Copyright © 2024 Kaseya Limited





USER GUIDE

VulScan Instructions to Perform Vulnerability Scanning 4/11/2024 3:52 PM





rapidfiretools.com



support@rapidfiretools.com

Contents

VulScan Introduction	9
Key features	
VulScan Components	
Set Up VulScan	
Add an Organization	11
Create VulScan Site	13
Install VulScan Appliance	
VulScan Appliance Types and Install Instructions	19
Create Scan and Notification Tasks	
Create Internal Scan Task	20
Scan Task "Run Now"	
Edit/Delete Scan Task	
Create External Scan Task	27
Create Notification Tasks	
Edit/Delete Notification Task	
Kaseya Hosted External Vulnerability Scan	
Step 1 – Provision Hosted External Vulnerability Scanner	
Step 2 – Set up Hosted External Vulnerability Scan Task	
Step 3 – Keep Track of Hosted External Scan License Limit	
Configure Device Matching Criteria to Reduce False Positives	
Matching Examples	40
Scan Credentials	
Add Credentials to a VulScan Site	
Custom Scan Profiles	44
Create New Profile	
Invite Users to VulScan Site	
<u>Client View</u>	
Step 1 – Create User and Assign Client View Role	

Ston 2 Invite Learte VulSeen Site	
Step 2 – Invite User to VulScan Site	
Step 3 – Client View User Accesses VulScan Site and Views Issues/Creates 7	Fickets 51
VulScan Site Roles	
Using VulScan	
View Vulnerability Scan Results	54
Filter Scan Results	
Review Scan Results	
Scan Result Notification Emails	
Available Issue Meta Data	
How Vulnerability Totals are Presented	60
Mark Issues as False Positives, Accepted, or Mitigated (Site-level)	
False Positive Management (Site Level)	64
Add Exclusion Rule at the Site Level	64
Edit/Delete Exclusion Rule	66
Create Ticket from Issue	67
Generate VulScan Issues and Detail Reports	70
Generate VulScan Trending Reports	
Step 1 — Navigate to VulScan Trending Reports	73
Step 2 — Filter Vulnerability Data	74
Step 2 — Filter Vulnerability Data Step 3 — Generate Dynamic Graphs	
	75
Step 3 — Generate Dynamic Graphs	75 76
Step 3 — Generate Dynamic Graphs When are Trend Reports updated?	
Step 3 — Generate Dynamic Graphs When are Trend Reports updated? Open Ports Report	
Step 3 — Generate Dynamic Graphs When are Trend Reports updated? Open Ports Report Step 1 — Navigate to VulScan Open Ports Reports	
Step 3 — Generate Dynamic Graphs When are Trend Reports updated? Open Ports Report Step 1 — Navigate to VulScan Open Ports Reports Step 2 — Filter Open Ports Vulnerability Data	
Step 3 — Generate Dynamic Graphs When are Trend Reports updated? Open Ports Report Step 1 — Navigate to VulScan Open Ports Reports Step 2 — Filter Open Ports Vulnerability Data Step 3 — Download Open Ports Report and Invite Client Users	
Step 3 — Generate Dynamic Graphs When are Trend Reports updated? Open Ports Report Step 1 — Navigate to VulScan Open Ports Reports Step 2 — Filter Open Ports Vulnerability Data Step 3 — Download Open Ports Report and Invite Client Users VulScan Vulnerability Reports	
Step 3 — Generate Dynamic Graphs When are Trend Reports updated? Open Ports Report Step 1 — Navigate to VulScan Open Ports Reports Step 2 — Filter Open Ports Vulnerability Data Step 3 — Download Open Ports Report and Invite Client Users VulScan Vulnerability Reports Export Notification Tasks to RocketCyber	75 76 77 77 77 78 78 79 80 80
Step 3 — Generate Dynamic Graphs When are Trend Reports updated? Open Ports Report Step 1 — Navigate to VulScan Open Ports Reports Step 2 — Filter Open Ports Vulnerability Data Step 3 — Download Open Ports Report and Invite Client Users VulScan Vulnerability Reports Export Notification Tasks to RocketCyber Step 1 — Enable VulScan from the RocketCyber App Store	75 76 77 77 77 78 79 80 80 80 80

Step 5 — Browse VulScan Issues from RocketCyber Dashboard	83
Set Up Remote Internal Vulnerability Scanner	
Introduction	
Step 1 — Provision and Install Remote Internal Vulnerability Scanner	
Step 2 — Setting up the OpenVPN on the server	
Configure Router Port Forwarding	
Installing the OpenVPN program on the server	
Setting up your PKI infrastructure	
Generating a TLS authentication key	
Quick Recap	
Setup server configuration file	
Editing Windows network settings	
Opening Windows firewall	
Enabling IP forwarding	
Enable internet connection sharing	
Restart to apply changes	
Enable Routing and Remote Access	
Step 3 — Create Open VPN Configuration File	
Step 4 — Upload Open VPN Configuration File to VulScan	
Step 5 — Perform Remote Internal Vulnerability Scan	
Manage Portal Users and Access	107
	_
Manage Users (Global Level)	
Users and Global Access Roles	
Add User at Global Level	
Edit User at Global Level	
Enable Log In with KaseyaOne	114
Enable Log in with KaseyaOne at Account Level from Global Settings	
Log in with your KaseyaOne user	117
User Matching Criteria	118
Require Log In with KaseyaOne	118
Frequently Asked Questions	120

Enable Automatic User Creation for RapidFire Tools Portal	121
Step 1 – Enable Log in with KaseyaOne at Account Level from Global Settings	121
Step 2 – Enable Automatic User Creation	
Step 3 – KaseyaOne User Logs into RapidFire Tools Portal	
Change your Password	127
Recover Forgotten Password	128
Log Out of RapidFire Tools Portal	130
Enable Access Groups	131
Set Up Portal Branding	134
Set Custom Portal Theme	135
Set Custom Portal Subdomain	136
Set Custom Company Name	
Set Custom Company Logo	138
Set Up a Custom Subdomain to Access the RapidFire Tools Portal	140
Portal Administration	142
Set Time Zone	142
Report Date Format (Global Settings)	142
Admin Alerts (RapidFire Tools Portal)	144
Admin Alerts: Global Settings vs. Site Settings	144
Configure Admin Alerts	144
Delete a Site	145
Import IT Glue Organizations	147
Step 1 — Create and Copy API Key in IT Glue	147
Step 2 — Enable Connection to IT Glue from Portal Global Settings	148
Step 3 — Set Up Organizations	151
Step 4 — Synchronize Org Names with IT Glue	153
Pause Org Name Synchronization	
Import IT Glue Orgs when Creating New Organizations	154
Create an API Key	
Appendices	158

VulScan Integration with Network Detective	161
Migrate Inspector 2 to VulScan	161
Log in to RapidFire Tools Portal and Access VulScan Site	163
Next Steps for New VulScan Users	
Generate Internal Vulnerability Reports in Network Detective using VulScan	
VulScan and Reporter	
Set Up and Assign a Ticketing/PSA System Integration to a Site	
Step 1 — Gather Credentials and Set Up your PSA System	
Step 2 — Set Up a Connection to your Ticketing System/PSA	
Step 3 — Map your Site to a Ticketing System/PSA Connection	173
Set Up Autotask Integration	
Set Up Autotask (SOAP) Integration	179
Set Up ConnectWise REST Integration	
Step 1 — Download and Install the ConnectWise Manage Internet Client Application	
Step 2 — Select the ConnectWise Ticket System API Member Account to Inte	egrate
with	
Create Minimum Permissions Security Role for API Member	
Table Setup Configuration	
Step 3 — Create an API Key in the ConnectWise Ticketing System	
Step 4 — Configure Service Tables in ConnectWise	
Step 5 — Remove "Disallow Saving" Flag from Company	
Set Up ConnectWise SOAP Integration	
Set Up Kaseya BMS Integration	
Data Collectors for VulScan	
Function of VulScan Data Collectors	
Internal Vulnerability Data Collector	199
External Vulnerability Data Collector	199
Portable Data Collector	
Remote Internal Vulnerability Scanner	
Provision VulScan	
Manage Site Data Collectors	
Data Collector Commands	

Enable Discovery Agents for Local Data Collection (VulScan)	207
Discovery Agent Firewall Requirements	207
Step 1 — Enable Discovery Agents at the Organization Level	208
Step 2 — Install Windows Discovery Agent on PC on target network	209
Step 3 — Confirm Discovery Agent install from your Organization	211
Step 4 — (Optional) Enable Access for Site Admin and Technician Users	212
Step 5 — Schedule Scans for Discovery Agent	213
Step 6 — Assign Labels to Agents	214
Step 7 — Configure VulScan Agent Imports	215
How Scan Data Import Configuration Works	216
Remove Discovery Agents	217
Application Vulnerability Scan for Windows	219
Step 1 — Deploy Discovery Agents on Endpoints	219
Step 2 — Enable Application Vulnerability Scan for Windows for Discovery Agents	219
Step 3 — Review Application Vulnerabilities	220
Install Linux and macOS Discovery Agents	221
Find and Copy Install Key for Discovery Agents	221
Default Scripted Linux Install	222
Default Scripted macOS Install	223
Install Script Options	224
Silent Install for Discovery Agent (Windows)	226
Uninstall Script for Discovery Agent	227
Portable VulScan Set Up	. 228
Step 1 — Provision Portable VulScan Appliance	228
Step 2 — Install Portable VulScan Appliance on target Network	228
Step 3 — Create VulScan Site and opt not to provision appliance	228
Step 4 — Assign Portable VulScan Appliance to Site	229
Step 5 — Set Up and Perform Internal Scan and Notification Tasks	230
Step 6 — Remove PVS appliance from Site	230
Step 7 — Assign PVS appliance to new VulScan Site	231
Enable Global Two-Factor Authentication (2FA) for Portal Users	232
Step 1 — Master user enables 2FA for all portal users	232

Step 2 — Portal user logs in and sets up 2FA Access	
Step 3 — Portal Users enter Authentication Code after initial login	
Import IT Glue Organizations	235
Step 1 — Create and Copy API Key in IT Glue	
Step 2 — Enable Connection to IT Glue from Portal Global Settings	
Step 3 — Set Up Organizations	
Step 4 — Synchronize Org Names with IT Glue	241
Pause Org Name Synchronization	241
Import IT Glue Orgs when Creating New Organizations	242
License Usage (Global Settings)	

VulScan Introduction

VulScan enables automated internal and external vulnerability scanning and threat notifications. **VulScan** consists of the RapidFire Tools Portal and a virtual appliance that you install on the target network to be assessed. **Network Detective** users can likewise leverage VulScan data to create internal vulnerability reports. This guide demonstrates how to set up, configure, and schedule automated scan tasks and vulnerability notifications using **VulScan**.

Key features

- Perform automated internal and external vulnerability scans
- Drill down into scan results using the VulScan dashboard
- Create and send Email Notifications
- Create and export Tickets to PSA systems
- Leverage scan data to generate vulnerability reports in Network Detective

VulScan Components

VulScan Component	Description
VulScan Software Appliance	The VulScan Server is a Windows application helps perform internal or external vulnerability scans. There are currently several types of VulScan appliances:
	 Internal Scan Appliance (IVS): Installed on a PC on the client's internal network and performs internal scans.
	• External Scan Appliance (EVS): Installed on the MSP network and performs external scans against the target network.
	 Portable Scan Appliance (PVS): Installed on a physical device that can be moved from site to site to perform internal vulnerability scans.
	• Remote Internal Vulnerability Scanner (RIVS): Installed on the MSP network. Can be shared by multiple sites for the purpose of remote scanning internal IP addresses through a proxy agent.
	• Discovery Agent (AGT): Installed on a device on the client's internal network to perform local scans on that device. The Agent compares local data, such as the device's application inventory

VulScan Component	Description
	and OS, with the CVE catalog to identify additional vulnerabilities. Multiple agents can be deployed on the target network.
VulScan Web Portal	VulScan Web Portal serves as a hub for you to manage your VS deployments across various client sites. From each site, you can configure VS scan tasks, tickets/notifications, and drill down into the issues detected.

Set Up VulScan

Setting up VulScan consists of a few basic steps:

- 1. "Add an Organization" below and "Create VulScan Site" on page 13
- 2. "Install VulScan Appliance" on page 18
- 3. <u>"Create Scan and Notification Tasks" on page 20</u>

Once you complete these steps, you can begin <u>"Using VulScan" on page 54</u> to address identified issues.

Add an Organization

Before you begin your first IT or compliance assessment, you can optionally create an **organization**. Think of an organization as a folder in which you can store assessment projects for a particular client.

To add an Organization:

1. Access the RapidFire Tools Portal at <u>https://www.youritportal.com</u> and log in with your credentials.

	RapidFire			
	Username			
	ndtest10@rapidfiretools.com			
	Password	Forgot Password?		
	•••••			
	Remember me			
Log in				
	Or			
	🥑 Log in with IT	Complete		
	Help & Support © I	Kaseya 2022		

2. Access the **Organizations** page from the top-menu. Select **All Organizations** from the side menu.

Micro Consulting	Organizations	
Filter Organizations	Corganizations 22	QS
All Organizations	ABLE Manufacturing West Coa	:
All Sites	st	
🗋 ABLE Manufacturing West Coast	U Sites	
C Accent Fit	Alpha Investments	
Accent Fit - Guest Network		:
Acme Group	2 Sites	

3. Then click Add Organization.

		() ()	0	ĸ
•	_		Add Organizati	ion
Acme Group	:	Acme Organization	:	
🗅 2 Sites		11 Sites		

4. Enter an Organization name. For example, this might be the name of a large company for whom you want to create multiple sites and types of IT and compliance assessments. Then click **Confirm**.

Add Organization	
Organization Name*	Add from IT Glue
Grande Vista	
Organization names must start with only include alphanumeric character less than 50 characters long.	
	Cancel Confirm

5. You can see each organization you've created from the left-side menu.

Micro Consulting	Organizations	
Filter Organizations	C Organizations 22	QS
All Organizations	ABLE Manufacturing West Coa	:
🗋 All Sites	st	
ABLE Manufacturing West Coast		
C Accent Fit	Alpha Investments	:
Accent Fit - Guest Network	2 Sites	•
🗋 Acme Group		

6. From the button you can rename or delete the Organization. From the Organization tile, you can also see the number of sites grouped under the Organization.

Organizations 22	0	Search for site by name
ABLE Manufacturing West Coa st	÷	Accent Fit :
🗅 0 Sites	Rena	ame] 3 Sites
	Dele	te
Alpha Investments	:	Beautiful British Columbia
2 Sites		D Sites

Create VulScan Site

Tip: We recommend you get started by making a "practice site" and running your first assessment in-house. Use this to familiarize yourself with VulScan and the installation and configuration process.

The first step in deploying VulScan is creating a "Site". Sites help you organize your assessments. This task is performed by the Site Administrator. To create a site:

1. Access the RapidFire Tools Portal at <u>https://www.youritportal.com</u> and log in with your credentials.

RapidFire	A Kaseya company
Username	
ndtest10@rapidfiretools.com	
Password	Forgot Password?
Remember me	
Log in	
Or	
🤦 Log in with IT	Complete
<u>Help & Support</u> © K	aseya 2022

2. From the Sites page, click Add Site.

	?	ଡ଼	S IT Pro	ĸ
Discovery Agents	Mo	ove Site	+ Add	Site

3. Enter a **Site Name**. This can be the name of the client for whom the assessment is being performed, for example.

Important: Once you create a site, you cannot change the site name.

4. Under Site Type, select VulScan. Click Next.

Cancel	Next
	Cancel

5. Choose an Org Folder for the site and click **Next**.

Add S	Site
i	Select Organizational Folder for Micro International
Initiat	ive Group 🗸
	Back Next

6. Choose whether to provision an IVS appliance for the new site. Then click **Confirm**.

RapidFireTools^{*}

Note: You should only select **No** if you plan to use a Portable VulScan appliance. See "Portable VulScan Set Up" on page 228

Add Site
Automatically provision Internal Vulnerability Scanner for the new site? Yes No
You are about to create a new VulScan site. This site will count against your licensed total.
Back Confirm

The site dashboard will appear. From here you can see:

- Status of appliances associated with the Site
- High-level graphical overview of scan results by issue severity
- Itemized list of highest risk issues
- Audit log of recent site activity

VulScan Dashboard Scan Results Reports Settings	Vulnerabilities by Device					
Reports Settings	Vulnerabilities by Device					
Settings	vumerabilities by Device	View All	Vulnerabilities Over Time	View All	Appliance Status	Manage
	Last 30 Days		Last 30 Days		ID	Host Type
					AGT-23HNCJ	Server
		Critical			AGT-76JRKH	Server
Audit Log		1			EVS-FTTJ71	Server
		High	10		EVS-JSKR23	Server
	13	6			EVS-KZFC70	Server
	TOTAL	Medium	5		EVS-NYZJ10	Server
		5	0		EVS-QRVQ19	Server
		Low	21.500 and 59.00 and	int shat shat	EVS-TQQF90	Server
		1	ういんちゃくくゃくいない	15 19	EVS-TZBV27	Server
			30-day Moving Wind	low	IVS1-CNXM28	Server
					IVS1-HKMD10	Server
					IVS1-KFFW83	Server
					KVS1-SPHC69	Server
	Highest Risk Devices	View All	Critical and High Risk CVE	View All	NDA1-9535BA	Server
	Last 30 Days		Last 30 Days	₽	NDA1-9608NZ	Server
					Highest risk Issues	View All
	199.38.222.181	1	CVE-2020-15778 1		Last 30 Days	VIEW Par
	199.30.222.101		CVE-2021-23017		case on only a	
					Issue	CVSS
	172.31.56.12 (0E:1C:	7.8	CVE-2013-0337 1		CF Nginx End of Life	
			CVE-2016-2183	2	HF OpenSSH <= 8.6 0	
	EC2AMAZ-LEOSPN7 (172	7.5	CVE-2016-6329		nginx 0.6.18 - 1.2	

Install VulScan Appliance

Some VulScan workflows require you to install an appliance on the target network or outside of the network. The appliance performs automated scans and collects data for the assessment environment. VulScan employs several types of appliances for both internal and external vulnerability scans. See <u>"VulScan Appliance Types and Install Instructions"</u> on the facing page for a list of appliance types, including guidance on where and how to install each appliance.

Note: Be sure to associate the appliance with the correct site. During the install process, you will need to choose the correct **Data Collector ID**. You can find this for the site either from the site dashboard or from **[Your Site] > Home > Data Collectors**.

☆ Home	*	Vulnerability Scanner 202	1	
Dashboard Data Collectors		Home / Data Collectors		
Users Roles		Data Collectors 💿		+ Provision Vulnerability Scanner
Advanced Options		Internal Vulnerability Scanner	s External Vulnerability Scanners Discovery Agents	Reporter
 VulScan 		Data Collector Type:	Internal Vulnerability Scanner	
🛱 Audit Log		Data Collector ID:	IVS1-H	0
		Description:	AWS	0
		Last Check-in:	17 Jan 2023 5:54 PM GMT-05:00	
		Update Status:	오 up-to-date	
		Manage Data Collector:	Manage	

Tip: Once you install the appliance on the target site, it may take about 10 minutes for it to appear as active in the site. Once active, it will appear with a **green light** • in the site Appliance Status panel from **VulScan** > **Dashboard**.

VulScan		
Appliance Stat	us	Manage
ID	Description	Host Type
AGT-01A	Example	Server
AGT-180	SMClient	Server
IVS1-KSF	New	Server
IVS1-QQX		Server

VulScan Appliance Types and Install Instructions

VulScan Appliance Type	Prefix	Install Location	Scan Type	Install Instructions
Internal Vulnerability Scanner	IVS	Device on target network	Internal	<u>Virtual Appliance</u> <u>Installation Guide for</u> <u>VulScan</u>
External Vulnerability Scanner	EVS	Device on MSP and/or outside network	External	 <u>Virtual Appliance</u> <u>Installation Guide for</u> <u>VulScan</u>
Portable Vulnerability Scanner	PVS	Physical device moved from site to site	Internal	 <u>"Portable VulScan</u> <u>Set Up" on page 228</u> <u>Virtual Appliance</u> <u>Installation Guide for</u> <u>VulScan</u>
Remote Internal Vulnerability Scanner	RIVS	MSP network; scans customer network through a proxy agent	Internal	 "Set Up Remote Internal Vulnerability Scanne r" on page 86 Virtual Appliance Installation Guide for VulScan
Discovery Agent	AGT	Device on target network	Local Scan	 "Enable Discovery Agents for Local Data Collection (VulScan)" on page 207 "Install Linux and macOS Discovery Agents" on page 221

Create Scan and Notification Tasks

Once you have installed the VulScan appliance for your site, it's time to configure Scan and Notification Tasks. **Scan and Notification Tasks** are the heart of VulScan.

- Scan tasks allow you to configure, schedule, and perform vulnerability scans on the site network at regular intervals. See <u>"Create Internal Scan Task" below</u> and <u>"Create External Scan Task" on page 27</u>.
- Notification tasks allow you to send email reports of identified vulnerabilities to your technicians and/or customers. You can also configure notification tasks to export this data as tickets in your chosen PSA system. See <u>"Create Notification Tasks" on page 30</u>.

Create Internal Scan Task

In order to collect vulnerability data from the target network, you need to set up scan tasks. Follow these steps to create an internal vulnerability scan task with VulScan:

- 1. From your site, go to VulScan > Settings > Scan and Notification Tasks.
- 2. From the Scan Tasks tab, click Create Scan Task.

VulScan	*	VulScan / Settings	Scan And Notificati	on Tasks									
Dashboard		Scan Tasks	Notificati	an Taeke									
Scan Results													
Settings	*	Quick Filter									+ Create	Scan Tas	
Overview													-
General		Task ID 🗘	Appliance ID $\ensuremath{\hat{\ominus}}$	Appliance Description $\hat{\circ}$	Task Label 🗘	Description 0	Scan Type 🗘	Status 🗘	Next Run 🗘	Repeats 0			
Report Preferences Scan Credentials Custom Scan Profiles Scan and Notification T Exclusion Rules IT Complete	asks	82	kvs1-	Updated	Internal Vulnerability Scan Two	Perform an Internal Vulnerability scan on the IP Range [10.200.1.14,10.200.1.116- 10.200.1.133,10.200.1.140- 10.200.1.33,10.200.1.140- 10.200.1.255,131 IP Addresses will be excluded. Config: Low Impact.	Internal Scan	Pending	2023/01/01 01:51:00 PM	Yearly	Run Now	/ 8	ð
Audit Log		9	EVS-	Not in AWS	External Scan (out of AWS)	Perform an External Vulnerability scan on the IP Range [45.33.32.156].	External Scan	Pending	2023/06/26 09:35:00 PM	Once	Run Now	0	1

3. From Scan Type, select Internal Vulnerability Scan and click next.

Note: If you are using the **Remote Internal Vulnerability Scanner**, select that option.

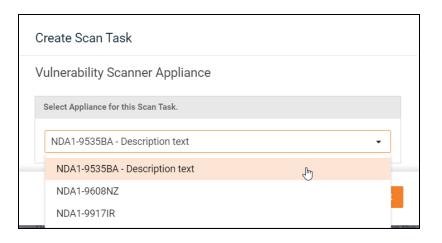
Create Scan Task	
Select Scan Type	
Select the type of scan to be scheduled.	
Internal Vulnerability Scan	
O External Vulnerability Scan	
Remote Internal Vulnerability Scan (via Vu	ulScan Proxy)
\bigcirc Hosted External Vulnerability Scan	
	Cancel Previous Next

4. Select the Appliance from the drop-down menu and click Next.

Note: This feature is used when multiple IVS appliances are assigned to scan the target network. See <u>"Provision VulScan" on page 200</u>.

In this case, create separate internal scan tasks to assign to the individual appliances. Define a sub-set of the IP range for each scan task to distribute the work between the available appliances. This can reduce overall scan time on larger networks.

Important: Do not use multiple appliances to scan the same subnet or IP range. This may produce errors in your scan results.



5. Select the **Scan Profile**. You can select from the available profiles, or you can use your own "Custom Scan Profiles" on page 44.

Create Scan Task							
Select Scan Profile							
We strongly recommend using the Low Impact or Standard Scan to start your Internal Vulnerability assessment. Selecting a Comprehensive Scan will significantly increase scan time.							
Any scan will create increased load and could affect performance on systems with existing vulnerabilities while the scan is running. For minimal impact, we recommend selecting Low Impact and running scans during non-working hours. Scans may take several hours to complete and possibly days for very large networks when selecting a Comprehensive Scan.							
Low Impact Scan							
Standard TCP ports and Top 1000 UDP. Does not include brute force login attempts.							
🔿 Standard Scan							
Standard TCP ports and Top 1000 UDP							
O Comprehensive Scan							
All TCP (1-65535) and Top 1000 UDP NOTE: Comprehensive scans may take a significant amount of time and incur increased load on the network.							
○ Custom							
Scan Profile: Select a Custom Scan Profile Create Profile Refresh							
Cancel Previous Next							

The available options are in the table below. Click Next.

Scan Profile	Description	Notes
Low Impact Scan	Standard TCP ports and Top 1000 UDP	Does not include brute force login attempts
Standard Scan	Standard TCP ports and Top 1000 UDP	
Comprehensive Scan	All TCP (1- 65535) and Top 1000 UDP	Comprehensive scans may take a significant amount of time and incur increased load on network

 Next configure IP ranges. The VulScan appliance will automatically suggest an IP Range for the scan. If you do not wish to scan the default IP Range, select it and click Clear All Entries. Use this screen to enter additional IP Addresses or IP Ranges and click Add.

You can also enter hostnames. Ensure they are fully qualified, as in the example: **desktop1.mylocalnetwork.local**.

Important: Enter hostnames is not supported for Windows Workgroups names, or for local names if the machine joined AD and AD is a DNS server and DHCP is pointing to AD/DNS.

By default, VulScan will **Only scan pingable devices**, or devices that VulScan can talk to. Unselect this option to scan the entire IP range even when no device is detected at an IP address.

Important: Do not use multiple appliances to scan the same subnet or IP range. This may produce errors in your scan results.

Create Scan Task	
Scan Targets	
Auto-Detected IP Ranges on Remote Appliance	
10.159.5.0-10.159.5.255	
Scan Targets Example IP Range Format: 192.168.0.0-192.168 Example Hostname Format (FQDN): desktop1.r	
Single IP or IP Range or Hostnam + Add	
10.159.5.0-10.159.5.255 pro1.micropro.com pro2.micropro.com	Exclude IPs Reset to Auto-Detected Remove Selected Entry Clear All Entries
Only scan pingable devices	
	Cancel Previous Next

From this screen you can also:

- Click Reset to Auto-detected to reset to the automatically suggested IP Range.
- Exclude IPs or IP ranges from the scan.

Note: Key network component IP addresses should be excluded in order to prevent scans being performed from impacting the performance of a device when it is being scanned. For example, a company might want to exclude the IP Address range for their voice over IP telephone system if they are performing a scan during business hours.

Tip: If you are using multiple appliances to perform internal vulnerability scans for a site, define a sub-set of the IP range for the scan task. Create multiple scan tasks to distribute the work between the available appliances.

- 7. Click **Next Page** once you have configured the IP ranges for the scan.
- 8. From the Credentials for Authenticated Scans screen, select whether you use credentials for the internal scan. Note that you must first have entered these credentials from <u>"Scan Credentials" on page 42</u>.

Cre	eate Scan Task				
Cre	edentials for Authenticated Scar	าร			
	SSH:			on Port	
	None		•	22	
	SMB:				
	None		•		
	ESXi:				
	None		•		
	SNMP				
	None		•		
		Cancel	Pre	evious	Next

For each protocol, select the credentials you wish to use from the drop-down menu. When you're finished, click **Next**.

- SSH: Use this protocol to scan for devices that use the SSH protocol.
- **SMB**: Use this protocol to scan for network shares, such as file and printing shares.
- EXSi: Use this protocol to scan for VMware hosts.
- **SNMP**: Use this protocol to scan for devices such as switches, bridges, routers, access servers, computer hosts, hubs, and printers.
- 9. From the Verify and Schedule menu, configure the scan task:

Create Scan Task	
Verify and Schedule	
Send email notification when schedule completes	
Task Label	
Time Zone	
(UTC-05:00) Eastern Time (US & Canada)	•
Schedule	
Every Select interval	✓ at 12:00 AM ③
Vulnerability Scan Setting Enable Scan Task	
Skip devices with all ports filtered	
	Cancel Previous Save

- a. Select whether to send an **email notification** when the scan completes then enter an email recipient for the notification.
- b. Enter a task label to describe the scan task.
- c. Select the **time zone** from the drop-down menu.
- d. Next choose a day and time to **schedule** the scan.
- e. **Enable** or **disable** scan task; you can then later edit the scan task to enable/disable at any time.
- f. Choose whether to skip devices that have all ports filtered.
- 10. Click Save.

The internal vulnerability Scan Task will be created. You can see the details for the task in the scan tasks table.

Scan Tasks	Notificati	on Tasks									
Quick Filter									+ Create S	Scan Ta	sk
Task ID 💠	Appliance ID 💠	Appliance Description \diamondsuit	Task Label 💠	Description 💠	Scan Type 💠	Status 💠	Next Run 💠	Repeats 💠			
8298471	KVS1-	Updated	Internal Vulnerability Scan Two	Perform an Internal Vulnerability scan on the IP Range [10. 10.	Internal Scan	Queued	01/01/2024 11:51:00 AM	Yearly	Run Now	0	Û
				10. 10.							
				10.]. 13 IP Addresses will be							
				excluded. Config: Low Impact.							

Scan Task "Run Now"

You can choose to run a scheduled scan task immediately. To do this, click **Run Now** next to the chosen task. The vulnerability scan will then enter the scan queue and will begin as soon as any current scan finishes.

	+ Create Scan Task						
Repeats ≑							
Once	Run Now	Ø					

Edit/Delete Scan Task

- To edit a scan task, click the pencil icon next to a task. Make and save your changes.
- To delete a scan task, click the trash icon next to a task.

Create External Scan Task

Note: Before you can create an external vulnerability scan task, you first need to provision and install an external vulnerability scan appliance. See <u>"Install VulScan</u> <u>Appliance" on page 18</u> and <u>"Provision VulScan" on page 200</u>. If you wish to perform external scans without using an appliance, see <u>"Kaseya Hosted External Vulnerability Scan" on page 34</u>.

Follow these steps to create an external vulnerability scan task with VulScan:

- 1. From your site, go to VulScan > Settings > Scan and Notification Tasks.
- 2. From the Scan Tasks tab, click Create Scan Task.

VulScan	¥	VulScan / Settings	/ Scan And Notificati	on Tasks									
Dashboard		Scan Tasks	Notificati	on Tasks									
Scan Results													
Settings	*	Quick Filter									+ Create	Scan Ta	sk
Overview													
General		Task ID 🗘	Appliance ID 🗘	Appliance Description $\hat{\circ}$	Task Label 🗘	Description 0	Scan Type 🗘	Status 🗘	Next Run 🗘	Repeats 0			
Report Preferences Scan Credentials			h			Perform an Internal Vulnerability scan on the IP Range [10.200.1.104-							
Custom Scan Profiles	Tasks	82	KVS1-	Updated	Internal Vulnerability Scan Two	10.200.1.114,10.200.1.116- 10.200.1.133,10.200.1.134- 10.200.1.139,10.200.1.140- 10.200.1.2551,13 IP	Internal Scan	Pending	2023/01/01 01:51:00 PM	Yearly	Run Now	0	1
Exclusion Roles						Addresses will be excluded. Config: Low Impact.							
Audit Log		91	EVS-	Not in AWS	External Scan (out of AWS)	Perform an External Vulnerability scan on the IP Range [45.33.32.156].	External Scan	Pending	2023/06/26 09:35:00 PM	Once	Run Now	0	1

3. From Scan Type, select External Vulnerability Scan and click Next.

Create Scan Task	
Select Scan Type	
Select the type of scan to be scheduled.	
O Internal Vulnerability Scan	
External Vulnerability Scan	
Remote Internal Vulnerability Scan (via	a VulScan Proxy)
\bigcirc Hosted External Vulnerability Scan	
	Cancel Previous Next

4. Select the Appliance from the drop-down menu and click Next.

Create Scan Task	
Vulnerability Scanner Appliance	
Select Appliance for this Scan Task.	
EVS-QRV	•
	Cancel Previous Next

5. Enter the IP addresses for the external vulnerability scan. You can enter individual IPs or IP ranges. You can also enter fully qualified domain names, such as **www.example.com**. Click **Next Page**.

Important: You must ensure that no other Network Detective or Compliance Manager products are being used to perform an External Vulnerability Scan on the same external IP Address range at the same time. Allow at least several hours between repeat external vulnerability scans. Scheduling external scans at the same time will result in reports with missing or incomplete data.

Create Scan Task	Create Scan Task								
Scan Targets									
Ensure IP Addresses are not local addresses.									
Example Domain Name Format (FQDN): w	ww.example.com								
Single IP or IP Range or Domain Name	+ Add								
micro-pros.com salient-industries.com 12.50.12.50	Remove Selecte	:d							
	Cancel Previous	Next							

6. From the Verify and Schedule menu, configure the scan task:

Create Scan Task				
Verify and Schedule Email Notification Send email notification when schedule completes Email Address Task Label				
Time Zone				
(UTC-05:00) Eastern Time (US & Canada)				•
Schedule				
Every Select interval	•	at	12:00 AM	0
Vulnerability Scan Setting				
Skip devices with all ports filtered				
	Cancel	P	revious	Save

- a. Select whether to send an **email notification** when the scan completes then enter an email recipient for the notification.
- b. Enter a task label to describe the scan task.
- c. Select the time zone from the drop-down menu.
- d. Next choose a day and time to schedule the scan.
- e. **Enable** or **disable** scan task; you can then later edit the scan task to enable/disable at any time.
- f. Choose whether to skip devices that have all ports filtered.
- 7. Click Save.

The external vulnerability Scan Task will be created. You can see the details for the task in the scan tasks table.

