:51 IST 2022|DEBUG|42]: Up Notification received... breaking the waiting thread....

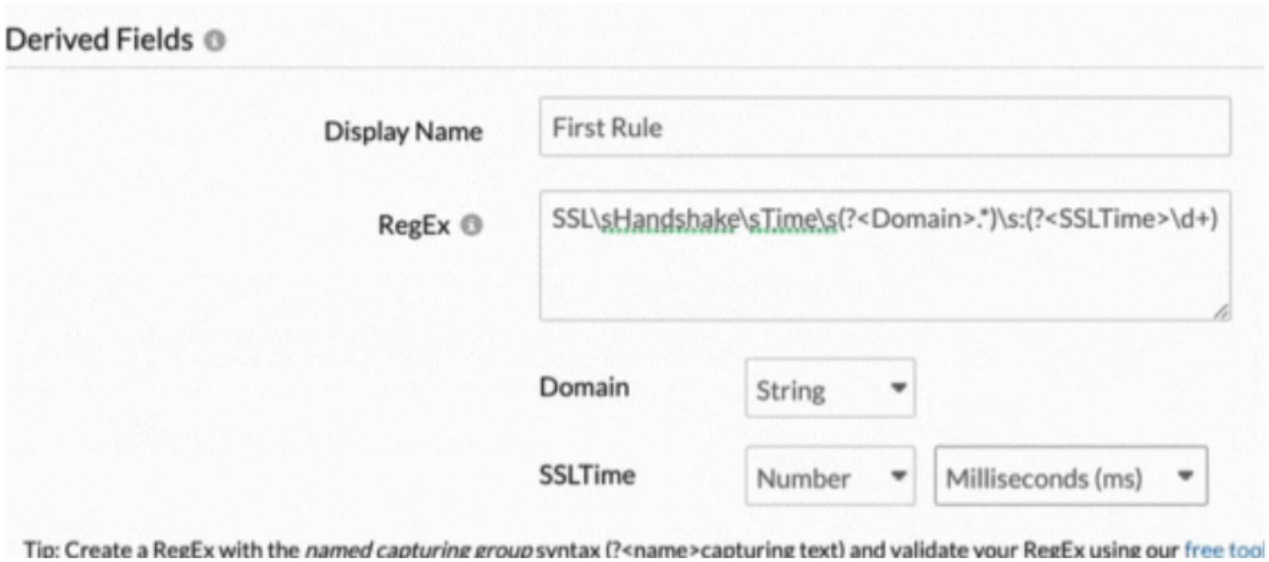
"[$Datetime:date:EEE MMM dd HH:mm:ss z yyyy$|$LogLevel$|$Time$]:$Message$"

[Thu Aug 12 14:52:23 IST 2022|DEBUG|39]: HttpConnection : After successful gzip extraction downloaded response(22015) was extracted to 80132 of content-length

[Thu Aug 12 14:52:23 IST 2022|DEBUG|39]: HttpConnection : Failed to connect

"[$Datetime:date:EEE MMM dd HH:mm:ss z yyyy$|$LogLevel$|$Time$]:$Message$"

Derived Field Configuration...



Adding Derived Fields in dashboard

AppLogs Query Language

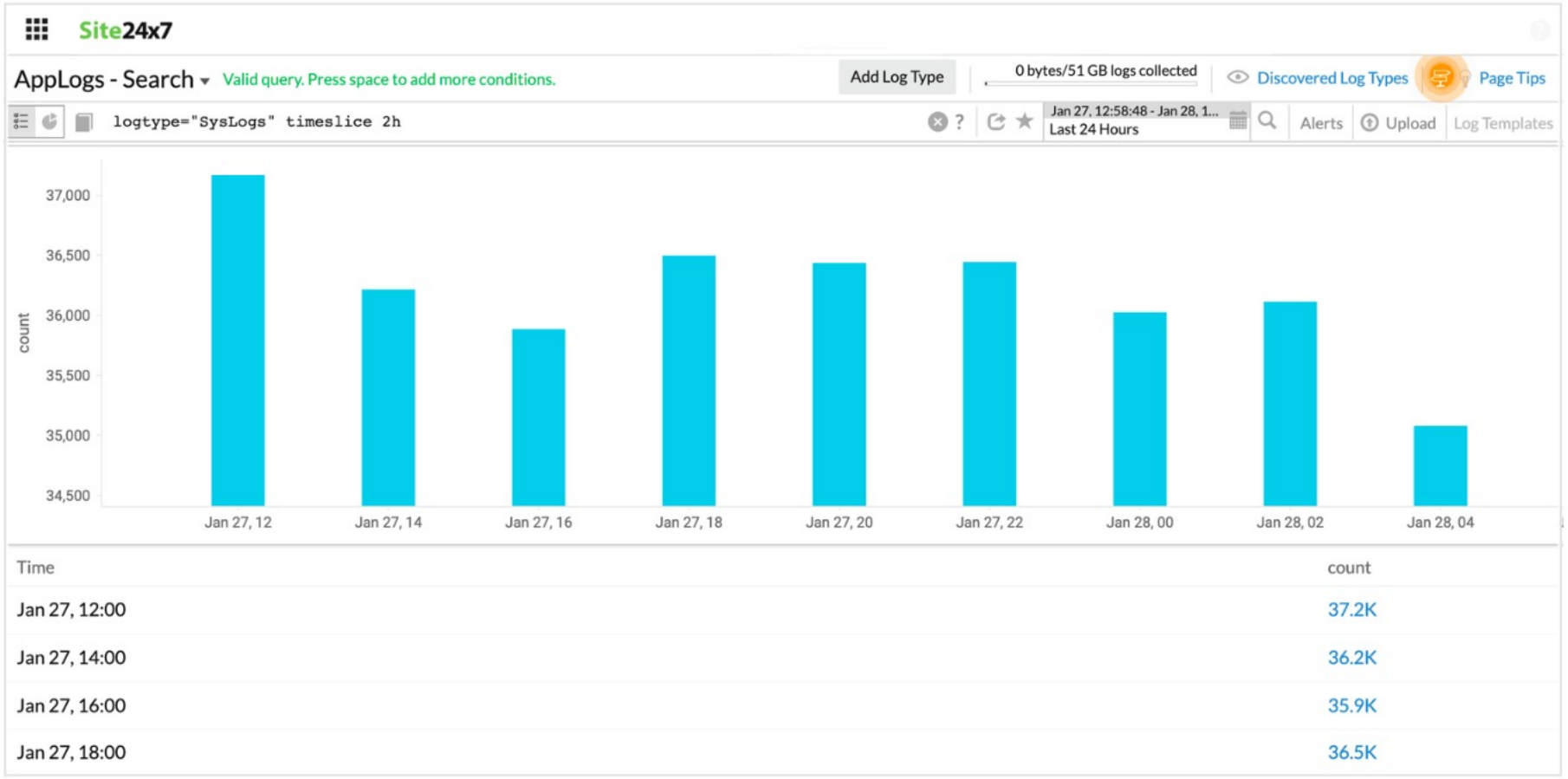
- Collect, consolidate, index, and search logs to gain actionable insights using Site24x7 AppLogs
- Easy to understand language search by filtering out invalid values and obtain actionable results quickly

