VULSCAN

by RapidFire Tools

USER GUIDE

VulScan

Instructions to Perform Vulnerability Scanning

4/11/2024 3:52 PM

Kaseya®

+1-678-323-1300

rapidfiretools.com

support@rapidfiretools.com

Contents

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. "Create Scan and Notification Tasks" on page 20

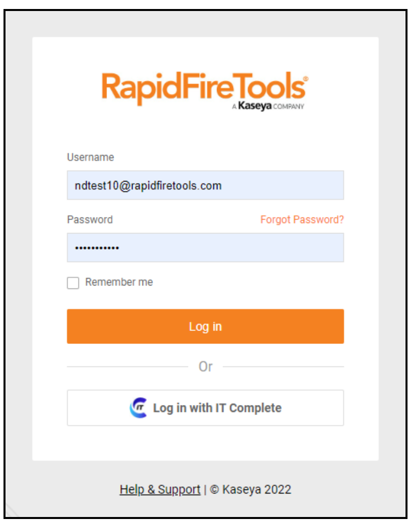
Once you complete these steps, you can begin "Using VulScan" on page 54 to address identified issues.

Add an Organization

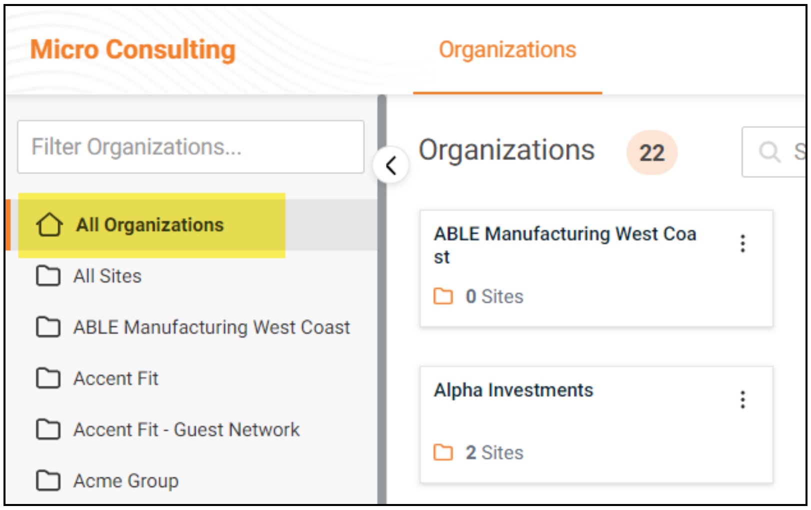
Before you begin your first IT or compliance assessment, you can optionally create an **organization**. Think of an organization as a folder in which you can store assessment projects for a particular client.

To add an Organization:

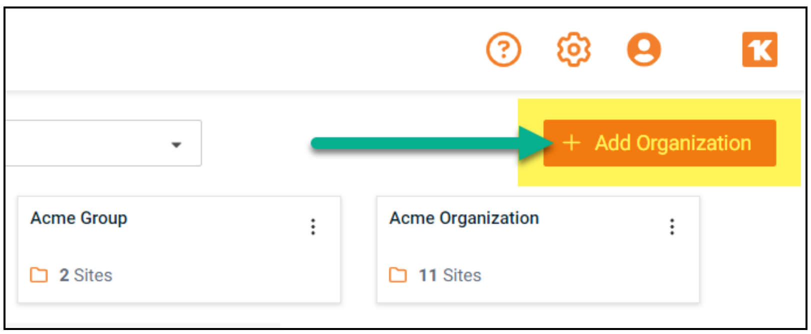
1. Access the RapidFire Tools Portal at https://www.youritportal.com and log in with your credentials.



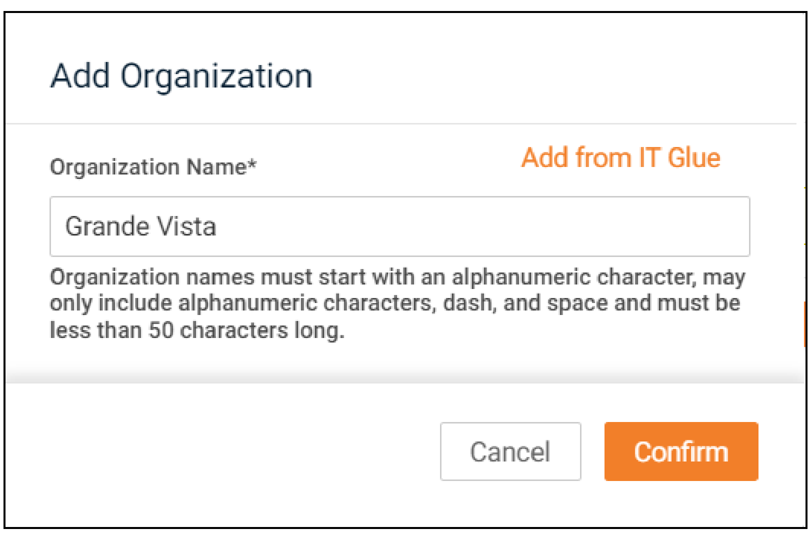
2. Access the **Organizations** page from the top-menu. Select **All Organizations** from the side menu.



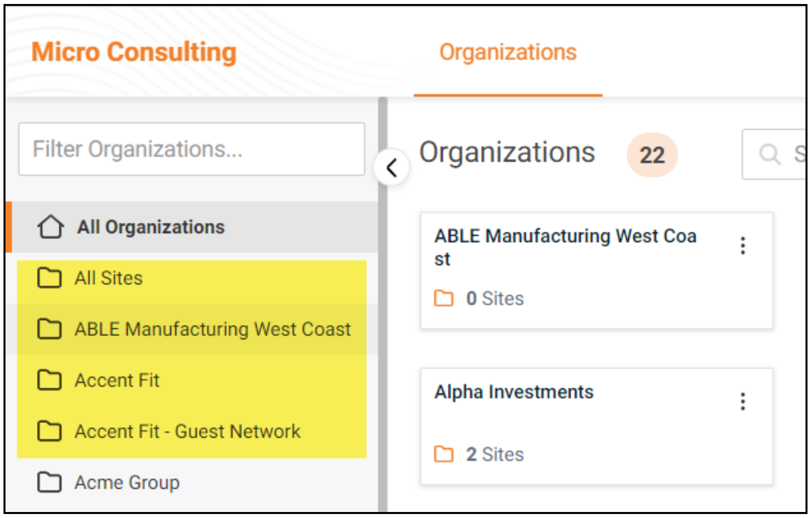
3. Then click **Add Organization**.



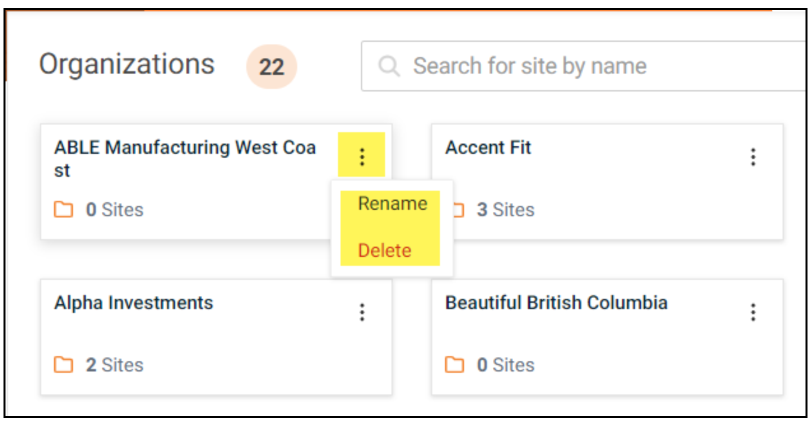
4. Enter an Organization name. For example, this might be the name of a large company for whom you want to create multiple sites and types of IT and compliance assessments. Then click **Confirm**.



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



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.

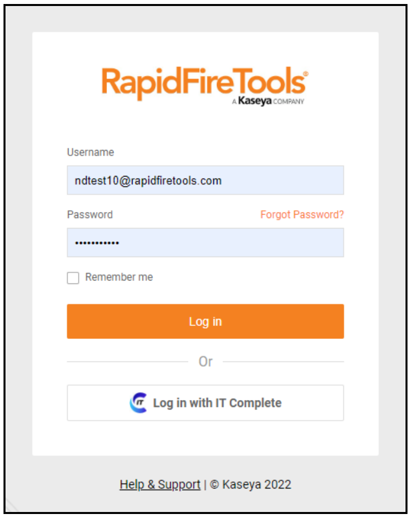


Create VulScan Site

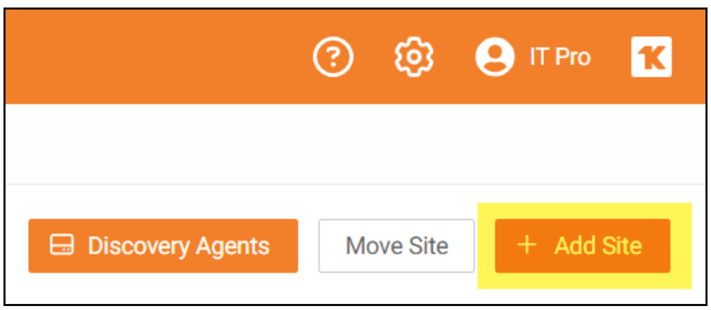
Tip: We recommend you get started by making a "practice site" and running your first assessment in-house. Use this to familiarize yourself with VulScan and the installation and configuration process.

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 https://www.youritportal.com and log in with your credentials.



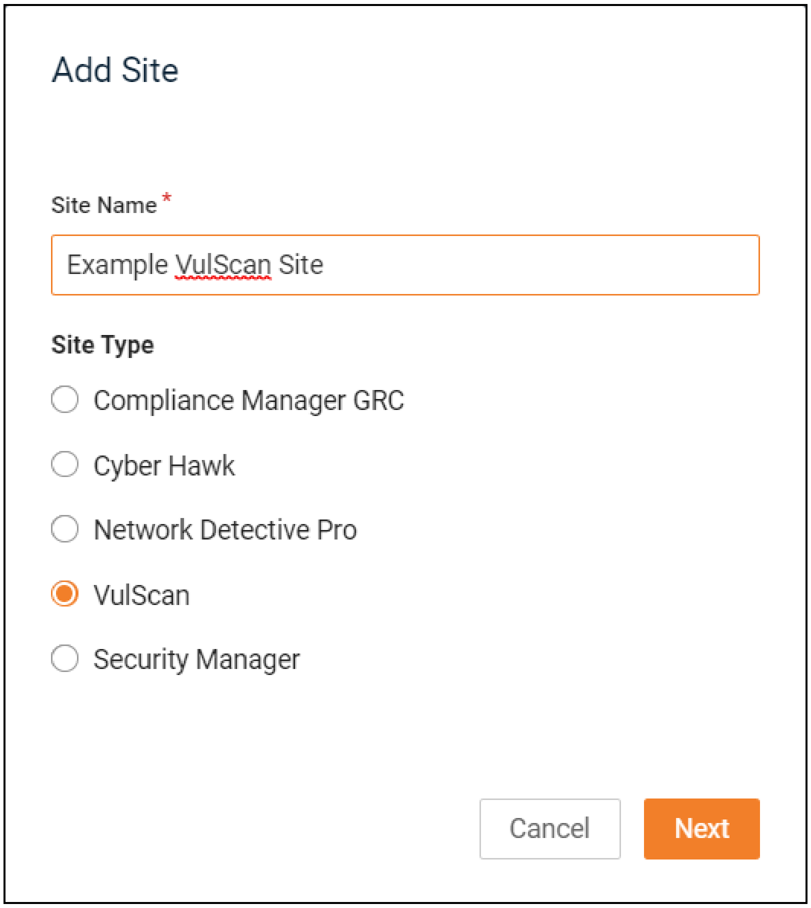
2. From the Sites page, click **Add Site**.



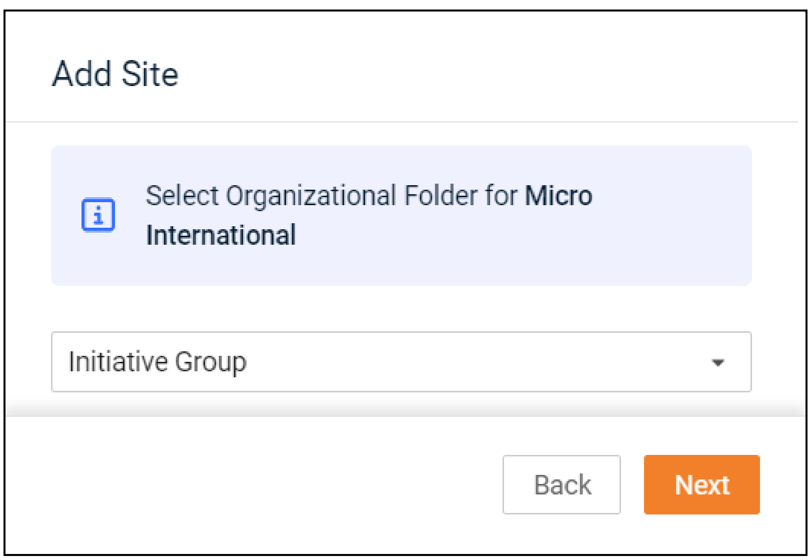
3. Enter a **Site Name**. This can be the name of the client for whom the assessment is being performed, for example.

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

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

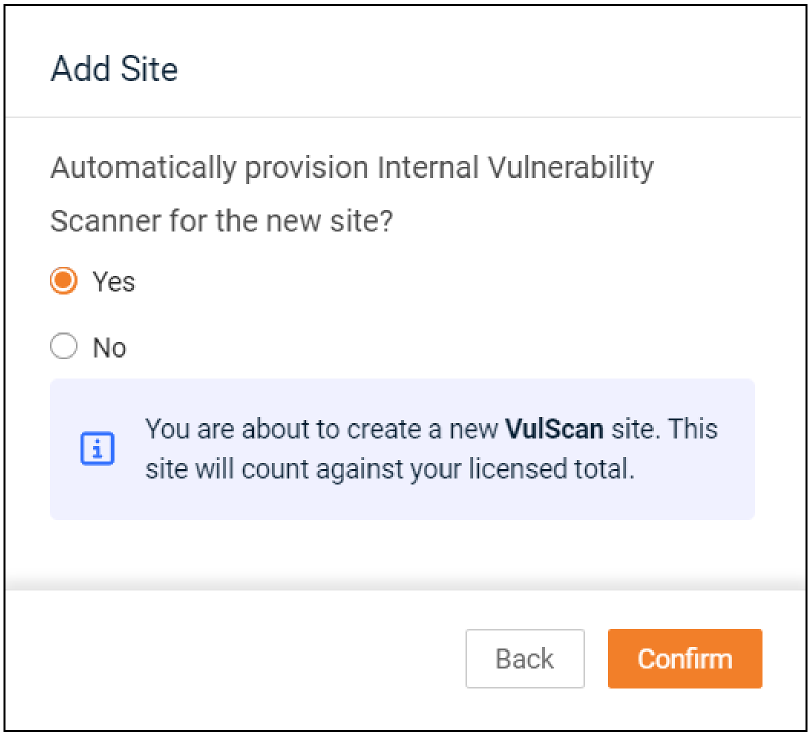


5. Choose an Org Folder for the site and click **Next**.



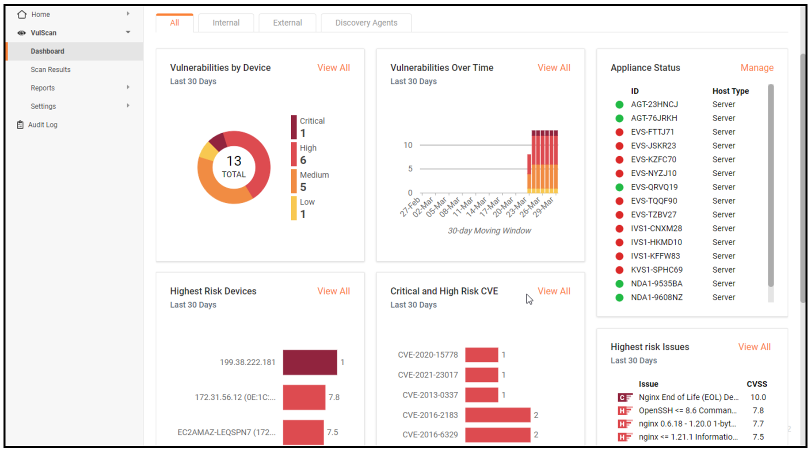
6. Choose whether to provision an IVS appliance for the new site. Then click **Confirm**.

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



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

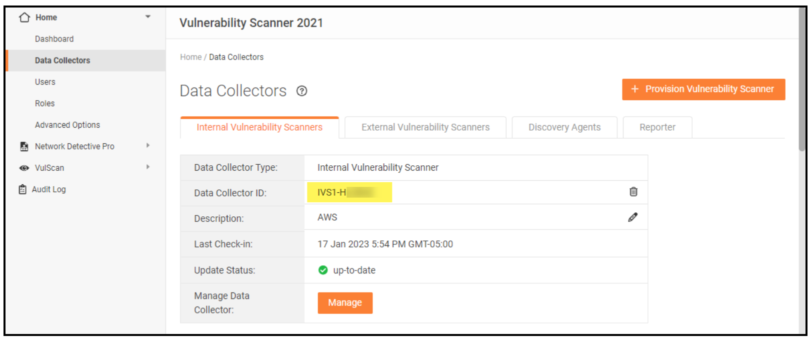
- Status of appliances associated with the Site
- High-level graphical overview of scan results by issue severity
- Itemized list of highest risk issues
- Audit log of recent site activity


Home
VulScan
Dashboard
Scan Results
Reports
Settings
Audit Log
All
Internal
External
Discovery Agents
Vulnerabilities by Device
Last 30 Days
View All
13
TOTAL
Critical
1
High
6
Medium
5
Low
1
Vulnerabilities Over Time
Last 30 Days
View All
30-day Moving Window
Appliance Status
Manage
ID
Host Type
AGT-23HNCJ Server
AGT-76JRKH Server
EVS-FTTJ71 Server
EVS-JSKR23 Server
EVS-KZFC70 Server
EVS-NYZJ10 Server
EVS-QRVQ19 Server
EVS-TQQF90 Server
EVS-TZBV27 Server
IVS1-CNXM28 Server
IVS1-HKMD10 Server
IVS1-KFFW83 Server
KVS1-SPHC69 Server
NDA1-9535BA Server
NDA1-9608NZ Server
Highest Risk Devices
Last 30 Days
View All
199.38.222.181
172.31.56.12 (0E:1C:...
EC2AMAZ-LEQSPN7 (172...
Critical and High Risk CVE
Last 30 Days
View All
CVE-2020-15778
CVE-2021-23017
CVE-2013-0337
CVE-2016-2183
CVE-2016-6329
Highest risk Issues
Last 30 Days
View All
Issue
CVSS
Nginx End of Life (EOL) De... 10.0
OpenSSH <= 8.6 Comman... 7.8
nginx 0.6.18 - 1.20.0 1-byt... 7.7
nginx <= 1.21.1 Informatio... 7.5

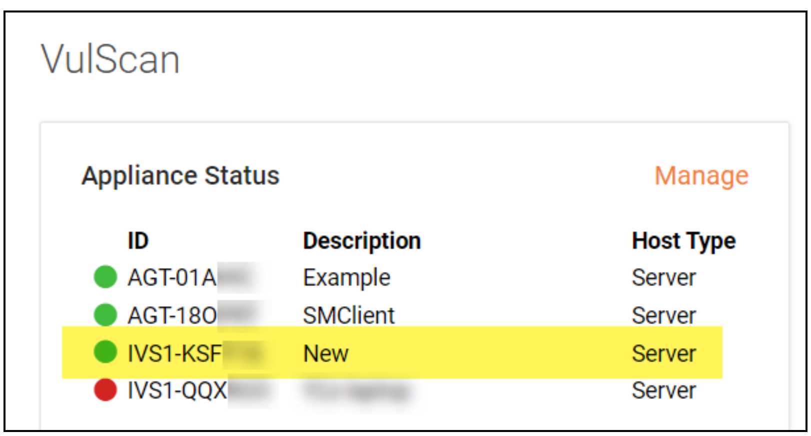
Install VulScan Appliance

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 "VulScan Appliance Types and Install Instructions" 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**.