11063801	IVS1- CN>		Test	Perform an Internal Vulnerability scan of the Scan Target (172.31.56.0- 172.31.56.15). No IP Addresses will be excluded. Config: Low Impact.	Internal Scan	Disabled	N/A	Once	Run Now	0	Û
11064608	EVS- QRV	1000	Test	Perform an External Vulnerability scan of the Scan Target [199.38.222.181].	External Scan	Pending	24/03/2024 01:27:00 PM	Once	Run Now	0	Û
11178421	NDA1- 9		External Scan (out of AWS)	Perform an Internal Vulnerability scan of the Scan Target [10.159.1,1- 10.159.1,255]. No IP Addresses will be excluded. Config: Low Impact.	Internal Scan	Queued	04/12/2023 06:00:00 AM	Monthly	Run Now	0	Û

RapidFireTools[®]

Create Notification Tasks

The results of your scan tasks will appear in the VulScan Dashboard for your site, where you can drill down into detected issues. In addition, you can **send the results of your vulnerability scans as email notifications** to assigned recipients. Likewise, you can configure notification tasks to export identified issues as tickets in your chosen PSA system. To do this:

- 1. From your site, navigate to VulScan > Settings > Scan and Notification Tasks.
- 2. From the Notification Tasks tab, click Create Notification Task.

Scan Tas	ks Notification Task	s						
Quick Filter. Task ID \$	Task Label ≑	Description 🗢	Status ¢	Next Run 🗢	Repeats	+ Create Notific	cation ⁻	Task
2	kvs notification task label	Send Notification Once via email.	Disabled	N/A	No	Run Now	Ø	Û
15	YL - Summary with grouping By Issue (OID)	Send Notification Once via email.	Disabled	N/A	No	Run Now	Ø	1

3. From the **Notification Task Type** menu, select whether to send an email. Enter the notification email recipient and subject line.

Create Notific	ation Task			
Notification T	ask Type			
● Email / Crea	ate Ticket d Email Notification Recipient Email Address Notification Subject Subject			
Cree Send to Roc	ate PSA Ticket			
		Cancel	← Previous	Next

4. Select whether to **Create PSA Ticket**. This option only becomes available once you have enabled a **Connection** for your site from **Global Settings**. It will then display the name of the Connection.

Note: You will need to set up the integration between your VulScan site and your chosen PSA system before you can use this feature. See <u>"Set Up and</u> <u>Assign a Ticketing/PSA System Integration to a Site" on page 167</u> for a complete walkthrough.

- 5. Alternatively, you can choose Export to RocketCyber. This action will make detected issues available to browse in RocketCyber. See <u>"Export Notification Tasks</u> to RocketCyber" on page 80.
- 6. Click **Next** once you've configured the notification type.
- 7. Choose from among the available notification parameters:

Create Notification Task Notification Parameters Specify which issues to generate notifications on and he	ow those notifications are presented.
Issue Type All Issues	Issue Discovery Time Range
Grouping (By Issue/By Device) By Issue (OID)	Issue Detail Verbosity Summary
Truncate Returned Results After 20 Records	CVSS Filter >= 1 <= 10
Host / IP Filter Any IP Address	
	Cancel ← Previous Next

- **Issue Type**: Select whether to notify for all detected issues or only the most recently detected issues.
- **Issue Discovery Time Range**: Select whether to filter vulnerability issues by the available time ranges.
- **Grouping**: Choose whether to organize issues by vulnerability type (OID) or by device.
- **Issue Detail Verbosity**: Select whether to provide only a summary or detailed vulnerability data.
- **Truncate Returned Results After**: Select whether to truncate ("cut off") after X number of issues. By default no records are truncated (value="0").

- **CVSS Filter**: Select whether to filter issues by CVSS (Common Vulnerability Scoring System). For example, you can set the value to be >=7 and <=10, thus notifying only for issues with a 7-10 CVSS score.
- Host/IP Filter: Choose whether to include all scanned IP addresses or a specified range. Specify a range in the same way you specify a range for the scan task.
- 8. If you opted to create a PSA ticket, configure the following options and then click **Next**.
 - Ticket Summary: Enter a summary for the tickets
 - Create separate tickets per issue: Choose whether to create individual tickets for each device affected by a single issue type. THIS MAY CREATE A LARGE NUMBER OF TICKETS IN YOUR PSA.
 - Exclude issues with open tickets: Choose whether to filter out issues that already have open tickets to avoid repeat tickets.

PSA Ticket Options				
' Ticket Summary				
Vulnerability Detected by VulScan				
If Create separate tickets per issue option is selected	ed, Vulnerability title wi	ill be added to the Ticket Sun	nmary	
Options Create separate tickets per issue	2			
Exclude issues with open tickets				
		Cancel	← Previous	Next

9. From **Select Schedule**, enter a task label and schedule your notifications. Click **Save**.

Create	Notification Task	
Select	Schedule	
Task Labe	əl *	
Examp	le Notification	
Time Zon	e	
(UTC-0	5:00) Eastern Time (US & Canada)	~
Schedule		
Every	Select interval	✓ at 12:00 PM ③
🗹 En	able Notification Task	
		Cancel ← Previous Save

Note: Use **Enable Notification Task** option to enable/disable the task. This can he helpful if you wish to pause a notification task.

10. The created item will appear under notification tasks.

can and Notification Tasks ③						
Scan Tasks Notification Tasks						
Quick Filter					Create Notific	ation Task
				· · ·	Create Notific	Sation raon
Task ID 💠 🛛 Task Label 🗘	Description \$	Status ≑	Next Run \doteqdot	Repeats \$		

Edit/Delete Notification Task

- To edit a notification task, click the pencil icon next to a task. Make and save your changes.
- To delete a notification task, click the trash icon next to a task.

Kaseya Hosted External Vulnerability Scan

The Kaseya Hosted External Vulnerability Scanner that allows users to seamlessly perform remote external scans using Kaseya's secure data center. You set up the Kaseya hosted scan task the same way you would using the external scan appliance, but without the complexity of deploying and setting up an appliance.

Follow these steps to create a Kasyea Hosted External Vulnerability Scan Task with VulScan:

Step 1 – Provision Hosted External Vulnerability Scanner

First, contact your account representative to provision the Kaseya Hosted External Vulnerability Scanner. Your license will allow you scan a certain number of external IPs per month. Once your account is provisioned, you can set up the external vulnerability scan task.

Step 2 – Set up Hosted External Vulnerability Scan Task

- From your VulScan site, go to VulScan > Settings > Scan and Notification Tasks.
- 2. From the Scan Tasks tab, click Create Scan Task.

WulScan *	VulScan / Settings	/ Scan And Notificati	on Tasks									
Dashboard	Scan Tasks	Notificati	on Tasks									
Scan Results												
Settings *	Quick Filter									+ Create	Scan	Task
Overview												
General	Task ID 🗘	Appliance ID 🗘	Appliance Description \updownarrow	Task Label 🗘	Description 0	Scan Type 🗘	Status 🗘	Next Run 🗘	Repeats 0			
Report Preferences Scan Credentials Custom Scan Profiles Scan and Notification Tanks Exclusion Rules If Complete	82	KVS1-	Updated	Internal Vulnerability Scan Two	Perform an Internal Winerability scan on the IP Range [10.200.1104- 10.200.1143[0.200.1.134- 10.200.1.138].0.200.1.134- 10.200.1.353[0.200.1.140- 10.200.1.255] 13 IP Addresses will be excluded. Config: Low Impact.	Internal Scan	Pending	2023/01/01 01:51:00 PM	Yearly	Run Now	0	8
Audit Log	9	EVS-	Not in AWS	External Scan (out of AWS)	Perform an External Vulnerability scan on the IP Range [45.33.32.156].	External Scan	Pending	2023/06/26 09:35:00 PM	Once	Run Now	0	8

3. From Scan Type, select External Vulnerability Scan and click Next.

Create Scan Task	
Select Scan Type	
Select the type of scan to be scheduled.	
Internal Vulnerability Scan	
External Vulnerability Scan	
💿 Remote Internal Vulnerability Scan (via V	VulScan Proxy)
Hosted External Vulnerability Scan	
	Cancel Previous Next

4. Enter the IP addresses for the external vulnerability scan. You can enter individual IPs or IP ranges. Click **Next Page**.

Important: You must ensure that no other Network Detective or Compliance Manager products are being used to perform an External Vulnerability Scan on the same external IP Address range at the same time. Allow at least several hours between repeat external vulnerability scans. Scheduling external scans at the same time will result in reports with missing or incomplete data.

Create Scan Task		
Scan Targets		
Ensure IP Addresses are not local addresses.		
Example Domain Name Format (FQDN): w	vw.example.	.com
Single IP or IP Range or Domain Name	+ Add	
micro-pros.com salient-industries.com 12.50.12.50		Remove Selected Remove All
	Cancel	Previous Next

RapidFireTools^{*}

5. From the Verify and Schedule menu, configure the scan task:

Create	Scan Task		
Email Not	email notification when schedule completes		
Email Address Task Label			
Time Zon (UTC-0 Schedule	: 5:00) Eastern Time (US & Canada)		•
Every	Select interval -	at	12:00 AM 🔇
Vulnerability Scan Setting C Enable Scan Task Skip devices with all ports filtered			
	Cancel	P	revious Save

- a. Select whether to send an **email notification** when the scan completes then enter an email recipient for the notification.
- b. Enter a task label to describe the scan task.
- c. Select the **time zone** from the drop-down menu.
- d. Next choose a day and time to **schedule** the scan.
- e. **Enable** or **disable** scan task; you can then later edit the scan task to enable/disable at any time.
- f. Choose whether to skip devices that have all ports filtered.
- 6. Click Save.

The hosted external vulnerability Scan Task will be created. You can see the details for the task in the scan tasks table.

Scan Tasks	Notificati	on Tasks									
uick Filter									+ Create	e Scan	Task
Fask ID \Diamond	Appliance ID $\ensuremath{\hat{\Rightarrow}}$	Appliance Description \updownarrow	Task Label 🗘	Description \diamondsuit	Scan Type 🗘	Status 🗘	Next Run 🗘	Repeats ≑			
11286165	Hosted EVS		Kaseya Hosted External Scan	Perform an External Vulnerability scan on the IP Range	External Scan	Pending	06-Oct- 2023 12:00:00 PM	Quarterly	Run Now	0	Û
				[1.1.1.1].							
1244501	IVS1- PQMV31		Apogee Internal Scan	Perform an Internal Vulnerability scan on the IP Range [10.80.0.0- 10.80.1.255]. No IP Addresses	Internal Scan	Queued	23-Sep- 2023 12:00:00 PM	Weekly	Run Now	0	

Step 3 – Keep Track of Hosted External Scan License Limit

When you work with your account manager to provision Kaseya Hosted External Vulnerability Scans, you will agree to a certain number of hosted scans that you can perform per month. You can see your remaining hosted external scans from the VulScan Dashboard (**Home > Dashboard**).

Hosted External Vuli	nerability Scan Usage
8 External IP Scans Available	Reset Date 01-Oct-2023
88%	57 of 65 External IP Scans Used

When you are close to exceed your monthly limit, you will receive a License Usage Warning email as a portal Admin Alert.



Likewise, you will receive a second notification email when you reach your monthly limit of hosted scans.

LIC	CENSE USAGE WARNING
Host	ed External Vulnerability Scan License Warning
Host	ed External Vulnerability Scan License Limit reached.
	Maximum Number of External IP Scans (per month) allocated by your Hosted External Vulnerability Scanner
licen	se has been reached.
Any I	Hosted External Vulnerability scans scheduled for the current month will not be performed.
To in	crease the Maximum Number of External IP Scans (per month), please acquire additional licenses.

Configure Device Matching Criteria to Reduce False Positives

Some of your sites might employ devices with different network configurations, such as static or dynamic IP addresses. Accordingly, device attributes such as IP address or hostname might change over time.

VulScan allows you to set rules for how to identify individual devices — increasing the accuracy of your vulnerability scans. Here's how this works:

1. From your VulScan site, navigate to VulScan > Settings > General.

Micro Consulting		Organizations
Home VulScan Dashboard Scan Results Reports	۶ ۲	Granite Dynamics Micro Professionals / Granite Dynamics / VulScan / Settings / General General
Settings Overview General	×	Default Matching Rule ③
Report Settings Scan Credentials Custom Scan Prot Scan and Notifica Exclusion Rules		All selected attributes must match v Select attributes (must select at least 1 attribute): MAC Address Hostname IP Address

From here you can set "matching rules" for nailing down individual devices. This can help reduce false positive or duplicate issues that might result in scans over time.

- 2. First, set the Matching condition from the drop-down menu. You can select:
 - All selected attributes must match: If ALL of the selected attributes for two devices match, VulScan will treat them as the same device when it generates an issue.
 - Any selected attributes must match: If ANY of the selected attributes for two devices match, VulScan will treat them as the same device when it generates

an issue.

Dashboard	General
Scan Results	Default Matching Rule
Settings -	Condition All selected attributes must match 🗸
Overview	All selected attributes must match
General	Select attr <mark> Any selected attribute must match_):</mark>
Report Preferences	✓ Hoc Address✓ Hostname
Scan and Notification Tasks	✓ IP Address
False Positive Management	Save
Audit Log	

- 3. Next, select the attributes that VulScan will use to identify individual devices. These are:
 - MAC Address
 - Hostname
 - IP Address
- 4. When you're finished, click **Save**. VulScan will then match devices accordingly when it performs subsequent scans.

Matching Examples

Refer to the table below if you want to understand better how VulScan will treat individual devices with various matching criteria.

DEVICE A = 10.0.0.1 / AA-FF-FF / Desktop1

DEVICE B = 10.0.0.2 / AA-FF-FF / Desktop2

Matching Condition	Selected Device Attributes	Issue Results
ALL	Hostname, MAC, IP	Multiple issues generated
ANY	Hostname, MAC, IP	1 issue generated
ALL	Hostname	Multiple issues generated
ANY	Hostname	Multiple issues generated

Matching Condition	Selected Device Attributes	Issue Results
ALL	MAC	1 issue generated
ANY	MAC	1 issue generated
ALL	IP	Multiple issues generated
ANY	IP	Multiple issues generated
ALL	MAC, Hostname	Multiple issues generated
ANY	MAC, Hostname	1 issue generated
ALL	IP, MAC	Multiple issues generated
ANY	IP, MAC	1 issue generated

Scan Credentials

VulScan allows you the option of performing credentialed scans on the target network. The credentials allow VulScan to access an account on a network device — this enables a more thorough internal vulnerability scan. Credential scans also support SNMP community strings and other network protocols.

You can enter scan credentials for your VulScan sites and then assign these credentials to be used during the scan task. Scan credentials are not required to perform an internal scan, but adding them can help detect a wider range of security issues. Further, you can add multiple sets of credentials and assign these to multiple scan tasks, thus allowing you to scan a network from the perspective of several accounts.

Add Credentials to a VulScan Site

- 1. Here's how to add scan credentials to your VulScan site:
- 2. From your VulScan site, navigate to VulScan > Settings > Scan Credentials.

Micro Consulting	Organizations		⑦ 谗	IT Pro
Home ▶ WulScan ▼	Granite Dynamics			
Dashboard	Micro Professionals / Granite Dynamic	s / Vulscan / Settings / Scan Credentials		
Scan Results	Scan Credentials ③			
Reports Settings	Quick Filter		+ Cre	ate New Credential
Overview General	Name ≑	Type ≑	Comment 🗢	
Report Settings	Site SNMP credentials	SNMP v1/2c		Ø 🗊
Scan Credentials Custom Scan Profiles	SSH Encryption	Username + Password	Use this for dev machines	1 8
Scan and Notification Tasks	VMWare Detection	Username + Password		Ø 🗊
Exclusion Rules VulScan Proxy Settings				
IT Complete				
Audit Log				

- 3. Click Create New Credential.
- 4. Enter the credential details.

Add New Credential	
Name *	
Comment	
Type* Username + Password	~
Allow Insecure Use *	
Username *	Password *
	Show Password
	Cancel Add

- Name: Enter a label that helps your team understand this set of credentials.
- **Comment**: Enter any additional detail about the status or purpose of the credentials.
- **Type**: Choose from among the supported credential types. These are:
 - Username and Password
 - ° SNMP v1/2c
 - ° SNMP v3
- Allow Insecure Use: Select whether the VulScan appliance can use the credential for unencrypted or otherwise insecure authentication methods.
- 5. Continue entering the credentials until you are finished. The credentials will vary depending on the type. Click **Add**.
- 6. The new credentials will be saved to your site, where you can use them during the scan configuration. See <u>"Create Internal Scan Task" on page 20</u>. You can also return to your site to edit or delete the credentials.

Custom Scan Profiles

Custom Scan Profiles allow you to customize your VulScan tasks. Specifically, you can create scan profiles to target specific TCP and/or UDP ports. In this way, you can perform low impact scans that address only those ports with which you are concerned.

Create New Profile

To create a new Custom Scan Profile:

- 1. From your VulScan site, navigate to VulScan > Settings > Custom Scan Profiles.
- 2. Click Create New Profile.

☆ Home	Þ	Generative Solutions
WulScan	*	
Dashboard		Acme Group / Generative Solutions / Vulscan / Settings / Custom Scan Profiles
Scan Results		Custom Scan Profiles ③
Reports	Þ	
Settings	•	Quick Filter + Create New Profile
Overview		
General		Name 🔶 Comment 🗢 Ports
Report Preferences		No profiles
Scan Credentials		
Custom Scan Profiles	-	
Scan and Notification Ta	asks	
Exclusion Rules		

3. Enter a name for the profile and any relevant comment.

Vulnerability Scan	
Comment	
Common Ports	
Ports*	
T:22-100,555,560-570,777,U:53,161,450-560	
	li li
Guidelines:	41/8,000
1. Select Protocol: Use "T:" for TCP or "U:" for U	
 List individual ports or define ranges with da Use commas to separate ports and ranges. 	ishes (-).
4. Mixed Protocols: If using both UDP and TCP, ports.	specify TCP ports before UDP
Examples:	
	65535.

- 4. Next, enter individual port numbers or ranges using the correct format. First, use "U:" or "T:" to choose TCP or UDP ports. Then enter ports in the order of lowest to highest. Use a dash between numbers to define a range of ports to scan. Use a comma to delimit your entries with no spaces. Here are two examples:
 - Scan all TCP and UDP Ports T:1-65535,U:1-65535
 - Scan a mix of single ports and port ranges T:22-100,555,560-570,777,U:53,161,450-560

Note: Currently, brute force login attempts ARE included as part of a custom scan.

5. When you're finished, click **Add**. You can view and edit scan profiles for this site from the list. You can then proceed to <u>"Create Internal Scan Task" on page 20</u>.

Invite Users to VulScan Site

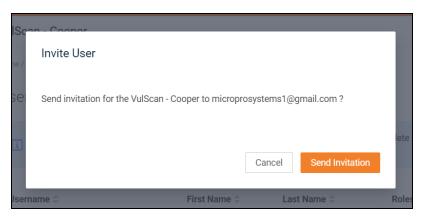
You can send an email to invite site users to join your VulScan site. Invited users then create a password and log in to the portal, where they can then access the site. Here's how this works:

- 1. From your VulScan site, navigate to Home > Users.
- 2. Find the user you wish to invite. Click the mail icon next to the user.

Note: You must have first assigned the user a site role before you can send the invite.

Aicro Consulting				(7	© ©	IT Pro	1
Home Dashboard	VulScan - Cooper						
Data Collectors	Home / Users						
Users	Users					+ Add U	ser
Roles	03613						
Advanced Options	Removing a user from the	table below only removes that u	ser's access from this site.	To delete a user, hav	ve the globa	el .	
VulScan	administrator remove the u						×
Audit Log							
	Username ≑	First Name 🗘	Last Name ≑	Roles ≑	Groups	÷	
	$(A_{i},A_{i}) = (A_{i},A_{i}) = (A_{i},A_{i}$	100110-0000-000	100704480 10070	Site Admin			Û
				Technician			۵
	phone and the second se			Site Admin			۵
	parts 2000 - 1000 - 100	1000	10000	Technician			۵
	microprosystems1@gmail.com	Zenith	Pro	Site Admin		2023.03.28	Û

3. Click Send Invitation.



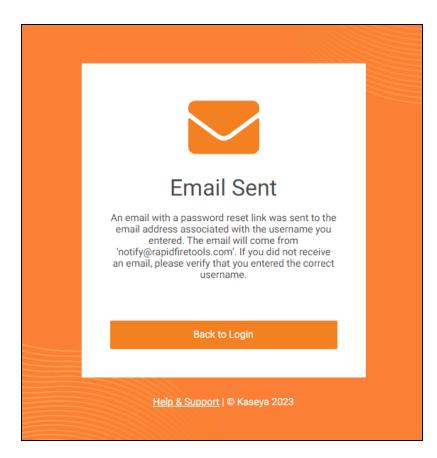
4. The user will receive an email with the subject "Assistance Requested." The user clicks the reset password link.

Assistance Requested Inbox x	8	
alerts@gdpr-central.com <alerts@gdpr-central.com> 4:03 PM (0 minutes ago) 🙀 🔌 to me 👻</alerts@gdpr-central.com>	¢	:
You have been invited as a user to access the VulScan Site VulScan - Cooper using the Kaseya-RapidFire Tools Your I	r Porta	L.
First-time users of the Your IT Portal should note the following:		
If you have never logged into the Your IT Portal previously, you have been assigned a temporary password by the Site Administrator referenced below.		
If you are a first-time user of the Your IT Portal, please visit this page https://www.yourtportal.com/login#reset-password new password for your user account.	to cre	ate a
Once you have created your new password, access the VulScan site by logging into the Your IT Portal https://www.alert staging.com/site/VulScan%20-%20Cooper/vulnerability-scanner.	-centra	F
This request was made by FIRSTNAME-ND (ndtest8@rapidfiretools.com).		
(fn Reply) (r Forward)		

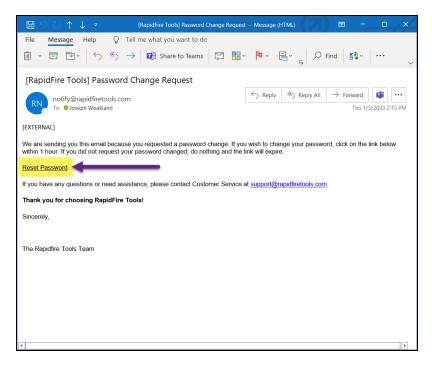
5. The user enters their email to receive the password change request.

Forgot Password	
Please enter your username below. An email with a new temporary password will be sent to the email address you provided when you registered.	
Username	
Submit	
Back to Login	
<u>Help & Support</u> © Kaseya 2023	

RapidFireTools*



6. The user then clicks **Reset Password** from the change request email.



Rapid Fire Tools					
Home	Products Pricing Contact Us Company				
You have requ	ested a password reset. Please enter the new password for your account joseph.weakland@kaseya.com.				
New Passwor	d:				
Confirm Pass	word:				
Reset Pass					
Reset Pass	word				

7. Once the user resets their password, they can log in to the portal and access the VulScan site.

RapidFireTools[°]

Client View

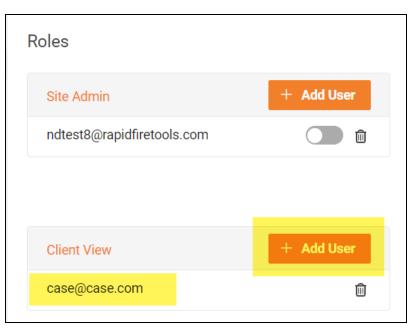
You can invite client users to view your VulScan Dashboard and Reports. This is useful for showing client users your vulnerability remediation efforts.

Note: Client users assigned to the **Client View** Role will have streamlined access to your site, and can only view **Scan Results**, the VulScan **Dashboard**, and **Reports**. See <u>"VulScan Site Roles" on page 52</u> for a complete description of VulScan Roles and their access levels.

Here's how to create a Client View user:

Step 1 – Create User and Assign Client View Role

- 1. From your VulScan site, first create a user for the client from **Home > Users**.
- 2. Next, navigate to **Home > Roles**. Assign the client user to the **Client View** Role.



Step 2 - Invite User to VulScan Site

 To invite the Client View user to the RapidFire Tools Portal, navigate back to Home > Users. 2. Find the user, and click the **Mail icon** to the right of the user. The user will receive an email invitation to the VulScan site. See also <u>"Invite Users to VulScan Site" on page 46</u>.

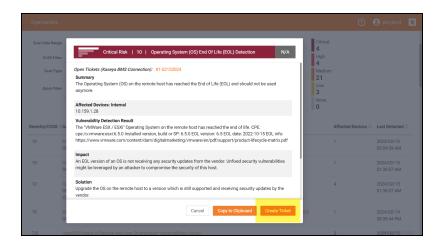
case@case.com	End	User	Client	
---------------	-----	------	--------	--

Step 3 – Client View User Accesses VulScan Site and Views Issues/Creates Tickets

Once the client user accesses the VulScan site, they can view vulnerability data from the Dashboard, Scan Results, and Reports.

VulScan / Scan Result	3		
Scan Results (0		
By Issue	By Device		
Scan Date Range:	Last 30 Days 🔹	Crit 5	ical
CVSS Filter:	Low (1.0+) •	Hig 19	
Scan Type:	All -	AL 33	
Quick Filter:		Lov 2 Nor 0	
Severity/CVSS	Issue ≑	Affected Nodes 🗘	Last Detected \diamondsuit
10	Missing Critical Security Patch – 2023-08 Cumulative Update for Windows 10 Version 22H2 for x64-based Systems (KB5029244) OID:	4	18-Aug-2023 02:22:45 AM
	010. 2da848768d117387ba754ef8b1096207bfc30d693d70af364d691ec39027cdaf		2023.09.06-0002

From **Scan Results**, Client View users can also open issues and click **Create Ticket** to generate a ticket.



© 2024 RapidFire Tools, Inc. All rights reserved.

RapidFireTools[®]

VulScan Site Roles

From your VulScan site, you can assign users to Roles from **Home** > **Roles**. Roles help secure site access by limiting users to only those site features defined by the Role. First create users for your site from **Home** > **Users**, and then assign these users the appropriate Role for your VulScan site.

Granite Partners			
Granite Org / Granite Partners / Home / Roles			
Roles			
Site Admin	+ Add User	Technician	+ Add User
Granite-Pro@Pro.com		micro-system@micro.com	1
Client View	+ Add User		
granite-partner@granite.com	Û		

For VulScan, the available site roles are Site Admin, Technician, and Client View.

- Site Admin: Has access to all site functionality, including the ability to create site users and assign roles
- **Technician**: Has access to most site functionality, but cannot create site users or assign roles
- Client View: Can only access VulScan dashboard and reports. Client View is used for end-users to view your vulnerability remediation efforts. See <u>"Client View" on</u> page 50.

Users access parts of a VulScan site based on their assigned site **Role**. The table below breaks down which parts of a VulScan site can be accessed by each Role. Refer to the table if you have questions about site access for a given Role.

	Roles			
VulScan Menu and Page UI Access	Site Admin	Technician	Client View	
Home	Access Granted	Access Granted	No Access	
Dashboard	Access Granted	Access Granted	No Access	
Data Collectors	Access Granted	Access Granted	No Access	
Users	Access Granted	No Access	No Access	

	Roles			
VulScan Menu and Page UI Access	Site Admin	Technician	Client View	
Roles	Access Granted	No Access	No Access	
Advanced Options	Access Granted	No Access	No Access	
VulScan	Access Granted	Access Granted	Access Granted	
Dashboard	Access Granted	Access Granted	Access Granted	
Scan Results	Access Granted	Access Granted	Access Granted	
Create Ticket from Issue	Access Granted	Access Granted	Access Granted	
Mark Issue as False Positive	Access Granted	Access Granted	No Access	
Reports	Access Granted	Access Granted	Access Granted	
Weekly Trend Report	Access Granted	Access Granted	Access Granted	
Monthly Trend Report	Access Granted	Access Granted	Access Granted	
Open Ports Report	Access Granted	Access Granted	Access Granted	
Settings	Access Granted	Access Granted	No Access	
Overview	Access Granted	Access Granted	No Access	
General	Access Granted	Access Granted	No Access	
Report Settings	Access Granted	No Access	No Access	
Scan Credentials	Access Granted	Access Granted	No Access	
Custom Scan Profiles	Access Granted	Access Granted	No Access	
Scan and Notification Tasks	Access Granted	Access Granted	No Access	
Exclusion Rules	Access Granted	Access Granted	No Access	
VulScan Proxy Settings	Access Granted	No Access	No Access	
IT Complete	Access Granted	No Access	No Access	
Audit Log	Access Granted	No Access	No Access	

RapidFireTools*

Using VulScan

View Vulnerability Scan Results

Once you have completed a vulnerability scan, you can view detailed results of the scan from **[Your Site] > Vulnerability Scanner > Scan Results**. Above the list of identified issues, you can see a graphical breakdown of identified issues and their severity.

🖒 Home	÷	Scan Results ③				
WulScan	*	Scan Results O				
Dashboard		By Issue By	Device			
Scan Results						
Reports	•	Scan Date Range: Las	t 30 Davs 👻	Critica	📥 Generate Rep	ports
Settings	+			29		
🛱 Audit Log		CVSS Filter: Lov	v (1.0+) 🔹	High 36		
		Scan Type: All		25 Mediu	m	
			T	OTAL 55		
		Quick Filter:		5		
			ISA's Known Exploited Vulnerabilities	None		
				0		
		Severity/C	∕SS [⊕] Issue [⊕]		Affected Nodes $\stackrel{\oplus}{=}$	Last Detected $\stackrel{\oplus}{=}$
		9.8	PHP Multiple Vulnerabilities (Jul 2017 - 01) - Linux		1	24-Sep-2023
			OID: 1.3.6.1.4.1.25623.1.0.811482			04:14:57 PM
			CVE: CVE-2017-7890, CVE-2017-9224, CVE-2017-9225, 2017-9227, CVE-2017-9228, CVE-2017-9229, CVE-2017-			
			11145, CVE-2017-11628, CVE-2017-12933			
		9.8	PHP Multiple Vulnerabilities - 01 - Aug16 (Linux) OID: 1.3.6.1.4.1.25623.1.0.808788		1	24-Sep-202328-0002 04:14:57 PM

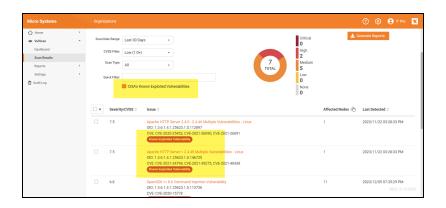
Filter Scan Results

You can filter scan results for detected issues by **Scan Date Range**, **CVSS Filter**, or Scan Type (Internal, External, or Discovery Agent). Alternatively, you can enter a text string in the **Quick Filter** to search for specific phrases or numbers.

Scan Results(3
By Issue	By Device
Scan Date Range:	Last 30 Days 🔹
CVSS Filter:	Low (1.0+) -
Scan Type:	All -
Quick Filter:	CISA's Known Exploited Vulnerabilities

You can also filter by **CISA's Known Exploited Vulnerabilities**. The **Known Exploited Vulnerability** catalog is a library of vulnerabilities that have been actively exploited in the wild. Use this information to help you prioritize remediation efforts on the subset of vulnerabilities that are known to be causing immediate harm.

Note: When an issue is marked as a Known Exploited Vulnerability, this does not mean that the issue has been exploited in the assessment environment you are scanning. Rather, it is an issue for which CISA has "reliable evidence that execution of malicious code was performed by an actor on a system without permission of the system owner". See also <u>https://www.cisa.gov/known-exploited-vulnerabilities-catalog</u>.



RapidFireTools[®]

Review Scan Results

From **[Your Site]** > **Vulnerability Scanner** > **Scan Results**, you can review a list of all vulnerabilities identified during the scan. From the **By Issue** tab, you can organize this list by *Severity/CVSS*, *Issue Description*, *Affected Nodes*, and the *Time/Date* at which the issue was last detected. You can also organize this data by *Device* from the **By Device** tab.

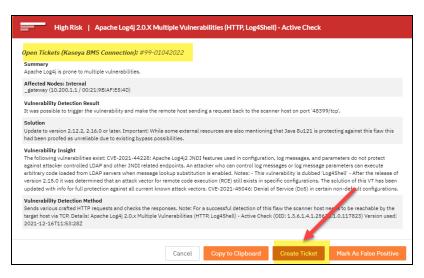
S	can Results	?			
	By Issue	By Device	2		
	Scan Date Range	e: Last 30 Da	Critic 29	al 🛓 Generate Rep	orts
	CVSS Filte	r: Low (1.0+)) · · ·		
	Scan Type	All	125 Medi	um	
	Quick Filte	r	Low		
	quinti inte		nown Exploited Vulnerabilities None		
			0		
	Seve	erity/CVSS $\stackrel{\bigcirc}{=}$	Issue 🔶	Affected Nodes $\stackrel{\diamondsuit}{\Rightarrow}$	Last Detected $\stackrel{\oplus}{=}$
	9.8		PHP Multiple Vulnerabilities (Jul 2017 - 01) - Linux OID: 1.3.6.1.4.1.25623.1.0.811482 CVE: CVE-2017-7800 CVE-2017-9224 CVE-2017-9225 CVE-2017-9226 CVE-	1	24-Sep-2023 04:14:57 PM
			By Device Last 30 Days Last 30 Days Last 30 Days Circical Circical Pipe Law (1.0+) Law (1.0+)		
	9.8		· · · · · · · · · · · · · · · · · · ·	1	
			CVE: CVE-2016-5773, CVE-2016-5772, CVE-2016-5769, CVE-2016-5768, CVE-		04.14.07 PMP0 0001

When viewing the scan results **By Issue**, click on the description for an issue to view additional details.