Query Language

> Support keywords in query language

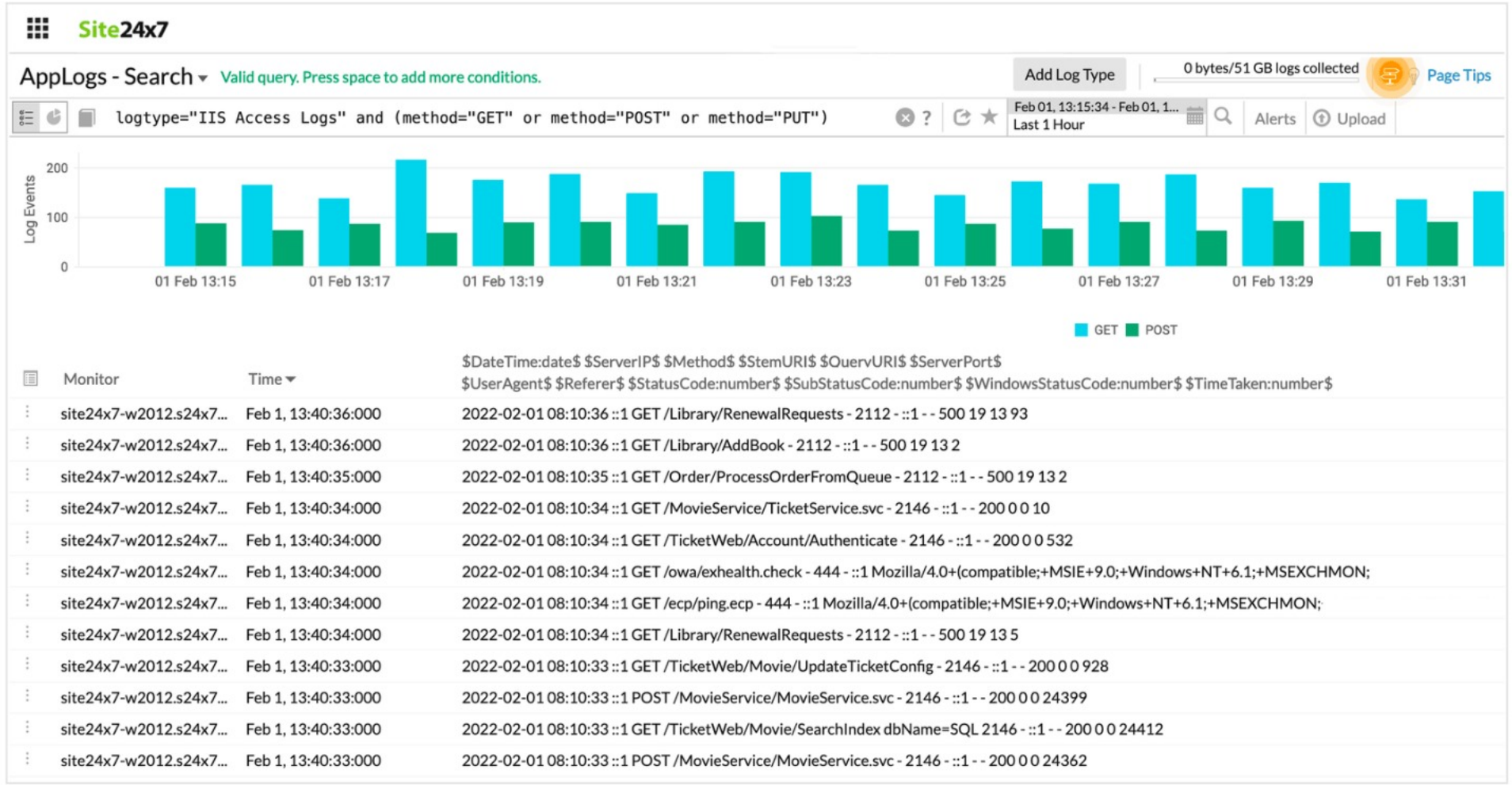
or	and	contains	notcontains
isempty	isnotempty	in	notin
like	startswith	>,<,>=,<=,=,!=	not
count	min	max	sum
avg	sd	percentile	ratio
count_distinct	groupby, having	histo, range	timeslice
tophits	sort	before	include|exclude
monitor_name	monitor_group	tags	

Time Slice Report

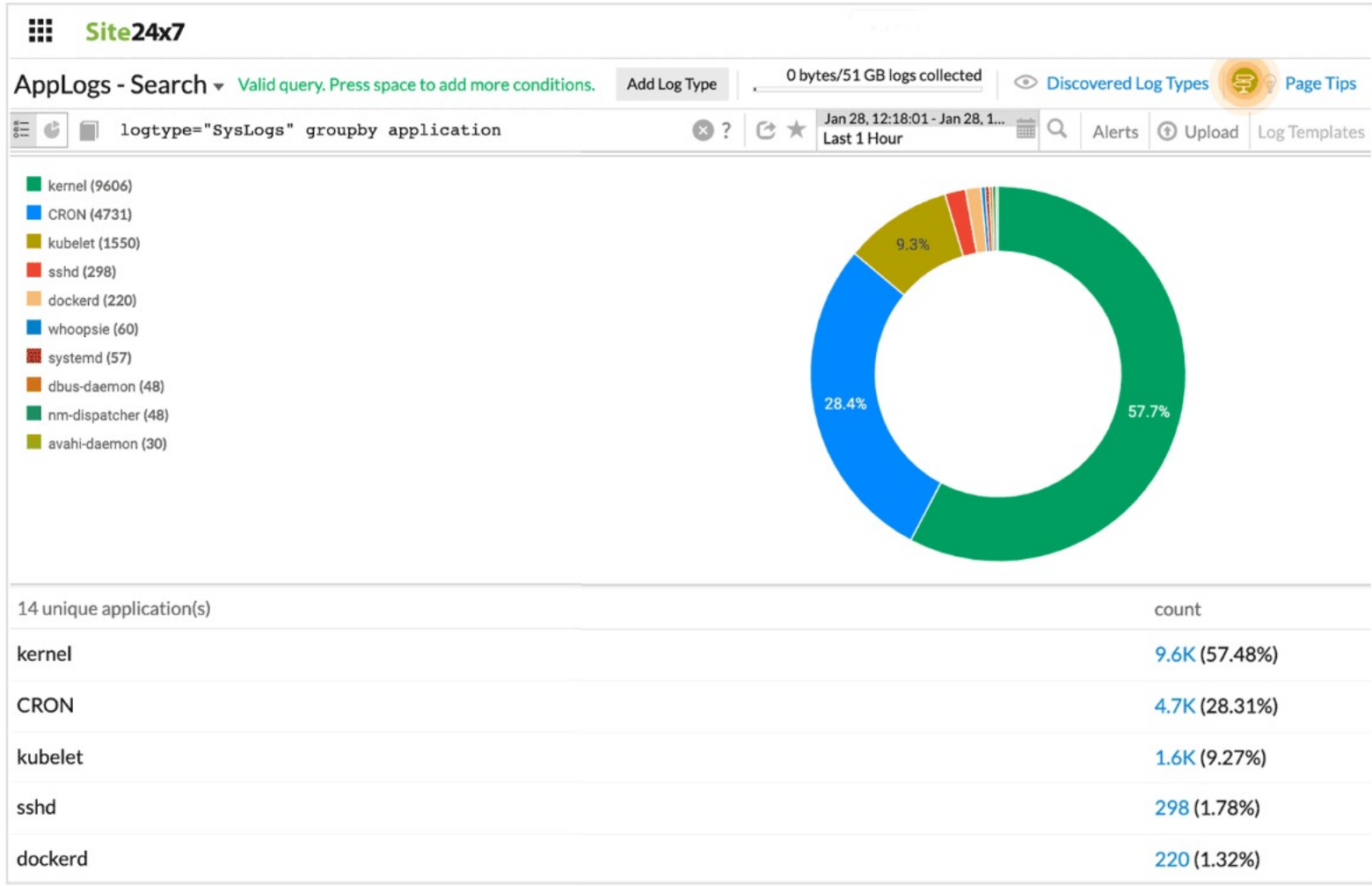


Time	count
Jan 27, 12:00	37.2K
Jan 27, 14:00	36.2K
Jan 27, 16:00	35.9K
Jan 27, 18:00	36.5K