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 Types and Install Instructions

VulScan Appliance Type	Prefix	Install Location	Scan Type	Install Instructions
Internal Vulnerability Scanner	IVS	Device on target network	Internal	• Virtual Appliance Installation Guide for VulScan
External Vulnerability Scanner	EVS	Device on MSP and/or outside network	External	• Virtual Appliance Installation Guide for VulScan
Portable Vulnerability Scanner	PVS	Physical device moved from site to site	Internal	• "Portable VulScan Set Up" on page 228 • Virtual Appliance Installation Guide for VulScan
Remote Internal Vulnerability Scanner	RIVS	MSP network; scans customer network through a proxy agent	Internal	• "Set Up Remote Internal Vulnerability Scanner" 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

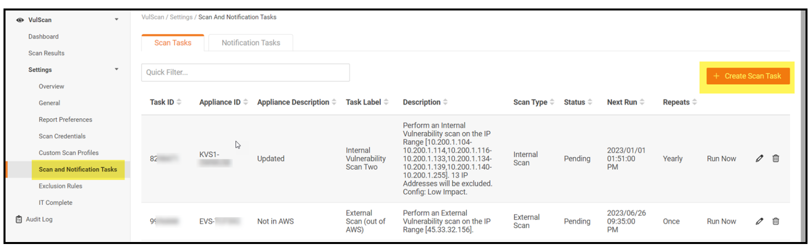
Once you have installed the VulScan appliance for your site, it's time to configure Scan and Notification Tasks. **Scan and Notification Tasks** are the heart of VulScan.

- **Scan tasks** allow you to configure, schedule, and perform vulnerability scans on the site network at regular intervals. See "Create Internal Scan Task" below and "Create External Scan Task" on page 27.
- **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 "Create Notification Tasks" on page 30.

Create Internal Scan Task

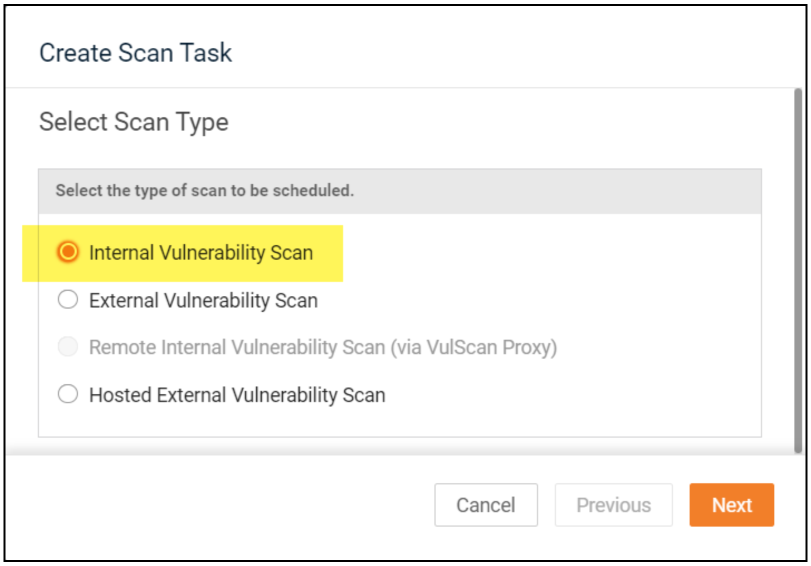
In order to collect vulnerability data from the target network, you need to set up scan tasks. Follow these steps to create an internal vulnerability scan task with VulScan:

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



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

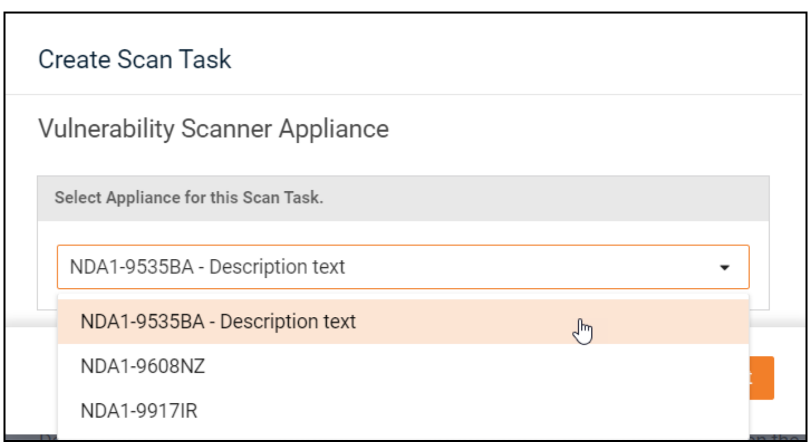
> **Note:** If you are using the **Remote Internal Vulnerability Scanner**, select that option.



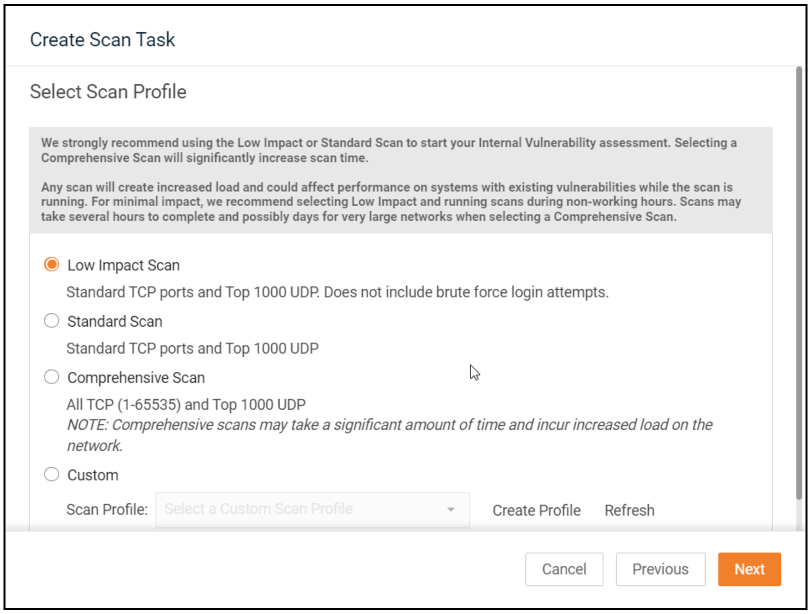
4. Select the Appliance from the drop-down menu and click **Next**.

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



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

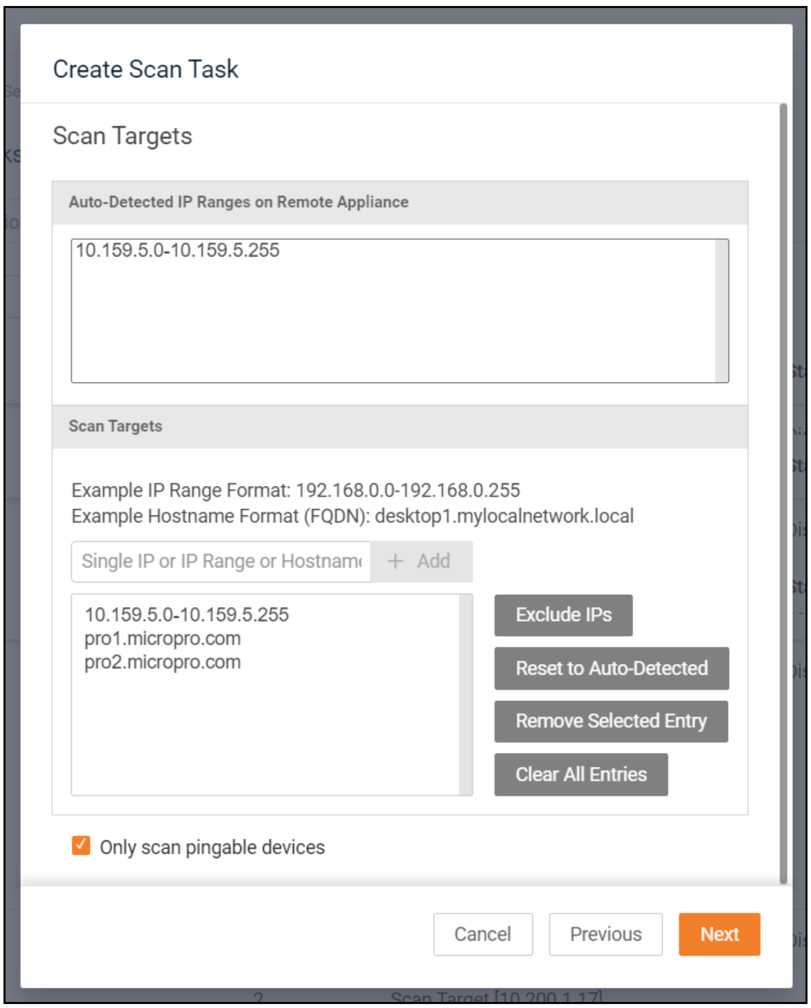
6. Next configure **IP ranges**. The VulScan appliance will automatically suggest an IP Range for the scan. If you do not wish to scan the default IP Range, select it and click **Clear All Entries**. Use this screen to enter additional IP Addresses or IP Ranges and click **Add**.

   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.



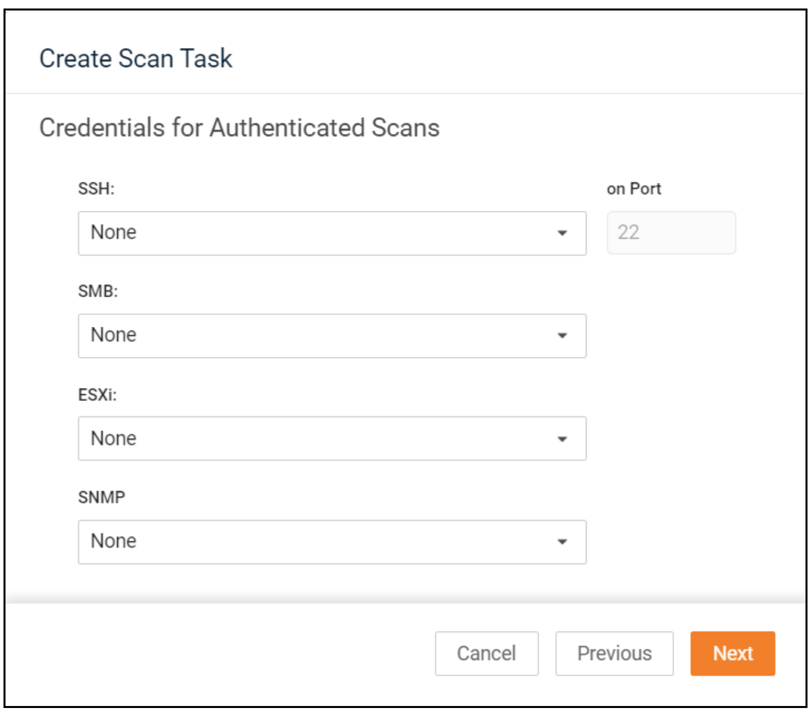
From this screen you can also:

- 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.

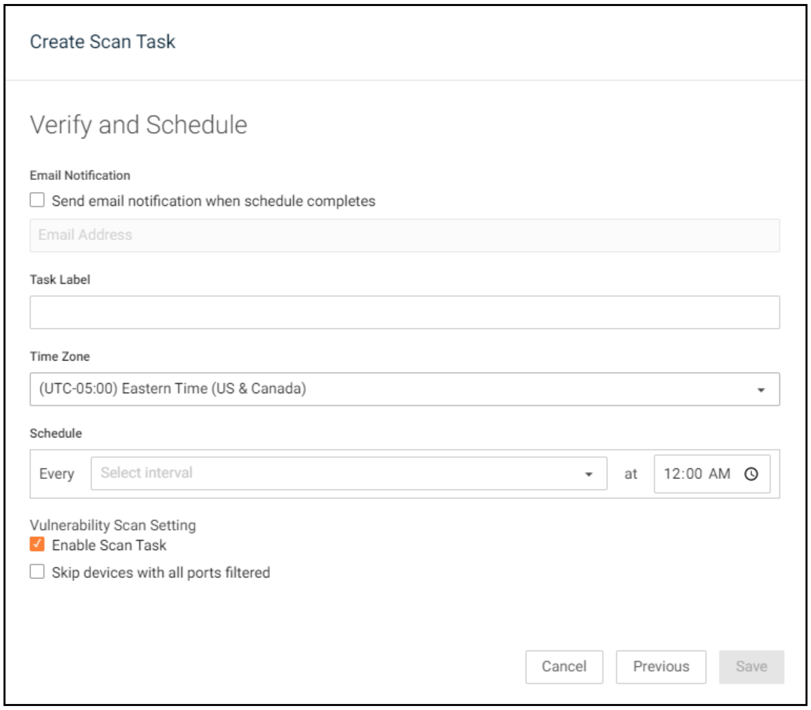
7. Click **Next Page** once you have configured the IP ranges for the scan.
8. From the Credentials for Authenticated Scans screen, select whether you use credentials for the internal scan. Note that you must first have entered these credentials from "Scan Credentials" on page 42.



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.

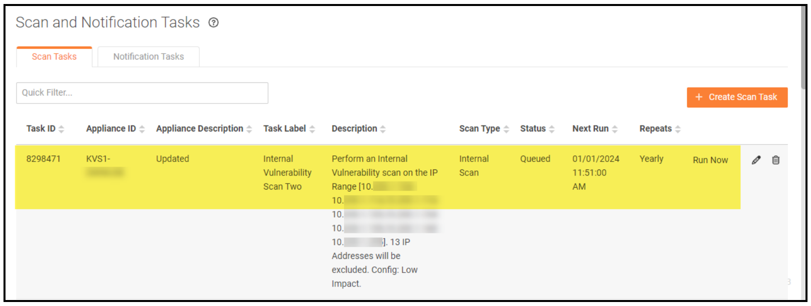
9. From the **Verify and Schedule** menu, configure the scan task:



   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**.

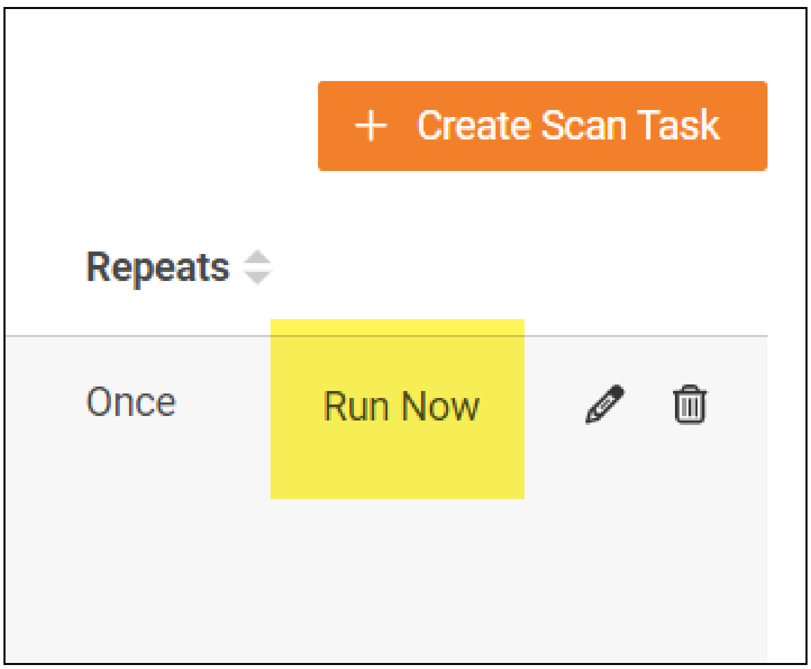
10. Click **Save**.

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

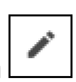
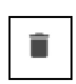


Scan Task "Run Now"

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.



Edit/Delete Scan Task

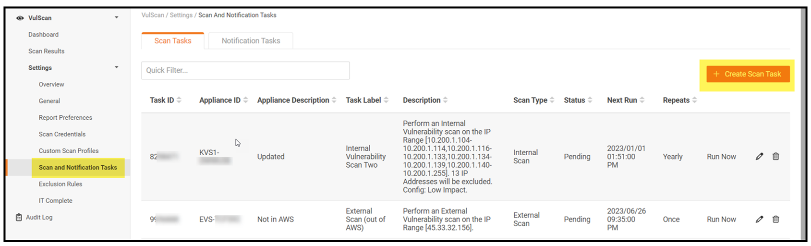
- To edit a scan task, click the pencil icon  next to a task. Make and save your changes.
- To delete a scan task, click the trash icon  next to a task.