Scan Date Range:		Critical L Generate Rep 29	ports
CVSS Filter:		High 36	
Scan Type:	A	Medium 55	
Quick Filter:		Low 5	
	CISA's Known Exploited Vulnerabilities	None D	
Severi	ty/CVSS [⊕] Issue [⊕]	Affected Nodes 🗢	Last Detected $\stackrel{\diamondsuit}{\Rightarrow}$
9.8	PHP Multiple Vulnerabilities (Jul 2017 - 01) - Linux OID: 13.61.41.25623.10.811482 CVE: CVE 2017-7890, CVE-2017-9224, CVE-2017-9225, CVE-2017-9226, CVE 2017-9227, CVE-2017-9228, CVE-2017-9229, CVE-2017-11144, CVE-2017- 11145, CVE-2017-11628, CVE-2017-12933	1	24-Sep-2023 04:14:57 PM
9.8	PHP Multiple Vulnerabilities - 01 - Aug16 (Linux) OID: 1.3.6.1.4.1.25623.1.0.808788 CVE: CVE-2016-5773, CVE-2016-5772, CVE-2016-5769, CVE-2016-5768, CVE 2016-5766, CVE-2016-5767	1	24-Sep-2023 04:14:57 PM
9.8	PHP Multiple DoS Vulnerabilities (Oct 2016) - Linux OID: 1.3.6.1.4.1.25623.1.0.809338	1	24-Sep-2023 ₂₈₋₀ 04:14:57 PM

From the Issue Details, you can perform several actions:

- Copy to Clipboard to paste the issue details somewhere else in plain text form.
- Mark as False Positive to dismiss the issue.
- Create Ticket to export the issue as a ticket in Kaseya BMS. See also <u>"Set Up and</u> Assign a Ticketing/PSA System Integration to a Site" on page 167.



When viewing the results **By Device**, click on an affected device to see a breakdown of vulnerabilities on the device.

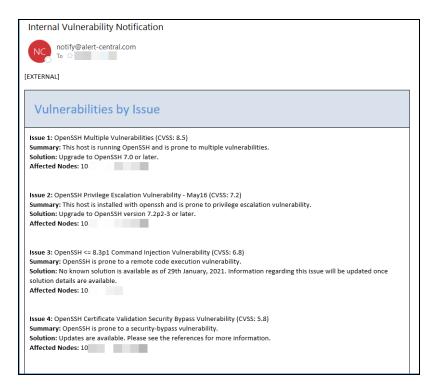
Scan Results (3			
By Issue	By Device			
Scan Date Range:	Last 30 Days	•	Critical Generate Rep 29	orts
CVSS Filter:	Low (1.0+)	•	High 37	
Scan Type:	All	• (151 Medium TOTAL 59	
Quick Filter:			Low 26	
	CISA's Known Exploited	d Vulnerabilities	None 0	
			0	
IP Add	Iress [‡] Hostname [‡]	MAC Address $\ensuremath{\hat{\diamond}}$ Severity/CVSS $\ensuremath{\hat{\diamond}}$	Issue 🗢	Last Detected $\stackrel{\diamondsuit}{\Rightarrow}$
10.80.	0.6	7.5	SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	24-Sep-2023 04:14:57 PM
			OID: 1.3.6.1.4.1.25623.1.0.108031 CVE: CVE-2016-2183, CVE-2016-6329, CVE- 2020-12872	
10.80.	0.6	5	TCP Sequence Number Approximation Reset Denial of Service Vulnerability OID: 1.3.6.1.4.1.25623.1.0.902815	24-Sep-2023 04:14:57 PM-0002

RapidFireTools[®]

80.0.6 (F	Return to all devices]		
	Critical 0 High 1	0.NA	
	3 TOTAL Low 0 None 0	443/rcp (https)	2
] 🕶	Severity/CVSS $\hat{\forall}$	isse [÷]	Last Detected $\stackrel{\oplus}{\Rightarrow}$
	7.5	SSL/TLS: Report Vulnerable Cipher Suites for HTTPS OID: 1.3.6.1.4.1.25623.1.0.108031 CVE: CVE-2016-2183, CVE-2016-6329, CVE-2020-12872	24-Sep-2023 04:14:57 PM
	5	TCP Sequence Number Approximation Reset Denial of Service Vulnerability OID: 1.3.6.1.4.1.25623.1.0.902815 CVE: CVE-2004-0230	24-Sep-2023 04:14:57 PM
	4.3	SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection OID: 1.3.6.1.4.1.25623.1.0.117274 CVE: CVE-2011-3399, CVE-2015-0204	24-Sep-2023 04:14:57 PM

Scan Result Notification Emails

After your scan and notification tasks occur, recipients will receive an email list of vulnerabilities by issue as pictured below. See also <u>"Create Notification Tasks" on page 30</u>.



Available Issue Meta Data

When VulScan detects vulnerabilities on the target network, it presents you with a wealth of information to help you categorize, understand, and resolve these issues. Here's a breakdown of the currently available meta data for each issue.

Note: We are constantly improving VulScan, and we may make additional data available for issues in future releases.

Meta Data	Description
Summary	Plan language summary of detected vulnerability
Related CVE	Identifier for the Common Vulnerabilities and Exposures (CVE) catalog
Affected Nodes	Notes whether the issue is internal or external-facing as well as the IP and/or hostname
Vulnerability Detection Result	Specific technical details regarding affected software versions, port numbers, etc.
Solution	Plan language suggestion for mitigating issue
Vulnerability Insight	Extended technical description of issue and related vulnerabilities
Vulnerability Detection Method	Technical description of how VulScan identified issue
References	Links to third-party software vendors or other parties relevant to detected issue
OID	Object identifier for the Greenbone Open Source Vulnerability Management API

How Vulnerability Totals are Presented

The table below provides additional details as to how vulnerability totals are presented on the **Dashboard** and **Scan Results** page. Refer to the table if you have questions regarding the data present in various UI elements, such as the "donut" chart and bar chart.

Scan Data Location and Format	Data Parameters
Vulnerability Scanner > Dashboard: Donut Chart	 Details vulnerabilities by severity identified in the last 30 days
VulScan	Refers to the total number of vulnerabilities identified across all devices
Vulnerrelatilities by Device Verw All Last 30 Days Otheral 1 1 1 1 6	Includes all vulnerability levels (CVSS 1.0+)
1074. Medam S Low 1	Omits issues marked as false positives (see False Positive Management)
Vulnerability Scanner > Dashboard: Bar Chart	Each bar represents a "running total" of all vulnerabilities identified on all devices in the last 30 days
Vulnerabilities Over Time View All Last 30 Days	 Total vulnerabilities "roll over" each day even for no-scan days
	•Unresolved issues roll over even when they are detected on devices that couldn't be reached in the latest scan
ాల్ చ్ ద్ గర్ గర్ గర్ 30-day Moving Window	Omits issues marked as false positives
Vulnerability Scanner > Scan Results: Donut Chart (By Issue)	Represents number of unique vulnerability types detected at site
	Review the table for breakdown of each issue and affected devices
	●Use filter to redefine chart and table data

Scan Data Location and Format	Data Parameters
Scan Results By Device By Issue By Device Scan Date Range: Last 30 Deys CvSs Filter: CvSs Filter: Quick Filter: ClSA's Known Exploited Vulnerabilities None 0	●Omits issues marked as false positives
Vulnerability Scanner > Scan Results: Donut Chart (By Device)	•Refers to the total number of vulnerabilities identified across all devices (will match the Dashboard donut chart with default filter settings)
Scan Results By Issue By Issue By Device	●Use filter to redefine chart and table data
Scan bate Ranget: Last 30 Days Cvtss Fitter: Low (1.8+) Scan Type: All Oulck Fitter: CISA's Known Exploited Vulnerabilities CisA's Known Exploited Vulnerabili	●Omits issues marked as false positives

RapidFireTools*

Mark Issues as False Positives, Accepted, or Mitigated (Sitelevel)

You can mark detected vulnerabilities as False Positives, Accepted, or Mitigated. This allows you to remove "noise" from your scans and to track only those issues that are relevant to you. To use this feature:

- 1. Navigate to VulScan > Scan Results.
- 2. Select the individual issues or devices that you wish to mark as false positives.
- 3. From the Select All box, click on the drop-down menu and select Mark As....



4. Enter details for the issues and click Confirm.

Mark as False Positive		
Mark the selected issues as False Positive		
\bigcirc False Positive \bigcirc Accepted \bigcirc Mitigated		
Exclusion Note		
Selected Issue and Devices PHP Multiple Vulnerabilities (Jul 2017 - 01) - Linux • 10.80.0.249		
PHP Multiple Vulnerabilities - 01 - Aug16 (Linux) • 10.80.0.249		
PHP Multiple DoS Vulnerabilities (Oct 2016) - Linux10.80.0.249		
3 selected	Cancel	Confirm

5. These items will then be removed from the list of scan results.

You can then manage these items for the site from **Your Site** > **VulScan** > **Settings** >**Exclusion Rules**. See also <u>"False Positive Management (Site Level)" on the next page</u>.

False Positive Management (Site Level)

Exclusion rules allow you to define specific issues to exclude from risk reporting – filters include OID, date range, site name, and so on.

Add Exclusion Rule at the Site Level

To create an exclusion rule that will apply to a specific VulScan site:

1. Navigate to [Your Site] > VulScan > Settings > Exclusion Rules.

VulScan	*	VulScan / Settings / Exclu	sion Rules							
Dashboard		Exclusion Rules								
Scan Results										
	-	Show one-time excl	usions	Qui	ick Filter:					+ Add Rule
Overview										1 Platitude
General		False Positive (81)	Acce	pted (3) Mitigated (3)						
Report Preferences										
Scan Credentials									1 /4 →	>i view 25 *
Custom Scan Profile Scan and Notification Task		Site Name o	Appliance ID 0	010 ¢	Condition 0	IP Address ©	Hostname ©	MAC Address ©	Date o	Exclusion Note o
Exclusion Rules		Any	Any	1.3.6.1.4.1.25623.1.0.117839	All	45.33.32.153	Al	All	Апу	GLOBAL RULE for 45.33.32.153
Audit Log		Any	Any	1.3.6.1.4.1.25623.1.0.117149	All	96.67.119.198	All	All	Any	General
		Any	Any	1.3.6.1.4.1.25623.1.0.117840	All	All	All	00:15:5D:01:07:1B	Any	MAC
		Any	Any	1.3.6.1.4.1.25623.1.0.117840	Апу	10.200.1.17	Al	All	Апу	MAC
		Any	Any	1.3.6.1.4.1.25623.1.0.117840	Any	10.200.1.51	desktop- 1595191.test.performanceit.com	00:15:50:01:07:31	Апу	MAC
		Any	Any	1.3.6.1.4.1.25623.1.0.103440	All	All	Al	All	2022/06/10 2022/06/30	
		JRinspector2Test	Any	1.3.6.1.4.1.25623.1.0.809154	All	All	AI	All	Апу	2022.06.21-1532

2. Click Add Rule.

VulScan / Settings / Exclusion Rules								
Exclusion Rules	Exclusion Rules							
Show one-time exclusions Quick Filter:								+ Add Rule
False Positive (81) Acce	epted (3) Mitigated (3)						
							/4 →	⇒ı view 25 *
Site Name 🌩	Appliance ID ¢	OID ©	Condition ¢	IP Address ©	Hostname ©	MAC Address ©	Date o	Exclusion Note ¢
Any	Any	1.3.6.1.4.1.25623.1.0.117839	All	45.33.32.153	All	All	Any	GLOBAL RULE for 45.33.32.153
Any	Any	1.3.6.1.4.1.25623.1.0.117149	All	96.67.119.198	All	All	Any	General
Any	Any	1.3.6.1.4.1.25623.1.0.117840	All	All	All	00:15:5D:01:07:1B	Any	MAC
Any	Any	1.3.6.1.4.1.25623.1.0.117840	Any	10.200.1.17	All	All	Any	MAC
Any	Any	1.3.6.1.4.1.25623.1.0.117840	Any	10.200.1.51	desktop- i595f9f.test.performanceit.com	00:15:50:01:07:31	Any	MAC
Any	Any	1.3.6.1.4.1.25623.1.0.103440	All	All	All	All	2022/06/10 - 2022/06/30	

3. The Add Exclusion Rule window will appear.

Add Exclusion Rule	
False Positive	Appliance ID:
Any	Any
OID: *	IP:
Hostname:	MAC Address:
Exclusion Note:	
Condition:	
All selected attributes must match $~~$	
Start Date: End Date:	
▼ To:	•
Leave Date fields empty if Rule applies to all scan dates	
	Cancel ✓ Add

- 4. Next, configure the false positive rule. You have several options, including:
 - Exclusion Type: Choose from False Positive, Accepted, or Mitigated.

Note: VulScan will treat exclusions the same regardless of exclusion type. Use the exclusion type categories to help you keep track of why and how issues are excluded.

- OID: You must enter the OID (Object Identifier) for a particular vulnerability. This is a required field. Enter the OID to exclude the specified issue from scan results. Once you have performed a scan, you can locate the OID for detected issues from [Your Site] > VulScan > Scan Results. The OID for each issue appears below the issue description.
- **IP, Hostname, and MAC Address**: Enter an IP, Hostname, and/or MAC Address address to exclude from the scan results for all sites.
- Add an Exclusion Note
- Set the matching Condition from the drop-down menu. You can select:
 - All selected attributes must match: If ALL of the selected attributes for two devices match, VulScan will treat them as the same device when it generates an issue.

- Any selected attributes must match: If ANY of the selected attributes for two devices match, VulScan will treat them as the same device when it generates an issue.
- See also <u>"Configure Device Matching Criteria to Reduce False</u> Positives" on page 39.
- Start Date and End Date: Enter a beginning and/or end date at which to exclude the OID or IP.
- 5. When you are finished, click **Add**. The rule will appear in the list of exclusions.

When you apply an exclusion rule at the site level, the specified issues will be filtered at this site ONLY.

Edit/Delete Exclusion Rule

- To edit an exclusion rule, click the pencil icon next to a rule. Make and save your changes.
- To delete an exclusion rule, click the trash icon next to a rule. When you delete a rule at the site level, the excluded scan results will return and appear for this specific site under Scan Results.

Create Ticket from Issue

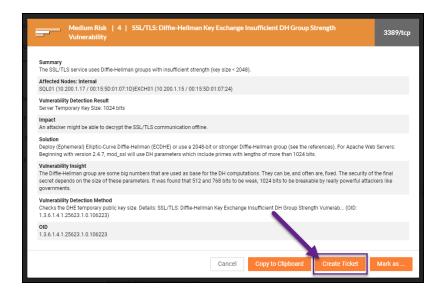
VulScan offers you flexibility in how you choose to handle identified issues. For example, you can <u>"Create Notification Tasks" on page 30</u> that automatically export detected issues as tickets to a PSA system.

However, you also have the option to create tickets from issues on a per-issue basis. This offers you more control over which issues to export to your PSA. Here's how it works:

- 1. First, be sure you have created a connection to your PSA and mapped that connection to your VulScan site. See <u>"Set Up and Assign a Ticketing/PSA System</u> Integration to a Site" on page 167.
- 2. Next, from your VulScan site access VulScan > Scan Results from the left menu.
 - Scan Results ③ By Device By Issue Critical 29 Scan Date Range: Last 30 Davs CVSS Filter: Low (1.0+) High 36 Scan Type: All 125 Medium 55 Low 5 Quick Filter: None 0 CISA's Known Exploited Vulnerabilities Severity/CVSS ⁺ Issue Affected Nodes Last Detected 9.8 24-Sep-2023 OID: 1.3.6.1.4.1.25623.1.0.811482 04:14:57 PM CVE: CVE-2017-7890, CVE-2017-9224, CVE-2017-9225, CVE-2017-9226, CVE-2017-9227, CVE-2017-9228, CVE-2017-9229, CVE-2017-11144, CVE-2017-11145, CVE-2017-11628, CVE-2017-12933 9.8 PHP Multiple Vulnerabilities - 01 - Aug16 (Linux) 24-Sep-2023 OID: 1.3.6.1.4.1.25623.1.0.808788 04:14:57 PM
- 3. Then click the issue you want to convert to a PSA ticket.

4. From the issue details, click Create Ticket.

RapidFireTools°



- 5. From the Create Ticket window, configure the ticket. Specifically:
 - Exclude nodes with open tickets: Enable this to prevent duplicate tickets
 - Create separate tickets per affected node: You can optionally choose to create separate tickets for affected devices or create one ticket detailing each affected device
 - Ticket Summary: Enter a description or title for the ticket

Create Ticket		
Connection: Kaseya BMS		
Affected Node	Open Ticket#	Ticket Date
DESKTOP-1QSHT11 (10.159.5.143 / 00:15:5D:01:07:66)		
Options C Exclude nodes with open tickets		
Create separate tickets per affected node		
Ticket Summary		
Vulnerability Detected by VulScan		
	Cancel	Create Ticket

6. Then click **Create Ticket**. A success notification will appear with the ticket ID.

 Ticket Created
 Ticket Created (Kaseya BMS) #38-01132022

If the ticket action would create only duplicates, no tickets will be created.

In the second second

RapidFireTools^{*}

Generate VulScan Issues and Detail Reports

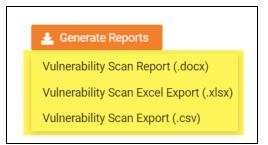
Once you perform one or more vulnerability scans, you can **generate reports** that detail site vulnerabilities. You can mail or print the report to provide as evidence of scanning or for compliance purposes. Here how it works:

- 1. From your VulScan Site, navigate to VulScan > Scan Results.
- 2. Then click **Generate Reports** from the right page.

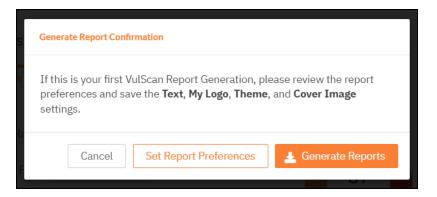
Note: You must first have performed one or more successful internal or external vulnerability scans to generate reports.

🖒 Home	Scan Results ③	
VulScan		
Dashboard	By Issue By Device	
Scan Results		Generate Reports
Reports •	Scan Date Range: Last 30 Days 👻	Critical Generate Reports
Settings	CVSS Filter: Low (1.0+)	High 1
	Scan Type: All - 15 TOTAL	Medium 9
	Quick Filter:	Low O
	CISA's Known Exploited Vulnerabilities	None O

3. From the drop-down menu, select the report type: .docx, .xlsx, or .csv.



4. Configure your **Report Settings** if you haven't done so already. Otherwise, click **Generate Reports**.



 If you generate the report with the By Issues tab open, the Vulnerability Scan Issues Report will appear as a download in your browser. This format is useful for technicians that are looking to resolve specific issues identified within the environment, rather than performing remediation on a particular system.

Vulnerability Scanner 2021					
A Home >	VulScan / Scan Results				
VulScan					
Dashboard	Scan Results				
Scan Results	By Issue By Device				
Settings 🕨					
🔒 Audit Log	Scan Date Range: Last 30 Days 🗸				
Vulnerability Scan Issues Generating report.	Report :: Low (1.0+) ~ :: All ~				
 Vulnerability Scan Issues Report Report ready for download. 					
Vulnerability_Scadocx					

If you generate the report with the By Device tab open, the Vulnerability
 Scan Detail Report will appear as a download in your browser. This format is useful when you want to identify specific devices for which to remediate

security issues.

	Scan Date Range:	Last 30 Days 🗸
	CVSS Filter:	Low (1.0+) V
<	Scan Type:	All ~
	Quick Filter:	
Uulnerability Scan Detail Ro Generating report.	eport	Hostname 🗢
	□ 10.200.1	.12 DC01
 Vulnerability Scan Detail Report ready for download. 		.12 DC01
Vulnerability_Scadocx ^		

Generate VulScan Trending Reports

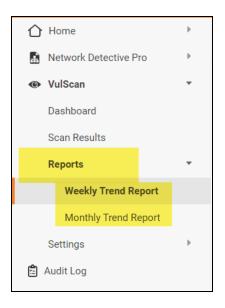
With VulScan **Trending Reports**, you can visualize vulnerability management on a weekly and monthly basis. These dynamic graphs display the results of your scans in a dashboard using filters that you configure. You can likewise download your custom graphics as Excel files.

Use this information to present to your stakeholders to show the value of the service and demonstrate the actions taken to resolve vulnerabilities.

To generate Trending Reports:

Step 1 — Navigate to VulScan Trending Reports

From your VulScan site, navigate to **VulScan > Reports**. Here you can choose from the **Weekly** or **Monthly Trend Report**.



The detected week over week or month or month vulnerabilities will appear in the data graph.

RapidFireTools[®]

 ₽	/eekly Vulnerability Trend Report	述 Download
@	CVSS: Report Range: Scan Type: Critical I High I Medium I Low Last 4 Weeks • All •	
	Week over Week Report Vulnerabilities	
	Critical High Medium Low	
	120 0	
	100	
	080	
	60 ;	
	40 \$	
	20	
	0 13-Feb 27-Feb	2023: <mark>0</mark> 3.13-1224 6-Mar

- **Total Vulnerabilities**: The total sum of all non-duplicated vulnerabilities for all scans during the time period. One vulnerability counts as a single Issue/Device combination.
- **Newly Discovered**: Vulnerabilities detected in the current week that were not detected in the previous week.
- Resolved: Vulnerabilities detected in the previous week that were not detected in the current week.

Note: This data may not accurately represent the total vulnerabilities if your scan schedule is irregular or if scanning is disrupted for any reason.

Step 2 — Filter Vulnerability Data

Once you select either the Weekly or Monthly Trend Report, you can configure the data that will appear in the vulnerability graph. The graph will update the vulnerability totals with your configuration.

- **CVSS**: Choose to filter the issue by Critical, High, Medium, and Low vulnerability severity levels.
- Report Range: Choose the number of weeks or months for the report time period.
- Scan Type: Filter the scan results by Internal or External scans, or by Discovery Agent scans.

VulScan / Reports / Weekly Trend Report						
Weekly Vulnerability Trend Report						
CVSS:	Report Range:	Scan Type:				
🗹 Critical 🗹 High 🗹 Medium 🗹 L	ow Last 4 Weeks 🗸	All	•			

Step 3 — Generate Dynamic Graphs

Once you configure your trend report, you can download the graph in a spreadsheet. To do this:

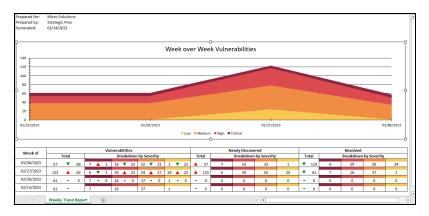
1. From the right page, click **Download**. The spreadsheet will appear as a download in your browser.



2. If you haven't done so already, first **Set Report Settings**. Then return and download reports.

Û	Weekly Vulnerability Tren	Denert	占 Download
6 0		Generate Report Confirmation	
Ê	cvss: 🚺 High 🚺 Medium	If this is your first VulScan Report Generation, please review the report pr and save the Text , My Logo , Theme , and Cover Image settings.	eferences
		Cancel Set Report Preferences 스 Gener	ate Report
		Critical High Medium Lo	
			6
	60	0	
	13-Feb	20-Feb :	222505.101224

3. The graph in the spreadsheet download will replicate your data configuration.



RapidFireTools°

When are Trend Reports updated?

The **Monthly Trend Report** is updated each second day of the month at 2:00 AM Eastern time.

The VulScan **Weekly Trend Report** is updated each Tuesday at 2:00 AM Eastern Time. At this time, you can view the scan results for the previous week.

For example, for the period of 1-Jan to 7-Jan, the results are calculated and become available to view on Tuesday, 9-Jan. The results then appear in the graph and end at the date 8-Jan (Monday at 12:00 AM).

The table below provides an example that you may find helpful for understanding the 7 day period and when results are updated.

1-Jan	Monday	Day 1
2-Jan	Tuesday	Day 2
3-Jan	Wednesday	Day 3
4-Jan	Thursday	Day 4
5-Jan	Friday	Day 5
6-Jan	Saturday	Day 6
7-Jan	Sunday	Day 7
8-Jan	Monday	
9-Jan	Tuesday	(results updated for period of 1-Jan to 7- Jan at 2:00 AM, ending at 8-Jan Monday in graph)

Open Ports Report

The **Open Ports Report** helps you visualize what ports are open within the network. Some open ports are necessary for apps and services. Others may require investigation and need to be closed. The Open Ports Report can be downloaded and shared with the interested parties for further analysis and development of an action plan.

Here's how to use the VulScan Open Ports Report:

Step 1 — Navigate to VulScan Open Ports Reports

From your VulScan site, navigate to **VulScan > Reports > Open Ports Report**. Note that you must have completed 1 or more internal and/or external vulnerability scans to view detected open ports.

	Home	Þ
0	VulScan	*
	Dashboard	
	Scan Results	
	Reports	*
	Weekly Trend Report	
	Monthly Trend Report	
	Open Ports Report	
	Settings	Þ
* :	Audit Log	

Step 2 — Filter Open Ports Vulnerability Data

Once you access the Open Reports Report, you can filter the dashboard to further analyze the results. The Open Ports graphs will update based on your input.

- **Report Range**: Choose a date range for the Open Ports Report
- Scan Type: Filter results by External or Internal scans
- Port: Select from among the detected ports to filter results by port
- Quick Filter: Enter a custom string to filter open ports results

pen Ports Report ③	0									Ł	5 Download
port Range	Scan Type		Port				Quick Filter				
08/06/2023 - 09/06/2023 🛱	All	~	All			~					
					т	op 10 Oper	n Ports				
	5/tcp (loc-srv) 2.1 %	8									
	2.1 /o 9/tcp (netbios-	7									
55		. 6	-								
	2.1 %	aojus 5		_	-	-	-				
	5/tcp iicrosoft-ds)	÷ 4	_								
	2.1 %	Number of Devices	_								
35	89/tcp	2	-	-							
	2.1 %	1									-
	her 1.5 %	0									
5	1.5 %	135/tcp	139/tcp	445/tcp	3389/tcp	5985/tcp	5986/tcp	137/udp	22/tcp	80/tcp	47001/tc
						P					
Port 🗘	IP Addres	\$\$		Hostname			MAC	Address 🗘		Last Detected	÷
80/tcp (http)	199.38.22	2.181								05-Sep-2023,	6:14 AM
443/tcp (https)	199.38.22	2.181								05-Sep-2023,	
1723/tcp	199.38.22									20 05-Sep-2023,)23.09.06-0

For each open port, you can see the Port name, IP Address, Hostname, MAC Address, and Last Detected date.

Port 🔶	IP Address ≑	Hostname \$	MAC Address ≑	Last Detected 🗢
47001/tcp	172.31.56.8	EC2AMAZ-3GV50EI	0E:D1:2A:DD:83:8D	24-Aug-2023, 1:16 PM
47001/tcp	172.31.56.10	EC2AMAZ-82FVJTH	0E:96:C1:7C:8C:CB	24-Aug-2023, 1:16 PM
31337/tcp	45.33.32.156	scanme.nmap.org		30-Aug-2023, 9:36 AM

Step 3 — Download Open Ports Report and Invite Client Users

Finally, you have two options to share the Open Ports Report with other users, including clients.

1. **Download** the Open Ports Report as an Excel file.



2. Use the <u>"Client View" on page 50</u> to invite client users to view the Open Ports Report directly from the site.

VulScan Vulnerability Reports

Below are the reports and notifications available to VulScan users.

Report Name	Description
Vulnerability Scan Issues Report	This report presents issues by their severity to enable technicians to prioritize the issues they are working on. Each issue includes technical insights, a proposed solution, affected devices, as well as several graphical breakdowns of the numerical disposition of issues on the target network. This email notification details external vulnerabilities by issue. This format is useful for technicians that are looking to resolve specific issues identified within the environment, rather than performing remediation on a particular system. Download as .docx, .xlsx, or .csv.
Vulnerability Scan Detail Report	This report details the results of a comprehensive scan, including security holes and warnings, informational items that can help make better network security decisions, plus technical information that can help you make better network security decisions. This is an essential item for many standard security compliance reports. Download as .docx, .xlsx, or .csv.
Vulnerability Notification Emails	VulScan can be easily configured to send an email notification when the scan completes. Create a notification task to automate alerts of the scan results to any recipient. These alerts can be configured to be distributed daily, monthly, weekly, etc. The notifications include both internal and external threats, and can be organized by Issue or Device.
Weekly and Monthly Trend Reports	With VulScan Trending Reports , you can visualize vulnerability management on a weekly and monthly basis. These dynamic graphs display the results of your scans in a dashboard using filters that you configure. You can likewise download your custom graphics as Excel files

Export Notification Tasks to RocketCyber

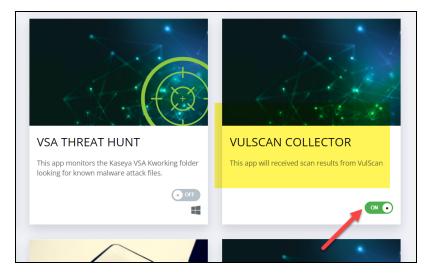
This topic covers how to export VulScan notification tasks to **RocketCyber** (<u>https://www.rocketcyber.com</u>). This integration allows you to view VulScan security issues from within your RocketCyber dashboard. In addition to your VulScan subscription, you will need a RocketCyber subscription to use this integration.

Here's how to set up the integration:

Step 1 — Enable VulScan from the RocketCyber App Store

First, you need to **enable VulScan** from the RocketCyber **App Store**.

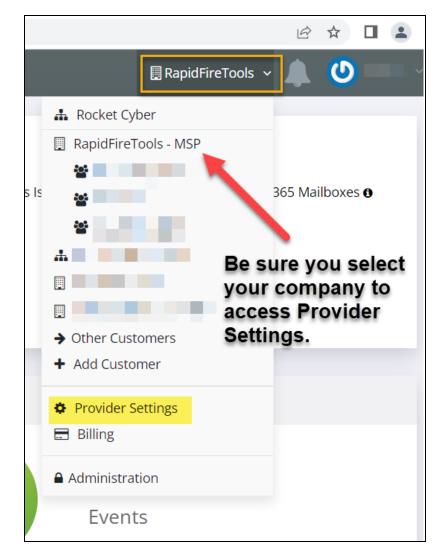
- 1. From your RocketCyber account, open the App Store.
- 2. Apps within the App Store are arranged in alphabetical order, so scroll down to "V" for VulScan.



3. Click the slider to enable the VulScan Collector.

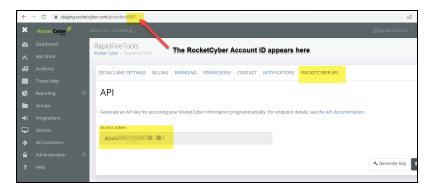
Step 2 — Gather API Credentials from RocketCyber Account

Next, we need to gather two pieces of data from your RocketCyber account to enable the integration.



1. From the top menu, select your company, and then open **Provider Settings**.

2. Click the RocketCyber API tab.



3. Copy the API access token.

RapidFireTools*

4. Then, copy the **number at the end of your browser URL** for this page. This is your account number.

Step 3 — Enable the RocketCyber integration in VulScan

Next, return to the RapidFire Tools portal and open your VulScan site.

- 1. Navigate to VulScan > Settings > IT Complete.
- 2. Click the sider to activate the RocketCyber integration.

Dashboard	IT Complete	
Scan Results		
Settings * Overvlew	Rocket Cyber Integration - Export Reports To Rocket Cyber - Beta	
General	Enable Rocket Cyber Integration	
Report Preferences	User Location *	
Scan Credentials Custom Scan Profile	USA	~
Scan and Notification Tasks	Rocket Cyber Account Id *	
Exclusion Rules	3(
IT Complete	Rocket Cyber API Key: *	
🔒 Audit Log	Ht	Check Connection
	Rocket Cyber Customer	
	R	~
		Save

- 3. Select your **User Location** for the site: USA or Europe.
- 4. Enter the **Account ID** and **API key** that you collected in <u>"Step 2 Gather API</u> Credentials from RocketCyber Account" on page 80.
- 5. Click **Verify** to test the connection. A modal will appear to inform you of a successful connection.
- 6. Next, **select the RocketCyber customer** from the drop-down menu. This should be the customer for which you want to export VulScan issues to RocketCyber.
- 7. When you are finished, click **Save**.

Step 4 — Create Notification Task for RocketCyber Export

Now we need to create a new notification task to export VulScan issues to RocketCyber.

Note: You must have first set up scan tasks to detect vulnerabilities to export. See <u>"Create Internal Scan Task" on page 20</u> and/or <u>"Create External Scan Task" on page 27</u>. 1. From your site, navigate to **Settings > Scan and Notification Tasks**.

My RapidFire Tools!								ව 🕸 9	IT Pro
♠ Home InDoc	F.	JR							
VulScan	•	VulScan / Settings	Scan And Notification	asks					
Dashboard Scan Results		Scan Tasks	Notification	Tasks					
Settings	*	Quick Filter						+ Create Notifi	cation Task
General		Task ID 💠	Task Label 💠	Description ¢	Status 💠	Next Run 💠	Repeats 💠		
Report Preferences		9	Daily Quick Report	Send Notification every Day via email.	Enabled	16-Jun-2022 05:54:00 PM	Daily	Run Now	Z #
Scan Credentials Scan and Notificatio Exclusion Rules	on Tasks	11	VulScan Daily Reports - By Issue - Summary	Send Notification every Day via email.	Enabled	16-Jun-2022 12:00:00 PM	Daily	Run Now	/ =
IT Complete		12	VulScan Daily Reports - By Issue - Detail	Send Notification every Day via email.	Enabled	16-Jun-2022 12:10:00 PM	Daily	Run Now	Z #
		13	VulScan Daily Reports - By Device- Summary	Send Notification every Day via email.	Enabled	16-Jun-2022 01:50:00 PM	Daily	Run Now	× 1
		28	123	Send Notification every Month to PSA	Enabled	28-Jun-2022	Monthly	Run Now 202	2 04 14 00

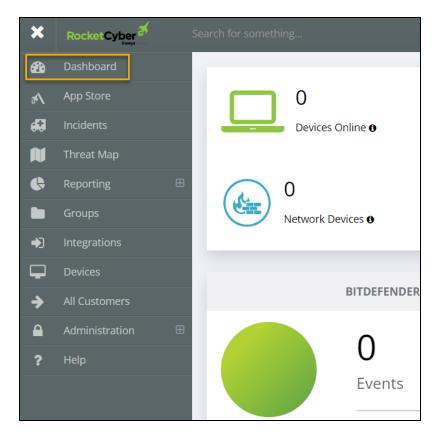
- 2. Open the **Notifications** tab and click **Create**.
- 3. From the **Notification Task Type** screen, select **Send to RocketCyber**. Then configure and save the notification task as you normally would. See also <u>"Create</u> <u>Notification Tasks" on page 30</u>.

eate Notification Task			
otification Task Type			
Email / Create Ticket			
Email Address			
Notification Subject			
Subject			
Create			
Send to Rocket Cyber			
			Next

Step 5 — Browse VulScan Issues from RocketCyber Dashboard

Once VulScan performs the notification task and exports VulScan issues to RocketCyber, you can view them in the RocketCyber Dashboard.