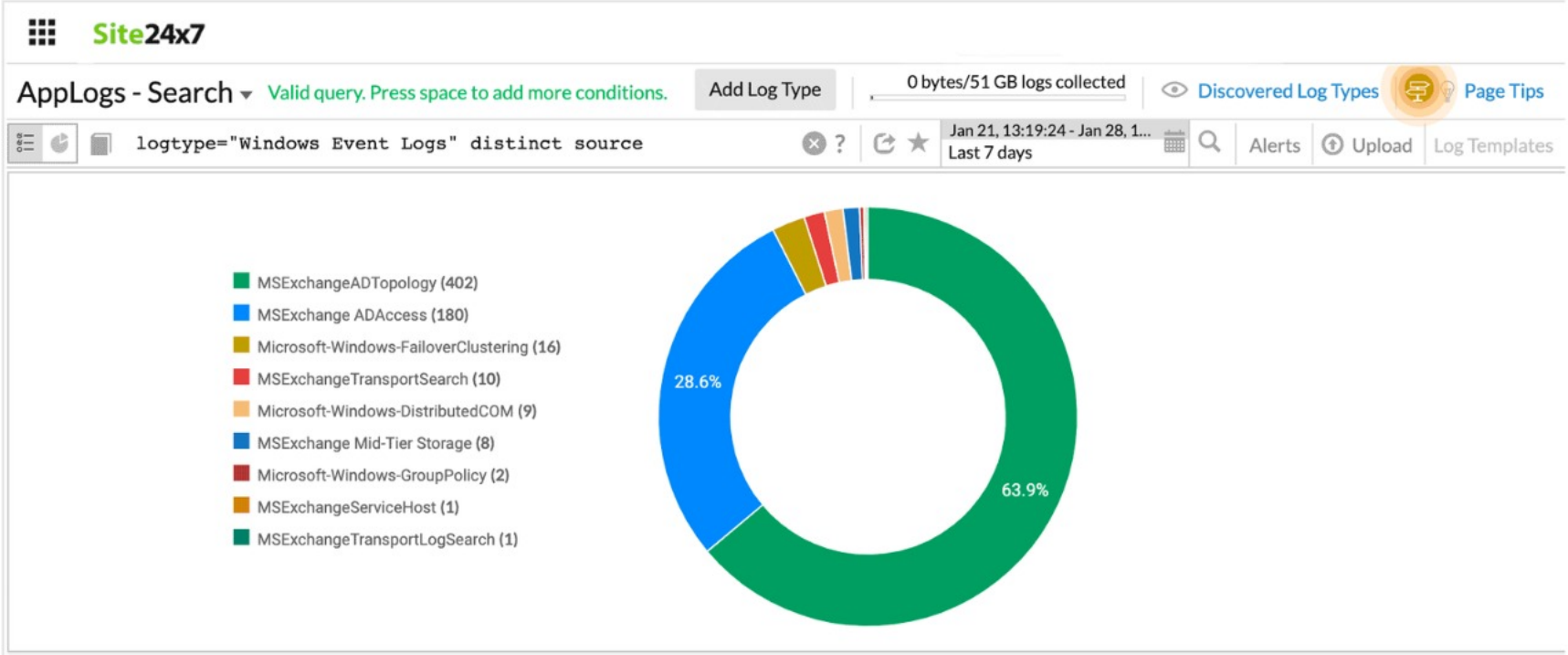
OR Report


Site24x7
AppLogs - Search
Valid query. Press space to add more conditions.
Add Log Type
0 bytes/51 GB logs collected
Page Tips
logtype="IIS Access Logs" and (method="GET" or method="POST" or method="PUT")
Feb 01, 13:15:34 - Feb 01, 1...
Last 1 Hour
Alerts
Upload
Log Events
200
100
0
01 Feb 13:15
01 Feb 13:17
01 Feb 13:19
01 Feb 13:21
01 Feb 13:23
01 Feb 13:25
01 Feb 13:27
01 Feb 13:29
01 Feb 13:31
GET
POST
Monitor
Time
$DateTime:date$ $ServerIP$ $Method$ $StemURI$ $QuervURI$ $ServerPort$
$UserAgent$ $Referer$ $StatusCode:number$ $SubStatusCode:number$ $WindowsStatusCode:number$ $TimeTaken:number$
site24x7-w2012.s24x7... Feb 1, 13:40:36:000 2022-02-01 08:10:36 ::1 GET /Library/RenewalRequests - 2112 - ::1 - - 500 19 13 93
site24x7-w2012.s24x7... Feb 1, 13:40:36:000 2022-02-01 08:10:36 ::1 GET /Library/AddBook - 2112 - ::1 - - 500 19 13 2
site24x7-w2012.s24x7... Feb 1, 13:40:35:000 2022-02-01 08:10:35 ::1 GET /Order/ProcessOrderFromQueue - 2112 - ::1 - - 500 19 13 2
site24x7-w2012.s24x7... Feb 1, 13:40:34:000 2022-02-01 08:10:34 ::1 GET /MovieService/TicketService.svc - 2146 - ::1 - - 200 0 0 10
site24x7-w2012.s24x7... Feb 1, 13:40:34:000 2022-02-01 08:10:34 ::1 GET /TicketWeb/Account/Authenticate - 2146 - ::1 - - 200 0 0 532
site24x7-w2012.s24x7... Feb 1, 13:40:34:000 2022-02-01 08:10:34 ::1 GET /owa/exhealth.check - 444 - ::1 Mozilla/4.0+(compatible;+MSIE+9.0;+Windows+NT+6.1;+MSEXCHMON;
site24x7-w2012.s24x7... Feb 1, 13:40:34:000 2022-02-01 08:10:34 ::1 GET /ecp/ping.ecp - 444 - ::1 Mozilla/4.0+(compatible;+MSIE+9.0;+Windows+NT+6.1;+MSEXCHMON;
site24x7-w2012.s24x7... Feb 1, 13:40:34:000 2022-02-01 08:10:34 ::1 GET /Library/RenewalRequests - 2112 - ::1 - - 500 19 13 5
site24x7-w2012.s24x7... Feb 1, 13:40:33:000 2022-02-01 08:10:33 ::1 GET /TicketWeb/Movie/UpdateTicketConfig - 2146 - ::1 - - 200 0 0 928
site24x7-w2012.s24x7... Feb 1, 13:40:33:000 2022-02-01 08:10:33 ::1 POST /MovieService/MovieService.svc - 2146 - ::1 - - 200 0 0 24399
site24x7-w2012.s24x7... Feb 1, 13:40:33:000 2022-02-01 08:10:33 ::1 GET /TicketWeb/Movie/SearchIndex dbName=SQL 2146 - ::1 - - 200 0 0 24412
site24x7-w2012.s24x7... Feb 1, 13:40:33:000 2022-02-01 08:10:33 ::1 POST /MovieService/MovieService.svc - 2146 - ::1 - - 200 0 0 24362

Groupby Report

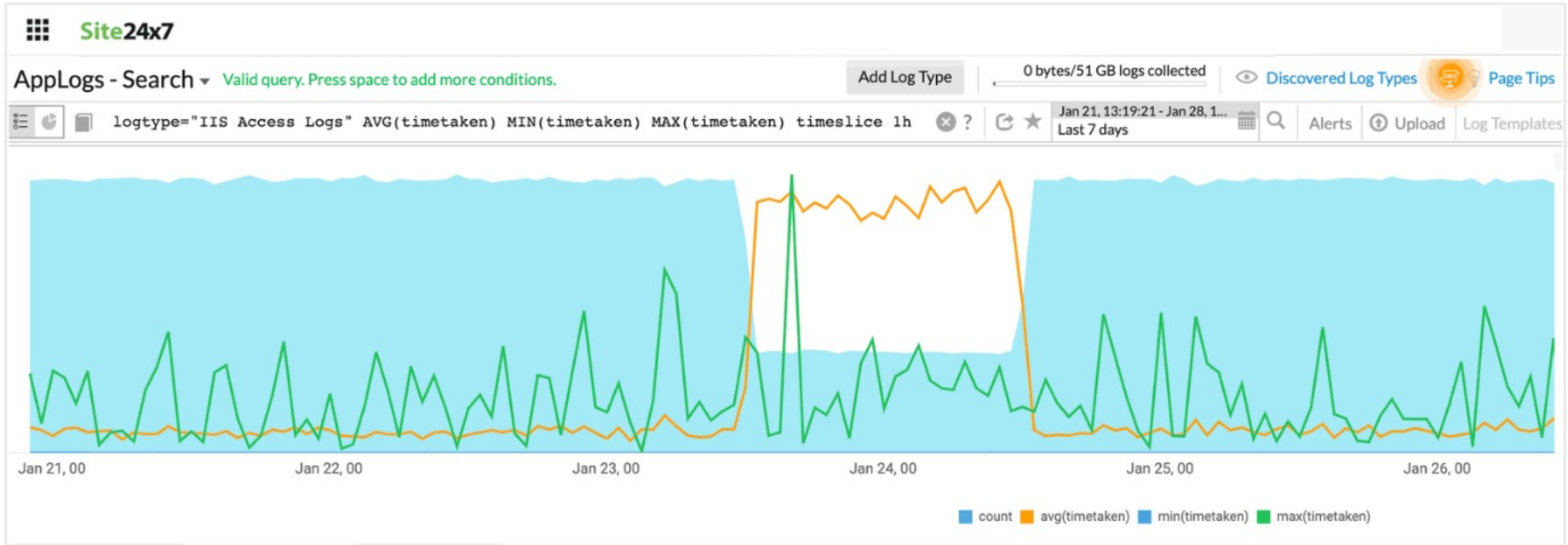


Distinct Report



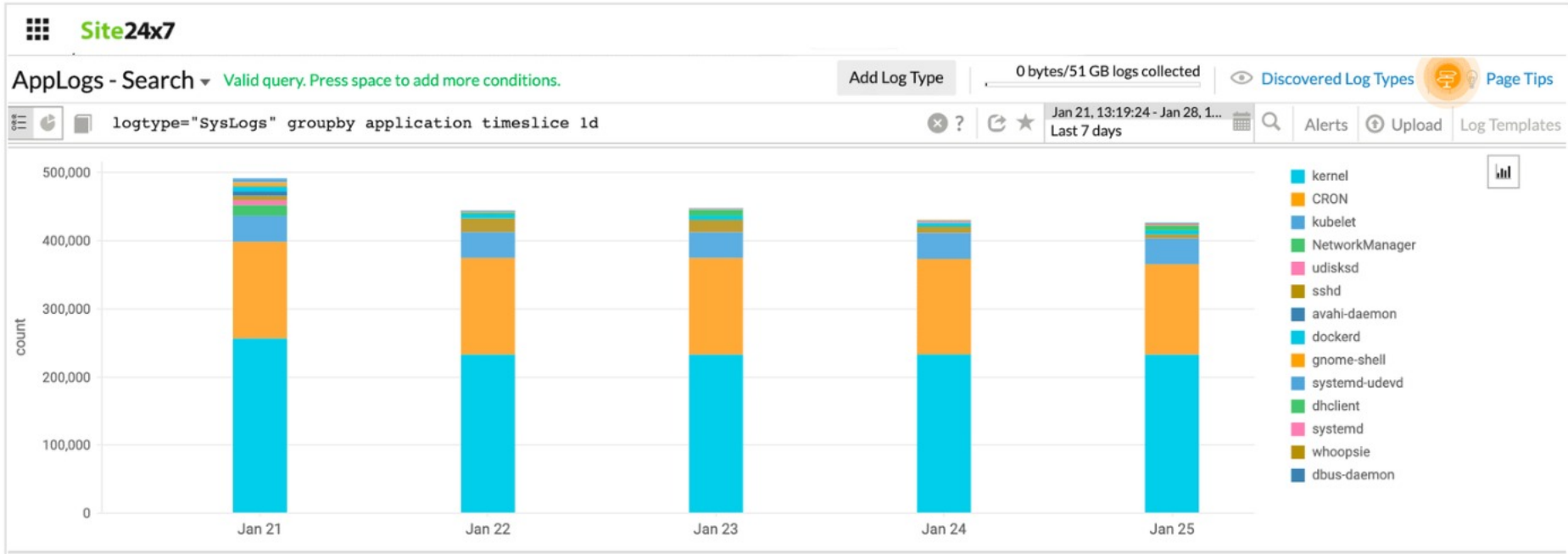
9 unique source(s)	count
MSExchangeADTopology	402 (63.91%
MSExchange ADAccess	180 (28.62%
Microsoft-Windows-FailoverClustering	16 (2.54%)
MSExchangeTransportSearch	10 (1.59%)
Microsoft-Windows-DistributedCOM	9 (1.43%)