Create External Scan Task

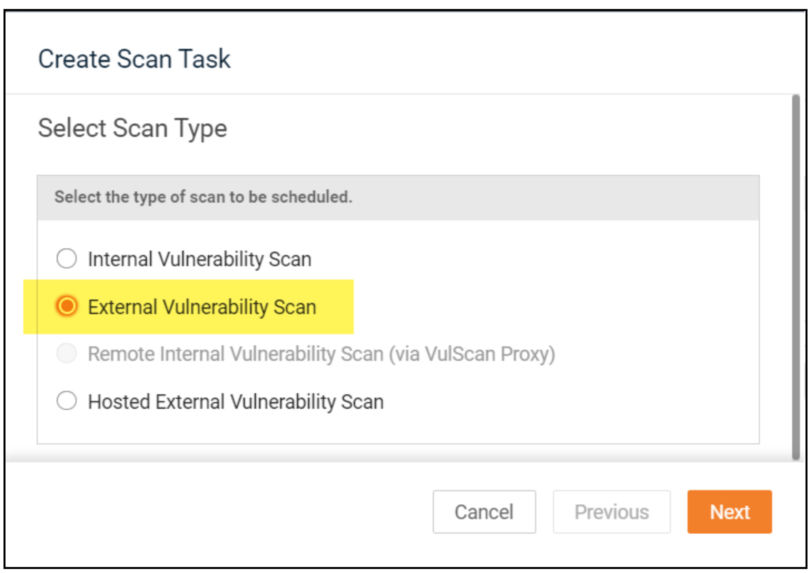
> **Note:** Before you can create an external vulnerability scan task, you first need to provision and install an external vulnerability scan appliance. See "Install VulScan Appliance" on page 18 and "Provision VulScan" on page 200. If you wish to perform external scans without using an appliance, see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

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

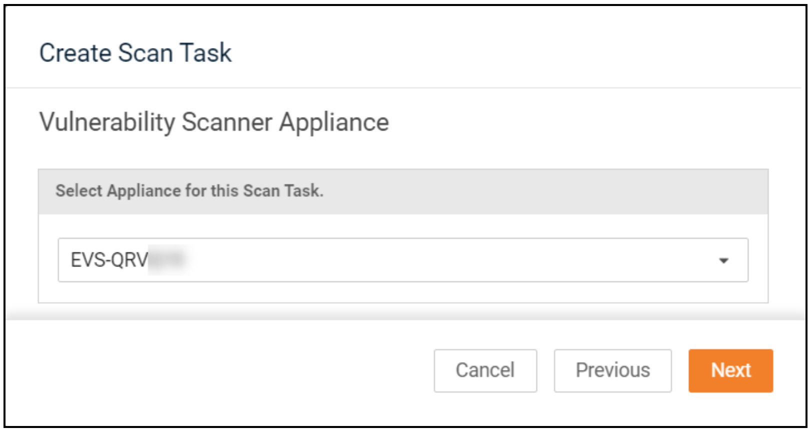
1. From your site, go to **VulScan** > **Settings** > **Scan and Notification Tasks**.
2. From the **Scan Tasks** tab, click **Create Scan Task**.



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

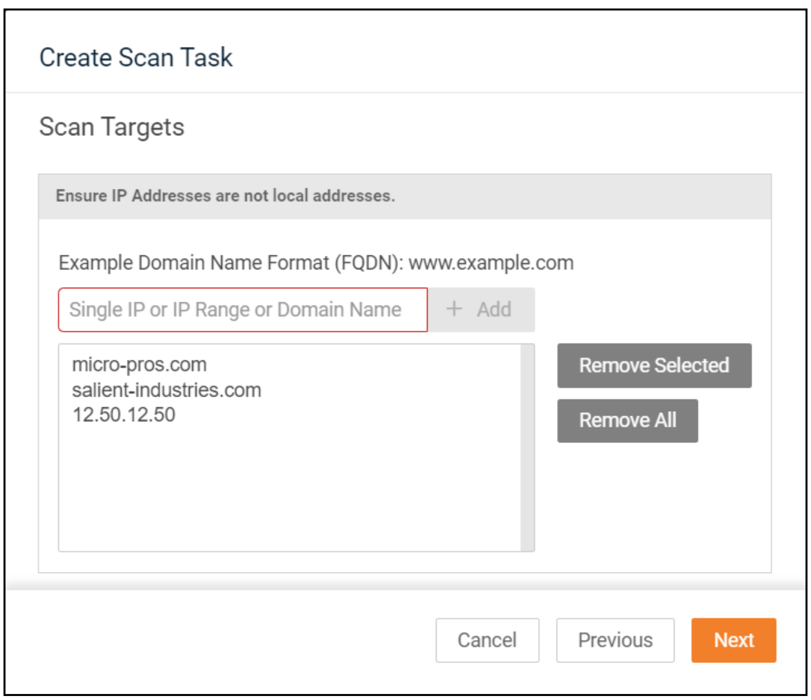


4. Select the Appliance from the drop-down menu and click **Next**.

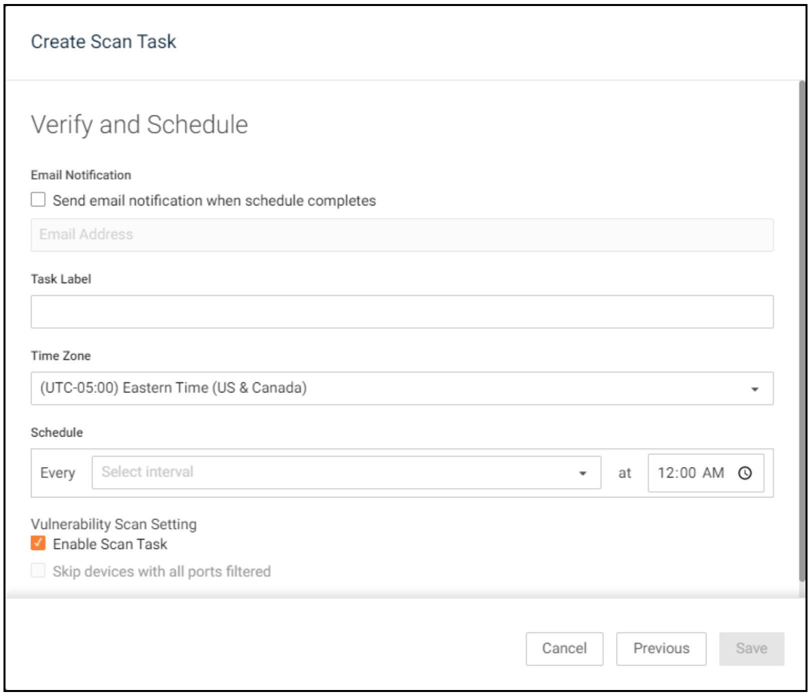


5. Enter the IP addresses for the external vulnerability scan. You can enter individual IPs or IP ranges. You can also enter fully qualified domain names, such as **www.example.com**. Click **Next Page**.

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.



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



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.

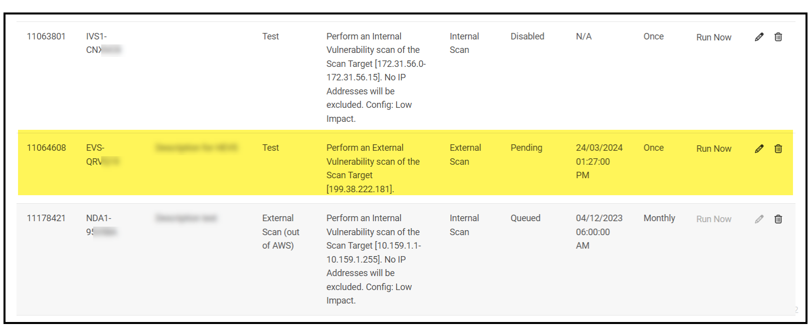
d. Next choose a day and time to **schedule** the scan.

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.

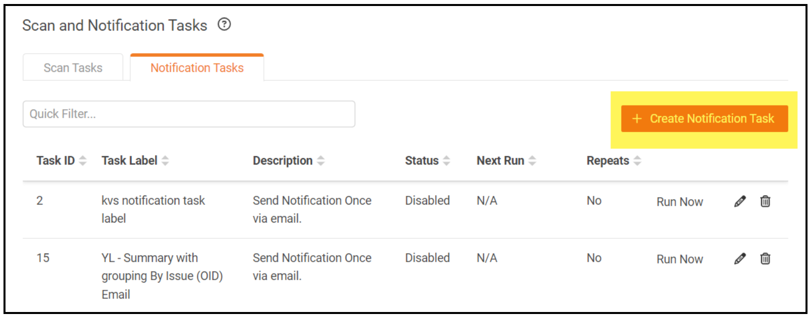


11063801	IVS1-CN		Test	Perform an Internal Vulnerability scan of the Scan Target [172.31.56.0-172.31.56.15]. No IP Addresses will be excluded. Config: Low Impact.	Internal Scan	Disabled	N/A	Once	Run Now
11064608	EVS-QRV		Test	Perform an External Vulnerability scan of the Scan Target [199.38.222.181].	External Scan	Pending	24/03/2024 01:27:00 PM	Once	Run Now
11178421	NDA1-95		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

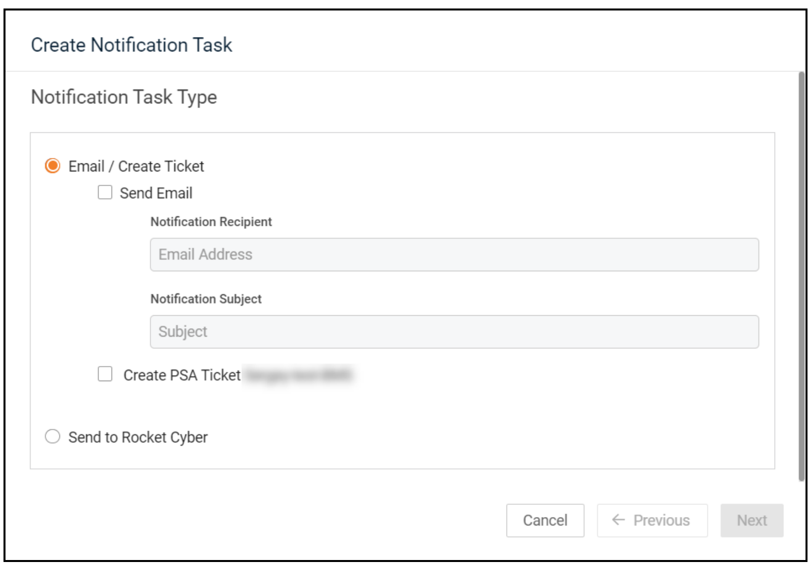
Create Notification Tasks

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**.



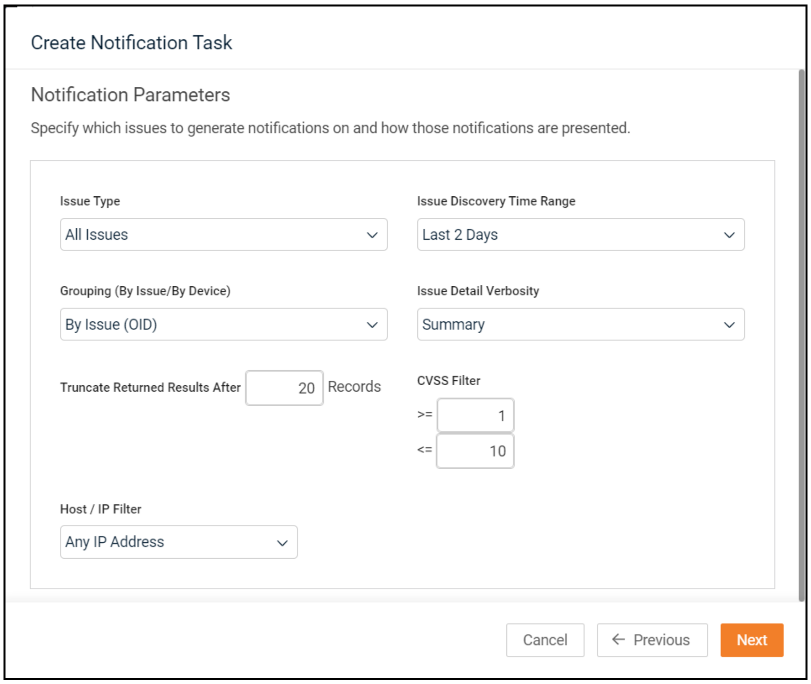
3. From the **Notification Task Type** menu, select whether to send an email. Enter the notification email recipient and subject line.



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 "Set Up and Assign a Ticketing/PSA System Integration to a Site" on page 167 for a complete walkthrough.

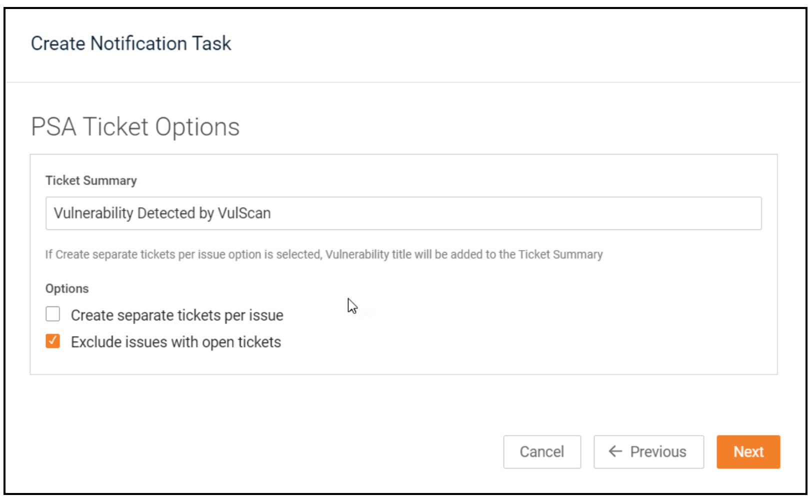
5. Alternatively, you can choose Export to RocketCyber. This action will make detected issues available to browse in RocketCyber. See "Export Notification Tasks to RocketCyber" on page 80.
6. Click **Next** once you've configured the notification type.
7. Choose from among the available notification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



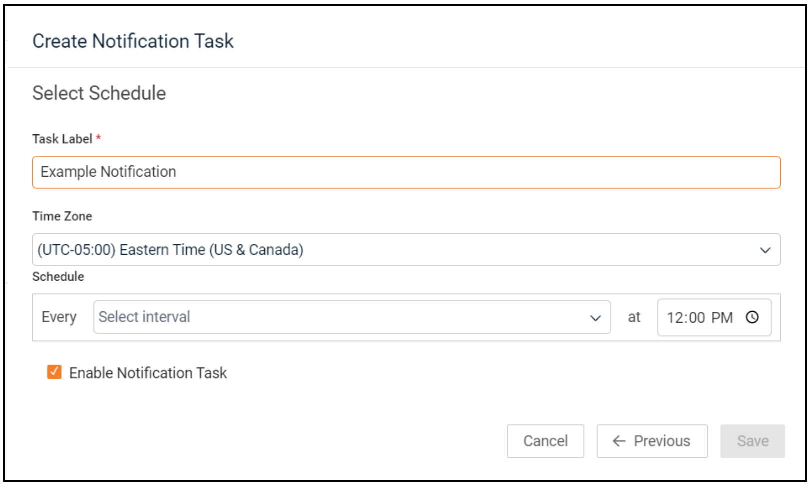
- **Issue Type**: Select whether to notify for all detected issues or only the most recently detected issues.
- **Issue Discovery Time Range**: Select whether to filter vulnerability issues by the available time ranges.
- **Grouping**: Choose whether to organize issues by vulnerability type (OID) or 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.

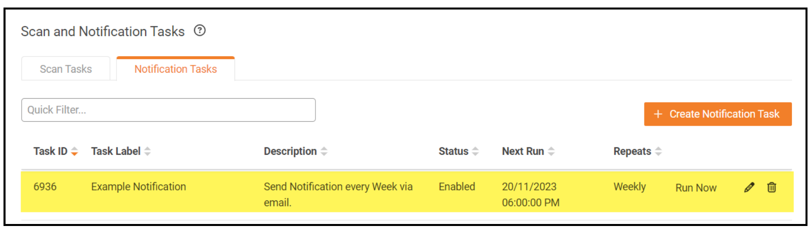


9. From **Select Schedule**, enter a task label and schedule your notifications. Click **Save**.

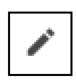
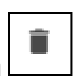


Note: Use **Enable Notification Task** option to enable/disable the task. This can he helpful if you wish to pause a notification task.

10. The created item will appear under notification tasks.



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.

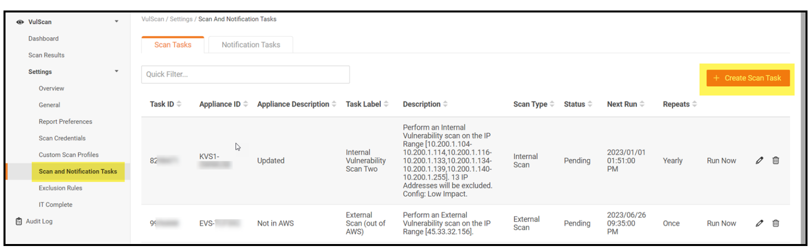
Follow these steps to create a Kasyea Hosted External Vulnerability Scan Task with VulScan:

Step 1 – Provision Hosted External Vulnerability Scanner

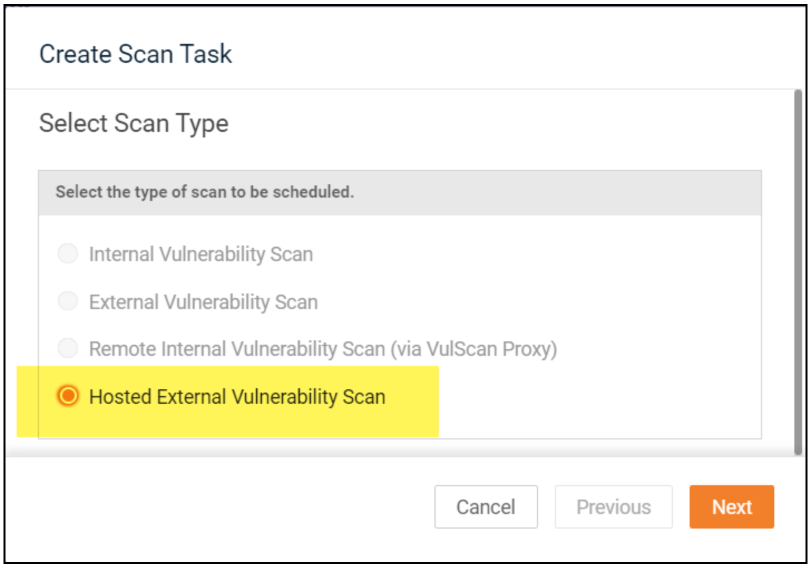
First, contact your account representative to provision the Kaseya Hosted External Vulnerability Scanner. Your license will allow you scan a certain number of external IPs per month. Once your account is provisioned, you can set up the external vulnerability scan task.