- 1. Open RocketCyber and select your company and customer.
- 2. Open the **Dashboard** from the left menu.



3. Scroll down to VulScan Collector and click View.

ber.com		🖻 🛧 🗖 🚨 🗄
	0	U
	Events	Events
	Review	Review
	Configure	© Configure
	PWND MONITOR	VULSCAN COLLECTOR
	0	0
	Events	Events
	Review	Review
	Kerten	
	Configure	& Configure
	o Configure	SP Configure

4. Here you can find a list containing the VulScan issues. Click **Details** to see additional information for each issue, as in the VulScan Scan Results page. You can also export these issues into other data formats.

6 20										
			SCAN COLI	ECTOR E	VENTS					
ø			FireTools							
N			o will received sca							
6	Sea	rch		Detection	Date	thru	Filter Clear	4	CSV	JSON
	•		Detected	Customer	Hostname II	Port	Issue	CVSS	Severity	
- -	0	4	06/09/22 4:26:29PM			12 3389/tcp	SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability	4	Medium	Details
	0	•	06/09/22 4:26:29PM			3389/tcp	SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	4.3	Medium	Details
	•	A	06/09/22 4:26:29PM			53/udp (domain)	DNS Cache Snooping Vulnerability (UDP) - Active Check	5	Medium	Details
	0	A	06/09/22 4:26:29PM			3389/tcp	Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSL/TLS, D(HE)ater)	5	Medium	Details
	0	4	06/09/22 3:08:20PM			443/tcp (https)	Test case on 6/03	10		Details

RapidFireTools*

Set Up Remote Internal Vulnerability Scanner

Note: Check out the <u>web version of this topic here</u>. The web version allows you to copy the commands and server configuration files to your clipboard.

Introduction

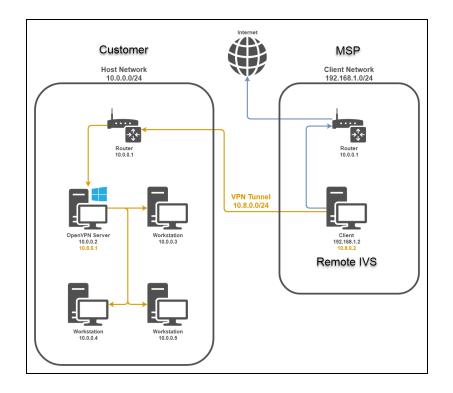
Not all customers (particularly small companies) have enough resources to maintain a separate device to perform internal vulnerability scans. The **Remote Internal Vulnerability Scanner** (Remote IVS) allows MSPs to offer a vulnerability scanning service to customers that do not have the available infrastructure to deploy a VulScan appliance within the target network.

This guide covers how to deploy the Remote Internal Vulnerability Scanner. This involves setting up an OpenVPN server on Windows. This allows the MSP network to access the customer network remotely to perform an internal vulnerability scan. The steps are:

- <u>"Step 1 Provision and Install Remote Internal Vulnerability Scanner" on the facing page</u>
- <u>"Step 2 Setting up the OpenVPN on the server" on page 88</u>
- "Step 3 Create Open VPN Configuration File" on page 101
- <u>"Step 4 Upload Open VPN Configuration File to VulScan" on page 104</u>
- "Step 5 Perform Remote Internal Vulnerability Scan" on page 106

Below is a diagram that details the traffic routes that we want to enable. Our aim is to:

- Allow the client (MSP) to communicate to all the workstations on the host network (customer).
- Keep all outbound internet traffic flowing through the client local network.



Step 1 — Provision and Install Remote Internal Vulnerability Scanner

First, install the Remote Internal Vulnerability Scanner appliance on the MSP network. To do this:

 Provision a new Remote IVS from your VulScan site from [Your VulScan Site] > Home > Data Collectors. Click Provision Vulnerability Scanner and select New Remote Internal Vulnerability Scanner. Click Yes.

See also <u>"Provision VulScan" on page 200</u>.

Provision New Vulnerability Scanner	
Select type of vulnerability scanner to install.	
Internal Vulnerability Scanner	
O New Internal Vulnerability Scanner	
New Remote Internal Vulnerability Scanner	
Existing Remote Internal Vulnerability Scanner	
	~
External Vulnerability Scanner	
O New External Vulnerability Scanner	
\bigcirc Existing External Vulnerability Scanner	
EVS-FFLW76	~
Portable Vulnerability Scanner	
	No Yes

2. Visit <u>https://www.rapidfiretools.com/vs-downloads</u> and download and run the **Virtual Appliance Installer for VulScan** on the MSP network.

See also VulScan Virtual Appliance Installation Guide.

Step 2 — Setting up the OpenVPN on the server

This section walks through the steps required to install and configure the OpenVPN client on the "server" machine. This device should be located on the customer network that you wish to scan.

Configure Router Port Forwarding

In order for the client machine to reach the server, you must forward port 1194 on your router to your OpenVPN server machine. Only UDP traffic must be passed. Consult <u>this</u> <u>website</u> to find detailed forwarding instructions for your specific router make and model.

Installing the OpenVPN program on the server

From the server device, download the latest stable OpenVPN release from the <u>official</u> <u>webpage</u>. For Windows you'll want to select the **Windows 64-bit MSI installer**.

Run the installer and select the **Customize** option.

🔀 Setup OpenVPN 2.5.8-1604		×
Choose setup type.		?
	Install Now Customize	

From **Custom Installation** screen, select the "OpenVPN Service" and "OpenSSL Utilities" packages.

體 Setup OpenVPN 2.5.8-1604	×
Custom Installation	$\mathbf{?}$
Click on the icons in the tree below to change the features to be installed:	
OpenVPN OpenVPN GUI Journal on User Logon OpenVPN Service	^
Will be installed on local hard drive Entire feature will be installed on local hard drive	J
Service wrappers	
This feature requires 29KB on your hard drive.	
Folder: C:\Program Files\OpenVPN\ Brow	se
Reset Disk Usage Install Nor	w

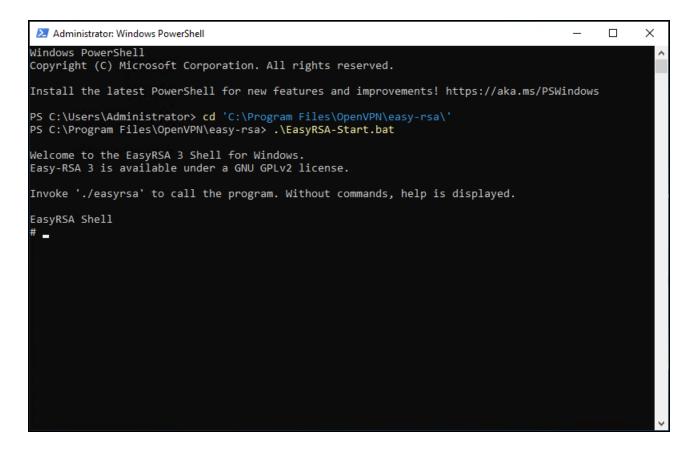
Next, click "Install Now" and wait for the client to install.

Important: Be sure to keep OpenVPN up to date with the latest version of the software.

Setting up your PKI infrastructure

On the same device, open up PowerShell or Command Prompt as an administrator and navigate to C:\Program Files\OpenVPN\easy-rsa.

Once in the directory, run the <code>EasyRSA-Start.bat</code> file.



We are now inside of the Easy-RSA 3 shell and can run commands to generate our certificate authority (CA), Diffie-Hellman parameters, and key pairs for the server and client machines.

To start, run the following two commands to start a new PKI and build our CA.

```
./easyrsa init-pki
./easyrsa build-ca nopass
```

The Common Name provided when building the CA does not matter; you can name it whatever you want.

Now that we have created our CA, run the following command to generate our Diffie-Hellman parameters. Be patient as this might take some time. ./easyrsa gen-dh

The next step will be to generate a key pair for our server. Run the following command:

```
./easyrsa build-server-full server nopass
```

The last thing we will do with Easy-RSA 3 is create our client keys. Run the following command:

```
./easyrsa build-client-full client01 nopass
```

You can now exit the Easy-RSA 3 shell by entering the exit command.

Generating a TLS authentication key

As an added measure of security, we will be generating a shared secret to be used by the server and clients.

```
In your PowerShell window, navigate to C:\Program Files\OpenVPN\bin.
```

From there run the following command to generate a new secret called ta.key.

.\openvpn --genkey secret ta.key

Quick Recap

We have now created all of the files we need to configure both our server and client machines.

Below is a table containing the information on these files, such as names and paths.

Filename	Path	Needed By	Purpose	Secret
ca.crt	"C:\Program Files\OpenVPN\easy- rsa\pki\ca.crt"	Server, Client	Root CA Certificate	No
ca.key	"C:\Program Files\OpenVPN\easy- rsa\pki\private\ca.key"	Server	Root CA Key	Yes
dh.pem	"C:\Program Files\OpenVPN\easy- rsa\pki\dh.pem"	Server	Diffie- Hellman	No
ta.key	"C:\Program Files\OpenVPN\bin\ta.key"	Server, Client	HMAC Signature	Yes
server.crt	"C:\Program Files\OpenVPN\easy- rsa\pki\issued\server.crt"	Server	Server Certificate	No
server.key	"C:\Program Files\OpenVPN\easy- rsa\pki\private\server.key"	Server	Server Key	Yes
client0.crt	"C:\Program Files\OpenVPN\easy- rsa\pki\issued\client0.crt"	Client	Client Certificate	No
client0.key	"C:\Program Files\OpenVPN\easy- rsa\pki\private\client0.key"	Client	Client Key	Yes

Subsequent steps will require you to move files around to complete the server and client configuration files. Refer back to this table at any time.

VulScan

Setup server configuration file

Move the following files to C:\Program Files\OpenVPN\config-auto. Use the table in the previous section to locate the files.

- "C:\Program Files\OpenVPN\easy-rsa\pki\ca.crt"
- "C:\Program Files\OpenVPN\easy-rsa\pki\dh.pem"
- "C:\Program Files\OpenVPN\easy-rsa\pki\issued\server.crt"
- "C:\Program Files\OpenVPN\easy-rsa\pki\private\server.key"
- "C:\Program Files\OpenVPN\bin\ta.key"

In the same <code>auto-config</code> directory, create a new file called <code>server.ovpn</code>. This will host our OpenVPN config options for the server.

Copy the following configuration into your server.ovpn file.

Note: You can download the server.ovpn file here.

```
# Which TCP/UDP port should OpenVPN listen on?
port 1194
# TCP or UDP server?
proto udp
# "dev tun" will create a routed IP tunnel,
dev tun
# SSL/TLS root certificate (ca), certificate
# (cert), and private key (key). Each client
# and the server must have their own cert and
# key file. The server and all clients will
# use the same ca file.
ca "C:\\Program Files\\OpenVPN\\config-auto\\ca.crt"
cert "C:\\Program Files\\OpenVPN\\config-auto\\server.crt"
key "C:\\Program Files\\OpenVPN\\config-auto\\server.key"
# Diffie hellman parameters.
dh "C:\\Program Files\\OpenVPN\\config-auto\\dh.pem"
```

Select subnet network topology (addressing via IP) topology subnet # Configure server mode and supply a VPN subnet # for OpenVPN to draw client addresses from. # The server will take 10.8.0.1 for itself, # the rest will be made available to clients. # Each client will be able to reach the server # on 10.8.0.1. server 10.8.0.0 255.255.255.0 # Maintain a record of client <-> virtual IP address # associations in this file. ifconfig-pool-persist ipp.txt # Push routes to the client to allow it # to reach other private subnets behind # the server. push "route 0.0.0.0 255.255.255.255 vpn gateway" # Ping every 10 seconds, assume that remote # peer is down if no ping received during # a 120 second time period. keepalive 10 120 # For extra security beyond that provided # by SSL/TLS, create an "HMAC firewall" # to help block DoS attacks and UDP port flooding. # # The server and each client must have # a copy of this key. # The second parameter should be '0' # on the server and '1' on the clients. tls-auth "C:\\Program Files\\OpenVPN\\config-auto\\ta.key" 0 # Selecting a cryptographic cipher. #cipher AES-256-CBC # The persist options will try to avoid # accessing certain resources on restart

RapidFireTools[®]

```
# that may no longer be accessible because
# of the privilege downgrade.
persist-key
persist-tun
# Output a short status file showing
# current connections, truncated
# and rewritten every minute.
status openvpn-status.log
# Set the appropriate level of log
# file verbosity.
#
# 0 is silent, except for fatal errors
# 4 is reasonable for general usage
# 5 and 6 can help to debug connection problems
# 9 is extremely verbose
verb 3
# Notify the client that when the server restarts so it
# can automatically reconnect.
explicit-exit-notify 1
```

For the VPN to work correctly, change the line that defines the route to the host network subnet.

This line tells connecting clients to use the VPN interface when accessing the local network. Replace the 0.0.0 and 255.255.255.255 with the subnet mask for the host network subnet.

```
push "route 0.0.0.0 255.255.255.255 vpn_gateway"
```

This can be found by running the *ipconfig* in your command prompt and inputting your IP and subnet mask into a subnet calculator.

For example, if your IP is 10.0.0.0 and your subnet mask is 255.255.255.0, replace the line with the following:

push "route 10.0.0.0 255.255.255.0 vpn_gateway"

Note: Repeat this command on a new line to create a separate route for each subnet that you plan to scan.

Important: You must use the push route command exactly as specified. For example, if you use the command push "redirect-gateway def1 bypass-dhcp", you will prevent the appliance from functioning.

Editing Windows network settings

Before starting the OpenVPN server, we need to edit a few Windows rules to allow for clients to connect and traffic to flow as expected.

Opening Windows firewall

With Command Prompt or PowerShell open as an administrator, run the following command to open UDP port 1194 on the Windows firewall.

```
netsh advfirewall firewall add rule name="OpenVPN UDP Port 1194"
dir=in action=allow protocol=UDP localport=1194
```

Enabling IP forwarding

Enable IP forwarding to allow the server to route incoming client traffic to workstation machines on the host network and vice versa.

To accomplish this, set the following registry key to a value of "1".

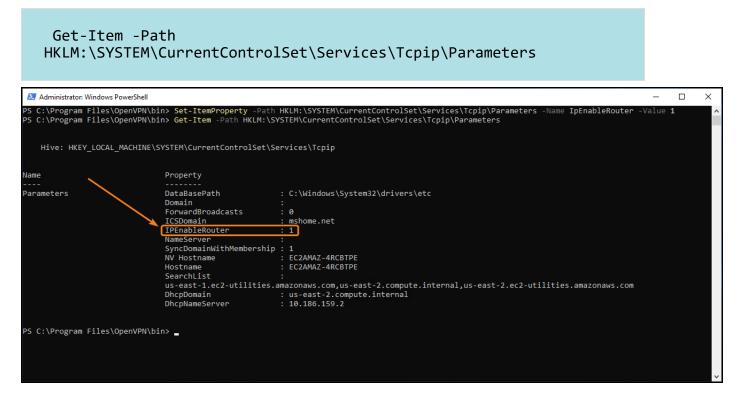
HKEY_LOCAL_ MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\IPEnabl eRouter

This can be done manually, or through an elevated PowerShell window with the command below:

RapidFireTools[®]

```
Set-ItemProperty -Path
HKLM:\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters -Name
IpEnableRouter -Value 1
```

Verify that the key was changed with the following command:

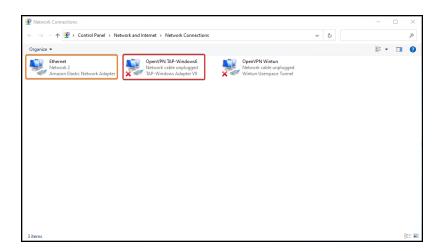


Enable internet connection sharing

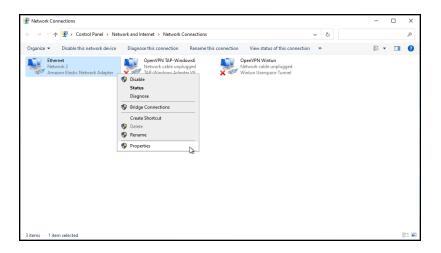
To allow the OpenVPN tunnel network adapter to access the local network, enable internet sharing on the local ethernet adapter.

Open the run dialog (Hmin + R) and enter ncpa.cpl to open the "Network Connections" menu in the control panel.

Locate your local network adapter (orange), and your OpenVPN TAP adapter (red).

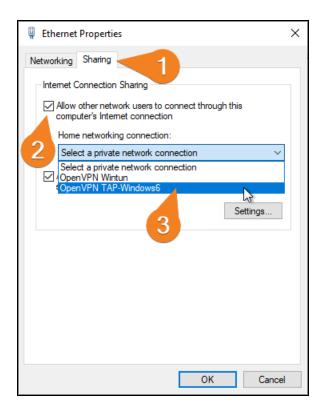


Right-click on the local network adapter and open the "Properties" menu.



Navigate to the "Sharing" tab, then check the box labeled "Allow other network users to connect through this computer's internet connection".

Finally, select the **OpenVPN TAP** adapter from the "Home networking connection" dropdown.



Restart to apply changes

Restart the computer to apply all of the Windows network settings we changed in this section.

Once the computer is restarted, the OpenVPN service will automatically run the configuration file we put inside of the auto-config folder.

If you wish to turn off the OpenVPN server at a later time, or want to refresh configuration options, you can do so by stopping and starting the "OpenVPNService" service.

Enable Routing and Remote Access

Finally, after the restart, enable the **Routing and Remote Access** Windows Service. Search for and open **Services** from the Windows Start Menu.

🤹 Remote Registry	Enables rem	Running	Automatic (Tri	Local Service
🤹 Retail Demo Service	The Retail D		Manual	Local System
RocketAgent Service	Cyber Securi	Running	Automatic	Local System
Routing and Remote Access	Offers routi	Running	Automatic	Local System
🍓 RPC Endpoint Mapper	Resolves RP	Running	Automatic	Network Se
🏟 Secondary Logon	Enables start	Running	Manual	Local System
🖏 Secure Socket Tunneling Protocol Ser	Provides sup	Running	Manual	Local Service
Security Accounts Manager	The startup	Running	Automatic	Local System

The Routing and Remote Access service is disabled by default. To enable it, right click on the service and select **Properties**. From **Startup Type**, select **Automatic**. Then **Start** the service.

General	Log On	Recovery	Dependencies					
Service	-	RemoteAc						
Display	name:	Routing an	Routing and Remote Access					
Descrip	tion:		Offers routing services to businesses in local area and wide area network environments.					
	executabl lows\Syste		st.exe -k netsvcs					
Startup	type:	Automatic	:			~		
Startup		Automatic Stopped	:			Ŷ		
Service				use	Resum	×		
Service	status: Start n specify tl	Stopped Stop				10		
Service Service You car from he	status: Start n specify tl	Stopped Stop) Pa			10		
Service Service You car from he	status: Start n specify tl re.	Stopped Stop) Pa			10		

Step 3 — Create Open VPN Configuration File

Next, you will create the **Open VPN Configuration File** for use with VulScan. This will allow the Remote Internal Vulnerability Scanner to access and scan the target network through the VPN.

Create a file called client01.ovpn anywhere on the machine (we recommend C:\Program Files\OpenVPN\config). You will need access to the additional files that you created earlier.

Copy the following configuration into this new file, making sure to adjust file paths as needed. Keep in mind that backslashes need to be escaped ($\backslash \backslash$). In addition:

- Provide the external IP or a domain name for the host network.
- In the certificate sections, paste the contents of each file you generated earlier within the corresponding tags. Example: <ca>[CA CERTIFICATE CONTENTS] </ca>

Note: You can download the client01.ovpn file here.

```
# Specify that we are a client and that we
# will be pulling certain config file directives
# from the server.
client
# TCP or UDP server?
proto udp
# "dev tun" will create a routed IP tunnel
dev tun
# External IP/domain of the host network
# Defines host's listening port
remote 0.0.0.0 1194
# Most clients don't need to bind to
# a specific local port number.
nobind
```

```
# Try to preserve some state across restarts.
persist-key
persist-tun
# Embed the required certificate and key files directly within the
# configuration file.
<ca>[CA CERTIFICATE CONTENTS from ca.crt]</ca>
<cert>[CERTIFICATE CONTENTS from client0.crt]</cert>
<key>[KEY CERTIFICATE CONTENTS from client0.key]</key>
# Verify server certificate by checking that the
# certificate has the correct key usage set.
remote-cert-tls server
key-direction 1
# If a tls-auth key is used on the server
# then every client must also have the key.
<tls-auth>[TLS-KEY CONTENTS from ta.key]</tls-auth>
# Selecting a cryptographic cipher.
#cipher AES-256-CBC
# Set the appropriate level of log
# file verbosity.
#
# 0 is silent, except for fatal errors
# 4 is reasonable for general usage
# 5 and 6 can help to debug connection problems
# 9 is extremely verbose
verb 3
# Keep trying indefinitely to resolve the
# host name of the OpenVPN server.
resolv-retry infinite
```

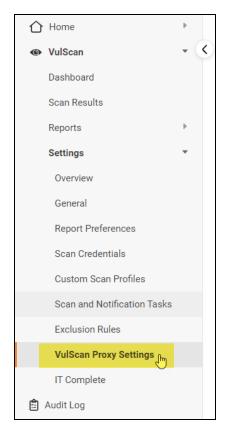
You have now created the Open VPN Configuration File for the Remote IVS. With this configuration, the Remote IVS can reach all of the machines on the host network as long as the VPN tunnel is active.

RapidFireTools[®]

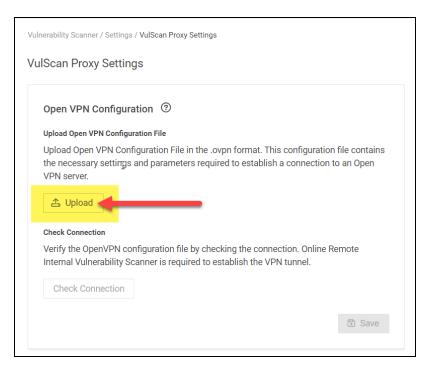
Step 4 — Upload Open VPN Configuration File to VulScan

After you create the Open VPN Configuration File in the previous step, next upload the file to your VulScan site.

1. From your site, navigate to VulScan > Settings > VulScan Proxy Settings.



2. Under **Upload Open VPN Configuration File**, click **Upload** and select the configuration file you created earlier.

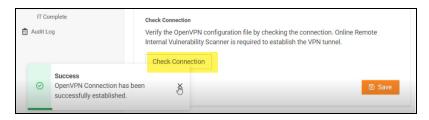


3. The configuration file will appear for the Open VPN Configuration.

	in the .ovpn format. This configuration file contains ers required to establish a connection to an Open
embedded_config.ovpn	Ū
Ø	
Check Connection	
, , , ,	e by checking the connection. Online Remote uired to establish the VPN tunnel.
Verify the OpenVPN configuration fil Internal Vulnerability Scanner is requ Check Connection	

RapidFireTools[®]

4. Click **Check Connection** to test the connection. You will receive a **Success** notification when the connection is established.



Step 5 — Perform Remote Internal Vulnerability Scan

You are now ready to perform scans using the Remote IVS.

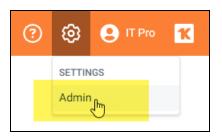
See <u>"Create Scan and Notification Tasks" on page 20</u> for a complete walkthrough.

Manage Portal Users and Access

This section covers how portal admins can create and manage users. This includes assigning users the appropriate level of access for their intended roles. Likewise, here you can review how individual users can manage how they authenticate their access to the portal.

Manage Users (Global Level)

You can manage users associated with your account from global **Settings (Admin)** > **Users**.



From the Users page, you can see a list of users associated with your account.

Micro Consulting		Organizations	
🚱 General		Global Settings / Users	
🖌 Branding			
 Connections 		Users ③	
🗘 Admin Alerts		Search	
C Users		Searcn	۹ All
Scompliance Manager GRC	Þ	Username 🔶	Display Name ≑
Q Network Detective Pro	Þ	osemane 🗸	
VulScan	•	writertech527@gmail.com	
E Service Plans	•		
🔂 Email Groups		wgibson@microconsulting.com	William Gibson
🗔 Data Collectors			
C IT Complete			

This includes user *Global Access* and *Site Access* role. You can see each site that a user is associated with, as well as the **Roles** they have been assigned to each site.

RapidFireTools°

Username ≑	Display Name 🗘	Global Access Level ≑	Site Level Access \updownarrow	2FA ≑		
billfoyers@itsolutions.com	Bill Foyers	Site Restricted	Salient Industries (Client)	Yes	Ø	Û
bv-admin@microsolutions.com		Admin	All / (Site Admin), Test CIS V8 IG1 site (Site Admin)	No	ø	Û
chuckp@microconsulting.com	Chuck Palahniuk	Site Restricted	Micro Consulting MSP (Unassigned)	No	ø	Ô
example-user@rapidfiretools.com	Example User 1	Site Restricted	Sample HIPAA Assessment (Unassigned)	No	0	Û

Users and Global Access Roles



• *Global Access Level* determines the level of access a user has to the RapidFire Tools Portal account, including which features and sites a user can access.

• *Site Access Level*, on the other hand, represents 1) the **Sites** to which a user has been assigned and 2) the **Role(s)** the user has been assigned at a Site. Roles include Site Admin, Technician, Internal Auditor, or SME. A user's level of Global Access does not limit the project role they can be assigned for a particular site.

From global **Settings (Admin)** > **Users**, you can assign users one of the following Global Access Levels:

Global Access Role	Description
MASTER/ALL	Has global access to all Organizations and Sites and the ability to manage billing, technical information, and confidential data/notes. Has access to <i>Site Settings</i> and <i>Global Settings</i> . Can access API Keys from Global Settings.
	Who should I assign this level to?
	IT Managers within your operation who have your highest level of trust, and who will:
	 be the "primary" admin for the RapidFire Tools Portal
	 handle sensitive data for all of your clients
	 purchase and provision additional RapidFire Tools Products
	 create and assign the appropriate security permissions for users within — and outside — of your operation who access the Portal
ADMIN	Has global access to multiple sites. Has access to Site Settings and

Global Access Role	Description
	Global Settings.
	Who should I assign this level to?
	 Users you trust within your operation to be "secondary" admins for the RapidFire Tools Portal
	Users you trust with sensitive data for all of your clients
	 Users you trust to create and assign the appropriate security permissions for users within — and outside — of your operation who access the Portal
RESTRICTED	Does not have global access to multiple organizations/sites. Site access must be defined by a Site Admin.
	Users in the Restricted Role can log in to the Network Detective application.
	Who should I assign this level to?
	 Techs or others in your operation who should only access specific Sites as a Site Admin or Technician
	 Techs or others in your operation who should also access sites in the Network Detective application
	Important: Users should not be assigned the Restricted Role unless you are using the Network Detective app in tandem with other RapidFire Tools Products. Instead, use the Site Redistricted Role.
SITE RESTRICTED	Does not have global access to multiple organizations/sites. Site access must be defined by a Site Admin.
	Who should I assign this level to?
	 Techs who should only access specific Sites as a Site Admin or Technician
	 Client users working with your team to perform IT or compliance assessments in the role of Technician, Internal Auditor, or SME

From the Users page, you can also:

- "Add User at Global Level" on the next page
- "Edit User at Global Level" on page 113

Add User at Global Level

Note: When you create a user from Global Settings, you will still need to 1) associate that user with a Site, and 2) add that user to a Project Role in your Site. This will allow the new user to access the Site.

You can add users to your account at the global level from the global **Settings (Admin)**

1. Click Add User.

lobal Settings / Users					
sers 🗇			_	_	+ Add User
Search	Q	• 🗹 🕅	equire Two-Factor Authen or All Accounts	tication 🗾 Ena for /	ble Discovery Agents All Users
Username 🔶	Display Name 💠	Global Access Level ≑	Site Level Access ≑	2FA ≑	
billfoyers@itsolutions.com	Bill Foyers	Site Restricted	Salient Industries (Client)	Yes	Ø û
bv-admin@microsolutions.com	ΒV	Admin	All / Bobs VulScan Site (Site Admin), Test CIS V8 IG1 site (Site Admin)	No	Ø û

2. Enter the user's information, including password.

Add User	
Username/Email Address: *	
micro-pro@user.com	
First Name: *	Last Name: *
Micro	Pro
Password: *	
•••••	
Confirm Password: *	
•••••	
Global Access Role: *	
Site Restricted	
	Close + Add

Important: You will need to send the user the email and password in order for them to access the RapidFire Tools Portal.

3. Choose a Global Access Role for the User.

From global **Settings (Admin)** > **Users**, you can assign users one of the following Global Access Levels:

Global Access Role	Description
MASTER/ALL	Has global access to all Organizations and Sites and the ability to manage billing, technical information, and confidential data/notes. Has access to <i>Site Settings</i> and <i>Global Settings</i> . Can access API Keys from Global Settings.

RapidFireTools^{*}

Global Access Role	Description
	Who should I assign this level to?
	IT Managers within your operation who have your highest level of trust, and who will:
	• be the "primary" admin for the RapidFire Tools Portal
	 handle sensitive data for all of your clients
	 purchase and provision additional RapidFire Tools Products
	 create and assign the appropriate security permissions for users within — and outside — of your operation who access the Portal
ADMIN	Has global access to multiple sites. Has access to <i>Site Settings</i> and <i>Global Settings</i> .
	Who should I assign this level to?
	 Users you trust within your operation to be "secondary" admins for the RapidFire Tools Portal
	Users you trust with sensitive data for all of your clients
	 Users you trust to create and assign the appropriate security permissions for users within — and outside — of your operation who access the Portal
RESTRICTED	Does not have global access to multiple organizations/sites. Site access must be defined by a Site Admin.
	Users in the Restricted Role can log in to the Network Detective application.
	Who should I assign this level to?
	 Techs or others in your operation who should only access specific Sites as a Site Admin or Technician
	 Techs or others in your operation who should also access sites in the Network Detective application
	Important: Users should not be assigned the Restricted Role unless you are using the Network Detective app in tandem with other RapidFire Tools Products. Instead, use the Site Redistricted

Global Access Role	Description
	Role.
SITE RESTRICTED	Does not have global access to multiple organizations/sites. Site access must be defined by a Site Admin.
	Who should I assign this level to?
	 Techs who should only access specific Sites as a Site Admin or Technician
	 Client users working with your team to perform IT or compliance assessments in the role of Technician, Internal Auditor, or SME

4. Click Add. The user will be added.

Edit User at Global Level

Note: Only *Master* and *Admin* users can edit users. And only Master users can edit other Master users. See <u>"Manage Users (Global Level)" on page 107</u> for more details.

To edit users:

- 1. Navigate to the global **Settings (Admin)** > **Users** page.
- 2. Click on the pencil icon next to the user you wish to edit and make your desired changes.

fs-admin@foresight.com	Foresight Admin	All	All	No	1
globalteam@itsolutions.com	Global Team	Site Restricted	Salient Industries (Unassigned)	No	<i>o</i> 🗊
itpro@prodynamics.com	IT Pro	All	All	No	<i>o</i> 🗊
itpro@tech-dynamism.net	Tech Pro	Site Restricted	Salient Industries (Site Admin)	No	ø 🗈

3. Click Save.

RapidFireTools°

Enable Log In with KaseyaOne

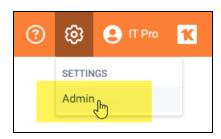
Once you are logged in with KaseyaOne, you can jump to any other IT Complete product without having to log in separately for each app. This provides a seamless workflow for IT Complete integrations. Follow these steps to enable users to log in with KaseyaOne.

Enable Log in with KaseyaOne at Account Level from Global Settings

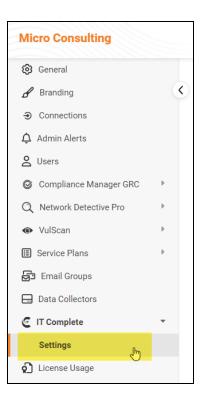
Before users can access the log in with KaseyaOne feature, a **GLOBAL ADMIN USER** must first enable the feature at the account level.

To do this:

1. Open global **Settings (Admin)** from the RapidFire Tools Portal top menu.



2. Open **IT Complete > Settings** from the left-hand settings menu.



3. Activate the Log in with IT Complete slider.

Global Settings / IT Cor	mplete / KaseyaOne	
IT Complete		
KaseyaOne	Bullphish ID	
Single Sign-On		
Enable Log	in with KaseyaOne	
This option	will allow your users t	o enable Log In with KaseyaOne for themselves. Learn More

4. The KaseyaOne portal will open in your browser. Enter your KaseyaOne login credentials.

Important: You must enter credentials for a **Master user** in KaseyaOne to enable this feature.

	seyaOne
Username	
j @rapidfi	retools.com
Password	Forgot password?
•••••	
Company Name	
Great Lakes Comp	uter Corporation
	Log In
	ive an account yet? t support to request one.

- 5. If prompted, enable two-factor authentication for your KaseyaOne account.
- 6. Once you log in to KaseyaOne, your browser will return to the RapidFire Tools Portal. The **Log in with KaseyaOne** feature will be activated for all portal users.

KaseyaOne Bullphish ID Single Sign-On Single Log in with KaseyaOne	
This option will allow your user	

Log in with your KaseyaOne user

- 1. Once you <u>"Enable Log in with KaseyaOne at Account Level from Global Settings"</u> on page 114, users can then log in to the RapidFire Tools Portal using their KaseyaOne credentials.
 - You must have a user with a unique matching email address or username in the RapidFire Tools Portal. If you do not, you will be unable to log in. See <u>"User Matching Criteria" on the next page</u>. You can also <u>"Enable Automatic User Creation for RapidFire Tools Portal" on page 121</u> – this will create a new portal user automatically upon login.
- 2. Click the **Log in with KaseyaOne** button directly from the RapidFire Tools Portal log in page.