Combining Timeslice and Aggregation Together



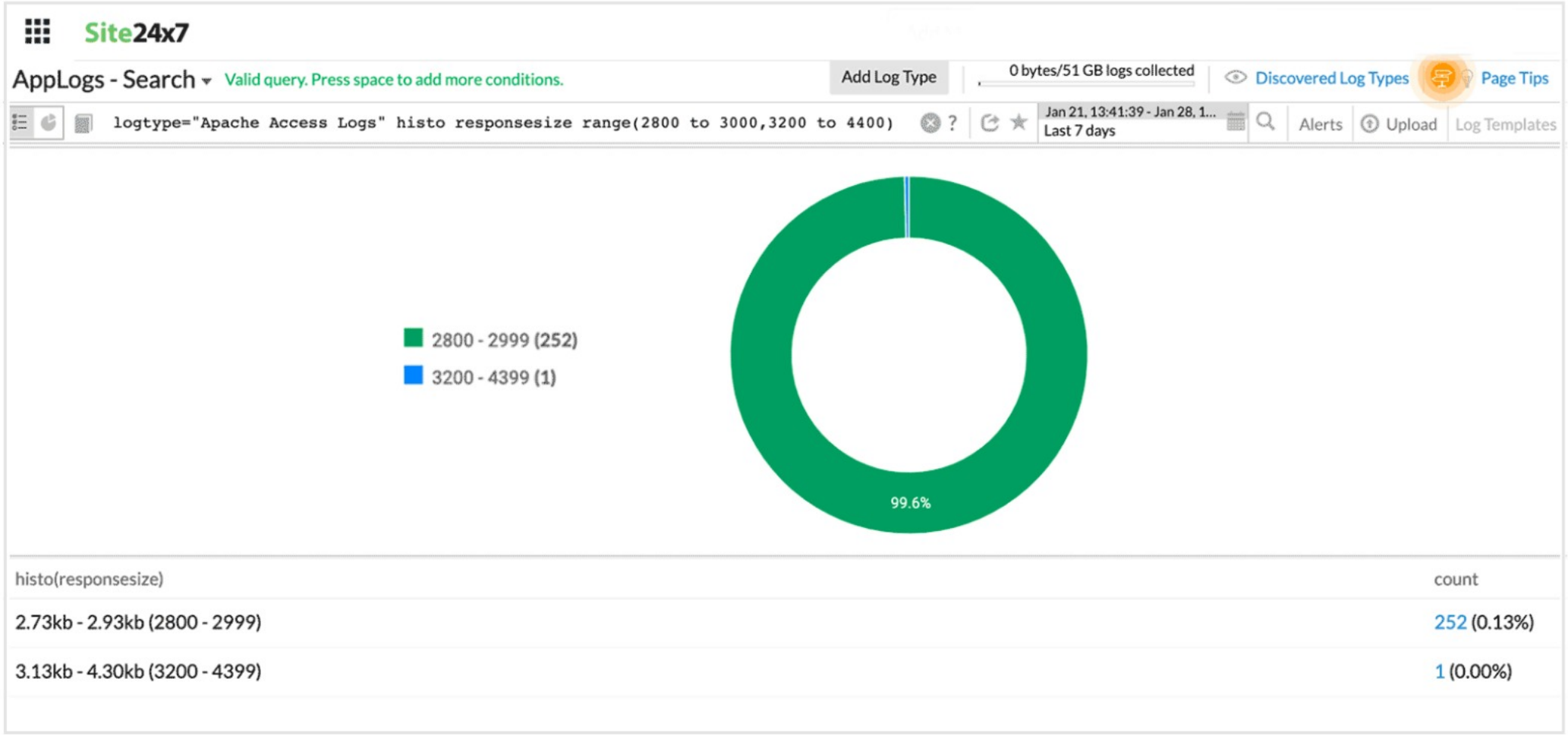
Time	count	avg(timetaken)	min(timetaken)	max(timetaken)
Jan 21, 13:00	20.8K	2.83s	0ms	1.54m
Jan 21, 14:00	20.8K	2.8s	0ms	1.19m
Jan 21, 15:00	20.8K	2.74s	0ms	1.56m
Jan 21, 16:00	20.8K	2.81s	0ms	1.51m
Jan 21, 17:00	20.8K	2.83s	0ms	1.33m

Combining Groupby and Timeslice Together

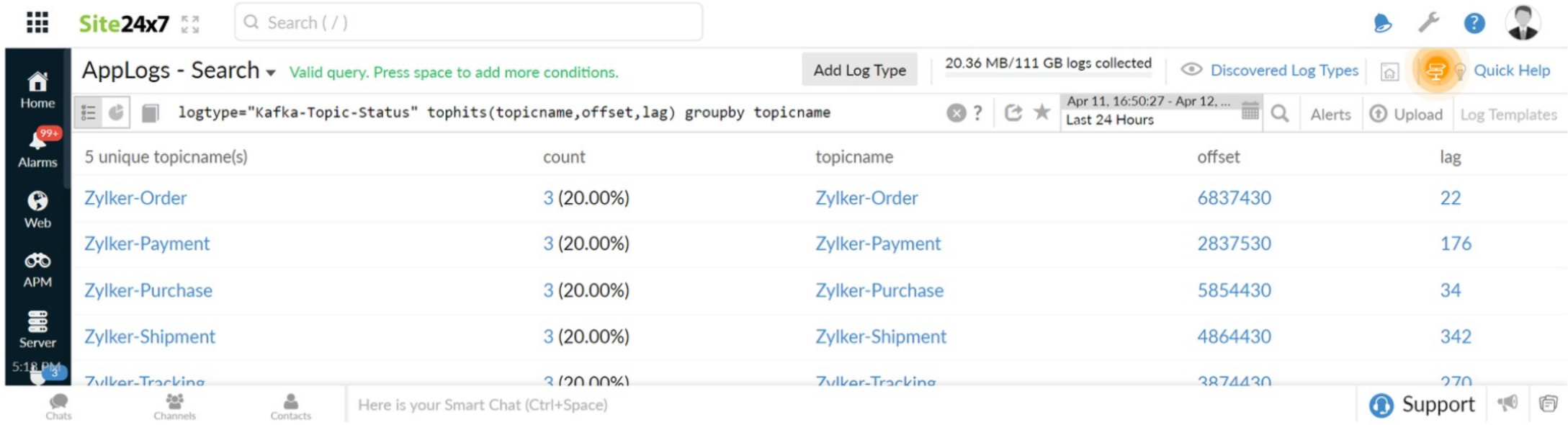


application	21 Jan	22 Jan	23 Jan	24 Jan	25 Jan
kernel	255.8K	232K	231.9K	232.3K	231.9K
CRON	141.6K	141.7K	141.8K	139.8K	132.5K
kubelet	38.1K	37.7K	37.5K	38K	38.1K
NetworkManager	15.7K	-	-	-	-
udisksd	6.9K	-	-	-	-
sshd	6.8K	20.4K	18.5K	9.5K	5.8K