Step 2 – Set up Hosted External Vulnerability Scan Task

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

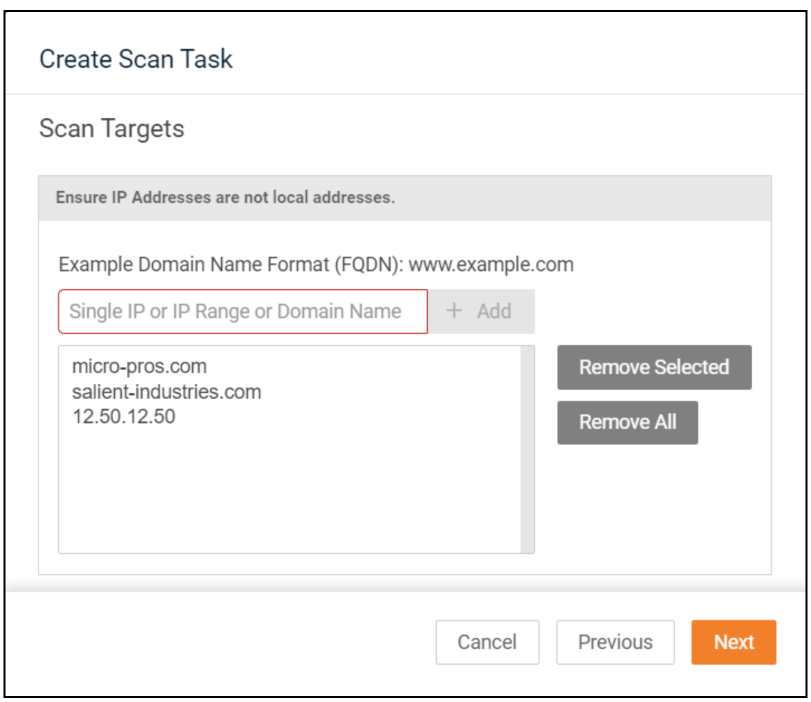


3. From Scan Type, select **External Vulnerability Scan** and click **Next**.

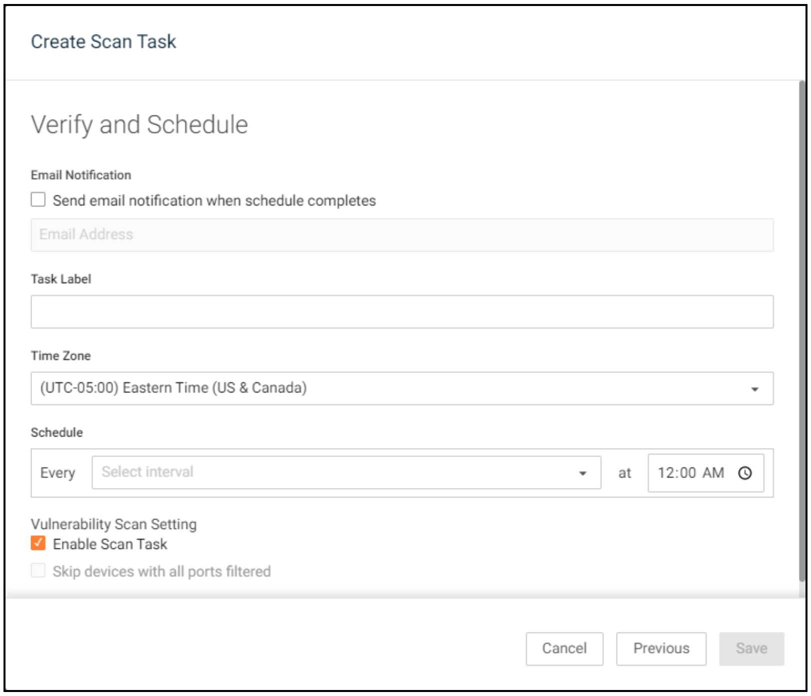


4. Enter the IP addresses for the external vulnerability scan. You can enter individual IPs or IP ranges. Click **Next Page**.

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.



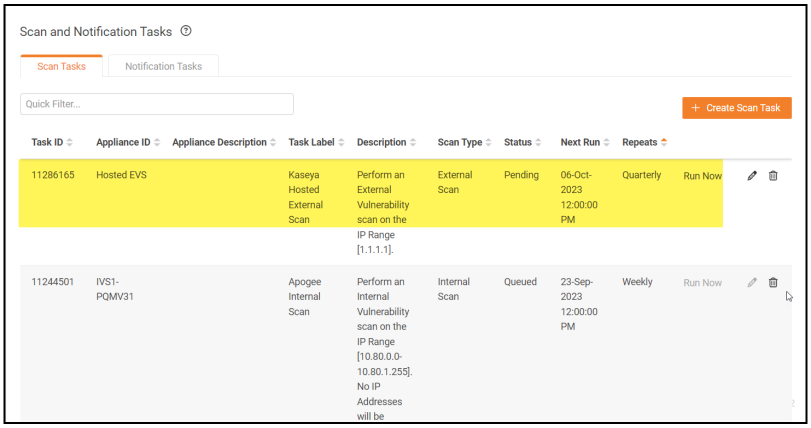
5. From the **Verify and Schedule** menu, configure the scan task:



   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**.

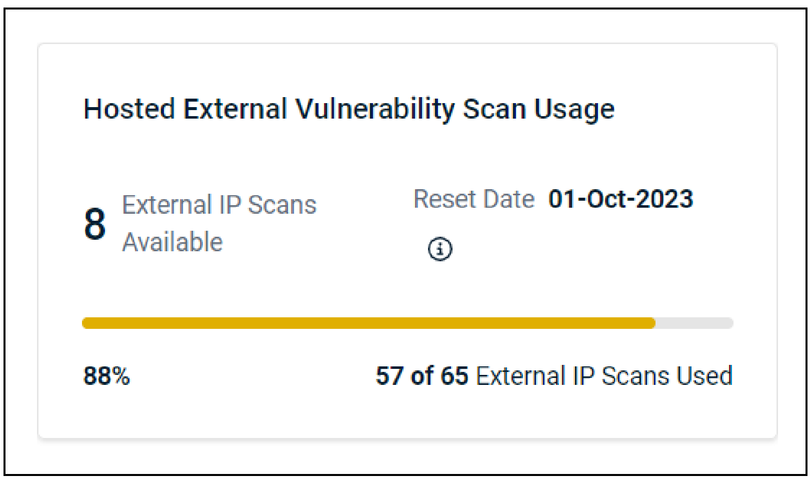
6. Click **Save**.

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

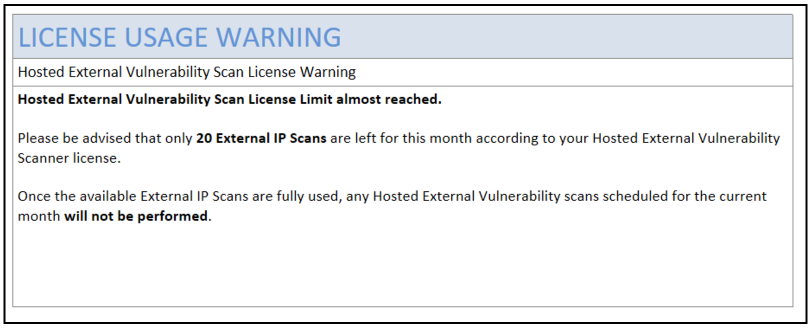


Step 3 – Keep Track of Hosted External Scan License Limit

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**).



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



LICENSE USAGE WARNING

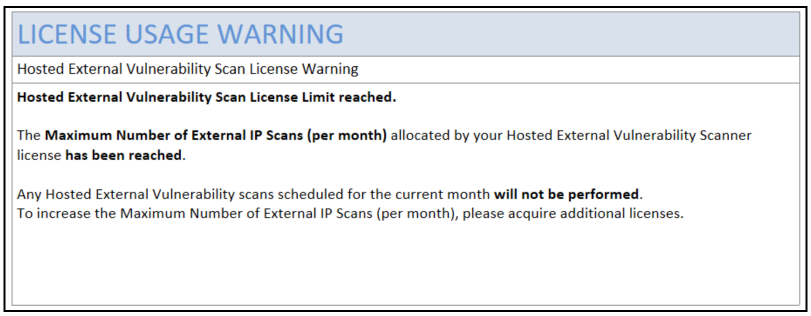
Hosted External Vulnerability Scan License Warning

Hosted External Vulnerability Scan License Limit almost reached.

Please be advised that only **20 External IP Scans** are left for this month according to your Hosted External Vulnerability Scanner license.

Once the available External IP Scans are fully used, any Hosted External Vulnerability scans scheduled for the current month **will not be performed**.

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



LICENSE USAGE WARNING

Hosted External Vulnerability Scan License Warning

Hosted External Vulnerability Scan License Limit reached.

The **Maximum Number of External IP Scans (per month)** allocated by your Hosted External Vulnerability Scanner license **has been reached**.

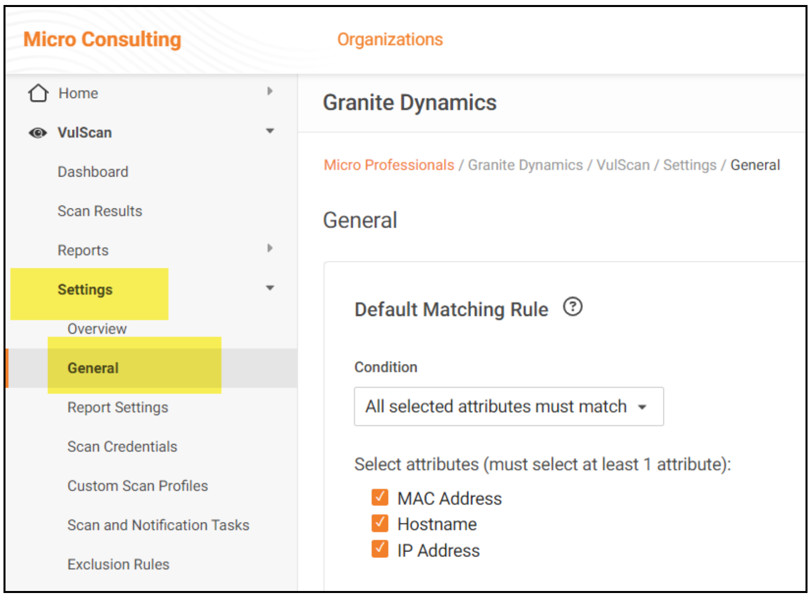
Any Hosted External Vulnerability scans scheduled for the current month **will not be performed**.
To increase the Maximum Number of External IP Scans (per month), please acquire additional licenses.

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:

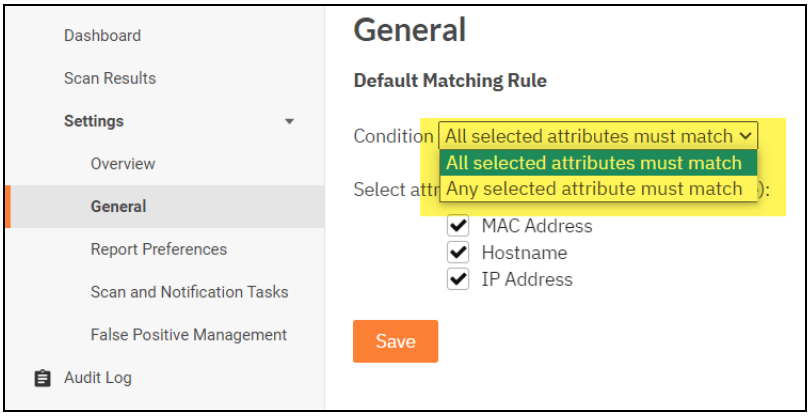
1. From your VulScan site, navigate to **VulScan** > **Settings** > **General**.



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.



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

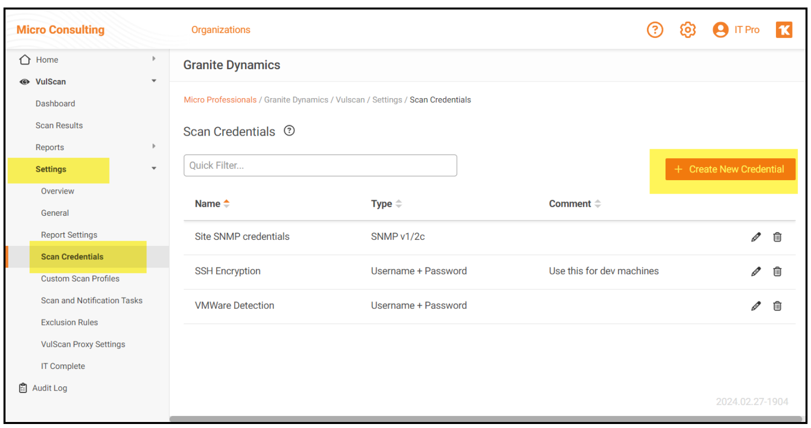
Scan Credentials

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.

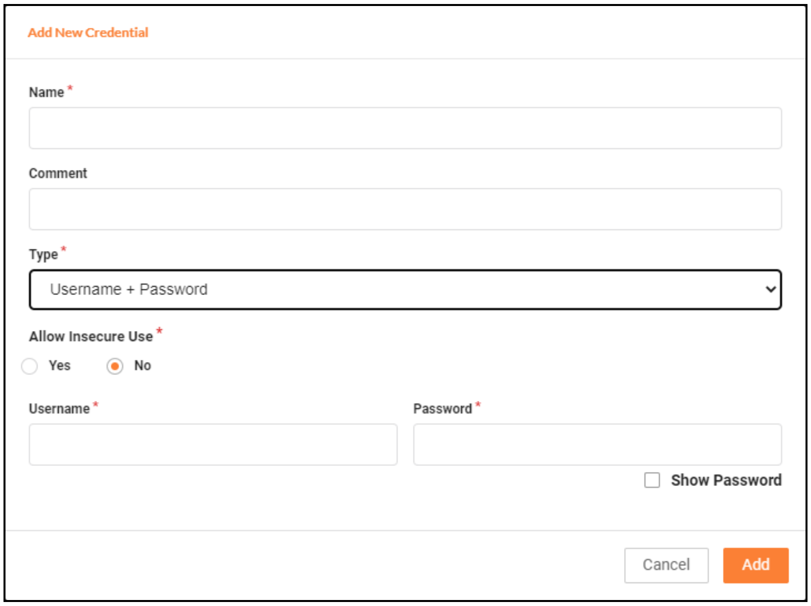
You can enter scan credentials for your VulScan sites and then assign these credentials to be used during the scan task. Scan credentials are not required to perform an internal scan, but adding them can help detect a wider range of security issues. Further, you can add multiple sets of credentials and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



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



- **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 "Create Internal Scan Task" on page 20. You can also return to your site to edit or delete the credentials.

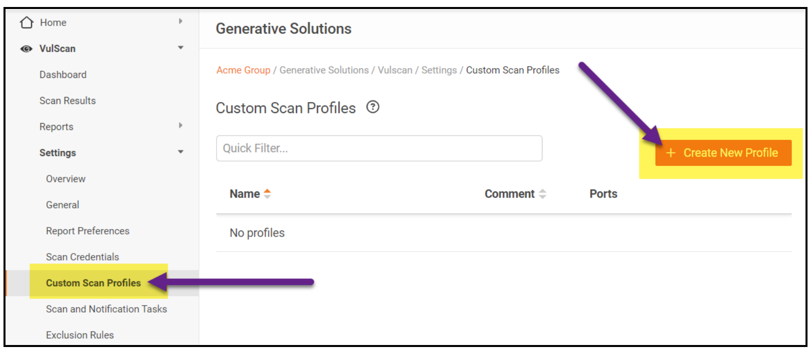
Custom Scan Profiles

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.

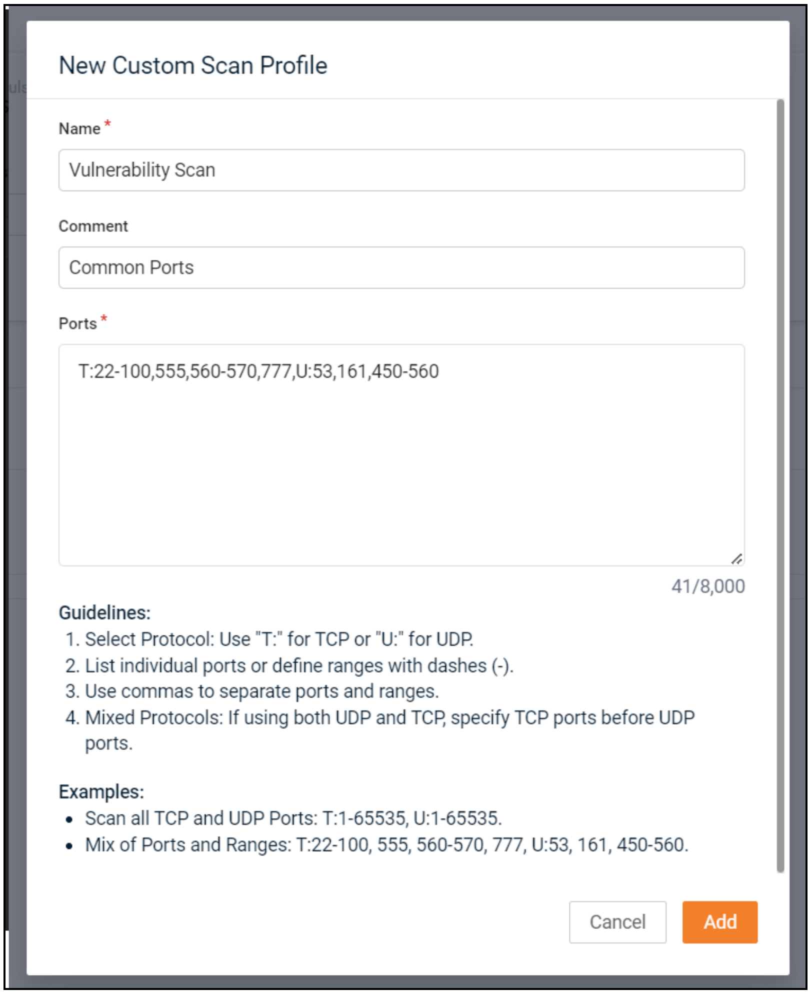
Create New Profile

To create a new Custom Scan Profile:

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



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



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 "Create Internal Scan Task" on page 20.

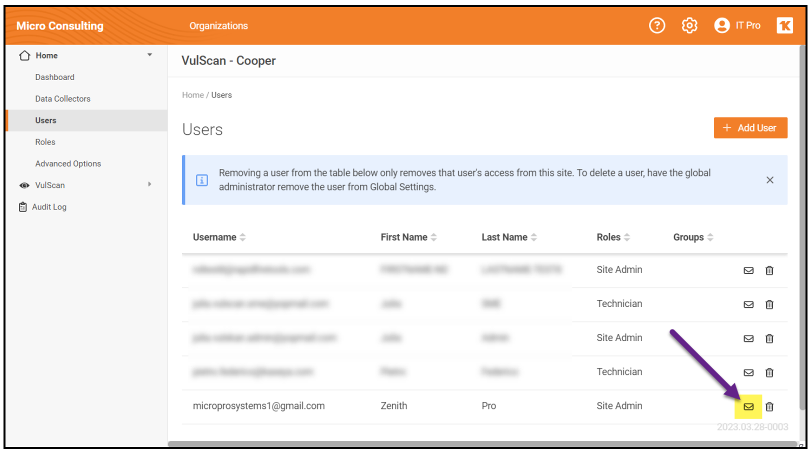
 RapidFireTools

Invite Users to VulScan Site

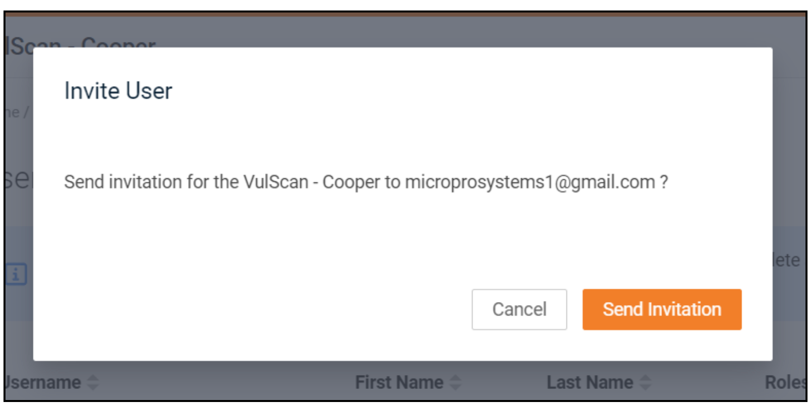
You can send an email to invite site users to join your VulScan site. Invited users then create a password and log in to the portal, where they can then access the site. Here's how this works:

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.