Username	
u	ser@rapidfiretools.com
Password	Forgot Password
Remember	me
	Log in
	Log in
P	

3. The KaseyaOne portal will open in your browser. Enter your KaseyaOne login credentials.

Kaseya You're logging in with	
Username	
j @rapidfiretools.co	om
Password	Forgot password?
Company Name	
Great Lakes Computer Corp	oration
Log In	
Don't have an acc Please contact support	

4. You will then enter the RapidFire Tools Portal with the user that corresponds to your KaseyaOne account.

User Matching Criteria

- If 2+ users in the RFT account have the same email address as the K1 user, you cannot log in
- If 1 user in the RFT account has the same email address as the K1 user, you will log in as that user
- If no users in the RFT account have the same email address as the K1 user, the portal checks for an RFT username that matches the K1 username

Require Log In with KaseyaOne

The following table describes what happens when you configure the Require Log In with

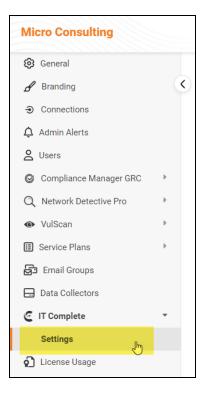
KaseyaOne setting from global **Settings (Admin)** > **ITComplete** > **Settings**.

Toggle	Setting	Action / Description
Require Log In with KaseyaOne	Enabled	Forces users to log into the module with their KaseyaOne Unified Login credentials - and prompts them to do so. Users with exceptions will still be able to log in using their local RapidFire Tools Portal credentials.

Toggle	Setting	Action / Description
Require Log In with KaseyaOne	Disabled	Allows users to log into the module with either their KaseyaOne Unified Login credentials (if <u>"Enable Log</u> <u>In with KaseyaOne" on page 114</u> is turned on) or
		their local RapidFire Tools Portal credentials.

To Enable Require Log in with KaseyaOne:

1. From the RapidFire Tools Portal, open **IT Complete** > **Settings** from the left-hand settings menu.



2. In the Require Log in with Kaseya One section, **select the Require Log In with KaseyaOne toggle switch** to enable the setting. Note that selecting the toggle switch again disables the setting.

 ire Log In with KaseyaOne ption will require users to log in with KaseyaOne Unified Login only. Learn More	
Require Log In with KaseyaOne	
User Overrides	
	~
Global Access Level Overrides	
	\sim

RapidFireTools°

• User Overrides: Here you can override the KaseyaOne login for selected users. Click the drop down and select the chosen users for the override. Users that you select can still log in using their RapidFire Tools Portal credentials.

	re Log In with KaseyaOne otion will require users to log in with Kase	yaOne Unified Login only. Learn More	
	Require Log In with KaseyaOne		
	User Overrides		
		\ \	~
	fkafka@microconsulting.com		
	chuckp@microconsulting.com		
	wgibson@microconsulting.com	լիդ	
Auton Once en		0	
created			
	☐ fs-admin@foresight.com		

• Global Access Level Overrides: Here you can override the KaseyaOne login for users with the selected Global Access Level. Click the drop down and select the chosen Global Access Levels. Users with this access level can still log in using their RapidFire Tools Portal credentials.

Require Log In with KaseyaOne This option will require users to log in with KaseyaOne Unified Login only. Learn More				
Require Log In with KaseyaOne	Require Log In with KaseyaOne			
User Overrides				
	~			
Global Access Level Overrides				
վեղ	~			
Admin				
Automa Once enal Restricted				
created. L 🔲 Site Restricted				
Enable Automatic User Creation				

Frequently Asked Questions

- 1. *I don't have a KaseyaOne login. How do I get one?* Contact your primary KaseyaOne administrator or account manager to get started.
- 2. *Is my KaseyaOne login the same for all IT Complete products?* Yes, you can use the same log in for all products that your administrator has enabled Log in with KaseyaOne on.
- 3. *What two factor applications are supported?* Passly Mobile or any OTP authenticator that supports 8-digit codes.

Enable Automatic User Creation for RapidFire Tools Portal

Once you are logged in with KaseyaOne, you can jump to any other IT Complete product without having to log in separately for each app. This provides a seamless workflow for IT Complete integrations.

Once you first <u>Enable Log in with KaseyaOne</u>, users can log in to the RapidFire Tools Portal using KaseyaOne, but must already have a unique matching email address or username in the RapidFire Tools Portal. However, if you then **enable Automatic User Creation**, your users in KaseyaOne who log in to the RapidFire Tools Portal will automatically have a user created. You can set the Global Access Level, Default Sites, and Default Site Role for new users created this way.

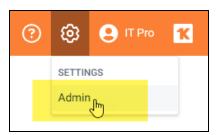
Here's how to enable Automatic User Creation for KaseyaOne users who will access the RapidFire Tools Portal:

Step 1 – Enable Log in with KaseyaOne at Account Level from Global Settings

Before users can access the log in with KaseyaOne feature, a **GLOBAL ADMIN USER** must first enable the feature at the account level.

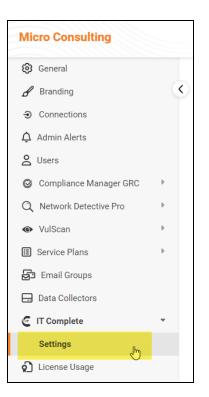
To do this:

1. Open global **Settings (Admin)** from the RapidFire Tools Portal top menu.



2. Open **IT Complete** from the left-hand settings menu.

RapidFireTools°



3. Activate the Log in with IT Complete slider.

Global Settings / IT Complete / KaseyaOne		
IT Complete		
KaseyaOne Bullphish ID		
Single Sign-On		
Enable Log in with KaseyaOne		
This option will allow your users	o enable Log In with KaseyaOne for themselves. Learn More	

4. The KaseyaOne portal will open in your browser. Enter your KaseyaOne login credentials.

Important: You must enter credentials for a **Master user** in KaseyaOne to enable this feature.

	ng in with IT Complete
Username	
j @rapidfir	etools.com
Password	Forgot password?
•••••	
Company Name	
Great Lakes Compu	iter Corporation
	Log In
	ve an account yet? t support to request one.

- 5. If prompted, enable two-factor authentication for your KaseyaOne account.
- 6. Once you log in to KaseyaOne, your browser will return to the RapidFire Tools Portal. The **Log in with KaseyaOne** feature will be activated for all portal users.

IT Complete		
KaseyaOne	Bullphish ID	
Single Sign-On		
Enable Lo	g in with KaseyaOne	
This optio	n will allow your users	to enable Log In with KaseyaOne for themselves. Learn More

Step 2 – Enable Automatic User Creation

Once you enable log in with KaseyaOne, the Enable Automatic User Creation option will become available. Here's how to set it up:

KaseyaOne Bullphish ID
Single Sign-On
Enable Log in with KaseyaOne This option will allow your users to enable Log In with KaseyaOne for themselves, Learn More
Automatic User Creation Once enabled, your users in KaseyaOne who are granted access to any RapidFire Tools module will automatically have a use created. Learn More
Enable Automatic User Creation
Choose Default Global Access Level
Site Restricted Admin
Choose Default Site(s)*
· · · · · · · · · · · · · · · · · · ·
Choose Default Site Role
Site Admin 👻

1. From Enable Automatic User Creation, activate the slider.

Once er	natic User Creation nabled, your users in KaseyaOne who are I. Learn More	granted access to any RapidFire Tools module will autor	natically have a user
	Enable Automatic User Creation Choose Default Global Access Level [®]		
	Site Restricted Admin Choose Default Site(s)*		
	Choose Default Site Role	•	
	Site Admin	•	

- 2. Choose the **Default Global Access Level**. This determines the user's level of access to the portal. There are two options:
 - Site Restricted: User can only access the Default Site(s) and organizations they are assigned. The Site Restricted user must also be assigned a Default Site Role.
 - Admin: User can access all sites and organizations

\odot	Enable Automatic User Creation	
	Choose Default Global Access Level*	
	Site Restricted Admin	
	Choose Default Site(s)*	
	Choose Default Site Role	
	Site Admin	

3. Next, choose the **Default Site(s)** that Site Restricted users should access from the drop-down menu. New Site Restricted users will only be able to access the sites you select.

1	. ,	able Log In with KaseyaOne for themselves. Learn Mor	e
Automa Once en	Buseline compliance Assessment	GRC	natically have a user
created.	BDR Site - Quick - 2018 - Datto		
	Black Lion IT Blue Bird Bus Company		
	Bonham Dental Arts	- ^(m)	
	Bullet Bus Company ×		•
	Site Admin		•

- 4. Finally, for Site Restricted users, choose the Default Site Role: **Site Admin** or **Technician**.
 - Site Admin: Can access all site functionality
 - Technician: Can access assessments and data collection, but not users

Enable Automatic User Creation Choose Default Global Access Level*
Site Restricted O Admin
Choose Default Site(s)*
Blue Bird Bus Company × Bonham Dental Arts ×
Site Admin 🥼
Technician
Site Admin

Step 3 – KaseyaOne User Logs into RapidFire Tools Portal

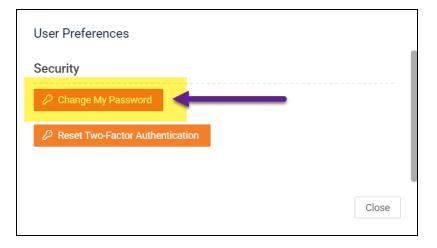
Once the Portal Admin enables Automatic User Creation for the KaseyaOne account, KaseyaOne users can log into the RapidFire Tools Portal from My IT Complete.

- The new user will have the level of access to the portal that you configured earlier.
- The new user will not have a unique password to access the Portal outside of KaseyaOne. Use the "Forgot Password?" link on the Portal login page to create a new password.

Change your Password

To change your password in the RapidFire Tools Portal:

- 1. Log into the RapidFire Tools Portal with your credentials.
- 2. From the portal, click the user icon in the top right hand corner of the screen.
- 3. Click User Preferences.
- 4. Click Change My Password.



5. Then enter your new password and confirm it again.

User Preferences		
Change My Password Current Password		
New Password		
Confirm Password		
	Close ← Back	✓ Confirm

6. Click **Confirm**.

Your password will then be changed.

RapidFireTools°

Recover Forgotten Password

To recover a forgotten password:

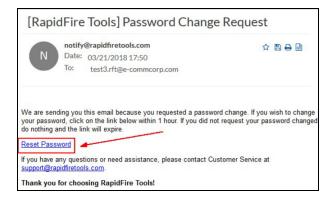
1. Open the RapidFire Tools Portal at <u>https://www.youritportal.com</u>.

Greys Profess	tone sionals
Username	
Password	Forgot Password?
••••••	
Remember me	
Log	in
Log Or	
	r

- 2. Click Forgot Password?
- 3. Enter your user account's email address.

Forgot Password	
Please enter your username below. An email with a new temporary password will be sent to the email address you provided when you registered.	
Username	
Submit	
Back to Login	
Help & Support © Kaseya 2023	

4. Click **Submit**. You will receive an email with a link to change your password. Click **Reset Password**.



5. Follow the on-screen prompts to complete recovering your password.

RapidFireTools[®]

Log Out of RapidFire Tools Portal

To maintain data security, log out of the RapidFire Tools Portal when you are not using it.

- 1. From the portal, click the user icon in the top right hand corner of the screen.
- 2. Click Logout.
- 3. You will return to the RapidFire Tools Portal Login page.

Enable Access Groups

Access Groups allow you to map users in KaseyaOne Access Groups to the appropriate user roles in the RapidFire Tools Portal. If you have Access Groups set up in KaseyaOne, you can enable Access Groups in the RapidFire Tools Portal to allow new users to join with the exact permissions that you specify.

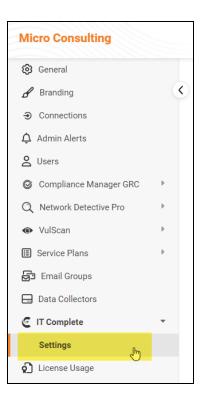
Note: In order to set up Access Groups for KaseyaOne and the RapidFire Tools Portal, you must first <u>"Enable Log In with KaseyaOne" on page 114</u>.

The following table describes what happens when you configure the Enable Access Group setting for the RapidFire Tools Portal.

Toggle	Setting	Action / Description
Enable Access Groups	Enabled	Enables Access Groups for KaseyaOne users to the RapidFire Tools Portal whereby KaseyaOne Access Groups are mapped to Portal Global Access Levels. This will ensure new logins to the RapidFire Tools Portal have the privileges relevant to their KaseyaOne Access Group.
Enable Access Groups	Disabled	Disables Access Groups for KaseyaOne Access Groups in the RapidFire Tools Portal.

Here's how to enable Access Groups:

1. From the RapidFire Tools Portal, open global **Settings (Admin)**. Then open **IT Complete > Settings** from the left-hand settings menu.



2. In the Access Groups section, select the **Enable Access Groups** toggle switch to enable the setting. Note that selecting the toggle switch again disables the setting.

Access Select the r		roup. Changes to access group settings will change these settings	for users. Learn More
•••	Enable Access Group		
#	KaseyaOne Access Group	Global Access Level	Site(s)

3. Click **Add Access Group** to create a new KaseyaOne Group-to-RapidFire Tools Portal Role mapping.

ange these settings for users. Le		27-Nov-2023, 8:45 PM 🛛 📿 Sync
		+ Add Access Group
Site(s)	Site Role	
	~	 ✓

4. Map each KaseyaOne Access Group to a Global Access Level.

Access Group Select the role you would like to assign each KaseyaOne Access Group. Changes to access group settings will change these settings for users. Learn More				
	Enable Access Group			
#	KaseyaOne Access Group	Global Access Level	Site(s)	
1	Everyone v	Admin		

5. For **Site Restricted** users, from the drop-down select the **Site(s)** to which the Group should have access. Likewise, choose a **Site Role** for Site Restricted users.

Choose Default Site Role '					
				•	
Acces	s Group			AR GRC	Iov-2023, 8:34 PM 🖉 Sync
Select th	e role you would like to assign each KaseyaOne Acce	ss Group. Changes to access group settings will cha	angi	AWS RIVS - VulScan	
	C Enable Access Group			Beautiful British Columbia - Vancouver	+ Add Access Group
				CH - VulScan integration	
#	KaseyaOne Access Group	Global Access Level			
				CM - NIST	
1	Everyone 🗸	Site Restricted V		×	~ û

Once you set up Access Groups for the RapidFire Tools Portal, new users who log in with their KaseyaOne credentials will enter the Portal with the permissions that you specify.

Set Up Portal Branding

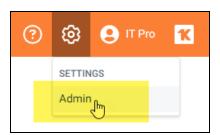
The RapidFire Tools Portal allows you to customize many elements to fit with your organization's brand and identity. This topic covers how you can modify the Portal's look and feel.

1. Visit <u>https://www.youritportal.com</u> and log into the RapidFire Tools Portal.

Note: In order to configure the settings in the Portal, the login credentials you use to access the Portal will require the Master User rights.

	ireTools [®]
Password	Forgot Password?
Remember me	
Lo	g in
(Dr
🗙 Log in v	vith KaseyaOne
Learn More ab	out KaseyaOne

2. Click global Settings (Admin) > Users.



3. Click Branding.

Micro Consulting	Organizations
ⓒ3 General	Global Settings / General
🖌 Branding	
Onnections	General
🗘 Admin Alerts	Time Zone ③
O Users	(UTC-05:00) Eastern Time (US & Canada)
Compliance Manager GRC	
Q Network Detective Pro ▶	Date Format ③
VulScan	dd-MMM-yyyy
E Service Plans	

From this page, you can then:

- "Set Custom Portal Theme" below
- "Set Custom Portal Subdomain" on the next page
- "Set Custom Company Name" on page 137
- "Set Custom Company Logo" on page 138

Set Custom Portal Theme

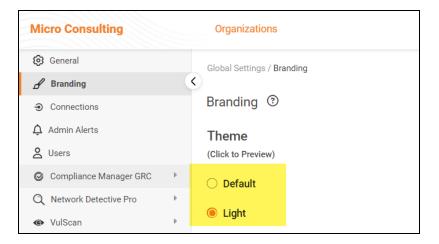
You can choose from two different color-themes for the Portal. To do this:

1. From global **Settings (Admin)** > **Branding**, select the *Default* or *Light* under theme.

Micro Consulting		Organizations
(2) General		Global Settings / General
🖌 Branding		
➔ Connections		General
🗘 Admin Alerts		Time Zone 💿
2 Users		(UTC-05:00) Eastern Time (US & Canada)
Scompliance Manager GRC	Þ	
Q Network Detective Pro	Þ	Date Format ③
VulScan	•	dd-MMM-yyyy
Service Plans	Þ	

RapidFireTools*

2. As you can see, the Light theme is more minimalistic.



3. When you select the theme, you can click around the Portal and preview it. You

must click **Save** from global **Settings (Admin) Branding** to apply your changes. This change will apply to all users.

Set Custom Portal Subdomain

You can enter a custom subdomain to communicate your company name/brand to users when they access the URL for the portal. To do this:

1. From global **Settings (Admin)** > **Branding**, scroll down and enter the custom **Subdomain** name in the Site Subdomain field.

Site				
Subdo	omain			
http	ps://	greystone	.alert-central-dev.com	

- 2. Click Save.
- 3. Log out of the RapidFire Tools Portal.
- 4. Next, access the RapidFire Tools Portal by using the URL for the new Subdomain you configured to access the Portal's login screen.

\leftrightarrow \rightarrow	ò	C	Â	greystone.alert-central-dev.com/login	
					Greystone Professionals
					Username
					Password Forgot Password?
					Remember me

Important: Be sure to communicate the custom URL to your users. Note that users who navigate to the default URLs for the portal will still be in the right place once they log in.

Set Custom Company Name

You can set a custom company name that will appear in the top left-hand corner of the Portal.

Micro Consulting	Organizations
🔞 General	Global Settings / Branding
🖌 Branding	
 Connections 	Branding ③
🗘 Admin Alerts	Theme
O Users	(Click to Preview)

To do this:

1. From global **Settings (Admin)** > **Branding**, enter your custom company name under Custom Branding.

RapidFireTools°

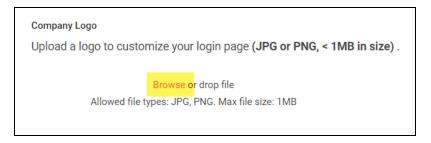
🙆 General					
🖌 Branding		Custom Branding 🥑			
 Connections 		Company Name			
🗘 Admin Alerts		Displayed in top left of menu bar			
OUSERS		Micro Consulting			
© Compliance Manager GRC	•				
Q Network Detective Pro	Þ				
VulScan	•				
🖽 Service Plans	•				
Email Groups					

2. Click **Save**. Your custom name will then appear in the top-left corner of the portal for all users to see.

Set Custom Company Logo

You can set a custom company logo on the Portal login screen to communicate your brand to users. To do this:

1. From global **Settings (Admin) Branding**, click **Select** under Company Logo and **Upload** a custom image.



2. Click Save. Your chosen image will be scaled and appear for users who reach the

login screen.

Gr Pro	reystone fessionals
Username	
Password	Forgot Password
Remember me	
	Log in
Learn Mo	ore about KaseyaOne

RapidFireTools*

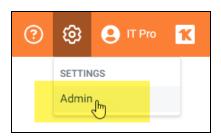
Set Up a Custom Subdomain to Access the RapidFire Tools Portal

1. Visit <u>https://www.youritportal.com</u> and log into the RapidFire Tools Portal.

Note: In order to configure the settings in the Portal, the login credentials you use to access the Portal will require the Master User rights.

	FireTools
Username	
Password	Forgot Password?
Remember me	
	Log in
	Or
Ҟ Logi	n with KaseyaOne
Learn More	about KaseyaOne

2. Click global Settings (Admin)



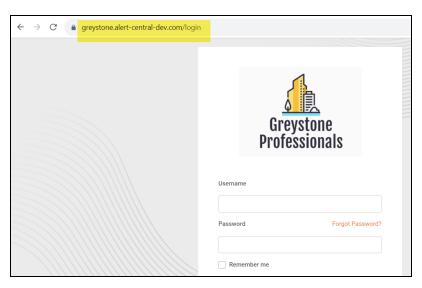
3. Click Branding.



4. Enter the **Subdomain** name you desire in the Site Subdomain field.

Site		
Subdomain		
https://	greystone	.alert-central-dev.com

- 5. Click Save.
- 6. Log out of the RapidFire Tools Portal.
- 7. Next, access the RapidFire Tools Portal by using the URL for the new Subdomain you configured to access the Portal's login screen.



RapidFireTools[®]

Portal Administration

This section covers basic administrative tasks for the RapidFire Tools Portal. To manage portal users at the global level, see <u>"Manage Portal Users and Access" on page 107</u>.

Set Time Zone

You can set your time zone from global **Settings (Admin)** > **General**. Set your time zone to schedule automated scans at your preferred local time. To configure time zones:



Micro Consulting	Organizations	?	ଡ଼	ĸ
Seneral Branding	Global Settings / General		1	
 ➔ Connections 	General		I	
🗘 Admin Alerts	Time Zone ③			
OUSERS	(UTC-05:00) Eastern Time (US & Canada)			~
S Compliance Manager GRC	•			
Q Network Detective Pro	Date Format ①			
WulScan	▶ dd-MMM-yyyy			~
E Service Plans	Þ			Save
Email Groups				
🕞 Data Collectors				
C IT Complete	Þ			
🔊 License Usage				
🖉 API Keys				

- 2. Select your time zone from the drop down menu.
- 3. Click Save.

Note that the time zone setting is relatively narrow in scope. For example, To Do task creation time is shown based on your browser's local time, *not* the time zone setting in Global Settings. The time zone setting effects a few items, including:

- start time for scans when using the limit scan start time feature for a site
- · last modified date of risk update reports
- last sync date and time for Kaseya BMS billing integration

Report Date Format (Global Settings)

You can set the **Date Format** for the reports and compliance documentation generated by Compliance Manager. You can do this from global **Settings (Admin)**

RapidFireTools°

Seneral settings.

1. Select your preferred format from the **Date Format** drop down menu.

General	
Time Zone [©]	•
Date Format [©]	•
	dd-MMM-уууу
	MM/dd/yyyy
	yyyy/MM/dd
	dd/MM/yyyy

2. Click Save.

Your documentation will now appear with your chosen date format.

The table below shows examples of the date formats converted to actual calendar dates.

Date Format	Example
dd-MMM-yyyy	31-Jan-2000
MM/dd/yyyy	01/31/2000
yyyy/MM/dd	2000/01/31
dd/MM/ yyyy	31/01/2000

Admin Alerts (RapidFire Tools Portal)

Within the RapidFire Tools Portal, you can set and configure Admin Alerts to inform you of events such as a completed or failed scan or notification error.

Admin Alerts: Global Settings vs. Site Settings

There are two levels at which you can configure Admin Alerts:

- From global **Settings (Admin)** > **Admin Alerts**, you can set the default Admin Alert settings for all of your Sites within the RapidFire Tools Portal. This can be useful if one group of recipients should receive admin alerts for all of your Sites.
- From [Your Site] > Home > Admin Alerts, you can override the default Global Settings for Admin Alerts. Your changes will be specific to that Site. This can be useful if you want different groups of recipients to receive admin alerts for different sites.

Configure Admin Alerts

To configure Admin Alerts:

- 1. Decide whether you want to change the Admin Alert settings for:
 - A. All of your Sites (Navigate to global **Settings (Admin)** > Admin Alerts)
 - B. Just for one specific Site ([Your Site] > Home > Admin Alerts)
- 2. Then, enter the email addresses for the users who will receive the Admin Alerts.

Micro Consulting	Organizations	?	Ø	IT Pro	ĸ
General	Global Settings / Admin Alerts		4		
🖌 Branding	Global Gettinge / Hamil Alerte				
Connections	Admin Alerts ③				
🗘 Admin Alerts	Email Addresses (Separate multiple addresses with a comma $({}^{"}_{\ \prime})$		-		
名 Users					
Ocompliance Manager GRC					
Q Network Detective Pro	Notices (Subject Prefix (added before notice type))				
VulScan	%%SITE%% -				
E Service Plans	Notification Error				
Email Groups	Reports Generated				
Data Collectors	 Scan Complete Scan Failed 				
IT Complete					
👌 License Usage					_
🖉 API Keys				Reset	Save

- 3. Add a Subject Prefix that will be included in email's subject line before the notice type.
- 4. Select which types of alerts to send to the listed users.
- 5. Click Save. You can also choose to Reset to Global Settings.

Delete a Site

If you wish to delete a site, follow these steps:

- 1. Select the site from the Sites page that you wish to delete.
- 2. From the site's Home tab, click on Advanced Options.

	Micro Consulting MSP			
Data Collectors				
Users	Home / Advanced Options			
Roles	Advanced Options			
Groups				
Admin Alerts	() Changing advanced options may incur additional charges.			
Advanced Options				
	License			
的 Audit Log	Consumed Licenses 1 Ste License(s)	License Usage Discovered Endpoints: 1		
	Delete Site			
	Warning: Deleting a site will permanently remove all associated data alerts, and To Do items related to the site.	including assessments, reports,		

3. Click Delete Site.

Important: Deleting a site will permanently remove all associated data, including assessments, reports, alerts, and To Do items related to the site.

4. Confirm that you wish to delete the site by typing the site's name. Then click Yes.

RapidFireTools[®]

The site will then be removed from the system.

Delet	re Site					
	Are you sure? Deleting a site will permanently remove all associated data, including assessments, reports, alerts, and To Do items related to the site.					
	delete the site, type the site name (Micro Consulting MSP) in the box ow: me					
	Cancel Delete Site					

Import IT Glue Organizations

You can import your IT Glue organizations directly into the RapidFire Tools Portal. This streamlines the process of onboarding IT Glue users who wish to leverage the RFT Portal's suite of IT and compliance assessment offerings.

Likewise, you can optionally synchronize your IT Glue org names with the imported orgs in the RFT Portal. Whenever you change the name of an org in ITGlue, that change will be reflected in the RFT Portal.

Note: You must subscribe to IT Glue Enterprise to access this feature.

Here's how to enable this feature:

Step 1 — Create and Copy API Key in IT Glue

First, you need to set up an API Key in IT Glue.

1. Create one or more **Organizations** in IT Glue. You will later select one of these orgs to send your data to the right place. You create new Organizations from the **Organizations** tab in IT Glue.

Dashboard Organizatio	ns My Tasks Global	Account Q Searc	:h 🕘 🕶	- 1
Organizations				
 Recents 			📩 Imp	ort + New
SR				
Sandbox RFT				

2. Create an IT Glue API Key for your use during integration and set up. You can do this from **Account > API Keys**.

Dashboard	Organizations	My Tasks	Global	Account		
Account						
Sett	ings					
Gene	ral Brand	ing A	Authenticati	ion	API Keys	Theme

RapidFireTools[®]

Custom API Keys					1	
The IT Glue API is a RESTful A	API that can be used to manage and retrieve info	ormation. Learn more			1	
rft_	ITG.614	Revoke	Password Access	-	l	
kreed_	ITG.0d6	Revoke	Password Access	-	l	
rft_	ITG.2eb	Revoke	Password Access	-	l	
Enter Name		Generate API Key	Password Access	-	l	
		_		+	l	
Important	For your reference	e, save a c	opy of the A	PIk	ey outside	e of IT Glu

- Step 2 Enable Connection to IT Glue from Portal Global Settings
 - 1. Next, from the RapidFire Tools Portal, navigate to global **Settings (Admin)** > **Connections**.
 - 2. From Your Connections, click Add.

Organizations				@ Ø	9 IT P	ro <mark>1</mark>
obal Settings / Connections						
onnections ③						
our Connections			_		- +	Add
Name ≑	Туре ≑	Login ≑				
Migration Connection for rapidfire_c	ConnectWise REST	101101-0017018			Ø	Ŵ
IT Glue	IT Glue	*****	Set Up Organizations	Sync Now	00 🖉	Ŵ
IT Glue	IT Glue	*****	Set Up Organizations	Sync Now	00 🖉	Û
IT Glue	IT Glue	*****	Set Up Organizations	Sync Now	00 🖉	Ŵ
Datto Unified Continuity	Datto Unified Continuity	1011			Ø	Ŵ
Dark Web ID	Dark Web ID	1			Ø	۵
BMS HIPAA	Kaseya BMS				2024.02	

3. Select IT Glue from the drop-down menu and enter the API Key.

4. Click Test Login.

Add Connection
API Key to get started.
 Additional setup may be necessary to configure the API user in the specific ticketing system. Please refer to the configuration documentation.
Connection Type *
– Choose Connection Type – 🗸 👻
Autotask
ConnectWise
ConnectWise REST
IT Glue
Kaseya BMS
TigerPaw
Cancel Test Login

RapidFireTools*

s/Connec Ctions	Add Connection Organizations with ongoing updates. Enter an IT Glue API Key to get started.	1
AA Conn	Additional setup may be necessary to configure the API user in the specific ticketing system. Please refer to the configuration documentation.	nd
bings awk Secul	Connection Type *	/ Compan
no p HIPAA S	API Key *	iired) iired)
	Region * North America	
	Cancel Test Login	j

5. Next select the **Organization Status** and **Organization Types** to delimit the categories of orgs imported into the RapidFire Tools Portal.

Add Connection
Select organization statuses and types to sync with the RapidFire Tools portal.
Organization Status
Active
Inactive
Organization Types
Cancellation
Competitor
Customer
Dead
Internal
Lead
Other
Partner
Prospect
Vendor
← Back Save
Note: These fields are configured in IT Glue.

- 6. Click Save.
- 7. Your new Connection will appear under Your Connections.

Step 3 — Set Up Organizations

Once you set up the Connection with IT Glue, you then have the options of 1) reviewing imported orgs and editing how they map with existing RFT portal orgs, and 2) importing new orgs from IT Glue into the portal.

1. From My Connections, click Set Up Organizations.

9	Global Settings / Connections				
d ⊕	Connections @				
ф Q	Your Connections				+ Add
ø	Name ¢	Type 💠	Login 💠		
•	BMS HIPAA Connection	Kaseya BMS			D 🛈
ii Gr	IT Glue	IT Glue	****	Set Up Organizations	II 🖉 🗒
⊟ ©	Site Mappings				+ Add
ଚ	Site 💠	Connection	÷	Account / Company	
	Cyber Hawk Secure Demo Site	BMS HIPAA	Connection	(not required)	Ŵ
	KSV Demo	BMS HIPAA	Connection	(not required)	Ŵ
	My Demo HIPAA Site	BMS HIPAA	Connection	(not required)	Ŵ

2. If you already have an org in the RFT Portal with the same name as an IT Glue org, the two orgs will be matched automatically. You can click the X to remove the mapping if you wish.

 Connections Admin Alerts Users 		t Up Organizations or match existing organizations	to IT Glue organizations.		
S Compliance Manager GRC	▶ Filt	er columns or search keywords.			6 of 6 results
VulScan Service Plans		Add from IT Glue			
Email Groups	0	rganization	IT Glue Organization	Rem	ove Matching
Data Collectors	A	BLE Manufacturing HQ	ABLE Manufacturing HQ	Х	
 IT Complete License Usage 	A	cme Organization	None	×	
	Ð	cample Organization	None	Х	
	М	icro Consulting	None	Х	
	Ν	ETWORK ORGANIZATION ITG	NETWORK ORGANIZATION ITG	Х	
	Si	mith School Bus Company	Smith School Bus Company	×	
		Cancel Sing save will store the matching	g and rename the current Organizatio	on name	e to the IT Glue Organization name.

- 3. To import IT Glue orgs, click **Add from IT Glue**.
- 4. Select the orgs to add from the drop-down menu. Then click Add.

lue INS	Add From ITGlue				
ations to IT Glue organizations.	Select your organizations from ITGlue to automatically create RapidFire Tools organizations. ITGlueOrganizations*				
IT Glue Organization	Select multiple Blue Bird Bus Company				
ABLE Manufacturing HQ None	Back Add				
None	×				
None	x				

5. The imported orgs will appear. Once more, you can see their names in the RFT Portal as well as IT Glue.

Step 4 — Synchronize Org Names with IT Glue

Once you import orgs from IT Glue into the RFT Portal, the org names will be synchronized; changes to org names in IT Glue will regularly update the corresponding org names in the RFT Portal.

You can view these mappings from Your Connections > Set Up Organizations.

Note: The sync is limited to org names and works one way from ITGlue into the RFT Portal. Note also that deleting orgs in the RFT Portal will not delete orgs in IT Glue.

Pause Org Name Synchronization

To stop synchronizing org names, find the ITGlue connection and click the pause button.

Micro Consulting		Organizations				@ @	9	IT Pro	ĸ
 ③ General ✔ Branding ④ Connections ↓ Admin Alerts ▲ Users 		Global Settings / Connections Connections ③ Your Connections	Туре 🗢	Login ¢				+ A	dd
Compliance Manager GRC Network Detective Pro VulScan	+ + +	Migration Connection for rapidfire_c	ConnectWise REST					0	Û
Email Groups	ŀ	IT Glue	IT Glue	*****	Set Up Organizations	Sync Now	⊳	0	Û
Data Collectors IT Complete	•	IT Glue	IT Glue	ki kininini k	Set Up Organizations	Sync Now	⊳	ı	Û
License Usage API Keys		IT Glue	IT Glue	*****	Set Up Organizations	Sync Now	⊳	0	Û
Success	was na	Datta Unified	Datto Unified Continuity	Miles .				0	Û
 IT Glue integration was p successfully. 		useu X	Dark Web ID	14100 (1410) (1410)					Û
		BMS HIPAA	Kaseya BMS	10000000				4.02.25	7-1904 前

To resume synchronizing org names, find the ITGlue connection and click the **play** button.