Histo with Range

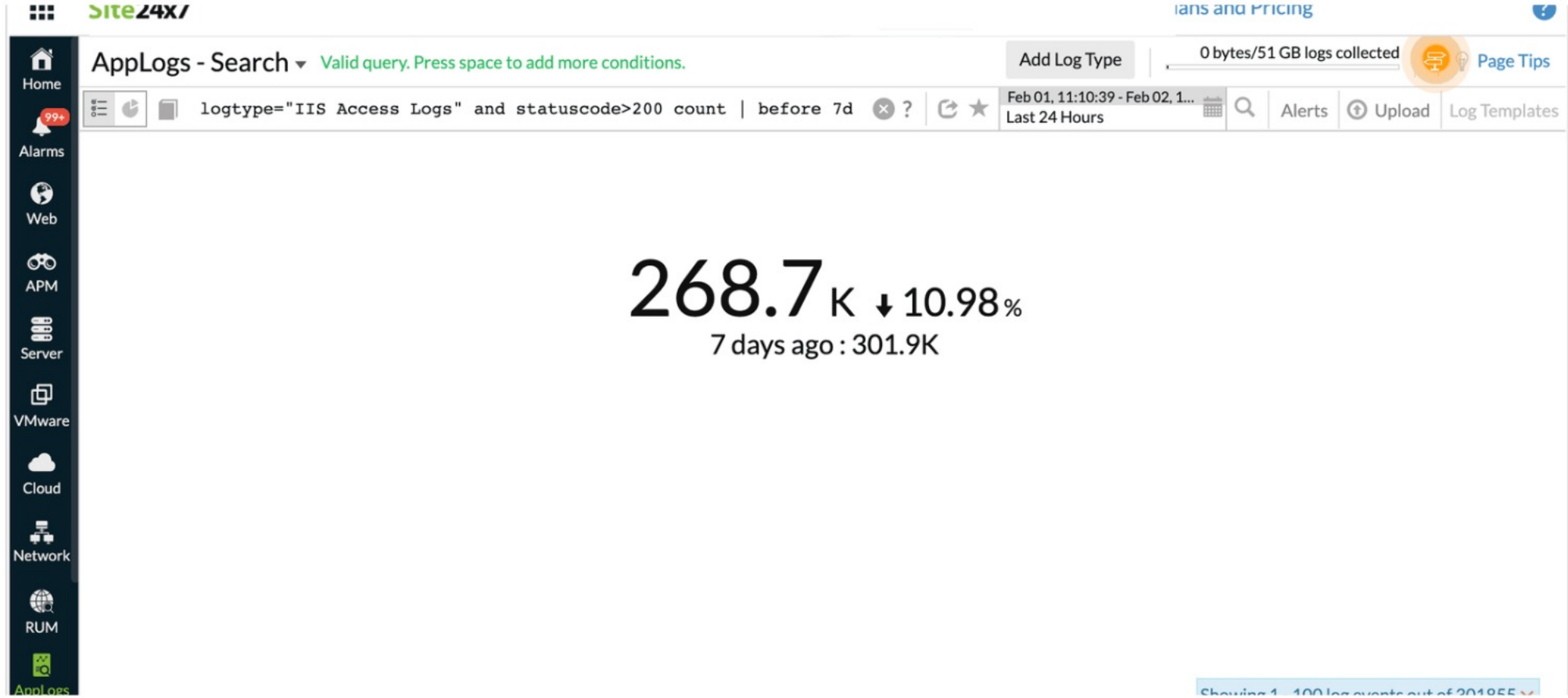


TopHits Query



Used to get current value of the grouped item. This is mainly useful for metric kind of logs

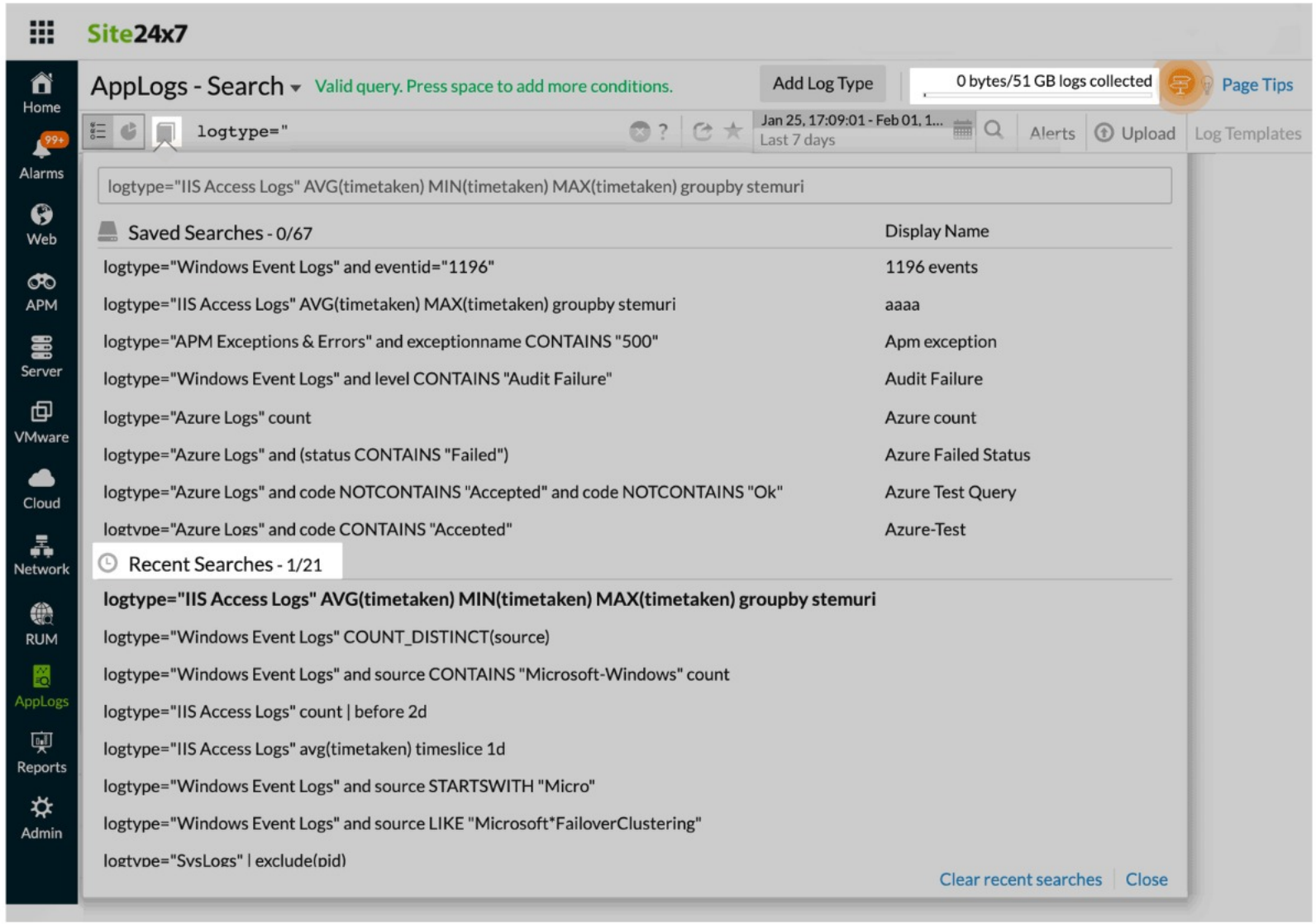
Key performance Indicator



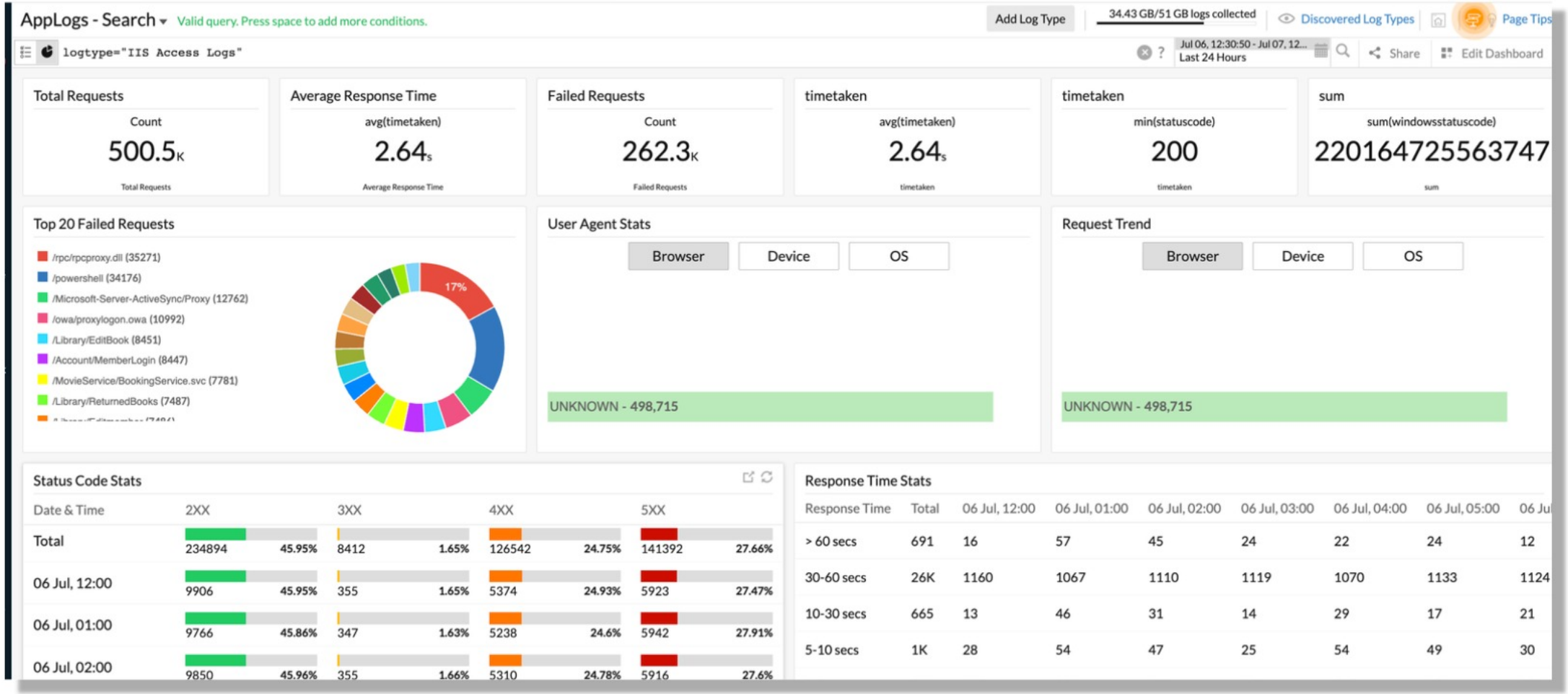
Key performance Indicator (Overtime)