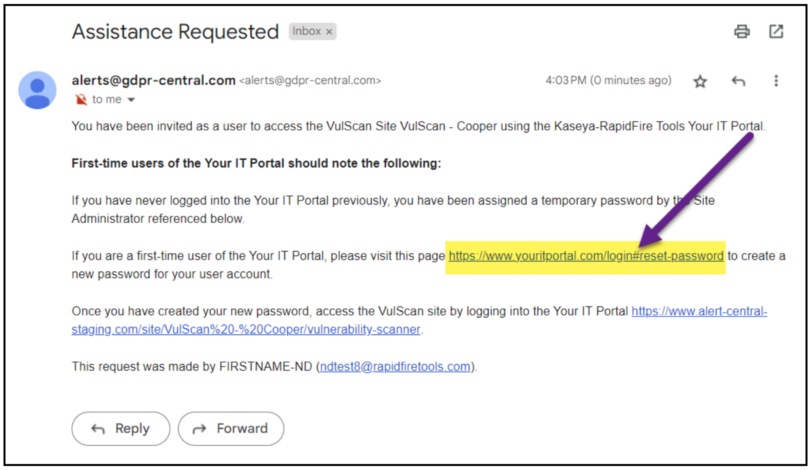
   Note: You must have first assigned the user a site role before you can send the invite.

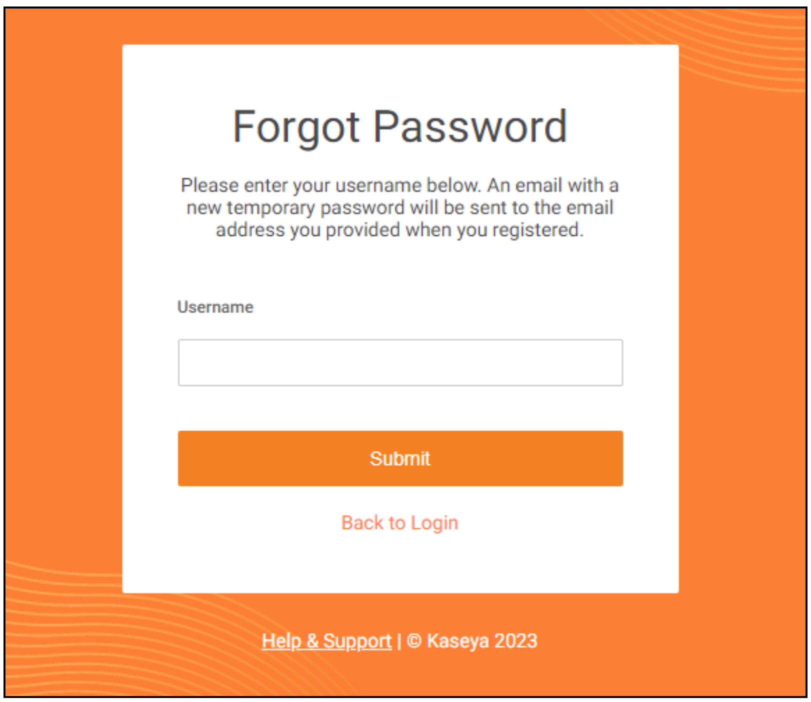
3. Click **Send Invitation**.

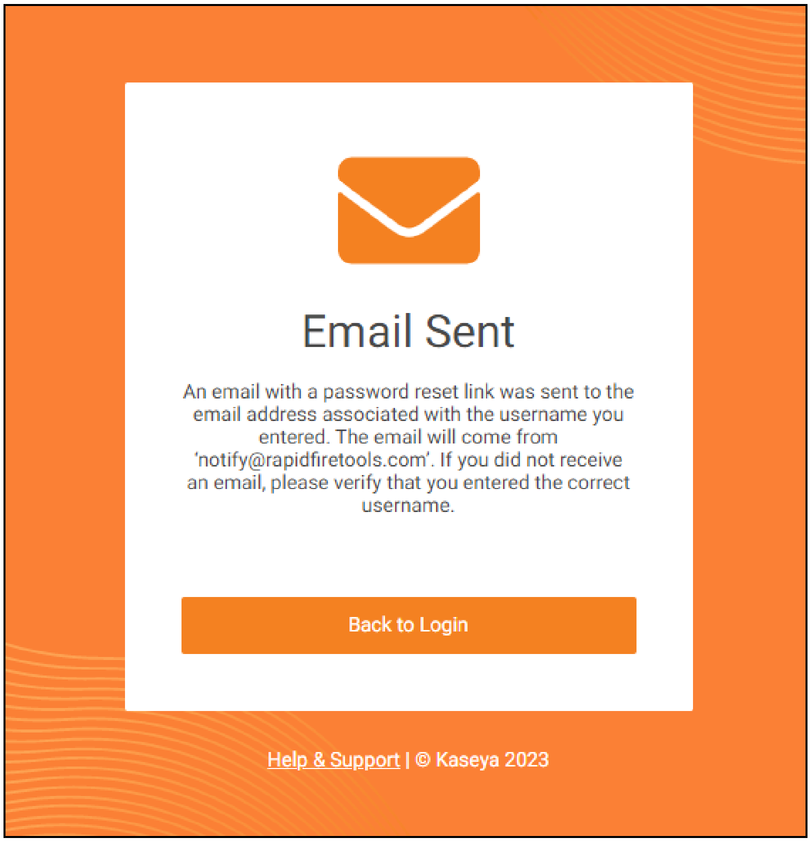
   

4. The user will receive an email with the subject "Assistance Requested." The user clicks the reset password link.

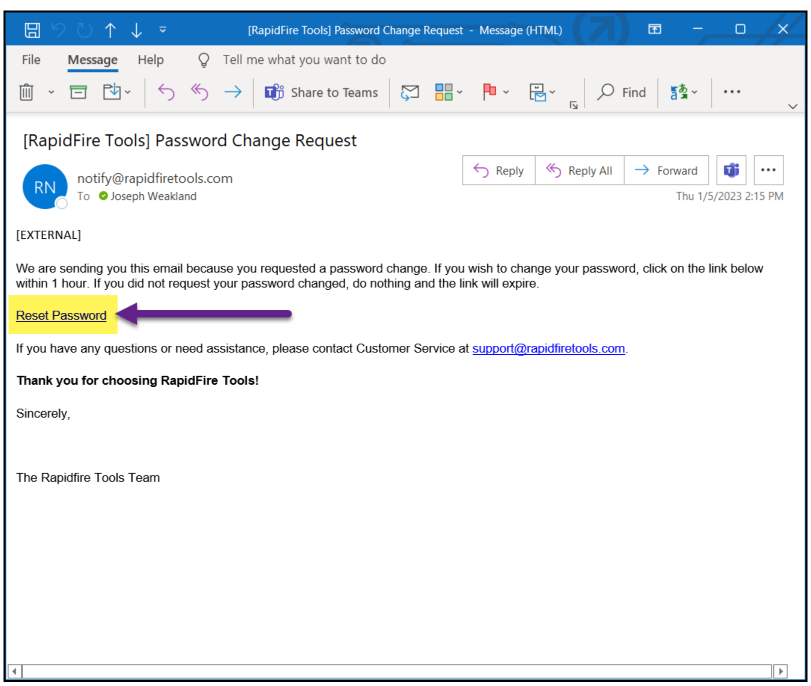


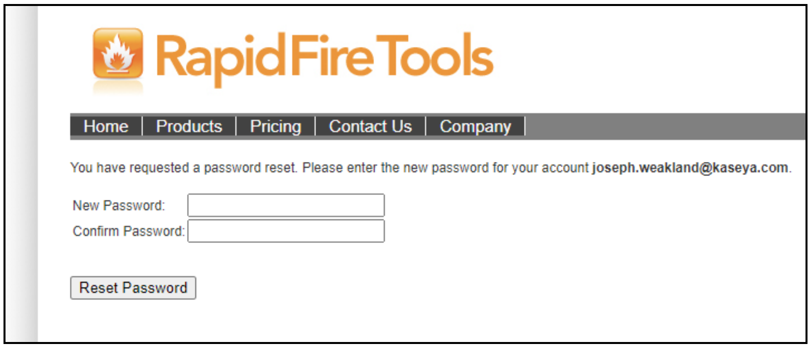
5. The user enters their email to receive the password change request.





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





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

Client View

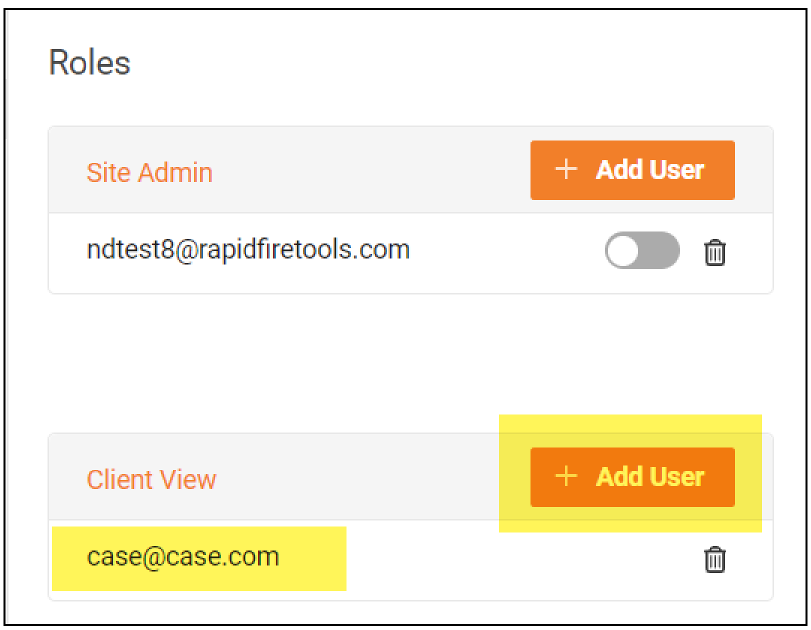
You can invite client users to view your VulScan Dashboard and Reports. This is useful for showing client users your vulnerability remediation efforts.

> **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 "VulScan Site Roles" on page 52 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

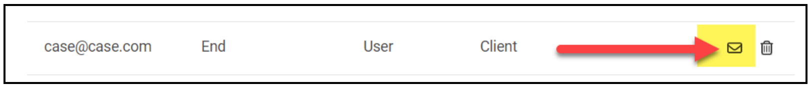
1. From your VulScan site, first create a user for the client from **Home** > **Users**.
2. Next, navigate to **Home** > **Roles**. Assign the client user to the **Client View** Role.



Step 2 – Invite User to VulScan Site

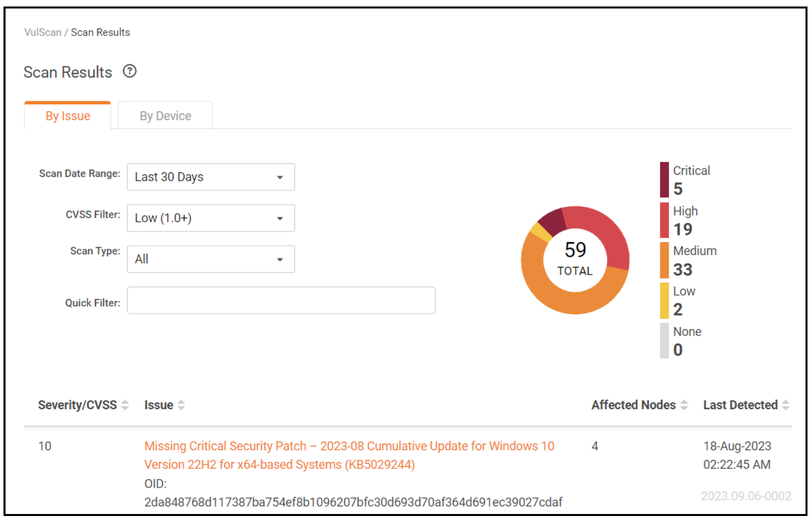
1. To invite the Client View user to the RapidFire Tools Portal, navigate back to Home > Users.

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 "Invite Users to VulScan Site" on page 46.

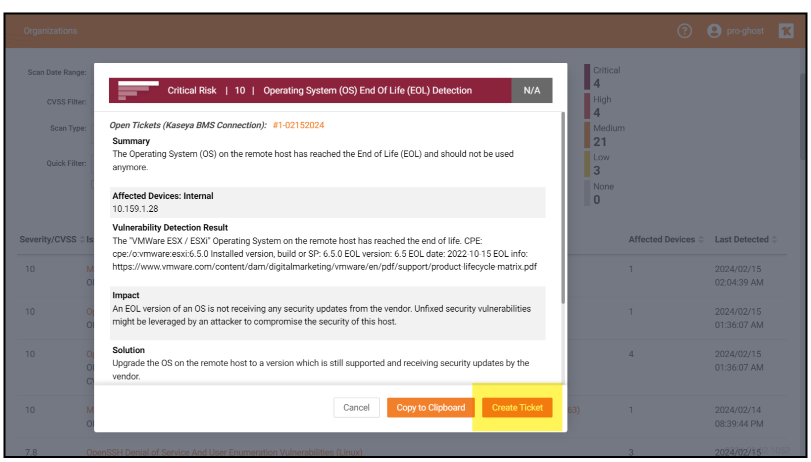


Step 3 – Client View User Accesses VulScan Site and Views Issues/Creates Tickets

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

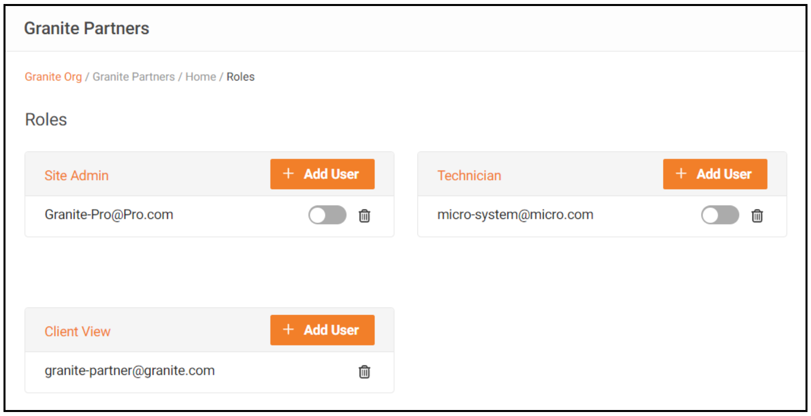


From **Scan Results**, Client View users can also open issues and click **Create Ticket** to generate a ticket.



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.



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 "Client View" on 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.

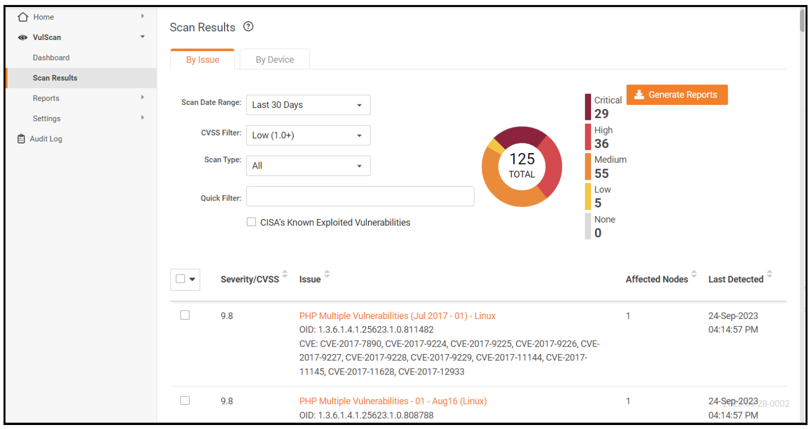
	Roles		
VulScan Menu and Page UI Access	**Site Admin**	**Technician**	**Client View**
Home	Access Granted	Access Granted	No Access
Dashboard	Access Granted	Access Granted	No Access
Data Collectors	Access Granted	Access Granted	No Access
Users	Access Granted	No Access	No Access

	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

Using VulScan

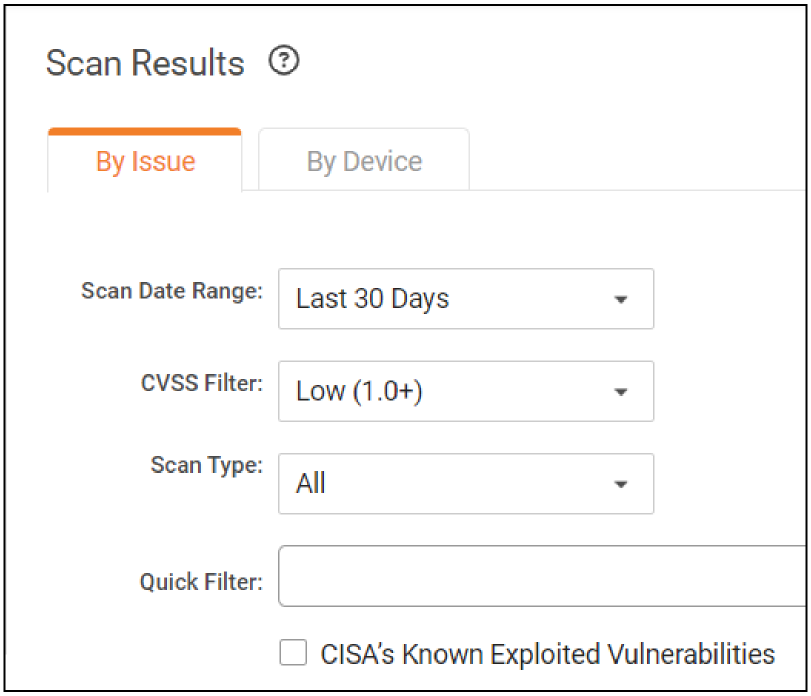
View Vulnerability Scan Results

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.