Micro Consulting	Organizations				?	¢	9	T Pro	K
General	Global Settings / Connections								
🖌 Branding									
Onnections	Connections ③								
Admin Alerts	Your Connections							+ A	dd
2 Users									
	Name ≑	Type ≑	Login ¢						
Q Network Detective Pro	Migration Connection	ConnectWise	The Contraction of the Contract					0	Û
♦ VulScan	for rapidfire_c	REST							0
Service Plans	IT Glue	IT Glue	******						~
Email Groups	IT Gibe	11 Gide		Set Up Organizations	Sync	Now	01	0 1	Û
Data Collectors	IT Glue	IT Glue	*****	Set Up Organizations	Sync	Now	03		Û
C IT Complete				out op organizatione	0)110				<u> </u>
License Usage	IT Glue	IT Glue	*****	Set Up Organizations	Sync	Now	00	0	Û
API Keys									
Success	Datta Unified	Datto Unified Continuity	10111					01	Û
 IT Glue integration was successfully. 	s started X	Dark Web ID	1					0 1	Û
	BMS HIPAA	Kaseya BMS	(contract)					02.27	-1904 🗊

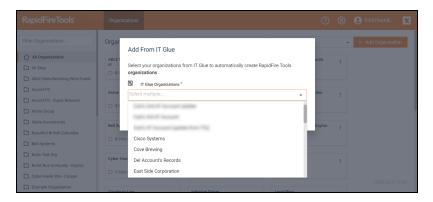
Import IT Glue Orgs when Creating New Organizations

Once you set up a connection with IT Glue, you can also import IT Glue orgs from the RFT Portal orgs page:

- 1. Click Add Organization from the RFT Portal home page.
- 2. Click Add from IT Glue.

RapidFireTools	Organizations		FIRSTNAME
Filter Organizations	Organizations	Add Organization	- Add Organization
All Organizations All Sites	ABLE Manufacturing st	Organization Name* Add from IT Glue	
ABLE Manufacturing West Coast Accent Fit Accent Fit - Guest Network	Acme Group	Organization names must start with an alphanumeric character, may only include alphanumeric characters, dash, and space and must be less than 50 characters long.	
Acme Group Alpha Investments	3 Sites Bell Systems	Cancel Confirm tes Company - Dayton .	
Beautiful British Columbia Bell Systems	2 Sites	Stes Stes	
Bobs Test Org Bullet Bus Company - Dayton Cyber Hawk Site - Ccoper	Cyber Hawk Site - Coo	er : Example Organization : Foresight Group : A Stes D 7.5tes	2024.02.27-1904

3. Select one or more IT Glue orgs from the drop-down menu and click Add.



RapidFireTools[®]

Create an API Key

You can create an API key for the RapidFire Tools Portal that can be used to retrieve information. This allows for integrations between the portal REST API and other apps.

Here's how to generate an API key:

1. First, access global **Settings (Admin)** > API Keys.

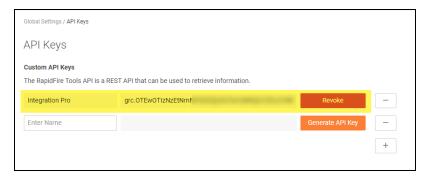
Micro Consulting	Organizations	?	ଡ଼	IT Pro	1
General	Global Settings / General		4		
🖌 Branding					
 Connections 	General				
🗘 Admin Alerts	Time Zone ①				
Our Sers	(UTC-05:00) Eastern Time (US & Canada)			~	
S Compliance Manager GRC	•				
Q Network Detective Pro	▶ Date Format ③				
VulScan	▶ dd-MMM-yyyy			~	
E Service Plans	•			Save	
Email Groups				ourc	
Data Collectors					
C IT Complete	Þ				
🕤 License Usage					
API Keys					1904
					1204

Note: Your user must have Global Access Role "**All**" (master user) to access this feature.

2. From Custom API Keys, enter a name for your key, then click Generate API Key.

Image: Sense
License Usage API Keys

3. Copy the value of the key for use with your API integration.



4. You can also **Revoke** an API key and click the "—" button to delete it.

API Keys			
Custom API Keys			
The RapidFire Tools API is a RES	ST API that can be used to retrieve information.		
Lighting Key	grc.NDIxMGYyNmQtYzU1Mi0	Revoke	-
Enter Name		Generate API Key	-
			+

RapidFireTools[®]

Appendices

Refer to the appendices listed below for the supplementary information referenced in this user guide:

VulScan Integration with Network Detective	. 161
Migrate Inspector 2 to VulScan	161
Log in to RapidFire Tools Portal and Access VulScan Site	
Next Steps for New VulScan Users	
Generate Internal Vulnerability Reports in Network Detective using VulScan	164
VulScan and Reporter	
Set Up and Assign a Ticketing/PSA System Integration to a Site	. 167
Step 1 — Gather Credentials and Set Up your PSA System	
Step 2 — Set Up a Connection to your Ticketing System/PSA	
Step 3 — Map your Site to a Ticketing System/PSA Connection	
Set Up Autotask Integration	
Set Up Autotask (SOAP) Integration	
Set Up ConnectWise REST Integration	
Step 1 — Download and Install the ConnectWise Manage Internet Client Application	
Step 2 — Select the ConnectWise Ticket System API Member Account to Integrate with	. 185
Create Minimum Permissions Security Role for API Member	186
Table Setup Configuration	. 187
Step 3 — Create an API Key in the ConnectWise Ticketing System	
Step 4 — Configure Service Tables in ConnectWise	
Step 5 — Remove "Disallow Saving" Flag from Company	
Set Up ConnectWise SOAP Integration	
Set Up Kaseya BMS Integration	197
Data Collectors for VulScan	.199
Function of VulScan Data Collectors	. 199
Internal Vulnerability Data Collector	199
External Vulnerability Data Collector	199
Portable Data Collector	200
Remote Internal Vulnerability Scanner	200
Provision VulScan	200
Manage Site Data Collectors	. 203
Data Collector Commands	. 204
Enable Discovery Agents for Local Data Collection (VulScan)	. 207
Discovery Agent Firewall Requirements	207

Step 1 — Enable Discovery Agents at the Organization Level	
Step 2 — Install Windows Discovery Agent on PC on target network	
Step 3 — Confirm Discovery Agent install from your Organization	
Step 4 — (Optional) Enable Access for Site Admin and Technician Users	212
Step 5 — Schedule Scans for Discovery Agent	213
Step 6 — Assign Labels to Agents	214
Step 7 — Configure VulScan Agent Imports	215
How Scan Data Import Configuration Works	
Remove Discovery Agents	217
Application Vulnerability Scan for Windows	219
Step 1 — Deploy Discovery Agents on Endpoints	
Step 2 — Enable Application Vulnerability Scan for Windows for Discovery Agents	219
Step 3 — Review Application Vulnerabilities	
Install Linux and macOS Discovery Agents	221
Find and Copy Install Key for Discovery Agents	
Default Scripted Linux Install	
Default Scripted macOS Install	
Install Script Options	
Silent Install for Discovery Agent (Windows)	
Uninstall Script for Discovery Agent	227
Portable VulScan Set Up	
Step 1 — Provision Portable VulScan Appliance	
Step 2 — Install Portable VulScan Appliance on target Network	
Step 3 — Create VulScan Site and opt not to provision appliance	
Step 4 — Assign Portable VulScan Appliance to Site	
Step 5 — Set Up and Perform Internal Scan and Notification Tasks	
Step 6 — Remove PVS appliance from Site	
Step 7 — Assign PVS appliance to new VulScan Site	
Enable Global Two-Factor Authentication (2FA) for Portal Users	
Step 1 — Master user enables 2FA for all portal users	
Step 2 — Portal user logs in and sets up 2FA Access	232
Step 3 — Portal Users enter Authentication Code after initial login	234
Import IT Glue Organizations	
Step 1 — Create and Copy API Key in IT Glue	
Step 2 — Enable Connection to IT Glue from Portal Global Settings	
Step 3 — Set Up Organizations	239
Step 4 — Synchronize Org Names with IT Glue	
Pause Org Name Synchronization	241

RapidFireTools*

Import IT Glue Orgs when Creating New Organization	s
License Usage (Global Settings)	

VulScan Integration with Network Detective

Migrate Inspector 2 to VulScan

Tip: You can find a video tutorial for upgrading to VulScan here.

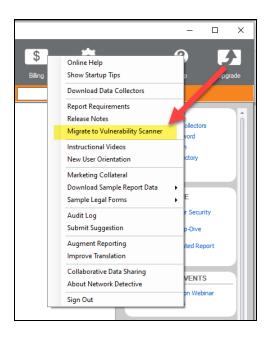
As of Monday, January 26, 2021, **Inspector 2** will be deprecated and replaced by **VulScan**.

- Inspector 2 users will no longer have the ability to configure scan tasks using Network Detective.
- Instead, users must manage scans and review scan data using the VulScan console in the RapidFire Tools Portal.
- Inspector 2 users will have the benefits of the new VulScan product, and be able to download data into Network Detective to generate Internal Vulnerability Reports. (See <u>"Generate Internal Vulnerability Reports in Network Detective using VulScan"</u> on page 164.)

Inspector 2 users should follow these steps to upgrade to VulScan.

Note: To migrate your site, you must have the latest version of Network Detective: version 4.0.1299 or higher.

- 1. Open Network Detective and log in to your account.
- 2. Click the Help menu and select Migrate to Vulnerability Scanner.



3. Review the prompt and click **OK**.

	A Enhance Very Committee	
Migratio	n to Vulnerability Scanner	×
?	This is a one-time process to migrate existing Inspector 2 sites to Vulnerability Scanner sites that can be accessed and managed in the RapidFire Tools portal. If a site with an equivalent name already exists in the RapidFire Tools portal and is being used for Cyber Hawk or Compliance Manager, a new site will be created with the suffix -VS (i.e., "My Site" would turn into "My Site-VS"). Press OK to proceed with the site migration?	
	OK Cancel	

Note: This is a one-time process to migrate existing Inspector 2 sites to VulScan sites that can be accessed and managed in the RapidFire Tools portal.

Important: If a site with an equivalent name already exists in the RapidFire Tools portal and is being used for Cyber Hawk or Compliance Manager, a new site will be created with the suffix -VS (i.e., "My Site" would turn into "My Site-VS"). If you had a Reporter assigned to this site, you will need to manually move the Connector to the new site ("My Site-VS").

- 4. All of your existing Inspector 2 sites will be migrated to VulScan sites in the **RapidFire Tools Portal**.
- 5. The **Queued Scan Tasks** for your Inspector 2 sites will be carried over as scan tasks that can be managed from your VulScan site in the RapidFire Tools Portal. **UNSCHEDULED SCAN TASKS IN THE TASK LIBRARY WILL NOT BE MIGRATED.**

Log in to RapidFire Tools Portal and Access VulScan Site

1. Once you migrate your site, access the RapidFire Tools Portal at https://www.youritportal.com and log in with your credentials.

Username
ndtest10@rapidfiretools.com
Password Forgot Password?
Remember me
Log in
Or
C Log in with IT Complete
<u>Help & Support</u> © Kaseya 2022

2. Select your new site from the Site page. You can then begin using VulScan.

Organizations				🤊 🕸 🕒 🗉	Pro Ҟ
Sites				Move Site +	Add Site
All 87 Compliance Manager GRC 1	Compliance Manager Legacy 8	Cyber Hawk 4	Network Detective Pro 41	VulScan 16	
Search keywords				16 0	f 16 Result:
Site ≑		Organization \diamondsuit			
ACME Customer		Initiative Group			
Apogee Group		Initiative Group			
Apogee Systems		Initiative Group			
Town and Country		Kepler Biz			
Generative Solutions		Acme Group			

- 3. All of your existing Inspector 2 sites will be migrated to VulScan sites in the **RapidFire Tools Portal**.
- 4. You an access these from [Your Site] > VulScan > Settings > Scan and

Notification Tasks.



Next Steps for New VulScan Users

MORE INFO:

- Documentation and downloads: You can access VulScan documentation and downloads at https://www.rapidfiretools.com/vs-downloads
- Onboarding and customer success: Contact Customer Success at customersuccess@rapidfiretools.com, or sign up for training at https://calendly.com/network-detective/vulscan-kickoff
- Technical support: Contact Technical Support at support@rapidfiretools.com

Generate Internal Vulnerability Reports in Network Detective using VulScan

With your **Reporter** and/or **Network Detective Pro** subscription, you can use VulScan to generate internal vulnerability (.ivul) scan files for your assessments. This allows you to leverage VulScan to generate internal vulnerability reports in Network Detective. To do this:

1. First, you need to set up and manage VulScan scan tasks from the RapidFire Tools Portal. From Network Detective, when you right click **Manage** for a VulScan appliance from the site options, you will be prompted to access the portal.

Active Project		ternone berecove re			a			
Addite Hoped	Name	Type	Manage	Update	Remove	Running Tasks		
	O KVS1-	Inspector 2.0	% Manage	🞐 Update	🗙 Remove	No queued tasks		
	O KVS1-	Inspector 2.0	% Manage	🖈 Update	🗙 Remove	No queued tasks		
	O KVS1-	Inspector 2.0	% Manage	🕈 Update	🗙 Remove	No queued tasks		
Archived Projects	Assessment-20	0210625						
	0% Complete 0 Complete	1 Required 1	Optional Creat	ed 25-Jun-202	1 11:03 AM U	odated 25-Jun-202	Manage KVS Settings	×
Progress Reports	Network Assessme	nt (Domain) 09	5 Complete 0	Complete 🚺	Required	1 Optional D	To manage KVS settings, log into the YourlTPortal and go to your	site.
Generated Reports	Detective Data Dat Collector co (NDDC) with the	un Computer la Collector on imputers that cannot be inned remot 2	Reports Not Ready				For Non-EU customers: <u>https://secure.youritportal.com</u> For EU customers: <u>https://secure.youritportal-eu.com</u>	
Downloaded Reports	Double-click items to open.						Cancel	
	Run Network De Run the Network Data C workstation on the network	ollector on the Doma	in Controller (f po	ssible), a comp	uter joined to the		nain Controller is not available, or from any	

2. When VulScan performs a successful internal vulnerability scan, you can click **Downland Scans**, select the .ivul file, and import it into your assessment.



- 3. You can then generate vulnerability scan reports using the Security module. Access this from the site reports console.
- 4. Select the relevant reports and click Create Reports.

Reports Create	Report	s						
All Reports	~	33% Available						
Standard Reports								
Security Risk Report (.docx) Security Management Plan (.docx)								
Outbound Security Report (.docx)								
Security Policy Assessment (.docx)								
Share Permission Report (.docx)								
Share Permission Report Excel (xlsx)								
	Share Permission Report by User (.docx)							
Share Permission Report by User Exc	Share Permission Report by User Excel (xlsx)							
External Vulnerability Scan Detail Re	ort (.doc)	<)						
External Vulnerability Scan Detail by	ssue Rep	ort (.docx)						
External Network Vulnerabilities Sum	nary Repo	ort (.docx)						
External Vulnerability Scan Detail Exc	el (.xlsx)							
Internal Vulnerability Scan Detail Rep	1 N N N N N N N N N N N N N N N N N N N	·						
Internal Vulnerability Scan Detail by Is								
Internal Network Vulnerabilities Summ		rt (.docx)						
Internal Vulnerability Scan Detail Exc	10 C 1							
Login Failures by Computer Report (.c	· · ·							
Login History by Computer Report (.d								
User Behavior Analysis Report (.docx)							
Anomalous Login Report (.docx) Security Assessment PowerPoint (.pp	hy)							
Security Assessment FowerFoint (.pp	LX J							

VulScan and Reporter

While you manage VulScan from the RapidFire Tools Portal, it works the same way with Reporter as the previous (deprecated) Inspector 2 product. To use VulScan with

RapidFireTools^{*}

Reporter:

Important: After you migrate to VulScan, if a site with an equivalent name already exists in the RapidFire Tools portal and is being used for Cyber Hawk or Compliance Manager, a new site will be created with the suffix -VS (i.e., "My Site" would turn into "My Site-VS"). If you had a Reporter assigned to this site, you will need to manually move the Connector to the new site ("My Site-VS").

- 1. **Ensure your scan tasks have been created and scheduled** from your VulScan site in the RapidFire Tools Portal.
- 2. Ensure your Reporter internal vulnerability report tasks are set up and scheduled to occur after your scans will have finished. See the <u>Reporter User</u> Guide for Network Detective Pro.
- 3. Once your report task finishes, the reports will be available to download from the Reporter appliance as before.

Set Up and Assign a Ticketing/PSA System Integration to a Site

To successfully configure a Ticketing/PSA system integration with the RapidFire Tools Portal, you will require the following information for the ticketing system you plan to set up for use with the Portal:

- your Username and Password for your Ticketing System/PSA Integration Account provided by the Ticketing System's manufacturer
- URL for the Ticketing/PSA system's API Integration system access

Step 1 — Gather Credentials and Set Up your PSA System

Before you begin, you will need:

- Valid Admin Login Credentials for RapidFire Tools Portal
- A RapidFire Tools Portal "Site" for which you wish to export items or create tickets in your PSA
- Valid Login Credentials for your PSA system account (if you wish to integrate with multiple PSA accounts, gather credentials for each PSA account)
- Other prerequisites specific to your chosen PSA system (refer to the table below)

PSA System	PSA Prerequisites
Autotask	The Autotask SOAP integration has been deprecated (see below). To use the new integration, all you need is a username and password for a non-API user.
	Important: The new Autotask integration is not supported by Network Detective or Network Detective on the web at this time. Continue to use the Autotask SOAP integration for these products.
	Autotask UsernameAutotask Password

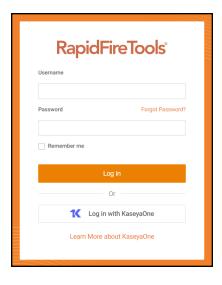
RapidFireTools°

PSA System	PSA Prerequisites
Autotask [®]	Autotask API UsernameAutotask API Password
SOAP (Deprecated)	
Connec+Wise [™]	 ConnectWise REST Public Key ConnectWise REST Private Key ConnectWise Company ID
	ConnectWise PSA URL
SOAP CONNEC-HWISE	 ConnectWise Username ConnectWise Password ConnectWise Company ID ConnectWise PSA URL
Tigerpaw	 Tigerpaw Username Tigerpaw Password Tigerpaw API URL
BMS by Kaseya	 Kaseya Username Kaseya Password Kaseya Tenant (i.e. company name) Kaseya API URL, example: "https://bms.kaseya.com" (you should receive the exact URL in an email from Kaseya)

Step 2 — Set Up a Connection to your Ticketing System/PSA

Follow these steps to set up a Connection to your Ticketing System/PSA in the Portal.

1. Visit <u>https://www.youritportal.com</u> and log into the RapidFire Tools Portal.

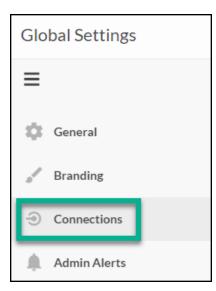


2. Click global Settings (Admin)

ଡ଼

Note: In order to configure the Global Settings in the Portal, you must be a global admin user.

3. Click Connections.



4. Click Add to create a new Ticketing System/PSA Connection.

Global Settings	
≡	Global Settings > Connections
🔅 General	
Branding	You do not have any Connections set up yet. You can add one Connection per Cyber Hawk site. Get started by creating a Connection.
Onnections	+ Add
Admin Alerts	
Users	

5. In the Setup New Connection window, configure the **Connection Type** by selecting the PSA/Ticketing system.

-		
. C. P	Connecting to other syste	
	a Connection Type below	pidFire Tools modules. Choose to get started.
nnection		
- Choos	e Connection Type –	•
Autotas	sk	
Connec	tWise	
Conner	ctWise REST	
oonnee		շիդ
Kaseya	BMS	\bigcirc
		\bigcirc

6. Then enter the information required to set up the Connection.

This information will include:

- Username and Password for your Ticketing System/PSA account
- URL for the Ticketing/PSA system API

Add Connection					
Setup New Connection Integrating with PSA and ticketing systems allows automated creation of tickets on a per- site basis. Enter the appropriate ticketing API credentials below.					
Additional setup may be necessary to configure the API user in the specific ticketing system. Please refer to the configuration documentation.					
Connection Type *					
Integrator Login *					
youritcompanylogin					
••••••					
Company ID *					
My Client Company					
PSA URL *					
https://na.myconnectwise.net					
⊘ Cancel 🔒 Test Lo	gin				

- 7. Click **Test Login** button to test your Connection login. After a successful test login, the second Add Connection Ticket Details window will be displayed.
- 8. Continue creating your Connection by entering in the necessary Ticket Details for your PSA.

RapidFireTools[®]

Ticket Details Specify how tickets shoul	ld be created	in the ticketing system.	
Work Type *		Assigned Resource	
Maintenance	•	Da Irown	•
Role		Due Date/Time *	
Standard MS Engineer	•	Now + 5	Minutes
Issue Type		Sub-Issue Type	
Maintenance	•	Workstation	•
Queue		Priority *	
Level I IT Management	•	Medium	•
Status *		Source	
New	•	Email	•
Test ticket will be created i Account Lookup	n the account s		
Q Account Name			
Account *			
			Ŧ

Click **Test Ticket**. The Add Connection Settings Confirmation window will be displayed after the Test Ticket process is successful.

- 9. In the Add Connection Confirm Settings window presented, enter a **Connection Name**.
- 10. Review the Connection's configuration details and click **Save**.

Confirm De Please confi	tails m the information below be	fore saving your new Con	nection.
💉 Connectio	n		
Connection Name *			
LW TP 532019 Prod			
Туре		TigerPaw	
Login		Performanceit	
Ticketing	Help Desk	Service Type	Break/Fix
ccount	Performance It	Representative	Ian Alexander
tatus	New	Priority	Medium

The new Connection created will be listed in the Portal's Connection list.

Global Settings > Connections Connections ? Your Connections			+	- Add
Name 🗢	Туре 💠	Login 💠		
AT	Autotask	dbrown@com	1	Î
BMS	Kaseya BMS	mw	1	Î

Step 3 — Map your Site to a Ticketing System/PSA Connection

Follow these steps to map a Ticketing System/PSA Connection to the RapidFire Tools Portal Site associated with your site.

1. In the Integrations window, click **Add** under Site Mappings. The Map Site to Connection window will be displayed.



2. Select the RapidFire Tools Portal **Site** you want to assign to this Ticketing System/PSA Integration.

Map Site to Connection	×
Select a Site below and a Connection	n to use to create tickets for that Site.
🗈 Site	5 Connection
Site for Customer ABC •	ConnectWise 🔹
	Company Lookup
	c Q
	Select Company *
	Customer ABC 👻
	Cancel Save

- 3. Next, **select the name of the Connection** that you want use to link the Site to your Ticketing System/PSA.
- After selecting the Connection name, use the Company Lookup field to search and select the Company name to be referenced when generating Tickets for the selected Site.
- 5. Click **Save**. The Site's mapping to your Ticketing System/PSA Integation will be saved and listed in the Site Mappings list.

te Mappings			+ Add
Site 🗢	Connection 💠	Account / Company	
Detect Suspicious Behavior		(not required)	Î
		(not required)	î

Your Portal account can now be used to create tickets for any Alerts or To Do items listed in the Portal for the RapidFire Tools Portal Site you selected.

RapidFireTools^{*}

Set Up Autotask Integration

The Autotask SOAP integration has been deprecated. To use the new Autotask integration, all you need is a username and password for a non-API user. Here's how it works:

Note: Currently, you cannot connect a single Autotask instance to two different RapidFire Tools Portal accounts. If you create a Connection for an Autotask instance to a second RapidFire Tools account, the previous Connection will no longer function.

- From the RapidFire Tools Portal, navigate to global Settings (Admin) > Connections.
- 2. From Your Connections, click Add.
- 3. From **Connection Type**, select the **Autotask** connection type (as opposed to the deprecated Autotask SOAP connection).

	Add New Connection
* ³	Connecting to other systems enable workflow integrations with your RapidFire Tools modules. Choose a Connection Type below to get started.
	al setup may be necessary to configure the API user in the ticketing system. Please refer to the configuration documentation
Connection Ty	pe *
– Choose C	onnection Type – 🗸 🗸 🗸
Autotask S	DAP
Autotask	վիդ
Autotask	
ConnectWi	se
ConnectWi	se REST

4. Click Authenticate in Autotask.

	Add New Connect Connecting to othe	orkflow inte	grations
*	with your RapidFire Type below to get s	oose a Conr	nection
Connection Ty	ne *		
Autotask	pe	 	~
Authorize	in Autotask 🖸		

5. Log in using your Autotask username and password. We recommend that you create the connection with a user that has **Admin** privileges in Autotask.

	utotask		
Username			
Rememb	per me		
	Continue		
	Or		
	Ҟ Log In with KaseyaOne		

6. If promoted, click **Reauthorize** to create the connection.



7. Configure the **Test Ticket**. When you finish, the new Autotask connection will become available, where you can map it to a site from **Site Mappings**.

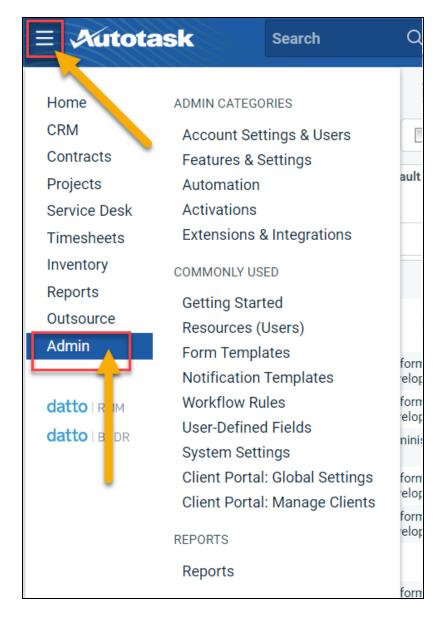
	Ticket Details Specify how tickets should be created in the ticketing system.				
Autotask Org	anization *	Ticket Category* Learn more			
– Choose Organization – 🗸 🗸		✓ Choose Category ✓			
Ticket Type *		Status *			
– Choose Ticket Type – 🗸 🗸		– Choose Status – 🗸 🗸			
Priority *					
– Choose I	Priority –	~			

Set Up Autotask (SOAP) Integration

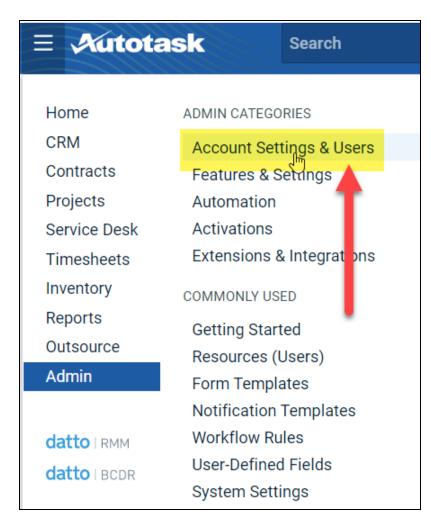
To set up a connection with the Autotask (SOAP) system, you will need to **create an API User in Autotask**. To do this:

- 1. Log in to Autotask with your admin user credentials.
- 2. Click on the Autotask home button on the left, then click Admin.

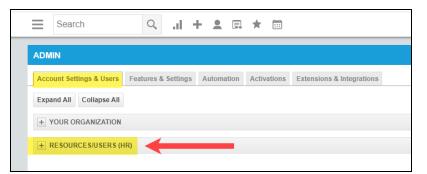
RapidFireTools°



3. From the Admin menu, click Account Settings & Users.



4. Next, click Resources/Users (HR) to expand the menu.



5. Then click **Resources/Users**.

RapidFireTools[®]

Admin	
Account Settings & Users Features & Settings Automation	Activations Extensions & Integrations
Expand All Collapse All	
✓ Your Organization	
Resources/Users (HR) Resources/Users (HR)	
Resources/Users Manage user accoul for people in your organization who have an Autotask login.	Time Off Policies Manage the time off categories and the number of days or hours in each category your resources are entitled to at each length of service titer.
Roles Set up billing roles that determine the rate at which labor will be billed.	Timesheet Approvers Set up the resources who will approve other resources' timesheets.
Departments Set up organizational entities in your company that are associated with resources and work types, and play a role in project security.	Expense Report Approvers Set up the resources who will approve other resources' expense reports.

6. Hover your mouse over the drop-down menu to the right of the **New** button, then select **New API User**.

∃ Autotask	Search	Q Dast	nboards Create	My Calendar
+ Resources				
🕂 New 🔹 Imp	port/Import History	🕹 📃 Show Inac	tive Find Resource	e
New Resource	Resource ID 🔷	Default Department	Security Level 🧅	License Type 🌲 🤇
		•		
			AT 144 (1498)	10.000

7. Enter information about the API user. Autotask will prompt you to enter the mandatory fields.

Add API User	0					
🖹 Save & Close 🛞 Cancel	Review Terms and Conditions for API Use					
General	í					
First Name*	Security Level *					
	•					
Last Name *	Date Format MM/dd/yyyy					
Email Address *	Time Format					
	hh:mm a 🔻					
Active	Number Format					
Locked						
	Primary Internal Location *					
Credentials						
💭 Generate Key	Generate Secret					
Username (Key) *	Password (Secret) *					
API Tracking Identifier						
API version 1.6 & later require the user of an API tracking identifier. On	ce assigned, this cannot be changed.					
 Integration Vendor Custom (Internal Integration) 						
, č						
Integration Vendor * RapidFire Tools - Network Detective						
Line of Business						
A line of business can be used to grant access or prevent access to da	ata associated with Contracts, Tickets, Projects, etc.					
Not Associated	Associated					
÷						
v.	-					
Resource can view items with no assigned Line of Business						
_						

- Enter a first and last name for the API user.
- Enter an email address for the API user.
- From Security Level, select API User (system).
- Select a Primary Internal Location for the API user.
- Enter/generate a **username** for the API user, then enter/generate a **password**.

Note: Take note of these credentials as you will enter these in Network Detective to enable the API integration.

• Under API Tracking Identifier, select Integration Vendor. Then select RapidFire Tools — Network Detective.

Add API User	0
🖹 Save & Close 🛞 Cancel	Review Terms and Conditions for API Use
Credentials	
⊖ Generate Key	◯ Generate Secret
Username (Key) *	Password (Secret) *
API Tracking Identifier API version 1.6 & later require the user of an API tracking ide	
Integration Vendor Custom (Internal Integration) Integration Vendor* rapidfire v	1
Perspectium - Middleware (ServiceNow) PropelYourMSP	^
Li Pulseway - RMM Quickpass - Password Management Quoter Software Inc Quoter QuoteWerks - Quotes, Proposals, and Procurement RapidFire Tools - Network Detective Recursyv - Seamless	ssociated with Contracts, Tickets, Projects, etc. Associated
Red Cactus - Bubble CRM Integrations Relokia - Data Migration Resale Partners - Telephony	v v

8. When you are finished configuring the new API user, click **Save & Close**. The new user will appear in the list.

Set Up ConnectWise REST Integration

To set up a connection to ConnectWise Ticketing system using the REST API you will be required to:

Step 1 — Download and Install the ConnectWise Manage Internet Client Application

To enable the integration, you will need to use the ConnectWise Manage Internet Client application. Download and install the app from <u>http://university.connectwise.com/install/</u>. Then log in using your credentials.

If you are using the ConnectWise Manage web app, you can continue to use the web app after you have completed the steps in this guide and enabled the integration.

Step 2 — Select the ConnectWise Ticket System API Member Account to Integrate with

1. From the ConnectWise dashboard, click **System** from the side menu.



- 2. Next, click Members.
- 3. Click on API Members Tab. The API Members screen will appear.

Note that the API Members Tab may not show by default and may need to be added. You can add this tab from the Tab Configuration menu on the Members page .

- 4. Click on the + button to create a new API Member. Fill in all required information.
- 5. Confirm that the API Member has been assigned Admin rights by checking the member's **Role ID** under **System**.

System			
Role ID* Admin	~	Location* Tampa Office	~
Level* Corporate (Level 1)	~	Business Unit* Admin	~

RapidFireTools*

Important: By default, the API Member must have Admin rights for the integration to function correctly. However, we provide a "least privilege" custom solution for the API Member Role ID below. See <u>"Create Minimum Permissions</u> Security Role for API Member" below.

Create Minimum Permissions Security Role for API Member

If you do not wish to assign the API member full Admin rights, create this custom security role and assign it to the API member:

- 1. Go to **System > Security Roles**.
- 2. Click the + button to create a new security role.
- 3. Set the permissions for the Role as detailed in the table below and click **Save**.
- 4. Assign this custom Security Role to the API Member instead of full Admin.

Module		Add Level	Edit Level	Delete Level	Inquire Level
Companies					
	Company Maintenance				All
	Configurations	All	All		All
	Contacts	All	All		All
Service Desl	<				
	Service Tickets	All	All		All
System					
	API Reports				All
	Table Setup* *Customized Table Setup: Allow Company / Company Status, Company / Configuration,	All			All

Module		Add Level	Edit Level	Delete Level	Inquire Level
	Opportunities /				
	Opportunity Status, Opportunities /				
	Opportunity Type				
	(See <u>"Table Setup</u>				
	Configuration" below				
	below for an				
	extended				
	explanation)				

Table Setup Configuration

From Table Setup, click **customize**.

Report Writer	None	\sim	None	\sim	None	\sim	None	\sim	
Security Roles	None	\sim	None	\sim	None	\sim	None	\sim	
System Reports (<u>customize</u>)	None	\sim	None	\sim	None	\sim	None	\sim	
Table Setup (<u>customize</u>)	All	\sim	None	\sim	None	\sim	All	\sim	
Today Links	None	\sim	None	\sim	None	\sim	None	\sim	
∧ Time & Expense									7/25/23
Expense Approvals	None	\sim	None	\sim	None	\sim	None	~	

Allow access to the items listed in the table above under **Table Setup**. You can also refer to the image below.