Site24x7

Recent and saved Searches

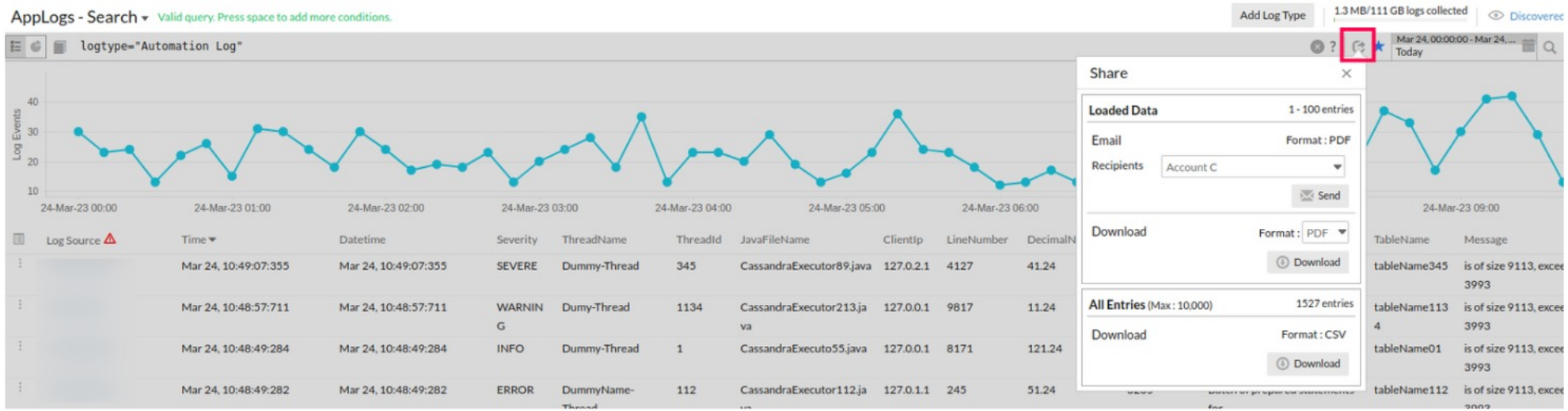


App log Dashboard



Site24x7

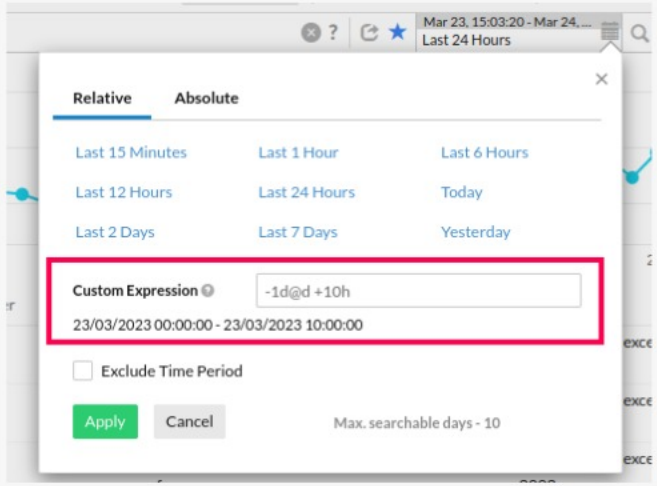
Export Search Result



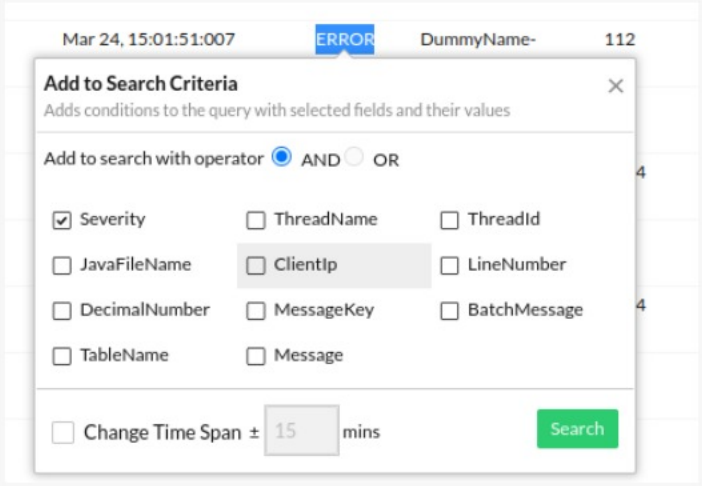
We can export the search result as CSV or PDF format. Limitation : Maximum 10K log lines
Also we have python script to download the logs via REST API