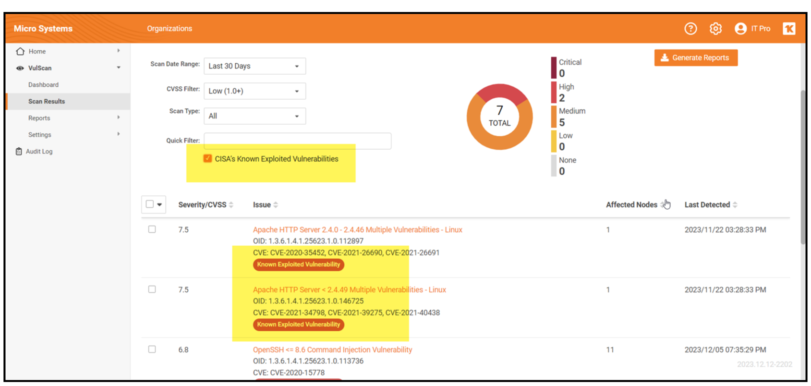
Filter Scan Results

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.



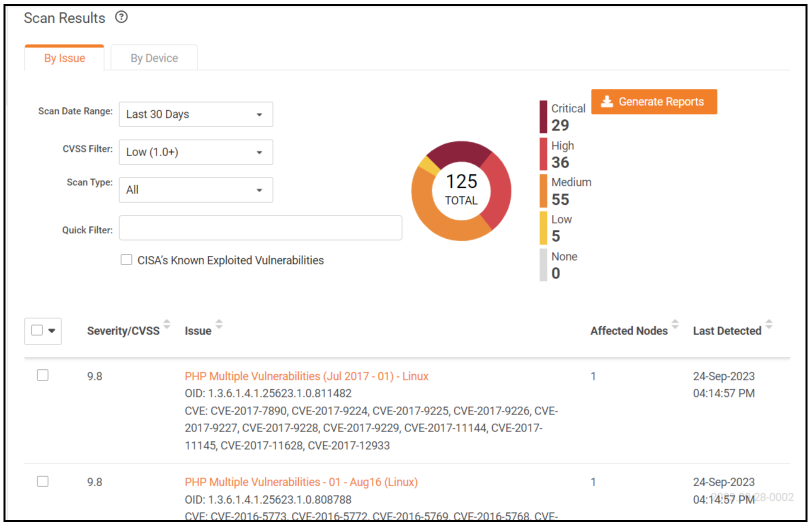
You can also filter by **CISA's Known Exploited Vulnerabilities**. The **Known Exploited Vulnerability** catalog is a library of vulnerabilities that have been actively exploited in the wild. Use this information to help you prioritize remediation efforts on the subset of vulnerabilities that are known 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 https://www.cisa.gov/known-exploited-vulnerabilities-catalog.

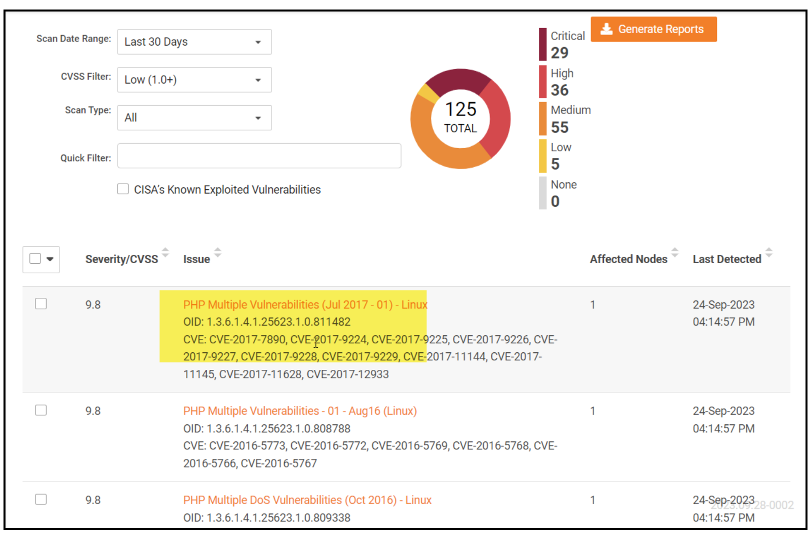


Review Scan Results

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.

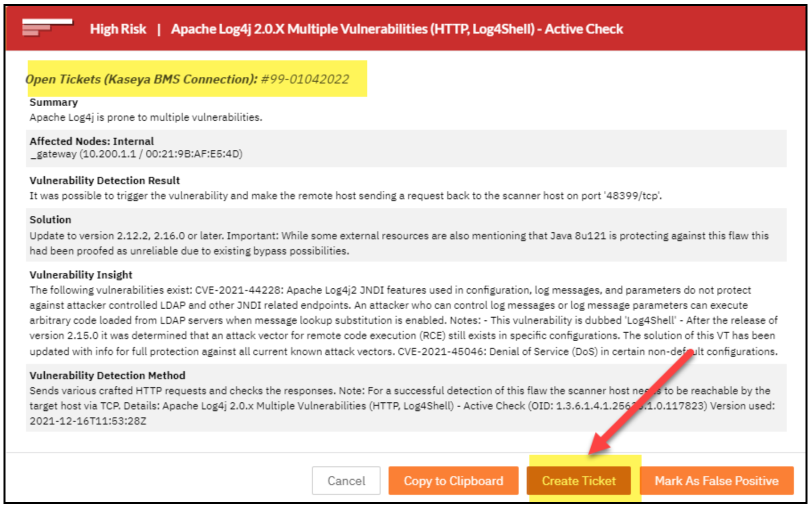


When viewing the scan results **By Issue**, click on the description for an issue to view additional details.

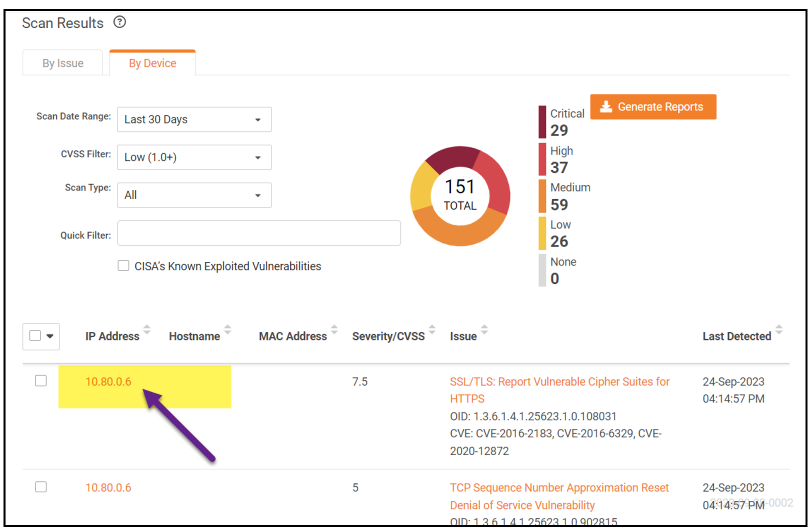


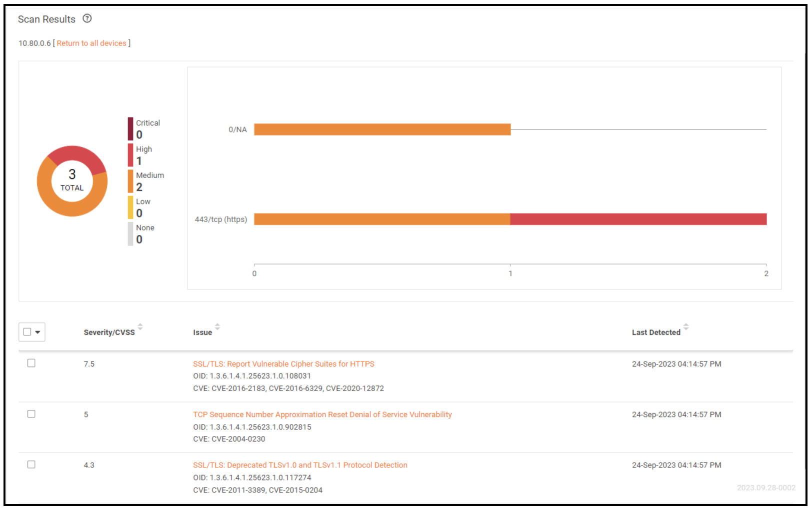
From the Issue Details, you can perform several actions:

- **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 "Set Up and Assign a Ticketing/PSA System Integration to a Site" on page 167.



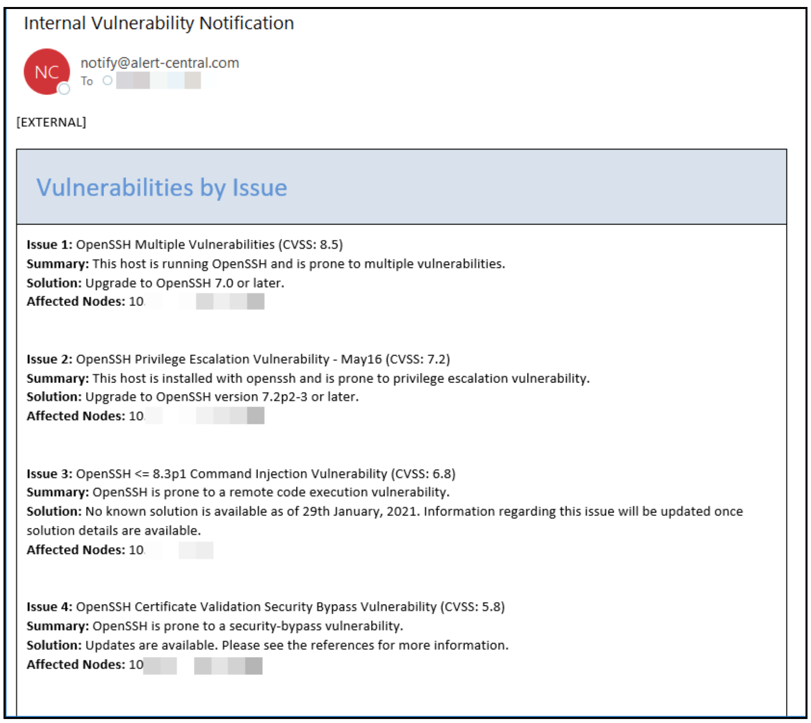
When viewing the results **By Device**, click on an affected device to see a breakdown of vulnerabilities on the device.





Scan 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 "Create Notification Tasks" on page 30.


Internal Vulnerability Notification

NC notify@alert-central.com
To

[EXTERNAL]

Vulnerabilities by Issue

Issue 1: OpenSSH Multiple Vulnerabilities (CVSS: 8.5)
Summary: This host is running OpenSSH and is prone to multiple vulnerabilities.
Solution: Upgrade to OpenSSH 7.0 or later.
Affected Nodes: 10

Issue 2: OpenSSH Privilege Escalation Vulnerability - May16 (CVSS: 7.2)
Summary: This host is installed with openssh and is prone to privilege escalation vulnerability.
Solution: Upgrade to OpenSSH version 7.2p2-3 or later.
Affected Nodes: 10

Issue 3: OpenSSH <= 8.3p1 Command Injection Vulnerability (CVSS: 6.8)
Summary: OpenSSH is prone to a remote code execution vulnerability.
Solution: No known solution is available as of 29th January, 2021. Information regarding this issue will be updated once solution details are available.
Affected Nodes: 10

Issue 4: OpenSSH Certificate Validation Security Bypass Vulnerability (CVSS: 5.8)
Summary: OpenSSH is prone to a security-bypass vulnerability.
Solution: Updates are available. Please see the references for more information.
Affected Nodes: 10

Available Issue Meta Data

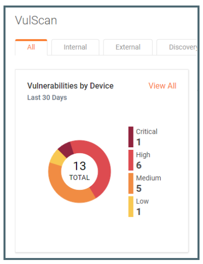
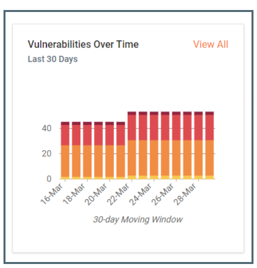
When VulScan detects vulnerabilities on the target network, it presents you with a wealth of information to help you categorize, understand, and resolve these issues. Here's a breakdown of the currently available meta data for each issue.

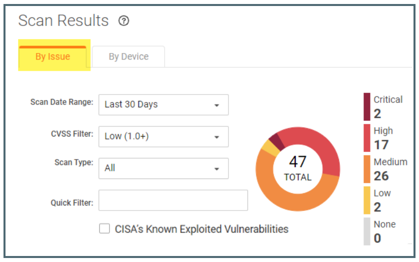
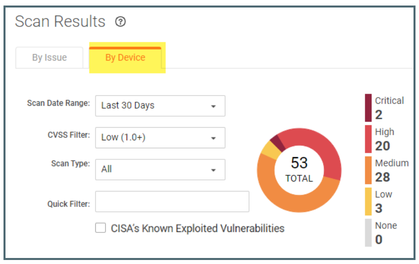
Note: We are constantly improving VulScan, and we may make additional data available for issues in future releases.

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.

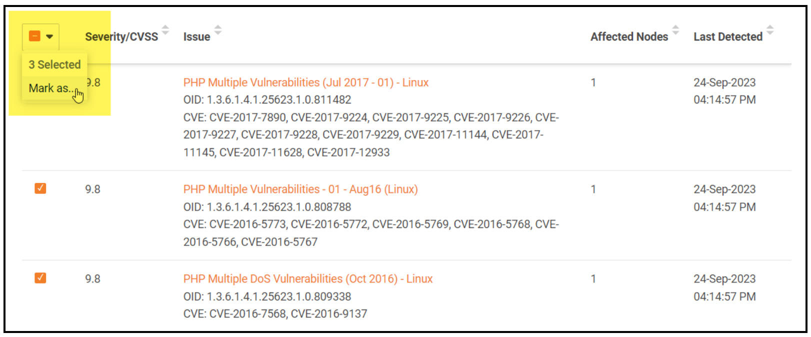
Scan Data Location and Format	Data Parameters
Vulnerability Scanner > Dashboard: Donut Chart 	●Details vulnerabilities by severity identified in the last 30 days ●Refers to the total number of vulnerabilities identified across all devices ●Includes all vulnerability levels (CVSS 1.0+) ●Omits issues marked 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 ●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 ●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
	●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) ●Use filter to redefine chart and table data ●Omits issues marked as false positives

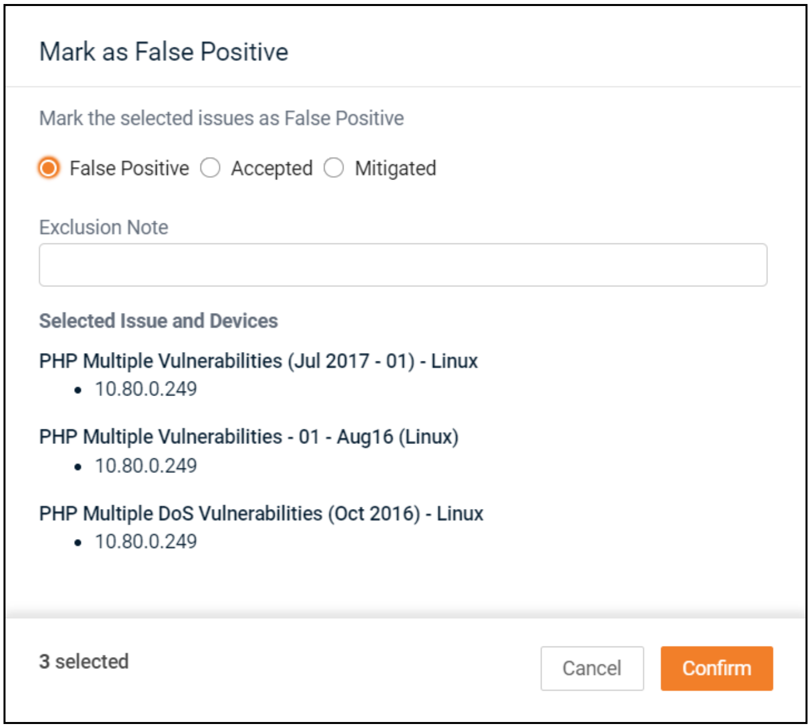
Mark Issues as False Positives, Accepted, or Mitigated (Site-level)

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**.



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 "False Positive Management (Site Level)" on the next page.

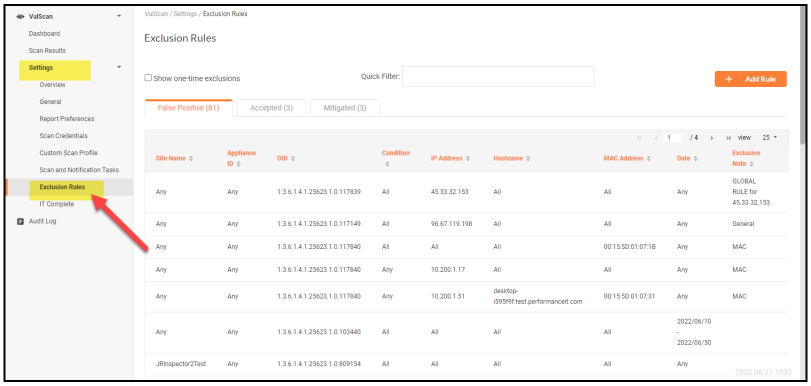
False Positive Management (Site Level)

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

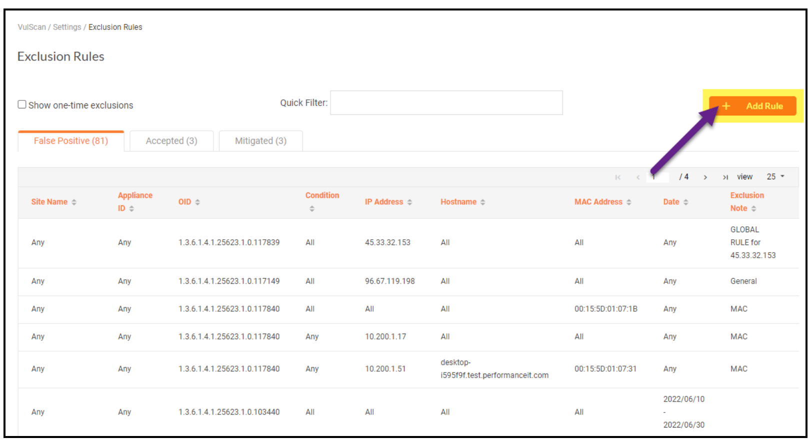
Add Exclusion Rule at the Site Level

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

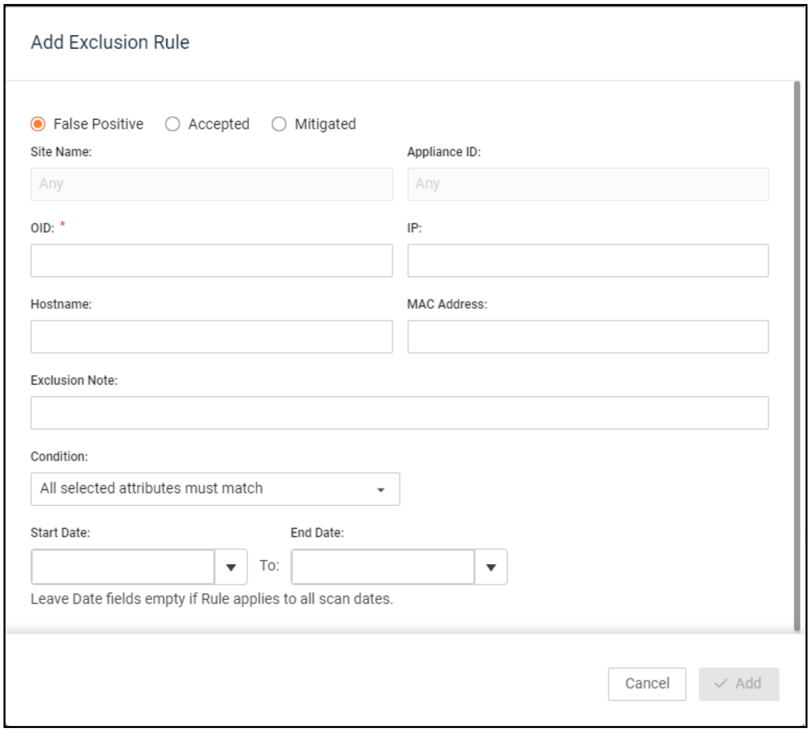
1. Navigate to **[Your Site]** > **VulScan** > **Settings** > **Exclusion Rules**.