Update Security Allow Access to these Company / Company Status Company / Configuration Opportunities / Opportunity Status Opportunities / Opportunity Type	> < »» «	Disallow Access to these Activities / Activity Status-CRM Activities / Activity Type Agreements / Agreement Type Agreements / Batch Company / Address Formats Company / Company Type		•	×
SAVE CANCEL		Company / Country Company / Currency	•	•	

RapidFireTools*

Step 3 — Create an API Key in the ConnectWise Ticketing System

- 1. Select the API Member that you created previously.
- 2. From the API Member details screen, click API Keys.



- 3. Click the + button.
- 4. Enter a **Description** for the API Key.
- 5. Click Save.
- 6. The newly generated API Key will appear.
- 7. Write down or take a screen shot of the Member's Public and Private API Key strings. This information will be required to set up the integration with ConnectWise.

Important: Note that the Private Key is only available at the time the key is created. Be sure to copy the keys for your records.

✓ You have successfully updated this record.						
Public API Key						
Description:	*	test1				
Public Key:	*					
Private Key:	*					
Note: The private key	is only av	ailable at the time the key is created. Please make a note of it.				

Step 4 — Configure Service Tables in ConnectWise

In order to export issues as tickets in ConnectWise, you will need to configure several **Service Tables** in ConnectWise. These tables ensure that the issues are "mapped" correctly to the tickets created within ConnectWise. You must configure the Service Tables correctly in order to establish the connection with ConnectWise.

You can configure the Service Tables in ConnectWise from **System > Setup Tables > Category > Service**. Configure the Service Tables as detailed below:

1. Service Board

You must have a Service Board created within ConnectWise. In addition, within the Service Board, you must create values for the following fields. You can create values for these fields from the Service Board page:

- a. Statuses
- b. Types
- c. Teams

You must create at least one value for each of these fields.



In addition, you must define values for two additional Service Tables:

2. Source

You must include at least one Source.

3. Priority

You must include at least one Priority level.

Service 🗸	<u> </u>	
Service	ConnectWise Manage Network	ConnectWise Manage Network settings.
Service	Email Connector	Folder setup for the Email Connector program
Service	Email Formats	Service Email Template setup
Service	IMAP Setup	Define IMAP configurations for Email Connector
Service	Knowledge Base	Create categories, subcategories, and change settings
Service	Priority	Priority is associated with SLAs (previously captioned Urgency)
Service	Service Board	Service Board Setup
Service	Service Sign Off	Service Sign Off Setup
Service	Severity	Service Severity and Impact
Service	SLA	Service Level Agreement setup
Service	Source	Example: Email, Phone
Service	Standard Note	Standard Note Setup
Service	Surveys - Service	Create and edit automated surveys for service tickets
Service	Ticket Template	Defines ticket templates that can be applied to tickets directly, or used to g

If your existing Service Tables already contain values for the fields listed above, you do not need to create new values.

Step 5 — Remove "Disallow Saving" Flag from Company

The final step is to ensure your companies are able to save data such as tickets. By default, your company may have the "**Disallow Saving**" option flag enabled; this will prevent you from exporting tickets to the company.

Here's how to remove the "Disallow Saving" flag:

1. Navigate to Setup Tables > Category > Company > Company Status.

Setup Tal Setup Tal			
SEARCH	CLEAF	2	
Category		Table ^	Description
Company	~		
Company		Address Formats	Address Formats
Company	5	Company Status	Example: Active, Inactive
Company		Company Type	Example: Customer, Prospect, Vendor
Company		Configuration	Types of configurations
Company		Configuration Status	Defines valid statuses to be used on the configuration screen.
Company		Country	Valid countries for addresses.

2. From Company Status, open the **not Approved** field.

Setup Tables > Comp. Company Status List	any Status List			
< + SEARCH	CLEAR			
Description	Default	Inactive	Notify	Custom Note
Active	_			
Inactive			\checkmark	
Imported			\checkmark	
Credit Hold			\checkmark	
<u>Problem</u>			\checkmark	
not-Approved	\checkmark		\checkmark	
Solid				
Attention needed			\checkmark	
<u>may Leave</u>			\checkmark	
<u>Delinquent</u>			\checkmark	

3. Uncheck the **Disallow Saving** flag.

RapidFireTools*

Setup Tables > Company Status List > Company Status Company Status	
< + 🖹 🗈 🤂 HISTORY ~ 🔳	
Company Status	
Description* not-Approved	✓ Default
	Inactive
Notification Parameters for Service, Project an	d Time
✓ Notify	
✓ Disallow Saving	
Notification Message	
Do not Service they have not been setup for Service yet check with their account manager	

Company Status	
Description* not-Approved	✓ Default
	Inactive
Notification Parameters for Service, Project a	nd Time
Votify	
Disallow Saving	
Notification Message	1
Do not Service they have not been setup for Service yet check with their account manager	

4. This will allow you to export tickets to companies with the **not Approved** status. Alternatively, you can set the company itself to a different status that allows saving before attempting the ticket export.

RapidFireTools°

	Company Search /licro Pro	> Compar	ny > Co	ompany Finar	ice Detail		
<	Summary	Recap	I	nvoices 0	Time	e O	Expenses 0
<	8	€ f	•~	History 🗸	Links	~	
	Company: Mic	ro Pro					
	Company: *	Micro Pro)				Phone:
	Company ID: *	123					Fax:
	Status: *	not-Appro	oved			\sim	🛱 Web Site:
	Туре: *						
	Prospect X						
ľ	Finance Detai	ls			¢.	Ê)	

Set Up ConnectWise SOAP Integration

This topic covers how to integrate Network Detective with ConnectWise via the ConnectWise SOAP API.

Important: The ConnectWise SOAP API is in the process of being deprecated by ConnectWise. We recommend that you use the <u>ConnectWise REST API</u> instead.

To set up the ConnectWise SOAP integration:

- 1. Navigate to System-> Setup Tables.
- 2. Type "Integrator" into the Table lookup and hit Enter.
- 3. Click the Integrator Login link.

Setup Ta Setup Ta		
SEARCH	CLEAR	
Category	Table 个	Description
	🗸 integrator	
General	Integrator Login	Setup Integrator Access

- 4. Click the "**New**" lcon to bring up the New Integrator login screen as shown on the right.
- 5. Enter and record **Username** and **Password** values which you will need later on when creating a connection in Network Detective.
- 6. Set the Access Level to "All Records."
- 7. Using the ConnectWise Enable Available APIs function, **enable the following APIs**:
 - ServiceTicketApi
 - TimeEntryApi
 - ContactApi
 - CompanyApi
 - ActivityApi
 - OpportunityApi

© 2024 RapidFire Tools, Inc. All rights reserved.

RapidFireTools°

- MemberApi
- ReportingApi
- SystemApi
- ConfigurationApi

Integra	tor Login		
Setup	Logs		
<	+ 🗄 🗄 🕂	HISTORY V 🔟	
Usern api	ame*		
Pass	vord		
	ss Level Records created by Integrat	tor O All Records	
Selec	t the available API integrati	ion(s) you wish to enable and configure below	
	API Name		
~	Activity	Callback URL	Use legacy o
	Agreement	Callback URL	Use legacy o
	Company	Callback URL	

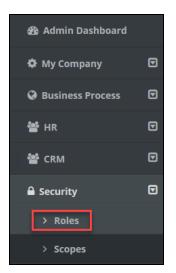
8. Click the **Save** icon to save this Integrator Login.

Note: If you already have an Integrator Login configured, you may use it as long as the Company and Configuration APIs are enabled.)

Set Up Kaseya BMS Integration

To export items to Kaseya BMS, you will need Administrator credentials in Kaseya BMS. To assign a Kaseya user to the Administrator role, follow these steps:

- 1. Log in to Kaseya BMS.
- 2. Go to **Security** > **Roles**.



3. Click **Open/Edit** on the Administrator Role.

Image: Project Manager Project Manager Image: Project Manager Service Desk Manager Image: Project Manager Service Desk Manager Image: Project Manager Administrator	ľ	CRM Manager	CRM Manager
	Ø	Project Manager	Project Manager
Image: Administrator Administrator	ľ	Service Desk Manager	Service Desk Manager
	ß	Administrator	Administrator

4. Click the **Role Users** tab.



5. Click Add.

RapidFireTools°

- 6. Search for the user to who will become a Kaseya Administrator and **Select** that user.
- 7. Click OK. This user can now invoke the Kaseya BMS API.

Data Collectors for VulScan

You can view the data collectors associated with a vulnerability scanner site from [Your Site] > **Home** > **Data Collectors**.

☆ Home	٣	Vulnerability Scanner 2	021	
Dashboard Data Collectors		Home / Data Collectors		
Users Roles		Data Collectors @)	+ Provision Vulnerability Scanner
Advanced Options	,	Internal Vulnerability Scar	ners External Vulnerability Scanners Discovery Agents	Reporter
 VulScan 		Data Collector Type:	Internal Vulnerability Scanner	
🛱 Audit Log		Data Collector ID:	IVS1-	Û
		Description:	AWS	0
		Last Check-in:	17 Jan 2023 5:54 PM GMT-05:00	
		Update Status:	up-to-date	
		Manage Data Collector:	(Data Collector Offline)	

Here you can review details regarding each data collector associated with the Site. Under **Manage Data Collector**, you can access several functions. See <u>"Manage Site Data</u> <u>Collectors" on page 203</u>.

Function of VulScan Data Collectors

Internal Vulnerability Data Collector

- In order to perform an internal vulnerability scan, you will need to provision and install an internal appliance. Install the internal appliance directly on the target network to be assessed.
- The internal scan appliance is marked with the prefix "IVS." When you create a new site, a single IVS appliance will be provisioned for the site automatically.
- You have the option to provision additional IVS appliances to a site. This allows you to break up larger scan jobs across two or more appliances that can scan parts of a large IP range simultaneously. See also <u>"Create Internal Scan Task" on page 20</u>.

External Vulnerability Data Collector

- In order to perform an external vulnerability scan, you will need to provision and install an external appliance. Install the external appliance on a SEPARATE network from the target network to be assessed. We recommend you install the external scan appliance your MSP network. You can use one external scan appliance to perform scans with several or all of our Sites.
- The external scan appliance is marked with the prefix "EVS." To assign an existing EVS appliance to a new Site, see <u>"Provision VulScan" on the next page</u>.

Portable Data Collector

• The Portable VulScan appliance can be installed on a physical device that you move from site to site. Otherwise, it functions in the same way as the internal scan appliance. See <u>"Portable VulScan Set Up" on page 228</u>.

Remote Internal Vulnerability Scanner

 The Remote Internal Vulnerability Scanner (RIVS) is installed on the MSP network. It can be shared by multiple sites for the purpose of remote scanning internal IP addresses through a proxy agent. See <u>"Set Up Remote Internal</u> <u>Vulnerability Scanner" on page 86</u>.

Provision VulScan

When you create a new VulScan site, a single data collector/appliance will be provisioned for the site automatically. However, you have the option to provision additional vulnerability scanner data collectors to a site. This allows you to break up larger scan jobs across two or more appliances that can scan parts of a large IP range simultaneously. To provision a new appliance:

- 1. Navigate to [Your Site] > Home > Data Collectors.
- 2. Click Provision Vulnerability Scanner.

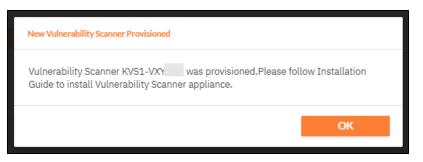
☆ Home	*	Vulnerability Scanner 2	021		
Dashboard Data Collectors		Home / Data Collectors			
Users Roles Advanced Options	,	Data Collectors @			ovision Vulnerability Scanner
 VulScan 	•	Data Collector Type:	Internal Vulnerability Scanner		
🖺 Audit Log		Data Collector ID:	IVS1-HLGB42	Û	
		Description:	AWS	Ø	
		Last Check-in:	17 Jan 2023 5:54 PM GMT-05:00		
		Update Status:	up-to-date		

3. Select whether to provision an **internal**, **external**, **portable** or **remote** vulnerability scanner. See <u>"Function of VulScan Data Collectors" on the previous page</u> for a breakdown of each appliance type.

Note: Some appliance types, such as the **external**, **portable**, and **remote** scanners, allow you to select from among existing appliances. In this way you can use one appliance to service multiple sites where you want to perform scans.

Provision New Vulnerability Scanner
Select type of vulnerability scanner to install.
Internal Vulnerability Scanner
New Internal Vulnerability Scanner
O New Remote Internal Vulnerability Scanner
Existing Remote Internal Vulnerability Scanner
·
External Vulnerability Scanner
O New External Vulnerability Scanner
O Existing External Vulnerability Scanner
EVS-FFLW76 👻
Portable Vulnerability Scanner
O Portable Vulnerability Scanner
No Yes
No Yes

4. Confirm your selection.



5. The new appliance will appear in the list of appliances.

RapidFireTools[®]

Vulnerability Scanner 202:	1		
=	Home > Data Collectors		
☆ Home ^	Data Collectors		+ Provision Vulnerability
Dashboard	Data Collector Type:	Vulnerability Scanner	
📇 Data Collectors	Data Collector ID:	KVS1-LE	
Lusers	Description:	La îi lu le lo La ii lu le lo La ii lu le lo La îi lu le lo La ii lu le lo La îi lu le lo La îi lu le lo La îi lu l	
Roles	Last Check-in:	NaN days ago	
Advanced Options	Update Status:	📀 up-to-date	
Vulnerability Scanner 🗸 🗸	Manage Data Collector:	+ Run (Beta)	
Audit Log			
	Data Collector Type:	Vulnerability Scanner	
	Data Collector ID:	KVS1-OWI	
	Description:	· · · · · · · · · · · · · · · · · · ·	
	Last Check-in:	NEVER	
	Update Status:	unknown	
	Manage Data Collector:	- (Data Collector Offline)	

- Unless you are using an existing appliance, you must then install the appliance on either the MSP or customer network, depending on the appliance type. See the <u>Virtual Appliance Installation Guide for VulScan</u> for more detailed instructions on installing the appliance on the target network.
- 7. Finally, you must create new scan tasks and assign them to the new appliances. You can then select from among the data collectors available for the site when you configure scan tasks. See <u>"Create Scan and Notification Tasks" on page 20</u>.

Manage Site Data Collectors

From the **Data Collectors** page, you can manage the available Data Collectors (also called "**appliances**") deployed for your Site.

Dashboard	Granite Dy	namics				
Data Collectors	Micro Professio	nals / Granite Dynamics	/ Home / Data Collectors			
Users Roles	Data Co	llectors ®			+ Provision	Vulnerability Sca
Advanced Options VulScan	Internal V	fulnerability Scanner	External Vulnerability Scanners	Discovery Agents		
Audit Log	Data Colle	ector Type:	nternal Vulnerability Scanner			
	Data Colle	ector ID:	VS1-YRVY83		0	
	Descriptio	in:			ø	
	Last Chec	k-in:	Vever			
	Update St	atus:	inknown			
	Manage E Collector:		Data Collector Offline)			

The **Data Collectors** page presents each "data collector" – also known as an *appliance* or *server* - deployed on the Site network. This includes data collectors for the various managed services: Cyber Hawk, Compliance Manager, Reporter, and other product types.

Note: Data Collectors may be referred to as "appliances" or "servers" throughout this document.

Important: You cannot manage the "Local Data Collector" from this menu; the Local Data Collector is used on a case-by-case basis for individual workstations that cannot be scanned remotely.

If multiple data collectors have been provisioned for a Site, they will appear one below the other.

Home Dashboard	٣	Data Collectors	D		+ Provision VL	Inerability Scanner
Data Collectors		Internal Vulnerability Scar	External Vulnerability Scanners	Discovery Agents	Reporter	
Uses Roles Advanced Options Network Detective Pro > Ovulscan > Austi Log		Data Collector Type: Data Collector ID: Description: Last Check-in: Update Status: Manage Data Collector:	Internal Vulnerability Scanner IV31- AWS 17 Jan 2023 5:54 PM GMF05:00 Upto-date (Data Collector Offline)		0	
		Data Collector Type: Data Collector ID: Description: Last Check-in: Update Status: Manage Data Collector:	Internal Vulnerability Scanner KVS1- La II lu le lo La II lu le lo 13 Jan 2023 10:37 AM GMT-05:00 up-to-date (Data Collector Offline)		0	

For each data collector, you can quickly see:

Data Collector Type	For example: Compliance Manager, Reporter, Cyber Hawk
Data Collector	Useful for troubleshooting purposes
Last check-in	Useful for troubleshooting purposes and indicates active status
Update status	Indicates whether the data collector has the latest update. In most cases the data collector should update automatically once an update becomes available.
Manager data collector	Select one of several <u>"Data Collector Commands " below</u> from the drop-down menu. If the Data Collector is not available, "Data Collector Offline" will appear.

Data Collector Commands

From a site's Data Collectors menu, you can select from one of several commands. To do this, **select the appliance and click Manage**. Choose a command and click **Run**. See the table below for details about each command.

Data Collector Type:	External Vulnerability Scanner	
Data Collector ID:	EVS-TC	Û
Description:	Not in AWS	Ø
Last Check-in:	17 Jan 2023 8:48 PM GMT-05:00	
Update Status:	📀 up-to-date	
Manage Data Collector:	Manage	

Manage Appliance EVS-TC	
Update	RUN
Set Auto-Update	RUN
Health Check	RUN
Download Logs	RUN
Manage Scans	RUN
Manage Reports	RUN
Download Audit	RUN
	Close

Update	Update the data collector to the latest version. Note that this will cancel all current scans.
Set Auto-Update	Order the data collector to automatically update itself when a new version becomes available.
Health Check	<text></text>
Download Logs	Download log files for troubleshooting purposes.

RapidFireTools*

lanage Scans	View and manag	e all scans assig	ned to th	ne applian	ce.	
	Manage Data Collector Scans - NDA1-033	I3NC				
				K	< 1 /1 > >	view 10 *
	ID \$ Assessment Name \$	Scan Type 💠	Size (MB) ¢	Start Date UTC 💠	End Date UTC \$	Status 💠
	11270906	Network Assessment (Cyber Hawk)	3.18	null 04:24:38 PM	null 04:34:22 PM	Done
	11270941	Push Deploy (ZIP)	40.74	null 04:42:15 PM	null 05:15:39 PM	Done
	11307821	Push Deploy (ZIP)	4.93	null 05:37:15 PM	null 05:48:56 PM	Done
	11411856	Network Assessment (Cyber Hawk) Push Deploy (ZIP)	3.09	null 01:21:13 PM	null 01:31:02 PM	Done
	11411057	Network Assessment (Cyber Hawk)	43.55	null 04:46:26 PM	null 04:56:15 PM	Done
	11432841	Push Deploy (ZIP)	43.22	null 04:46:26 PM	null 05:29:30 PM	Done
	Download Selected	Delete Selected Remo	ve from Queue	Cancel Selected		
						Close
					_	
	 Delete complete Remove queueo 	ed scans and the d scans	eir assoc	iated files		
Anage Reports		d scans n progress			appliance	
	Remove queued Cancel scans in Access and man	d scans n progress			appliance	
lanage Reports	Remove queue Cancel scans in	d scans n progress			appliance	
anage Reports	Remove queued Cancel scans in Access and man	d scans n progress age reports store	ed on the	Reporter		
anage Reports	Remove queued Cancel scans in Access and man	d scans n progress age reports store			10 *	
nage Reports	Remove queued Cancel scans in Access and man	d scans n progress age reports store	ed on the	Reporter 1 /66 > + view time (V/C) = 1/2020 05/53/04 PM	10 *	
inage Reports	Remove queued Cancel scans in Access and man	d scans n progress age reports store	ed on the	Reporter 1 /66 > + view time (V/C) = 1/2020 05/53/04 PM	10 *	
anage Reports	Remove queues Cancel scans in Access and man	d scans a progress age reports store Figure them : Second Asset Detail Reportdox 653997 802 Yeeds Analysis.dox 0	ed on the	Reporter 1 /65 > > > ver	10 -	
anage Reports	Remove queues Cancel scans in Access and man	Asset Deter Risk Report Korce Corce	ed on the Steteme Daries Ste 46/1 Daries Ste 46/1 Daries Ste 46/1 Daries Ste 46/1 Daries Ste 46/1	Constant and the second s	10 *	
nage Reports	Remove queues Cancel scans in Access and man	Ages cans a progress age reports store Report News 2 Asses Data Data Deports Store Report News 2 Store	ed on the	Reporter (16 > x) view (16 > x) (16 > x)		
nage Reports	Remove queues Cancel scans in Access and man	Asset Deter Risk Report Korce Corce	Correction C	Constant and the second s	10 °	
nage Reports	Remove queues Cancel scans in Access and man	A scans progress age reports store scale reports store scale file file file file Asset Schal file for the BRP PowerPrintigs 000 Heeds Analysis doc 100 Heeds Ana	ed on the state state or paries Site 04/1 Darries Site 04/1	Constant of the second se		
nage Reports	Remove queues Cancel scans in Access and man	A scans progress age reports store scalar sc	State Neurol Creat Darrion Site 04/1	Reporter /60 > 2 /40 /00 > 2 /40 //00 > 2 /40 //00 > 2 /40 //		
anage Reports	Remove queues Cancel scans in Access and man	A scans progress age reports store sace and monotice sace and mono	State Neurol Creat Darrion Site 04/1	Constant of the second se		
anage Reports	Remove queues Cancel scans in Access and man	A scans progress age reports store sace and monotice sace and mono	State Neurol Creat Darrion State 04/1	Constant of the second se		
anage Reports	Remove queues Cancel scans in Access and man	A scans progress age reports store sace and monotice sace and mono	State Neurol Creat Darrion State 04/1	Constant of the second se		
hage Reports of the former only (Remove queues Cancel scans in Access and man	A scans a progress age reports store scalar Aserbraitaportadox 68399 807 Need-Andyikadox 0 108 Need-Andyikadox 0 108 Need-Andyikadox 0 108 Need-Andyikadox 0 108 Need-Andyikadox 0 109 Need-Andyikadox	ed on the set of the or or Darrien Site 04/1 Darrien Site 04/1	Constant of the second se		

Enable Discovery Agents for Local Data Collection (VulScan)

The **Discovery Agent** for VulScan is a lightweight, streamlined option for collecting local data from specific network devices. You manage agents at the organization level, where they generate local scan files that are passed to your site via a secure connection. The Agent compares local data, such as the device's application inventory and OS, with the CVE catalog to identify additional vulnerabilities.

You can install any number of Agents for an organization, where they will perform local scans on the days of the week you designate. Finally, you can combine Discovery Agents with the other VulScan data collectors to customize your IT assessment for your exact purpose.

While the agent doesn't replace the internal and external VulScan appliances, it can give you a more detailed security picture for the devices where it is deployed.

Follow the steps below to enable Discovery Agents for your site and use them to perform local scans:

Discovery Agent Firewall Requirements

IT admins and end customers using RapidFire Tools products should configure the firewall rules on their networks to enable access to the following RapidFire Tools URLs.

- gatekeeper.rapidfiretools.com
- go.rapidfiretools.com
- au.rapidfiretools.com
- go-eu.rapidfiretools.com
- go-au.rapidfiretools.com
- wcflb.rapidfiretools.com
- wcflb-eu.rapidfiretools.com
- wcflb-au.rapidfiretools.com
- api.ndglue.com
- networkdetective.s3.amazonaws.com
- download.rapidfiretools.com

The RapidFire Tools Server and Discovery Agent requires access to port 443.

RapidFireTools[®]

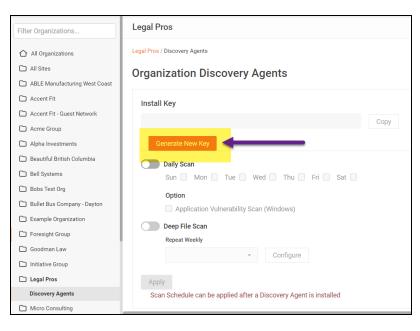
Step 1 — Enable Discovery Agents at the Organization Level

- 1. Log into the RapidFire Tools Portal and access the VulScan org where you want to deploy Discovery Agents. This should be the same org that contains your VulScan sites that will employ the agents.
- 2. Click Discovery Agents.

Note: The organization must contain at least one site for you to access to Discovery Agents.

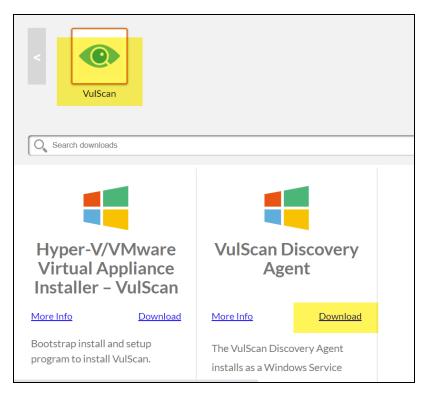
nitiative Grou	IP		
Sites		Discovery Agents	Move Site + Add Site
All 6	Compliance Manager GRC 1	Network Detective Pro 3	VulScan 2
Search keywords	ŝ		2 of 2 Results
Site ≑		Organization ≑	
Apogee Group		Initiative Group	
Apogee System	ns	Initiative Group	

3. Click **Generate New Key**. **Copy the key** to your clipboard. You will use this key to authenticate the Agent to your organization.



Step 2 — Install Windows Discovery Agent on PC on target network

1. Download the Discovery Agent from https://www.rapidfiretools.com/vs-downloads.



- 2. Open the app, proceed through the setup prompts, and click Install.
- 3. Confirm that you want to allow the Discovery Agent to make changes to your device. Once you finish the wizard, the Discovery Agents Installer will open.
- 4. Enter the install key that you generated in the previous step. Also enter a "label" to help you identify the device on which the agent is installed. You will later use the label to import the correct scan data into your assessment projects.

🔍 Disc	covery Agent Installer x
	Step 1: Enter Install Key
	Enter the Install Key for this Installation
	1c1b5355-5b78
	Enter a comment to help identify this computer (optional)
	Work laptop
	Enter a "label" to make it easier to select and use Discovery Agents (optional)
	Goodman Law
	Continue
	Privacy Policy Terms of Service

Finally, enter an optional comment to help identify the PC hosting the Agent.

5. Next, **Confirm** the site and key details for the Discovery Agent.

Q	Discovery Agent I	nstaller		x
		Confirm Install ack again if the Install Key i	-	
	Install Key: Account Site Name: Comment Label:	1c1b5355 @D3M201103 Goodman Law Work laptop Goodman Law	Back Confirm	
			Privacy Policy Terms of Se	vice

6. The installer will begin registering the Agent for your organization.

٩	Discovery Agent In	staller		x
	Step 3: I Registering Ag	nstall ent with your site		
	Site Key: Account Site Name: Comment Agent ID:	098e 190b-a06e-4c9c- PERF AgentTesting D <pending></pending>		
			Privacy Policy	Terms of Service

7. Click Finish when complete.

٩	Discovery Agent In	staller		×
	Step 3: I			
	Site Key: Account Site Name: Comment Agent ID:	098e 190b PER Agent Testing AGT-49	Finish	
			Privacy Policy Terms of	Service

Step 3 — Confirm Discovery Agent install from your Organization

- 1. Once you've installed the Agent(s) on the target network, return to the portal and navigate to [Your Organization] > Discovery Agents.
- 2. Under installed Discovery Agents, you will see the new Agent.
- 3. The appliance status will appear as green once the Agent checks in with the

RapidFireTools[®]

RapidFire Tools Portal.

Filter Organizations	Organization Discovery Agents
All Organizations All Sites ABLE Manufacturing West Coast Accent Fit	Install Key af Sa4TH (S109-559-8024- Copy Regenerate
Accent Fit - Guest Network Acres Goop Apple Annee Goop Bell Systems Boos Fet Og Utile Bus Company - Dayton Exemple Organization	Sun 12 Mon 2 Tue 2 Wed 1 The 2 Fri 2 Sat 12 Option Application Whenshilly Scan (Windown) Deep Fiel Scan Repart Weeky Configure
Foresight Group Goodman Law Initiative Group Legal Pros Micro Consulting Micro Consulting Micro Porfessionals	Rear. Image: Computer * Last Scan Discovery Agent ID * Comment * Label * Update Status * Last Check in * • K.APW 19-8pp-2022, 10:16 AM AGT522L52 MacOS MacOS Endpoint up-to-date 19-8pp-2022, 229 FM C
Nacho Town USA	KNYYYY 1996/2222, 10.16 MW NU192032 W8003 CHIDOBIE UP1008EE 1996/2222, 2.39 YW 2 U 2023 09.19 0022 2023 09.19 0022

Step 4 — (Optional) Enable Access for Site Admin and Technician Users

Next, you can optionally enable your Site Admin and Technician users to manage the Discovery Agents that you deploy. You can do this in two ways:

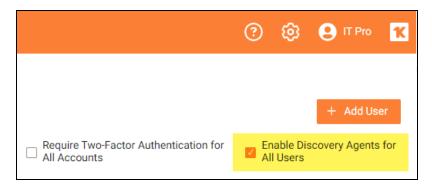
1. From your site, access **Roles**. Next to your Site Admin and/or Technician users, **turn on the slider**. These users can then access and manage Discovery Agents for the organization that contains the site.

Home / Roles			
Roles			
Site Admin	+ Add User	Technician	+ Add User
joe-admin-user@rapidfiretools.com	D	wgibson@microconsulting.com	1
mc-admin@microconsulting.com	D		
fkafka@microconsulting.com	D		

2. Alternatively, if you want to enable access to Discovery Agents for all Site Admin

and/or Technician Users in the portal, navigate to global **Settings (Admin)** > **Users**. From the top-right page, select **Enable Discovery Agents for All Users**. All site-restricted Site Admin and Technician users can then manage Discovery

Agents for their assigned organizations and sites.

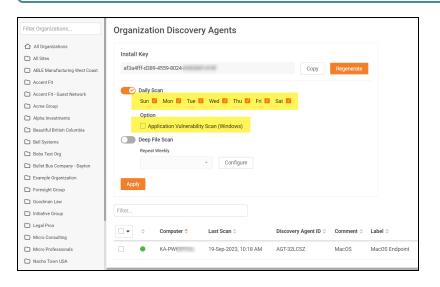


Step 5 — Schedule Scans for Discovery Agent

Before you can collect data using the Discovery Agent, you must first schedule scans.

- 1. From the RapidFire Tools Portal, navigate to [Your Org] > Discovery Agents.
- 2. From **Scan Schedule**, select one or more days of the week for the agent(s) to perform scans. Then click **Apply**.
- 3. You can optionally enable the **Application Vulnerability Scan for Windows**. This scan will detect unpatched applications installed on the device and will generate patch-related vulnerability issues for your review. The scan analyzes the latest version of installed apps and does not detect backporting. See also <u>"Application</u> Vulnerability Scan for Windows" on page 219.

Note: The **Deep File Scan** is only used by Compliance Manager GRC at this time.



RapidFireTools[®]

Note: To avoid disruption during normal business hours, Agent scans begin at 2:00am on the selected days for the Time Zone that you set from global
Settings (Admin) > General > Time Zone. See also <u>"Set Time Zone" on page 142</u>.

Step 6 — Assign Labels to Agents

If you didn't assign a label to your agent(s), be sure to do so now. To assign labels to agents:

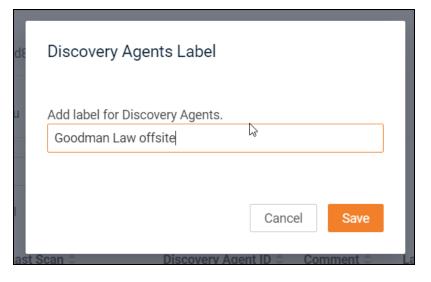
- 1. Navigate to [Your Organization] > Discovery Agents.
- 2. Select the agents where you want to add or edit labels.

	Option Application Vulnerability Scan (Windows) Deep File Scan				
	Repeat	Weekly	• Configure		
Appl	У Ф	Computer 🗢	Last Scan 🔶	Discovery Agent ID 🗇	Comment ⇔
 	•	DESKTOP-	19-Sep-2023, 4:18 PM	AGT-23	10.200.1.140
	•	DESKTOP-	19-Sep-2023, 4:18 PM	AGT-76	DevTest Network VulScan Agent
Showing 1	I - 2 of 2	2 Items			

3. Click the Select All button, and then click Update Label.

Con	nputer ≑	Last Scan 🗢	Discovery Agent ID \diamondsuit	Comment \$	Label ≑
1 Selected	w	03-Feb-2023, 3:02 PM	AGT-37B	Work laptop	Goodman Law
Run Scan Now					
Update Now					
Cancel Scans					
Remove Agents					
Update Comment					
Update Label 🖑					

4. Enter your label and click Save.



5. The label will be updated for the select agent(s).

10	•	rows pe	er page 1	of 1 K	< > >		
	•	\$	Computer ≑	Last Scan ≑	Discovery Agent ID \diamondsuit	Comment \$	Label \$
]	•	KA- PW	NEVER	AGT-01A	work laptop	Goodman Law offsite

Step 7 — Configure VulScan Agent Imports

Once you set up Discovery Agents, you can configure your VulScan site to import scan data from your deployed agents. Accomplish this by assigning the appropriate labels to pull the correct agent scan data into your site.

- 1. Navigate to VulScan > Settings > General.
- 2. Scroll down to Discovery Agents Scan Data Import Configuration.

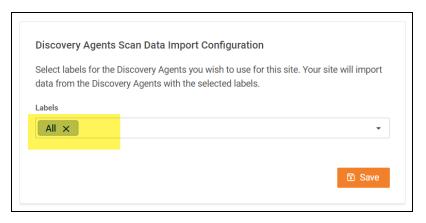
A 11-11-1	Þ	
VulScan	*	Default Matching Rule ⑦
Dashboard		Condition
Scan Results		
Settings	*	All selected attributes must match
Overview		Select attributes (must select at least 1 attribute):
General		MAC Address
Report Preference	s	Hostname IP Address
Scan Credentials		
Custom Scan Prof	iles	🖺 Save
Scan and Notificat	tion Tasks	
Exclusion Rules		
IT Complete		
🛱 Audit Log		Discovery Agents Scan Data Import Configuration
_		Labels
		-
		Foresight on premise devices

- From Labels, select the labels that designate the agents you wish to use for this site. You must have first created labels for your agents. See <u>"Step 6 Assign Labels to Agents" on page 214</u>.
- 4. Then click **Save**. Your VulScan site will then import scan data from the labeled agents. See <u>"How Scan Data Import Configuration Works" below</u>.