Site24x7

Search Options

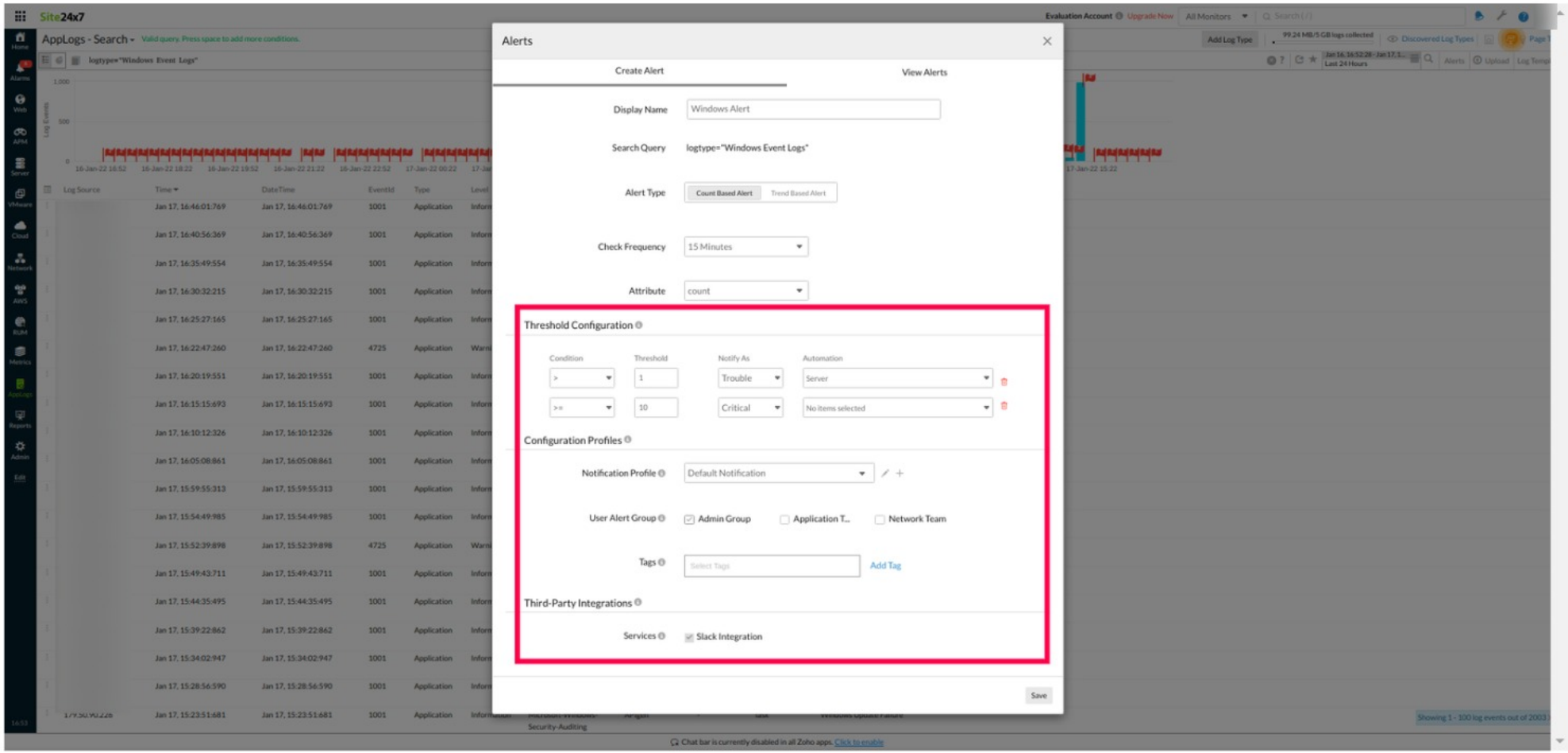


Relative Time Search



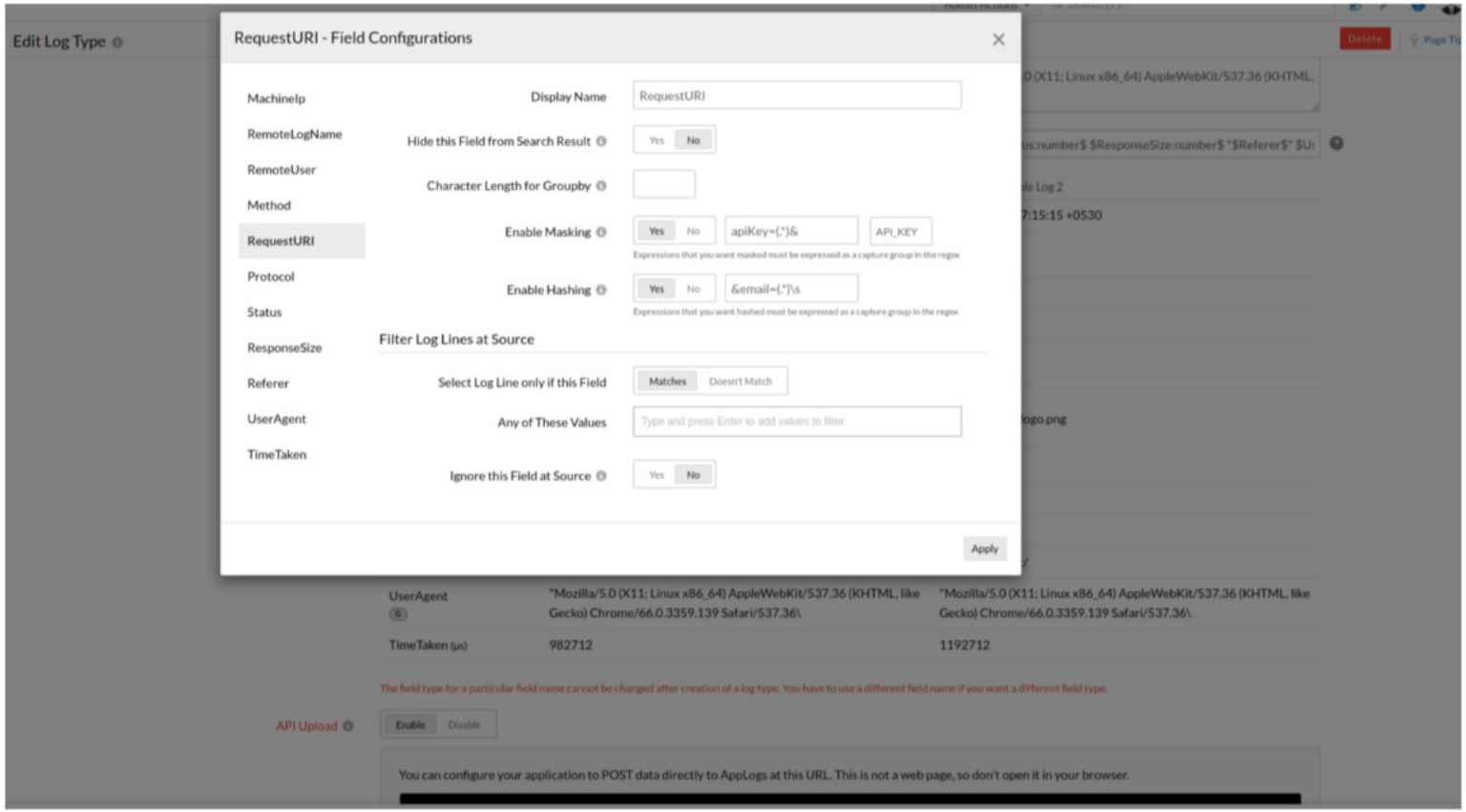
Add Conditions to Search

AppLogs Alerts



Masking and Hashing Log Data

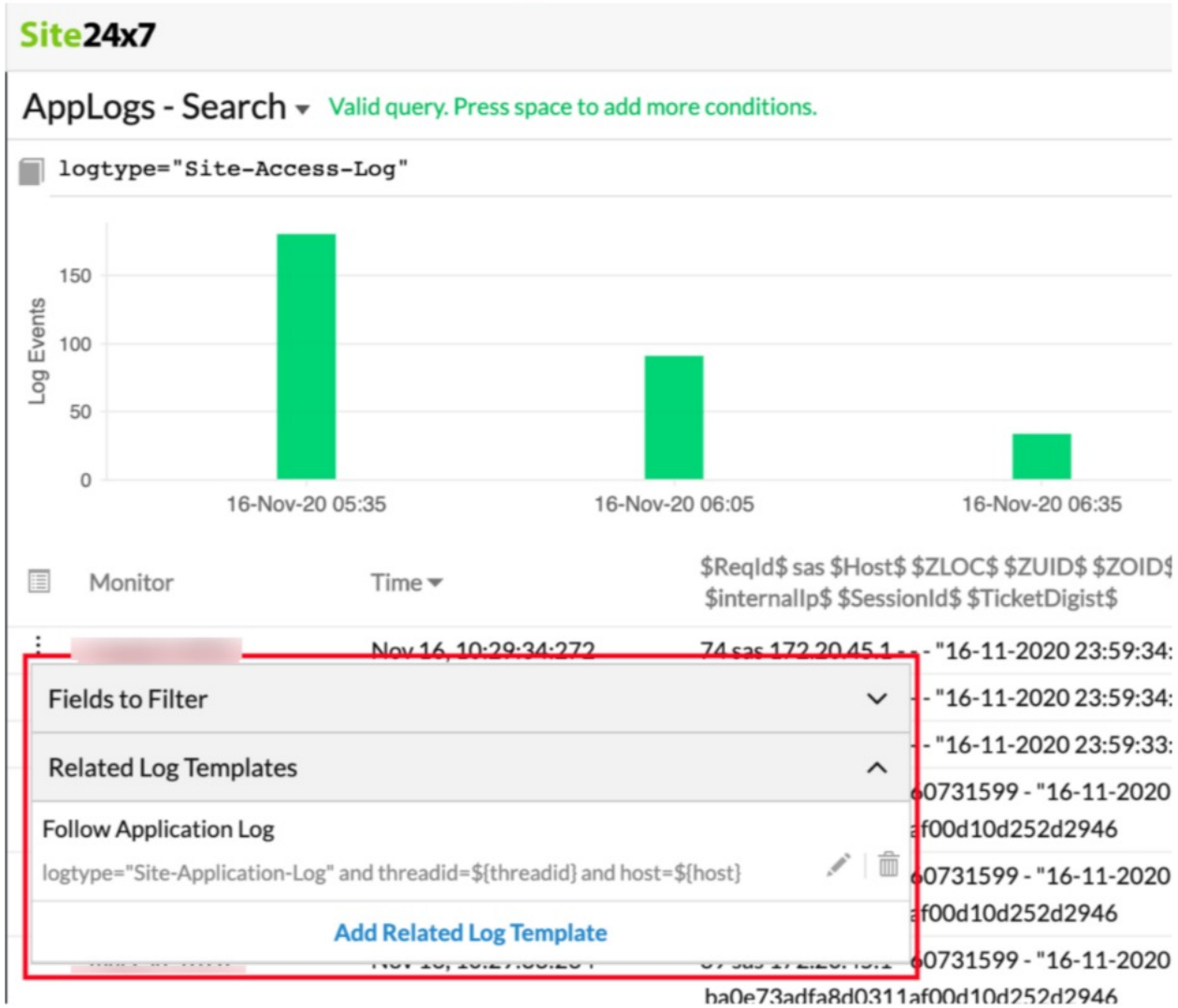
- Hide sensitive data while sending your logs to Site24x7 AppLogs



Related Log Templates

- Compare multiple fields in one log type with another by creating a template
- Simply define the template with a name by providing the necessary fields to be included
- This allows you to follow that particular field in another log type

Related Log Templates



Log Type Views

Too much data may make it difficult to focus on the relevant information during troubleshooting