2. Click **Add Rule**.



3. The **Add Exclusion Rule** window will appear.



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 "Configure Device Matching Criteria to Reduce False 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

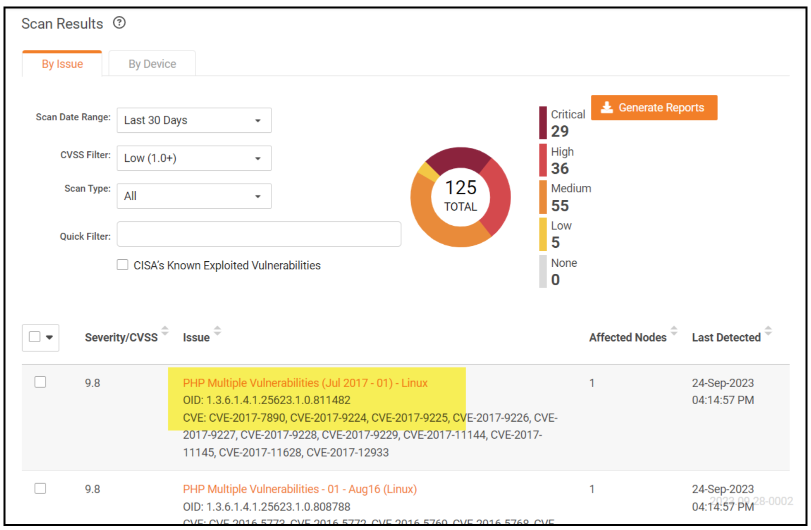
- To edit an exclusion rule, click the pencil icon next to a rule. Make and save your changes.
- To delete an exclusion rule, click the trash icon next to a rule. When you delete a rule at the site level, the excluded scan results will return and appear for this specific site under Scan Results.

Create Ticket from Issue

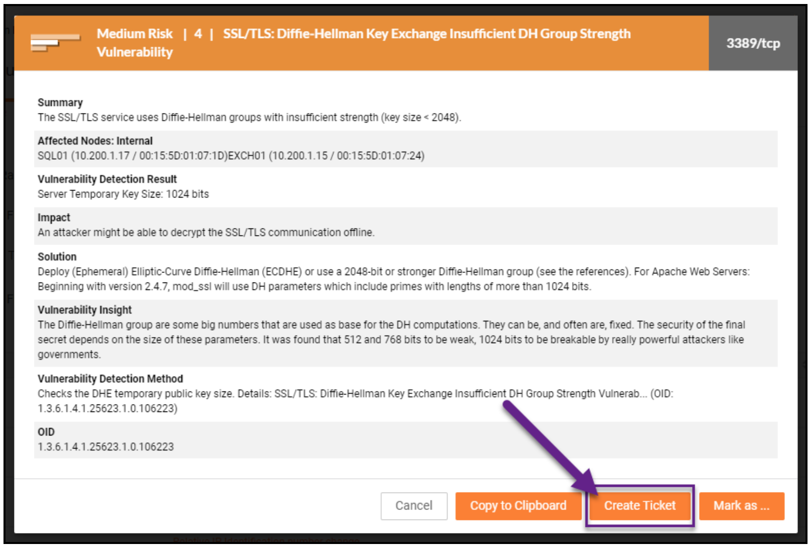
VulScan offers you flexibility in how you choose to handle identified issues. For example, you can "Create Notification Tasks" on page 30 that automatically export detected issues as tickets to a PSA system.

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:

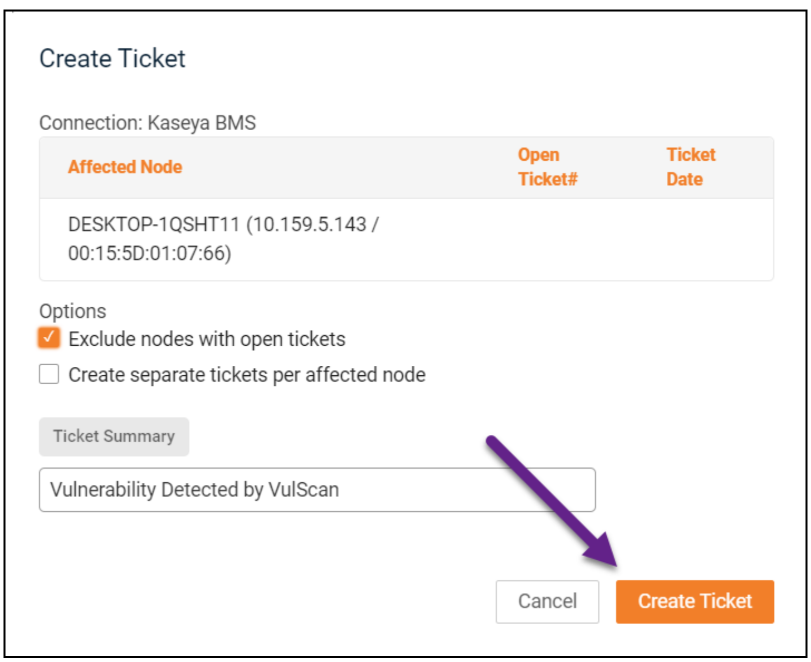
1. First, be sure you have created a connection to your PSA and mapped that connection to your VulScan site. See "Set Up and Assign a Ticketing/PSA System Integration to a Site" on page 167.
2. Next, from your VulScan site access **VulScan** > **Scan Results** from the left menu.
3. Then click the issue you want to convert to a PSA ticket.



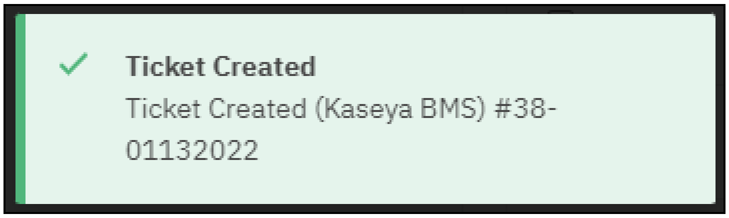
4. From the issue details, click **Create Ticket**.



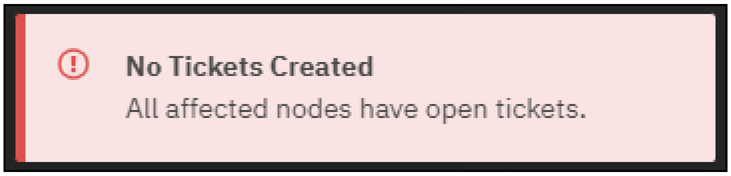
5. From the Create Ticket window, configure the ticket. Specifically:
    - **Exclude nodes with open tickets**: Enable this to prevent duplicate tickets
    - **Create separate tickets per affected node**: You can optionally choose to create separate tickets for affected devices or create one ticket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



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



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

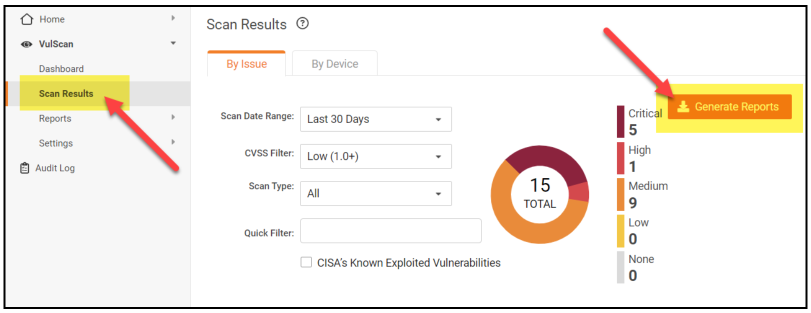


Generate VulScan Issues and Detail Reports

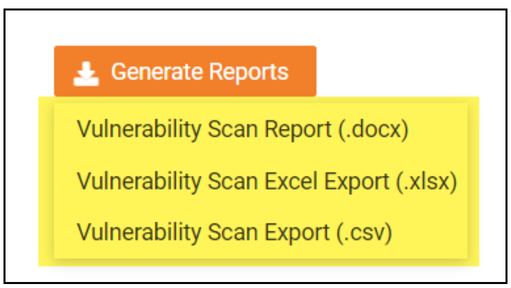
Once you perform one or more vulnerability scans, you can **generate reports** that detail site vulnerabilities. You can mail or print the report to provide as evidence of scanning or for compliance purposes. Here how it works:

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

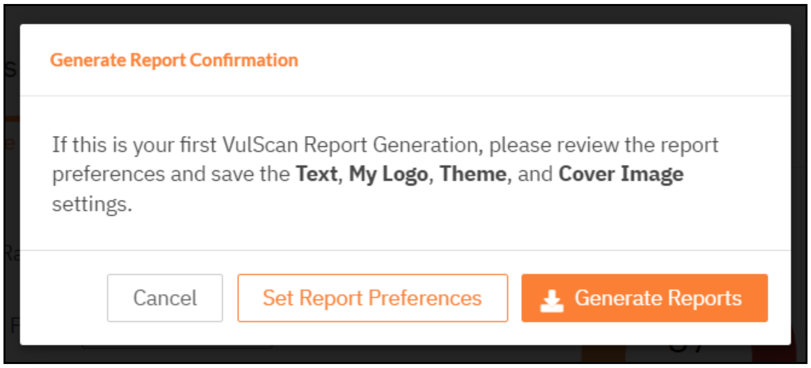
> **Note:** You must first have performed one or more successful internal or external vulnerability scans to generate reports.



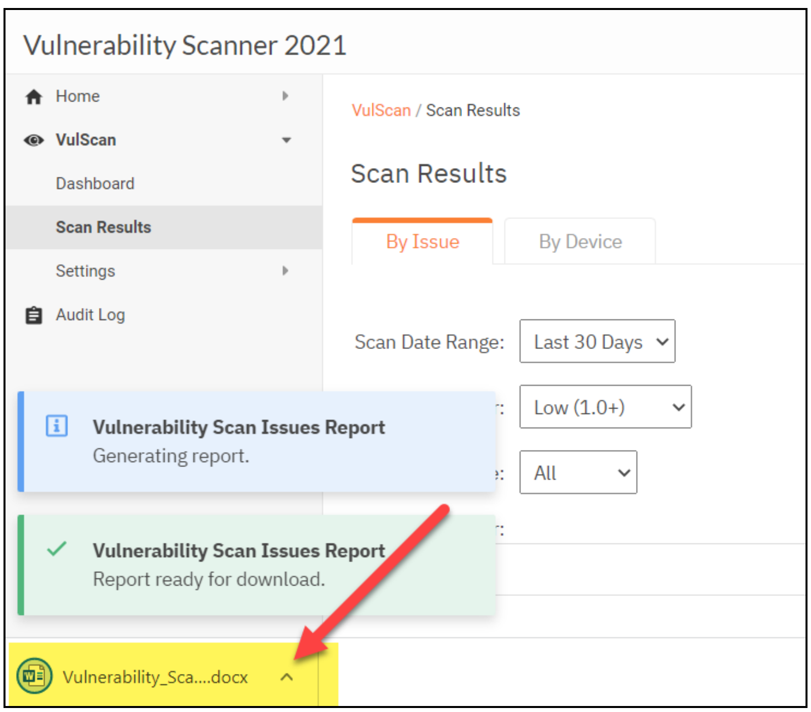
3. From the drop-down menu, select the report type: **.docx**, **.xlsx**, or **.csv**.



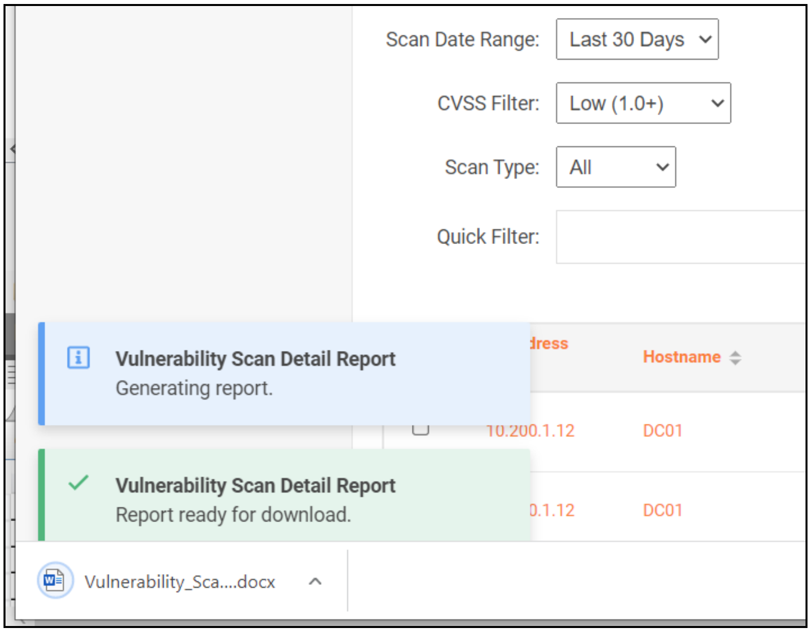
4. Configure your **Report Settings** if you haven't done so already. Otherwise, click **Generate Reports**.



- 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.



- 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.



Generate VulScan Trending Reports

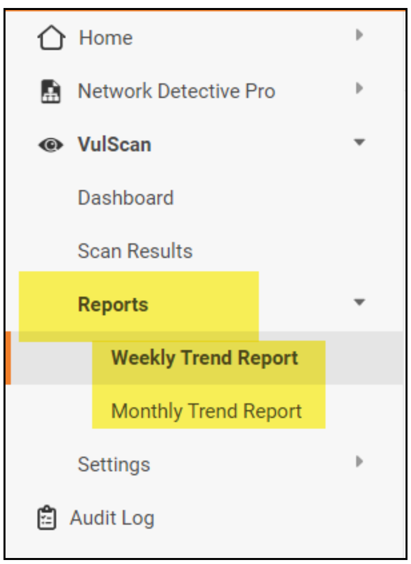
With VulScan **Trending Reports**, you can visualize vulnerability management on a weekly and monthly basis. These dynamic graphs display the results of your scans in a dashboard using filters that you configure. You can likewise download your custom graphics as Excel files.

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

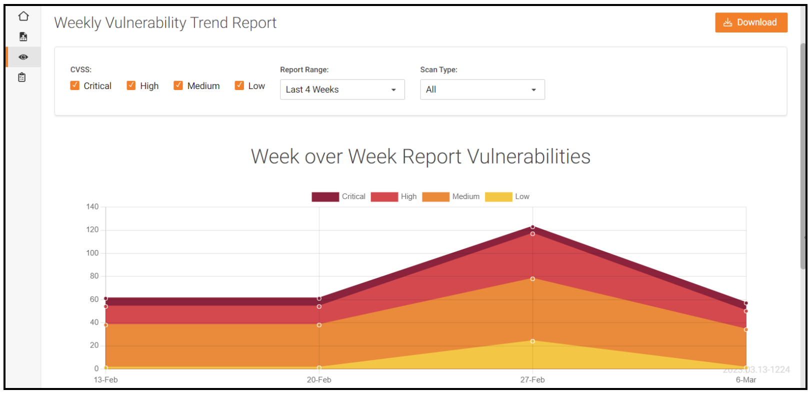
To generate Trending Reports:

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.



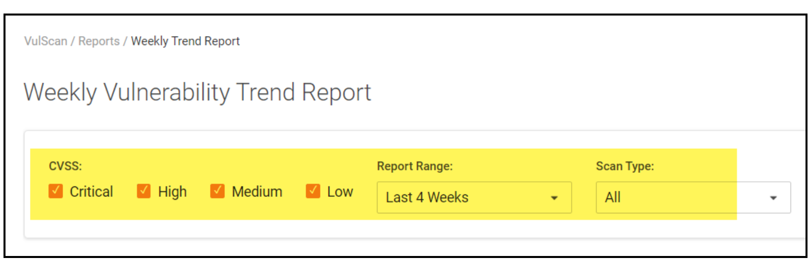
- **Total Vulnerabilities**: The total sum of all non-duplicated vulnerabilities for all scans during the time period. One vulnerability counts as a single Issue/Device combination.
- **Newly Discovered**: Vulnerabilities detected in the current week that were not detected in the previous week.
- **Resolved**: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

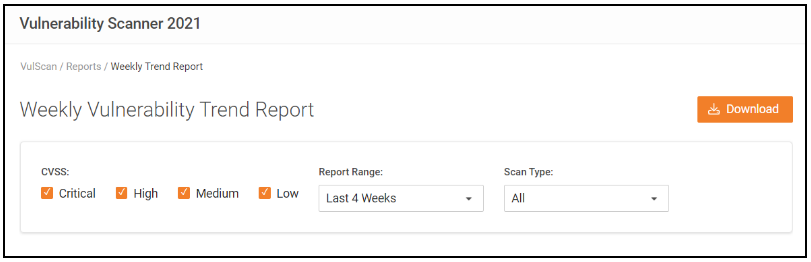
- **CVSS**: Choose to filter the issue by Critical, High, Medium, and Low vulnerability severity levels.
- **Report Range**: Choose the number of weeks or months for the report time period.
- **Scan Type**: Filter the scan results by **Internal** or **External** scans, or by **Discovery Agent** scans.