How Scan Data Import Configuration Works

When you configure VulScan Agent imports, here is what will happen:

• By default, the **All** label is applied. This will import scans from **all Agents**, both with and without labels.



• If you leave the selector field **blank**, scans will be imported only from agents with **NO label**.

Discovery Agents Scan Data Import Configuration				
Select labels for the Discovery Agents you wish to use for this site. Your site will import data from the Discovery Agents with the selected labels.				
Labels				
	•			
	🕄 Save			

• When you select **exact labels**, only scans from agents with the **assigned labels** will be imported.

Discovery Ag	ents Scan D	ata Import Config	uration		
Select labels for the Discovery Agents you wish to use for this site. Your site will import					
data from the I	Discovery Ager	nts with the selected	labels.		
Labels					
Micro Pro	× H3 ×	FirstInstallation	×	•	
				🕄 Save	

Remove Discovery Agents

To remove Discovery Agents:

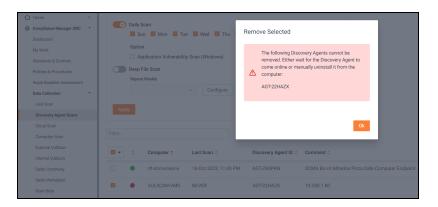
- 1. Access the Organization Discovery Agent page and ensure that the Discovery Agent to be removed is online. You cannot remove an Organization Discovery Agent that is offline.
- 2. **Select the checkbox** on the left of the Discovery Agent Appliance ID that is to be removed.
- 3. Select the **Remove Agents** menu option.

RapidFireTools[°]

Option	n Vulnerabilit	y Scan (Windows)						
Deep File Sca Repeat Weekly		- Configure						
ilter								
🕈 💠 Com	puter ≑	Last Scan 💠	Discovery Agent ID 💠	Comment \Rightarrow	Label 🗘	Update Status	🗧 Last Check-in 🗘	
	puter 🗢	Last Scan 0	Discovery Agent ID AGT-29GPKN	Comment ¢ DCMA BU of Alfredos Pizza Cafe Computer Endpoint	Label 🗘	Update Status up-to-date	Last Check-in ⇒ 19-Oct-2023, 3:09 PM	/ 8
Selected	-							ℓ€

- 4. The Discovery Agent will be removed from the Organization Discovery Agent Page.
- 5. Finally, uninstall the Discovery Agent app from the device. See also <u>"Uninstall Script</u> for Discovery Agent" on page 227.

You cannot remove an Organization Discovery Agent that is offline; you will receive the error message pictured below.



Application Vulnerability Scan for Windows

If you have deployed Discovery Agents for VulScan, enable the **Application Vulnerability Scan for Windows** to detect unpatched applications installed on endpoints. VulScan will then generate patch-related vulnerability issues for your review. The scan analyzes the latest version of installed apps and does not detect backporting.

Follow these steps to enable Application Vulnerability Scanning for Windows:

Step 1 — Deploy Discovery Agents on Endpoints

First, install Discovery Agents on each endpoint that you want to scan. See <u>"Enable</u> <u>Discovery Agents for Local Data Collection (VulScan)</u>" on page 207 for complete instructions.

Step 2 — Enable Application Vulnerability Scan for Windows for Discovery Agents

- 1. From your Organization, navigate to Discovery Agents.
- 2. From the Organization Discovery Agents scan settings, enable **Application Vulnerability Scanning (Windows)**.

Organizatio	on Discover	y Agents			
Install Key					
18dd8286-c9ef	f-42c6-9409-effb1b	77e543		Copy	
Daily Sc Sun Option Apply	Mon Tue	e Wed Thu y Scan (Windows)	🕻 Fri 🕻 Sat		
Filter					
÷	Computer ≑	Last Scan ≑	Discovery Agent ID \updownarrow	Comment ≑	Label ≑
	DESKTOP-	09/10/2023, 2:02 AM	AGT-23	10.200.1.140	10.200.1.140

RapidFireTools°

Step 3 — Review Application Vulnerabilities

Once you enable application vulnerability scanning, VulScan will generate notifications regarding unpatched applications. You can review these from **VulScan** > **Scan Results**.

an Resu By Issue	By Device			
Scan Date R	ange: Last 30 Days	~ Cr	itical	🛓 Generate Reports
CVSS	Filter: All	·	gh	
Scan	Type: Discovery Agent	- 8 MM	edium	
Quick	Filter:			
	CISA's Known	Exploited Vulnerabilities	one	Mark Selected as False Positive
s	Severity/CVSS 😄	Issue \Rightarrow	Affected Nodes \updownarrow	Last Detected $\ensuremath{\hat{\phi}}$
6	1.5	Google Chrome Medium Risk Vulnerability (CVE-2013-6662) DID: b925d5824d39716d13931917075b1558dr3ad72458bbd8888ee46bd7d92223bb CVE: CVE-2013-6662	6	09/20/2023 05:25:22 PM
4	1.3	Google Ohrome Medium Risk Vulnerability (CVE-2023-4901) 010: bb2c625070/f51d9452x295/f5b27ca90b6eca92118eb3ade401d8164835c86a32 CVE: CVE-2023-4901	4	09/20/2023 05:25:22 PM
7	.5	Zoom High Reik Vulnerability (CVE-2023-22881) OID: 457084317b668844befa8da3549f6a1641dead8df88ebe67e9889bbca44e6f1a CVE: CVE-2023-22881	2	09/20/2023 05:25:22 PM
7	.5	Zoom High Risk Vulnerability (CVE-2023-22882) OID: Scub lafbc302111a5273ac6691de91455988dd5ae78068b6f89b3e994b73263b CVE: CVE-2023-22882	2	09/20/2023 05:25:22 PM

Install Linux and macOS Discovery Agents

The help topic below demonstrates how to use scripts to deploy the Discovery Agent on Linux and macOS devices.

First, <u>"Find and Copy Install Key for Discovery Agents" below</u>. Then, run the install using the scripts below for Linux or macOS devices:

- "Default Scripted Linux Install" on the next page
- "Default Scripted macOS Install" on page 223

Find and Copy Install Key for Discovery Agents

In order to deploy the Agent with the scripts below, you will first need the **Install Key** for the Discovery Agent.

1. First, find and copy the **Install Key**. From the Organization where you wish to deploy the agent, click **Discovery Agents**.

Organizations			@ Ø	e IT Pro K
Sites		Discovery Agents	Move Site	+ Add Site
All 89 Compliance Manager GRC 35	Cyber Hawk 3 Network Detective	Pro 32 VulScan 19		
Search keywords	A	I Site Types	~	89 of 89 Results
Site ≑	Organization \doteqdot	Site Type 🔶	To Do	÷
Acme GRC Project	123	0		
Dynamic Medical Systems	123	8		
Ghost Technologies	123	8		
Granite Dynamics	123	8		
Macro Solutions	123	8		
Micro Solutions	123	0		

2. Generate and copy the Install Key. The exact Install Key should be inserted in

place of the <install_key> tag in the scripts below.

Bell Systems							
Bell Systems / Discovery Agents							
Organization Discovery Agents							
Install Key							
ebbb74a6-2b25-41f2-9b6a-4333	Copy Regenerate						
Daily Scan							
Option Application Vulnerability Scan (Windows)							
Deep File Scan							
Repeat Weekly							
✓ Configure							

Default Scripted Linux Install

Note: Commands must be executed by a user with super user privileges (i.e., root) or using the 'sudo' command.

curl -0

```
https://download.rapidfiretools.com/download/discoveryagent-
install-linux.tar.gz
```

```
tar zxf discoveryagent-install-linux.tar.gz
```

```
./discoveryagent-install-linux --install
```

```
/opt/discoveryagent/discoveryagent -register -installkey
<install key> -comment "my comment" -label "my label"
```

Note: Do not use the < and > characters when you enter the install key. For the optional comment and label, only use quotation marks if your entry is two or more words.

		System Requirements
Har	dware	Less than 20 MB disk space

	System Requirements				
Software	 Linux Operating System that employs Systemd (system daemon) for service management. (Note that most modern Linux distributions employ this method by default.) YUM, APT, or ZIPPY installed for package management. .NET 6.0 Runtime The following software packages. (The app will install these packages if they are not already present.) o curl o unzip 				
Other	Install Key for Discovery Agent.				
prereqs					

Default Scripted macOS Install

Before you can install a macOS Discovery Agent, you must first install the correct .NET 6.0 Runtime version on the target device. To do this:

- 1. Identify the chip type used on the target macOS device (**ARM64** or **x64**). <u>Refer to</u> this guide to for help determining the chip type for your macOS device.
 - Mac computers with an Apple chip (M1, M2, or M3) use the **ARM64** architecture.
 - Mac computers with an Intel chip use the x64 architecture.
- 2. Ensure the correct version of .Net 6.0 Runtime (ARM64 or x64) is installed on the target device. See <u>Download .NET 6.0</u> for the ARM64 and x64 versions of .NET 6.0 Runtime.

Note: Commands must be executed by a user with super user privileges (i.e., root) or using the 'sudo' command.

```
curl -0
https://download.rapidfiretools.com/download/discoveryagent-
install-osx.tar.gz
```

tar zxf discoveryagent-install-osx.tar.gz

```
./discoveryagent-install-osx --install
```

```
/opt/discoveryagent/discoveryagent -register -installkey
<install_key> -comment "my comment" -label "my label"
```

Note: Do not use the < and > characters when you enter the install key. For the optional comment and label, only use quotation marks if your entry is two or more words.

	System Requirements				
Hardware	Less than 20 MB disk space				
Software	 macOS 10.15 "Catalina" or higher .NET 6.0 Runtime (ARM64 or x64) The following software packages. (The app will install these packages if they are not already present.) o curl o unzip 				
Other	Install Key for Discovery Agent.				
prereqs					

Install Script Options

```
Note: Replace discoveryagent-install-linux with discoveryagent-install-osx on macOS.
```

./discoveryagent-install-linux --help

Syntax: discoveryagent-install-linux [command] [options]

commands:

--version|-v

--help|-h

```
--check-prereqs|-c
```

```
--install-missing-pkgs
```

Note: --install will do this automatically. Only use this option to install the pkgs without doing the full install.

--download-bundle

--url [url]

Overrides the URL used for downloading the install bundle.

--install

--install-dir [install dir]

Defaults to /opt/discoveryagent

--url [url]

Overrides the URL used for downloading the install bundle.

--bundle [install bundle zip file]

Use an install bundle already on the local machine.

```
--verify-install
```

--uninstall

Options:

--force

Non-interactive mode. Does not prompt for confirmation.

RapidFireTools[®]

Silent Install for Discovery Agent (Windows)

Use the commands below in a batch file, Powershell Script, or similar, to perform a silent install for the Discovery Agent. You can combine these commands with others you may use for your agent deployments.

1. First, find and copy the **Install Key**. From the Organization where you wish to deploy the agent, click **Discovery Agents**.

Organizations			@ @	e IT Pro 🕻
Sites All 89 Compliance Manager GRC 35 C	yber Hawk 3 Network Detecti	Discovery Agents	Move Site	+ Add Site
Search keywords		All Site Types	~	89 of 89 Results
Site ≑	Organization \Rightarrow	Site Type 🔶	To De	¢.
Acme GRC Project	123			
Dynamic Medical Systems	123	8		
Ghost Technologies	123	8		
Granite Dynamics	123	0		
Macro Solutions	123	⊗		
Micro Solutions	123	0		

2. Generate and copy the Install Key.

Bell Systems						
Bell Systems / Discovery Agents						
Organization Discovery Agents						
Install Key						
ebbb74a6-2b25-41f2-9b6a-4333	Сору	Regenerate				
Daily Scan						
Option Application Vulnerability Scan (Windows)						
Deep File Scan Repeat Weekly						
✓ Configure						

- 3. Next, download the agent on the target device. You can use this URL: https://download.rapidfiretools.com/download/DiscoveryAgent.msi
- 4. Save the agent installer in the same location where you will run the batch file.
- 5. Next, use the following two commands. Replace <your key> with the value for the Install Key that you copied earlier.

To install the agent:

msiexec /qn /i DiscoveryAgent.msi /L*V install-silent.log

To bind the agent to your site:

"C:\Program Files (x86)\DiscoveryAgent\Agent\bin\registerdevice.exe" -installkey <your key> (without the <>)

You can also append a label and comment to the command above. Example:

```
"C:\Program Files (x86)\DiscoveryAgent\Agent\bin\register-
device.exe" -installkey <your key> -label "Your Label" -
comment "Your Comment" (without the <>)
```

Uninstall Script for Discovery Agent

Use the command below to uninstall Discovery Agents:

Important: This command will not remove the Agent from appearing in the RapidFire Tools Portal. If you wish to uninstall an Agent, we recommend that you first remove it from the Portal. While the Agent is online, use the **Remove Agents** option from **[Your Organization]** > **Discovery Agents**, then run the command below on the device that hosts the agent. See the "Enable Discovery Agents" topic for a complete walkthrough.

msiexec /x DiscoveryAgent.msi /L*V uninstall-silent.log

Portable VulScan Set Up

The **Portable VulScan (PVS)** appliance allows you to use one scan appliance to assess multiple VulScan Sites. This is especially useful if you want to deploy VulScan from a physical device that you move from site to site. In this way, you can perform internal vulnerability scans for multiple sites without using up your allotment of VulScan site licenses.

Portable VulScan differs from the standard VulScan appliance only in the ability to move PVS between sites. Once you assign a PVS to a site, you will configure internal scan and notification tasks exactly the same way.

This topic presents the workflow for using PVS to perform internal vulnerability scans for your sites.

Step 1 — Provision Portable VulScan Appliance

Contact your RapidFire Tools account representative to provision a Portable VulScan appliance.

Step 2 — Install Portable VulScan Appliance on target Network

Next, you need to install the PVS appliance on your chosen device. Download the appliance installer and refer to the installation guide at <u>https://www.rapidfiretools.com/vs-downloads</u>.

During the install process, be sure to select **Portable VulScan appliance** from the available VulScan appliance types.

😫 Vulnerability Scanner Installer - v20	121.10.08.01 — 🗆 X
✔Install Target	Scanner Type
✓ Requirements (Hyper-V)	Scanner Type
✓ RapidFire Tools Credentials	Internal Vulnerability Scanner Internal Vulnerability Scanners are assigned to single sites for the purpose of scanning an internal network.
Scanner Type	C External Vulnerability Scanner
Appliance ID	External Wuhrenbillty Scanners can be shared by multiple sites for the purpose of scanning external facing IP Addresses only. Please assure the External Vulnerability Scanner is not installed on the same network that is to be scanned.
Download VMs	Portable Vulnerability Scanner Portable Vulnerability Scanners are assigned to single sites for the purpose of scanning an internal network.
Install Folder	Fortable vulnerability ocariners are assigned to single sites for the purpose of scanning an internal network.
Virtual Switches	

Step 3 — Create VulScan Site and opt not to provision appliance

While you can use Portable VulScan with your existing sites, you can also create VulScan "shell" sites to use with PVS without consuming your VulScan licenses. To do this:

- 1. From the RapidFire Tools Portal, click Add Site and create a new VulScan Site.
- 2. Before you finish creating the site, select "**No**" when prompted to provision a new internal VulScan appliance for the site.

Add Site	
Automatically provision Internal Vu Ves No	Inerability Scanner for the new site?
You are about to create a n against your licensed total.	ew VulScan site. This site will count
	Back Confirm

Step 4 — Assign Portable VulScan Appliance to Site

Next, connect the PVS appliance to the target network. It must have internet access to check in and become available to assign to your site. Then assign the Portable VulScan appliance to your site.

1. From [Your VulScan Site] > Home > Data Collectors, click Provision Vulnerability Scanner.



2. Select **Portable Vulnerability Scanner**. Then choose the **PVS appliance ID** from the drop-down menu and then **Confirm**.

Provison No	ew Vulnerability Scanner		
Select typ	e of vulnerability scanner to insta	Ш.	
O Ne	w Internal Vulnerability Scanner		
O Ne	w External Vulnerability Scanner		
🔵 Exi	sting External Vulnerability Scanner		
	EVS-FTTJ71		Ŧ
• Poi	table Vulnerability Scanner		
	PVS-GWSK25		•
	PVS-GWSK25		
		Yes	No

The PVS appliance will appear under the site Data Collectors.

Step 5 — Set Up and Perform Internal Scan and Notification Tasks

Once you install the appliance and it appears online, configure internal scan and notification tasks in exactly the same way you would with the standard internal scan appliance. See:

- "Create Internal Scan Task" on page 20
- "Create Notification Tasks" on page 30
- https://www.rapidfiretools.com/vs-downloads

Step 6 — Remove PVS appliance from Site

Once you perform one or more internal scans for your site and are satisfied with the results, you can remove the PVS appliance from the site and deploy it elsewhere. To do this:

- 1. Navigate to [Your VulScan Site] > Home > Data Collectors.
- 2. Next to the PVS appliance, click the trash icon. Confirm that you wish to remove the appliance.

Data Collector Type:	Portable Vulnerability Scanner
Data Collector ID:	PVS-BT
Description:	The only true PVS on this Site
Last Check-in:	13 Oct 2021 5:59 PM GMT-04:00
Update Status:	🕏 up-to-date
Manage Data Collector:	• Run

- 3. When you remove a PVS appliance from a VulScan Site, the following will occur:
 - Your current and queued scan jobs and notification tasks for PVS will be removed for the Site
 - The internal vulnerability and other scan data will remain and can be reviewed from the Scan Results dashboard
 - The removed PVS appliance will become available to be assign to another VulScan Site

Step 7 — Assign PVS appliance to new VulScan Site

Now you're ready to move your Portable VulScan appliance to a new site to continue your internal scanning! See <u>"Step 4 — Assign Portable VulScan Appliance to Site" on</u> page 229.

Enable Global Two-Factor Authentication (2FA) for Portal Users

Step 1 — Master user enables 2FA for all portal users

First, the user in the "Master" admin role – usually the user who initially provisions and first accesses the account – must enable global 2FA from the RFT portal global settings.

To do this:

- 1. Access the portal as the **Master admin**. Check with your team or Kaseya Account Representative if you're uncertain which user has been assigned this role.
- 2. After login, navigate to global **Settings (Admin)** > **Users**.
- 3. From the **Users** panel, click **Require Two-Factor Authentication for All Accounts** from the right page.

Micro Consulting		Organizations				?	ම	IT Pro	ĸ
 General Branding 		Global Settings / Users							
 Connections 		Users ⑦						+ Add Us	er
Admin Alerts		Search	Q All	- 🖬 Re	equire Two-Factor uthentication for All Accou	ints	Enabl	le Discovery Aç I Users	jents
Compliance Manager GRC	Þ	Username 🗢	Display Name 🗘	Global Access Level \diamondsuit	Site Level Access \Rightarrow	2FA ‡			
 VulScan Service Plans 	ь 	atech@zephyr-pros.com	A Tech	Site Restricted	Zephyr Pros (Internal Auditor)	No		0	Ì
ଟ Email Groups		billfoyers@itsolutions.com	Bill Foyers	Site Restricted	Salient Industries (Reports Viewer)	Yes		0 1	1
 IT Complete License Usage API Keys 	•	btech@zephyr-pros.com	B Tech	Site Restricted	Zephyr Pros (Subject Matter Expert)	No		0	1
		bv-admin@microsolutions.com	BV	Admin	Al-Tota Voltan Davidson Alexan Nacional Alexan Nacional Alexan	No		2024.02.27	∎ -1904

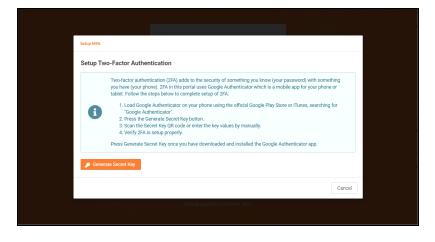
Note: Site Admins, as well as Global Admin and Master users, must configure 2FA regardless of this setting.

Step 2 — Portal user logs in and sets up 2FA Access

Once the Master admin enables global 2FA, other portal users follow these steps.

Note: You will require a **mobile device** and the **Google Authenticator** app to complete this process.

- 1. Access the Portal and log in.
- 2. You will be prompted to set up 2FA. Click Generate Secret Key.



Note: If you have not done so already, download and install the Google Authenticator app on your mobile device.

- 3. From the app, click + to add a new 2FA account.
- 4. Select **QR code**, and use your mobile device to scan the QR code that appears in the Portal.

Setup MFA	
Setup Tw	vo-Factor Authentication
Secret Key (T MJ5HF22	ext) 2VLBCDMNZ22MQJQEXKZPDOTRXD
	Using the Google Authenticator app, enter for the latest login code. The code will change periodically. If the code has changed, simply re-enter the code and press Verify again. Two-factor authentication will not be enabled until verification is complete.
G	
Login Code	

5. A setup confirmation modal will appear. Click OK.

Setup Two-Factor Authentication (2FA) has been enabled. You will be asked to provide a code every time you login, and to disable ZFA in the future.	Setup MFA		
to disable 2FA in the future.	Setup Two-Facto	r Authentication	
Patrovid Europa Passances?	Two-Fail to disab	ctor Authentication (2FA) has been enabled. You will be asked to pro le 2FA in the future.	ovide a code every time you login, and
			ок
Log in Or Cog in with IT Complete			
Or			
C Log in with IT Complete			

Step 3 — Portal Users enter Authentication Code after initial login

Once both the Master admin and individual portal users enable 2FA access, **all portal users must enter a one-time Authentication Code to access the Portal**. In this way, you can greatly enhance the security of the portal experience for all users.

Verification Liter the current code from the Google Authentication application. Muthematication Code Verify	
Help.& Support © Kaseya 2022	

Import IT Glue Organizations

You can import your IT Glue organizations directly into the RapidFire Tools Portal. This streamlines the process of onboarding IT Glue users who wish to leverage the RFT Portal's suite of IT and compliance assessment offerings.

Likewise, you can optionally synchronize your IT Glue org names with the imported orgs in the RFT Portal. Whenever you change the name of an org in ITGlue, that change will be reflected in the RFT Portal.

Note: You must subscribe to IT Glue Enterprise to access this feature.

Here's how to enable this feature:

Step 1 — Create and Copy API Key in IT Glue

First, you need to set up an API Key in IT Glue.

1. Create one or more **Organizations** in IT Glue. You will later select one of these orgs to send your data to the right place. You create new Organizations from the **Organizations** tab in IT Glue.

Dashboard Organizati	ons My Tasks Global	Account	Q Search	0 -	- 1
Organizations					
 Recents 				📩 Import	+ New
SR					
Sandbox RFT					
Sandbox RFT					

2. Create an IT Glue API Key for your use during integration and set up. You can do this from **Account > API Keys**.

Das	shboard	Organiz	ations	My Tasks	Global	Account				
A	ccount									
	Sett	ings	6							
	Gener	al	Brandi	ing	Authentic	ation	API Ke	ys	Theme	

RapidFireTools[®]

Custom API Keys					1	
The IT Glue API is a RESTful A	API that can be used to manage and retrieve info	ormation. Learn more			1	
rft_	ITG.614	Revoke	Password Access	-	l	
kreed_	ITG.0d6	Revoke	Password Access	-	l	
rft_	ITG.2eb	Revoke	Password Access	-	l	
Enter Name		Generate API Key	Password Access	-	l	
		_		+	l	
Important	For your reference	e, save a c	opy of the A	PIk	ey outside	e of IT Glu

- Step 2 Enable Connection to IT Glue from Portal Global Settings
 - 1. Next, from the RapidFire Tools Portal, navigate to global **Settings (Admin)** > **Connections**.
 - 2. From Your Connections, click Add.

Organizations				@ @	9 IT F	Pro 1
obal Settings / Connections						
onnections ③						
our Connections			_			- Add
Name ≑	Туре ≑	Login ≑				
Migration Connection for rapidfire_c	ConnectWise REST	101101-0017018			b	1
IT Glue	IT Glue	*****	Set Up Organizations	Sync Now	00 🖉	1
IT Glue	IT Glue	*****	Set Up Organizations	Sync Now	00 🖉	1
IT Glue	IT Glue	*****	Set Up Organizations	Sync Now	00 🖉	•
Datto Unified Continuity	Datto Unified Continuity	1011			b	1
Dark Web ID	Dark Web ID	1			6	•
BMS HIPAA	Kaseya BMS				2024.02	2.27-1904 D

3. Select IT Glue from the drop-down menu and enter the API Key.

4. Click Test Login.

Add Connection
API Key to get started.
 Additional setup may be necessary to configure the API user in the specific ticketing system. Please refer to the configuration documentation.
Connection Type *
– Choose Connection Type – 🗸 👻
Autotask
ConnectWise
ConnectWise REST
IT Glue
Kaseya BMS
TigerPaw
Cancel Test Login

RapidFireTools*

s/Connections	Add Connection	
nection	Organizations with ongoing updates. Enter an IT Glue API Key to get started.	
AA Conno Dings	Additional setup may be necessary to configure the API user in the specific ticketing system. Please refer to the configuration documentation.	nd
	-	/ Compan
wk Secu	Connection Type *	iired)
10	API Key *	ired)
D HIPAA S	ITG.286cadc21790t	ired)
	Region *	
	North America 👻	
	Cancel Test Login	

5. Next select the **Organization Status** and **Organization Types** to delimit the categories of orgs imported into the RapidFire Tools Portal.

Add Connection
Select organization statuses and types to sync with the RapidFire Tools portal.
Organization Status
Active
Inactive
Organization Types
Cancellation
Competitor
Customer
Dead
Internal
Lead
Other
Partner
Prospect
Vendor
← Back Save
Note: These fields are configured in IT Glue.

- 6. Click Save.
- 7. Your new Connection will appear under Your Connections.

Step 3 — Set Up Organizations

Once you set up the Connection with IT Glue, you then have the options of 1) reviewing imported orgs and editing how they map with existing RFT portal orgs, and 2) importing new orgs from IT Glue into the portal.

1. From My Connections, click Set Up Organizations.

9	Global Settings / Connections				
d ⊕	Connections @				
ф Q	Your Connections				+ Add
ø	Name ¢	Type 💠	Login 💠		
•	BMS HIPAA Connection	Kaseya BMS			D 🛈
ii Gr	IT Glue	IT Glue	****	Set Up Organizations	II 🖉 🗒
⊟ ©	Site Mappings				+ Add
ଚ	Site 💠	Connection	÷	Account / Company	
	Cyber Hawk Secure Demo Site	BMS HIPAA	Connection	(not required)	Ŵ
	KSV Demo	BMS HIPAA	Connection	(not required)	Ŵ
	My Demo HIPAA Site	BMS HIPAA	Connection	(not required)	Ŵ

2. If you already have an org in the RFT Portal with the same name as an IT Glue org, the two orgs will be matched automatically. You can click the X to remove the mapping if you wish.

 Connections Admin Alerts Users 		Organizations tch existing organizations	s to IT Glue organizations.		
S Compliance Manager GRC	▶ Filter colu	mns or search keywords.			6 of 6 results
VulScan Service Plans	Add	from IT Glue			
Email Groups	Organiza	tion	IT Glue Organization	Rem	ove Matching
Data Collectors	ABLE Ma	nufacturing HQ	ABLE Manufacturing HQ	×	
 IT Complete License Usage 	Acme Or	ganization	None		
	Example	Organization	None	Х	
	Micro Co	nsulting	None	Х	
	NETWOR	K ORGANIZATION ITG	NETWORK ORGANIZATION ITG	Х	
	Smith Sc	hool Bus Company	Smith School Bus Company	×	
	Save Pressing sa	Cancel	g and rename the current Organizatic	on name	e to the IT Glue Organization name.

- 3. To import IT Glue orgs, click **Add from IT Glue**.
- 4. Select the orgs to add from the drop-down menu. Then click Add.

lue INS	Add From ITGlue
ations to IT Glue organizations.	Select your organizations from ITGlue to automatically create RapidFire Tools organizations.
IT Glue Organization	Select multiple Blue Bird Bus Company
ABLE Manufacturing HQ None	Back Add
None	×
None	x

5. The imported orgs will appear. Once more, you can see their names in the RFT Portal as well as IT Glue.

Step 4 — Synchronize Org Names with IT Glue

Once you import orgs from IT Glue into the RFT Portal, the org names will be synchronized; changes to org names in IT Glue will regularly update the corresponding org names in the RFT Portal.

You can view these mappings from Your Connections > Set Up Organizations.

Note: The sync is limited to org names and works one way from ITGlue into the RFT Portal. Note also that deleting orgs in the RFT Portal will not delete orgs in IT Glue.

Pause Org Name Synchronization

To stop synchronizing org names, find the ITGlue connection and click the pause button.

Micro Consulting		Organizations				@ @	9	IT Pro	ĸ
 ③ General ✔ Branding ④ Connections ↓ Admin Alerts ▲ Users 		Global Settings / Connections Connections ③ Your Connections	Туре 🗢	Login ¢			I	+ A	dd
Compliance Manager GRC Ketwork Detective Pro VulScan	+ + +	Migration Connection for rapidfire_c	ConnectWise REST	Login (0	Û
Email Groups	ŀ	IT Glue	IT Glue	******	Set Up Organizations	Sync Now	⊳	0	Ū
Data Collectors IT Complete	•	IT Glue	IT Glue	******	Set Up Organizations	Sync Now	⊳	1	Û
 License Usage API Keys 		IT Glue	IT Glue	*****	Set Up Organizations	Sync Now	⊳	0	Û
Success	was pa	Datta Unified	Datto Unified Continuity	10111				0	Û
successfully.	muo po		Dark Web ID	Rentire (regulation of the					Û
		BMS HIPAA	Kaseya BMS	1000000				02.27	ー1904 値

To resume synchronizing org names, find the ITGlue connection and click the **play** button.

Micro Consulting		Organizations				?	¢	8	IT Pro	K
General		Global Settings / Connections								
🖌 Branding										
Onnections		Connections ③								
Admin Alerts		Your Connections							+ A	dd
2 Users										
Compliance Manager GRC	Þ.	Name ≑	Type 🗘	Login 🗘						
Q Network Detective Pro	Þ	Migration Connection	ConnectWise	The Contraction of the Contract					0	Û
 VulScan 	Þ	for rapidfire_c	REST						^p	0
E Service Plans	Þ	IT Glue	IT Glue	******						~
Email Groups		11 Glue	11 Gide		Set Up Organizations	Sy	nc Now	03	Ø	Û
Data Collectors		IT Glue	IT Glue	*****	Set Up Organizations	Sv	nc Now	03	0	Û
C IT Complete	Þ.				out op organizatione				5	
1 License Usage		IT Glue	IT Glue	*****	Set Up Organizations	Sy	nc Now	00	0	Û
🖉 API Keys										
Success		Datta Unified	Datto Unified Continuity	Mark .					0	Û
 IT Glue integration w successfully. 	vas sta	rted X	Dark Web ID	1					0	Û
		BMS HIPAA	Kaseya BMS	(matters)				202	02.2	7-1904 1

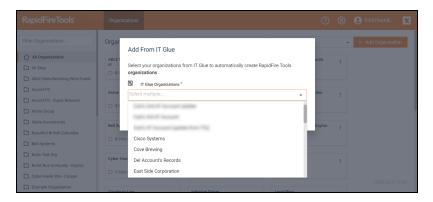
Import IT Glue Orgs when Creating New Organizations

Once you set up a connection with IT Glue, you can also import IT Glue orgs from the RFT Portal orgs page:

- 1. Click Add Organization from the RFT Portal home page.
- 2. Click Add from IT Glue.

RapidFireTools	Organizations	@ ® ·	e firstname
Filter Organizations	Organizations	Add Organization	+ Add Organization
All Organizations	ABLE Manufacturing	Organization Name* Add from IT Glue Fit - Guest Network :	
All Sites ABLE Manufacturing West Coast	C 0 Sites	tes	
Accent Fit Accent Fit - Guest Network	Acme Group	Organization names must start with an alphanumeric character, may only include alphanumeric characters, dash, and space and must be less than 50 characters long.	
Acme Group	3 Sites	Cancel Confirm	
Alpha Investments Beautiful British Columbia	Bell Systems	Jus Company - Dayton	
Bell Systems			
 Bobs Test Org Bullet Bus Company - Dayton 	Cyber Hawk Site - Co	per : Example Organization : Foresight Group :	
Cyber Hawk Site - Cooper		4 Sites 7 Sites	2024.02.27-1904

3. Select one or more IT Glue orgs from the drop-down menu and click Add.



RapidFireTools^{*}

License Usage (Global Settings)

From global **Settings (Admin)** > License Usage, you can see a breakdown of your available licenses for Compliance Manager GRC, VulScan, and Cyber Hawk.

Here you can see a license usage for each site – including the number of devices identified at the site during the most recent scan. Contact your sales representative to request additional licenses.

i General𝔐 Branding		Global Settings / License Usage			
 Connections 		License Usage 110 o	f 200	Compliance Manager 🗸 👻	Request More Licenses
Admin Alerts		Site Name ≑		# Devices 🔶	License Usage ≑
Compliance Manager GRC	÷	100000 M		60	1
 Network Detective Pro VulScan 	•	1007764		49	1
E Service Plans	•	1. (10%) (10%) (ar 17%)		16	1
🔂 Email Groups		100.000.000		9	1
IT Complete		Your Secured Company		7	1
2 License Usage		100 Tel: (01 100 100 1		5	1
🖉 API Keys		Security Solutions Agency		4	1

A Site License will be automatically consumed whenever the number of detected devices exceeds 250. For example:

- When 0 to 250 devices are detected, one Site License will be used
- When 251 Devices are detected, a second Site License will be used
- When 501 Devices are detected, a third Site License will be used, and so on

Use the drop-down menu to filter between Compliance Manager GRC, VulScan, and Cyber Hawk site license usage.

Global Settings / License Usage									
License Usage	110 of 200	Compliance Manager	•	Request More Licenses					
		Compliance Manager							
Site Name 🌩		VulScan							
		Cyber Hawk							