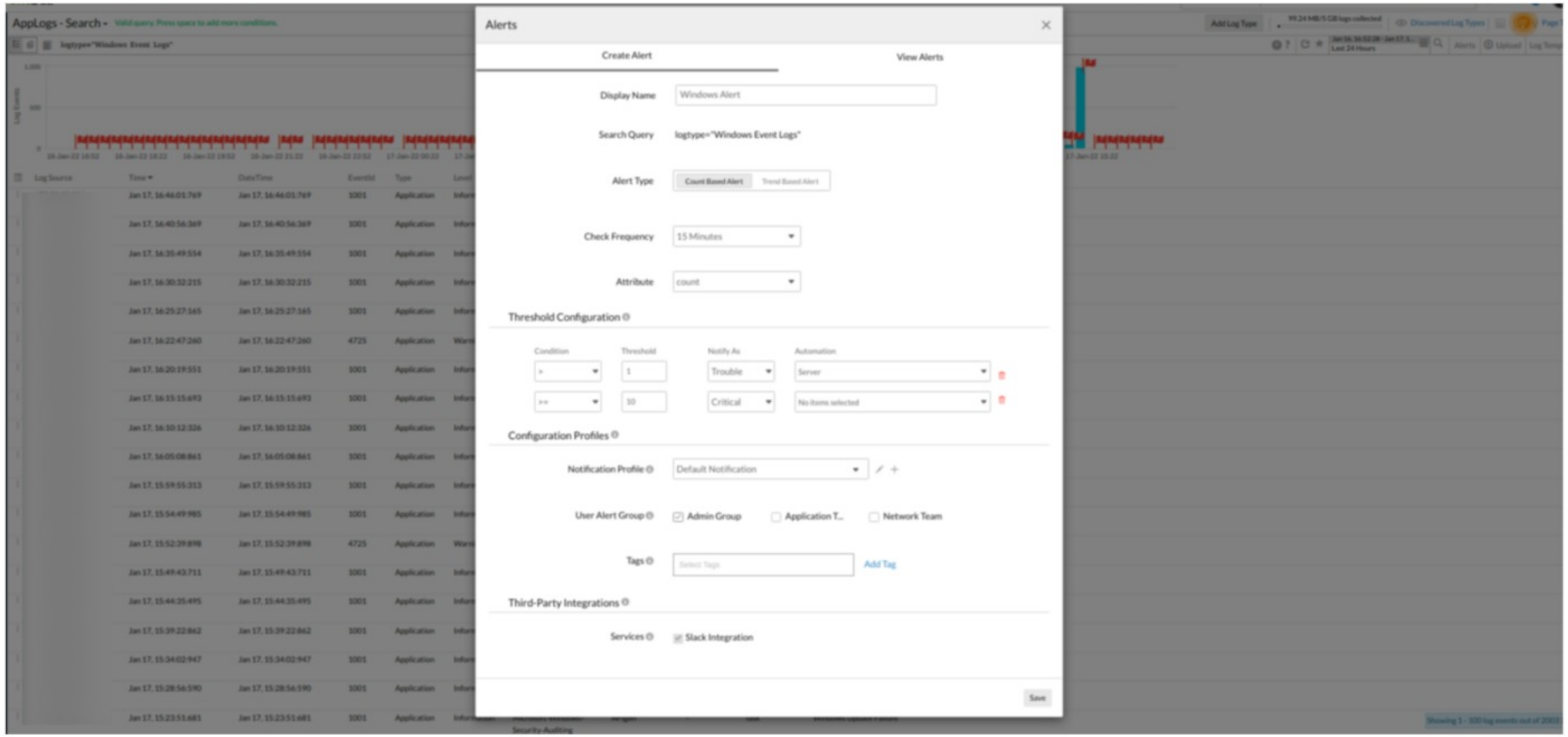
Schedule Reports - AppLog Dashboard

This report give you detailed insights into all configured widgets for the log types

AppLogs Usage Summary

Usage alert mail will send to configured user on 60%,80%,90% and 100%

AppLogs Monitoring and Third-party Integration Support



Site24x7

Benefits

- Receive alerts through third-party ITSM and collaboration tools like Jira, PagerDuty, Slack, Microsoft Teams, and others along with the email, voice call, and SMS alerts that are available currently
- Once you configure an alert for a Log Type in AppLogs, your Log Type will be treated as a monitor and any search query can be configured for alerting. This allows you to view your Log Type along with its status from the Home > Monitors page
- View and manage your alerts from the Alarms and Outages tabs along with other monitors
- If you have a planned maintenance for your servers, you can simply configure the server as undergoing maintenance and mute AppLogs Alerts for a particular duration
- Other monitor-level features like Notification Profiles and IT Automation that allow you configure actions for log alerts and fix common incidents without any manual intervention

2023 Q1 updates

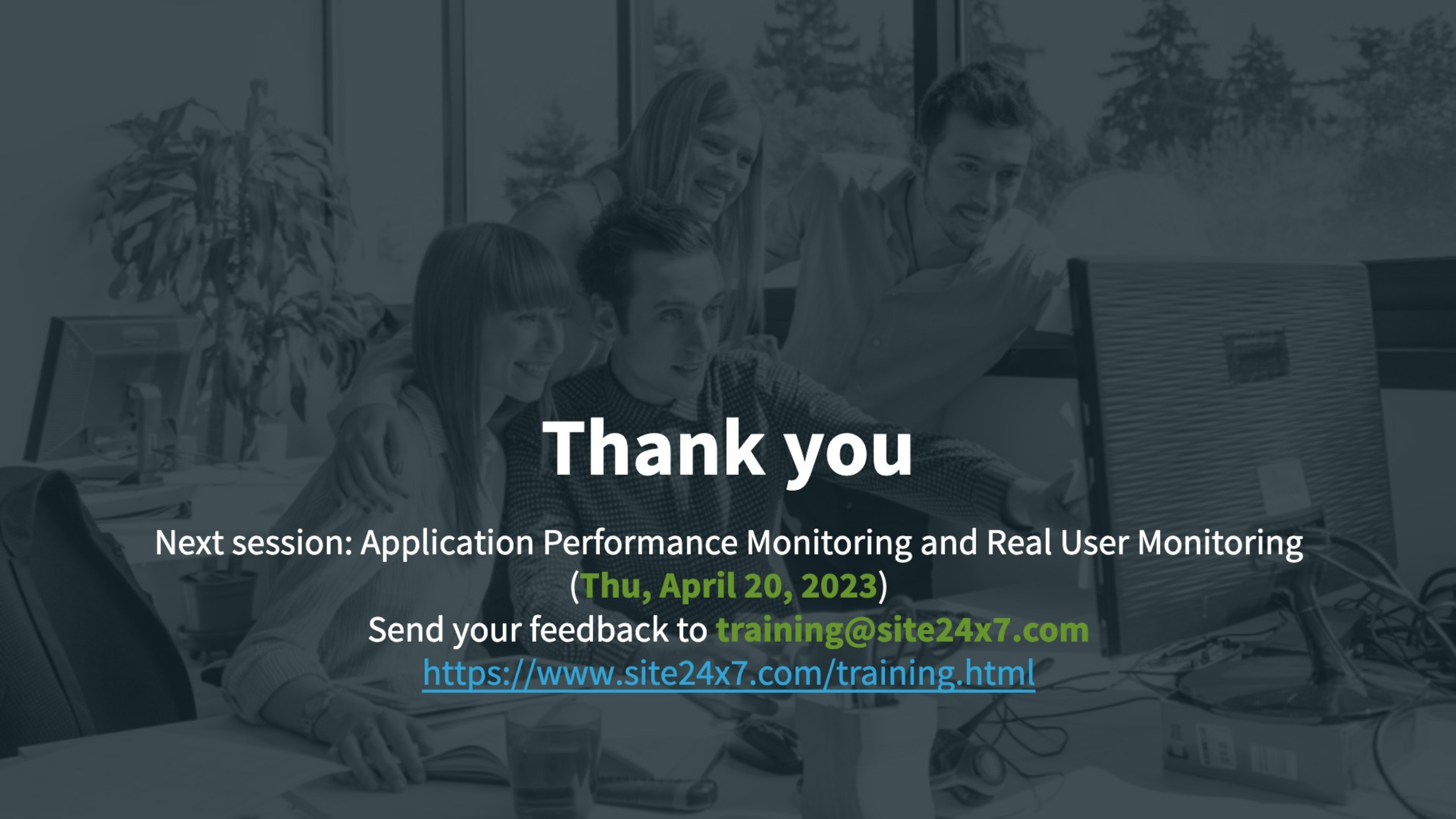
- Applogs now supports Kubernetes audit logs, Node.js logs, and Python logs.
- AppLogs now includes percents, percentile, and tophits in the supported operator's list.
- Bulk Update Credential option for ESXi to vCenter-based polling
- VMware cluster monitoring GA

Best Practices

- We always recommend you to use the latest version of On-Premise Poller for better performance
- Use High Availability On-Premise Poller
- Set thresholds and monitor the performance metrics effectively
- Install server agent in VMs to view both the VM metrics as well as guest OS metrics in a single unified console (integrated VM monitor console)

Learnings from the session

- Learned about On-Premise Poller and High Availability On-Premise Poller
- Installation of Network Monitoring, NetFlow Analyzer, NCM, Meraki Monitoring and VMware Monitoring
- Overview of VoIP Monitoring, Nutanix Monitoring and VMware Horizon Monitoring
- About AppLogs Monitoring



Thank you

Next session: Application Performance Monitoring and Real User Monitoring
(**Thu, April 20, 2023**)
Send your feedback to **training@site24x7.com**
https://www.site24x7.com/training.html