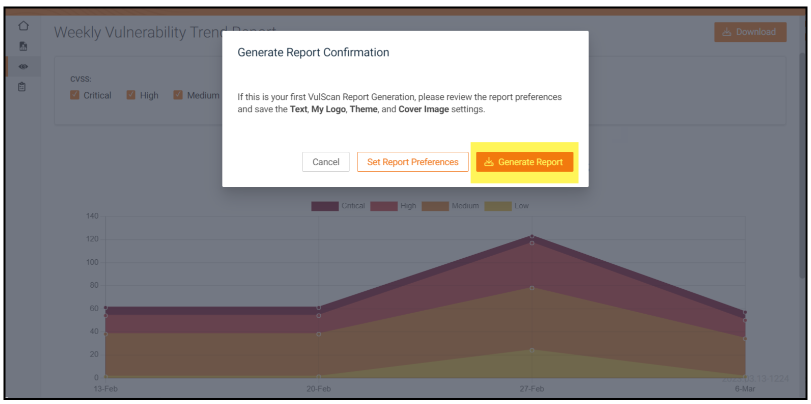
Step 3 — Generate Dynamic Graphs

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

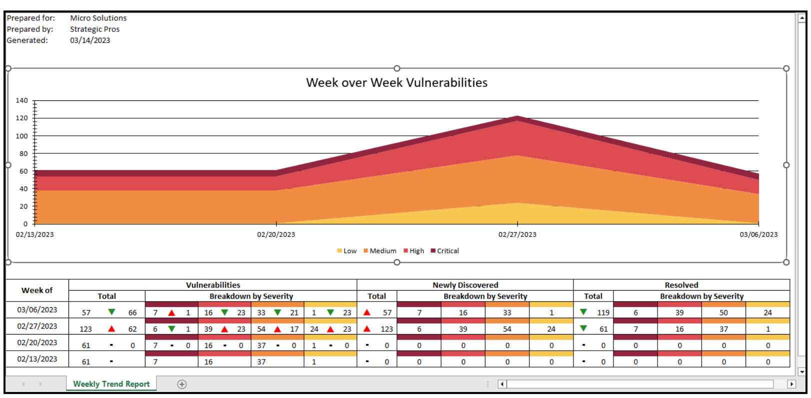
1. From the right page, click **Download**. The spreadsheet will appear as a download in your browser.



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



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



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)

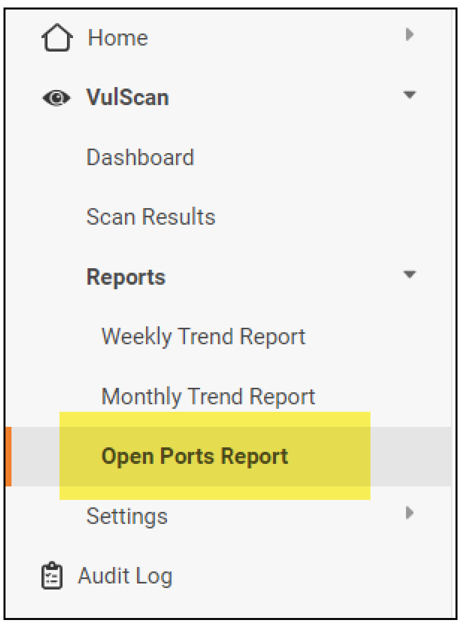
Open Ports Report

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

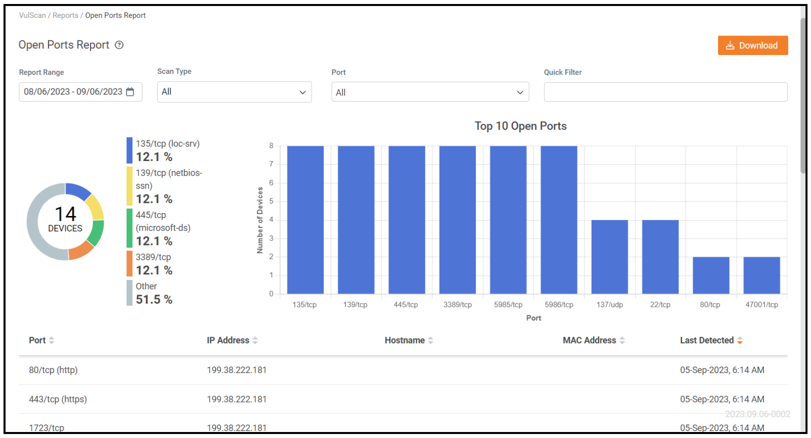
From your VulScan site, navigate to **VulScan** > **Reports** > **Open Ports Report**. Note that you must have completed 1 or more internal and/or external vulnerability scans to view detected open ports.



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



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-3GV5OEI	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 "Client View" on page 50 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

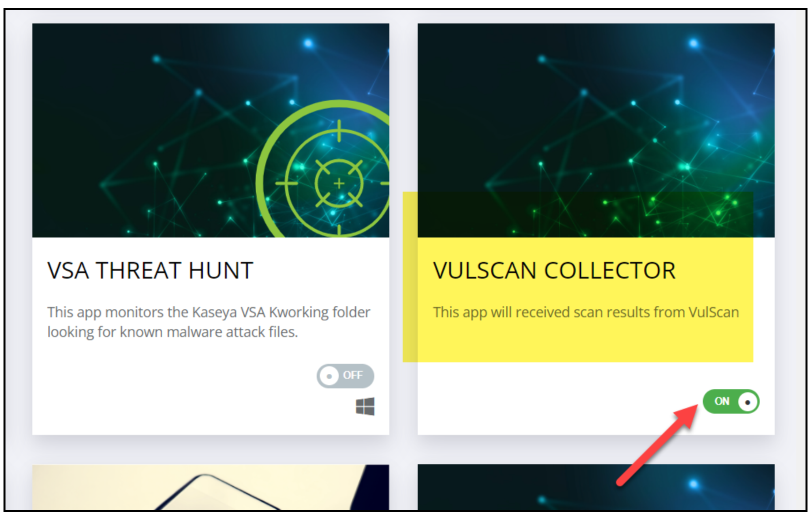
This topic covers how to export VulScan notification tasks to **RocketCyber** (https://www.rocketcyber.com). This integration allows you to view VulScan security issues from within your RocketCyber dashboard. In addition to your VulScan subscription, you will need a RocketCyber subscription to use this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

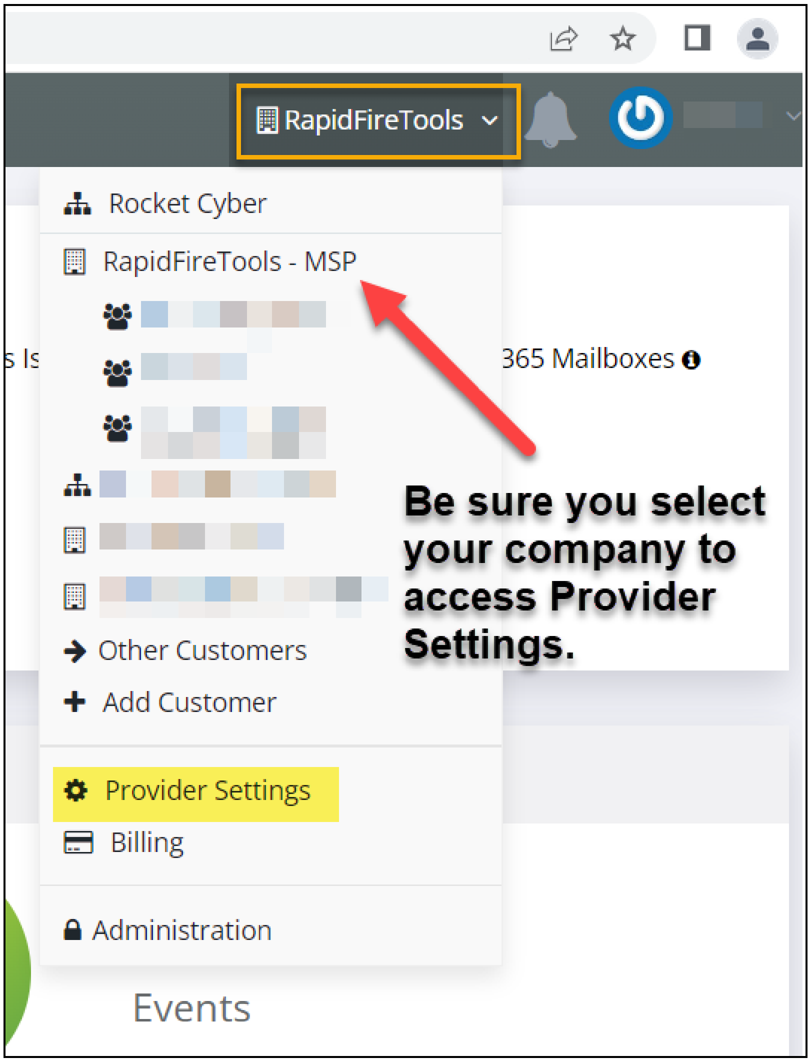


3. **Click the slider** to enable the VulScan Collector.

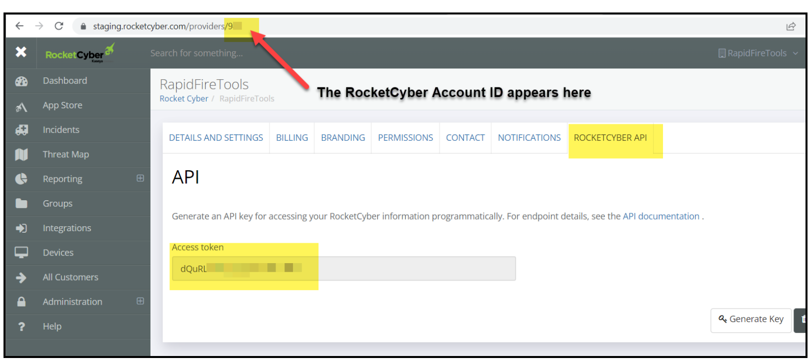
Step 2 — Gather API Credentials from RocketCyber Account

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.



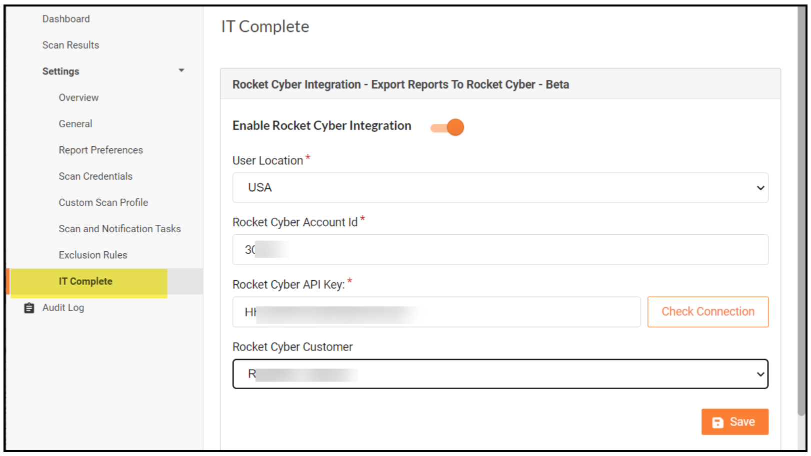
3. Copy the **API access token**.

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.



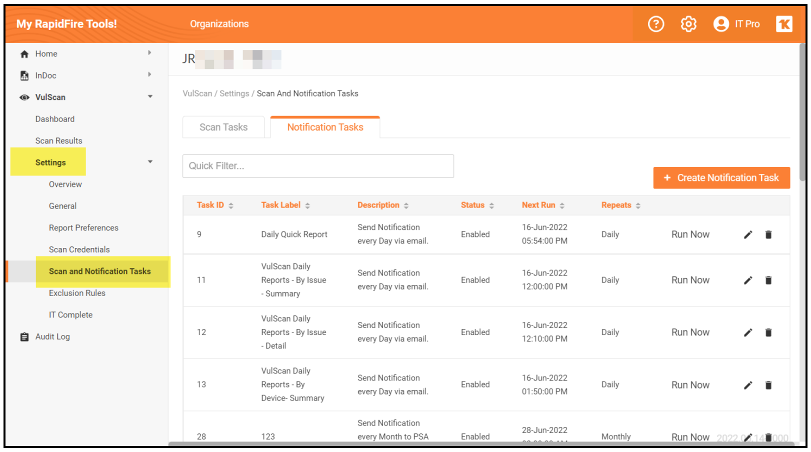
3. Select your **User Location** for the site: USA or Europe.
4. Enter the **Account ID** and **API key** that you collected in "Step 2 — Gather API Credentials from RocketCyber Account" on page 80.
5. Click **Verify** to test the connection. A modal will appear to inform you of a successful connection.
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

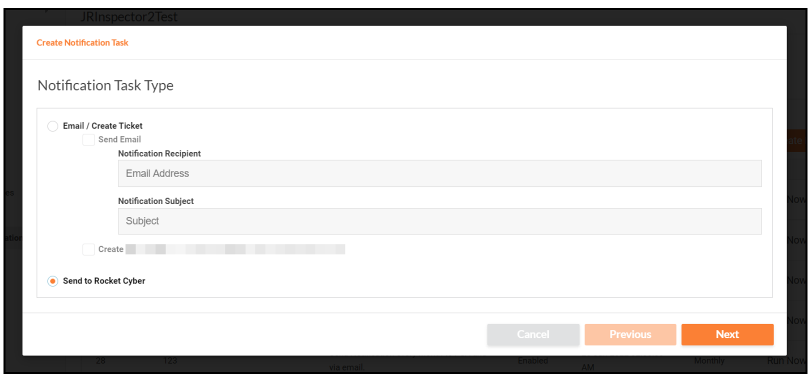
Now we need to create a new notification task to export VulScan issues to RocketCyber.

Note: You must have first set up scan tasks to detect vulnerabilities to export. See "Create Internal Scan Task" on page 20 and/or "Create External Scan Task" on page 27.

1. From your site, navigate to **Settings** > **Scan and Notification Tasks**.



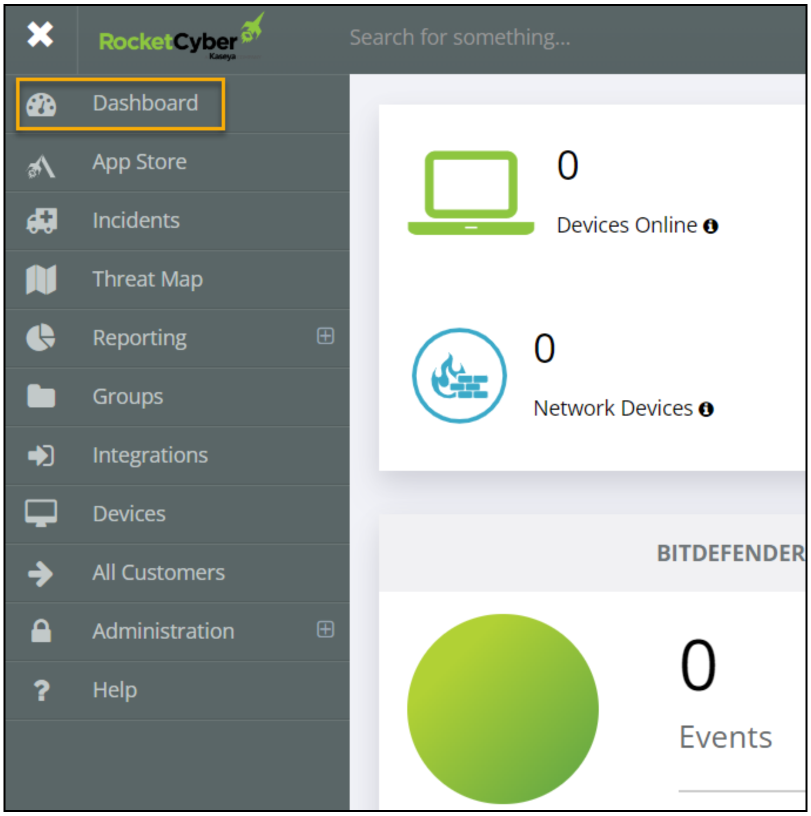
2. Open the **Notifications** tab and click **Create**.
3. From the **Notification Task Type** screen, select **Send to RocketCyber**. Then configure and save the notification task as you normally would. See also "Create Notification Tasks" on page 30.



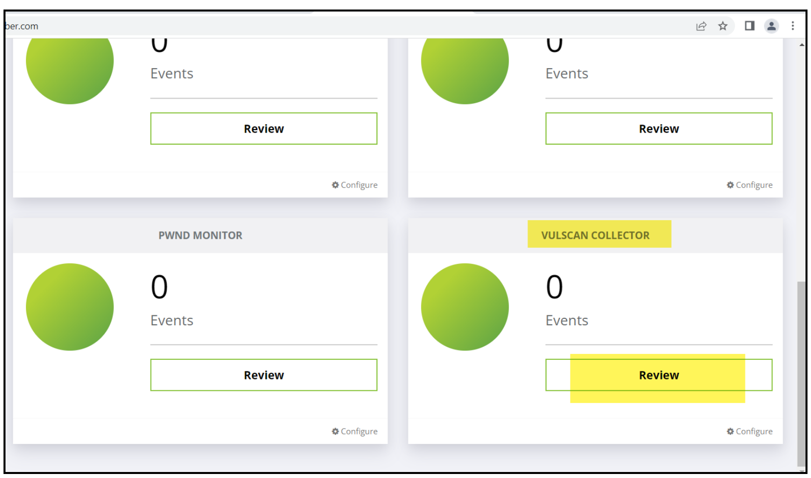
Step 5 — Browse VulScan Issues from RocketCyber Dashboard

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

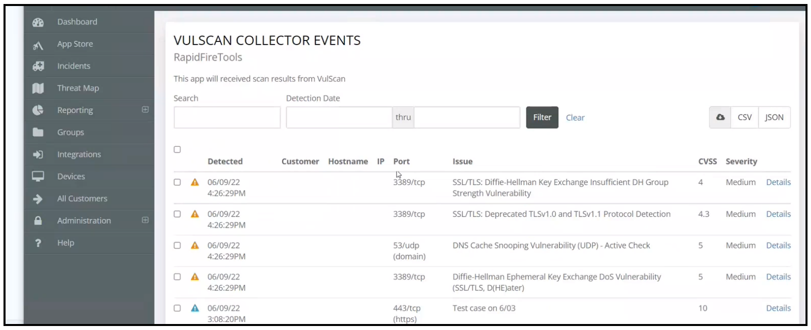
1. Open RocketCyber and select your company and customer.
2. Open the **Dashboard** from the left menu.



3. Scroll down to **VulScan Collector** and click **View**.



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.


Dashboard
App Store
Incidents
Threat Map
Reporting
Groups
Integrations
Devices
All Customers
Administration
Help
VULSCAN COLLECTOR EVENTS
RapidFireTools
This app will received scan results from VulScan
Search
Detection Date
thru
Filter
Clear
CSV
JSON
Detected
Customer
Hostname
IP
Port
Issue
CVSS
Severity
06/09/22 4:26:29PM
3389/tcp
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability
4
Medium
Details
06/09/22 4:26:29PM
3389/tcp
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection
4.3
Medium
Details
06/09/22 4:26:29PM
53/udp (domain)
DNS Cache Snooping Vulnerability (UDP) - Active Check
5
Medium
Details
06/09/22 4:26:29PM
3389/tcp
Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSL/TLS, D(HE)ater)
5
Medium
Details
06/09/22 3:08:20PM
443/tcp (https)
Test case on 6/03
10
Details

Set Up Remote Internal Vulnerability Scanner

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

Introduction

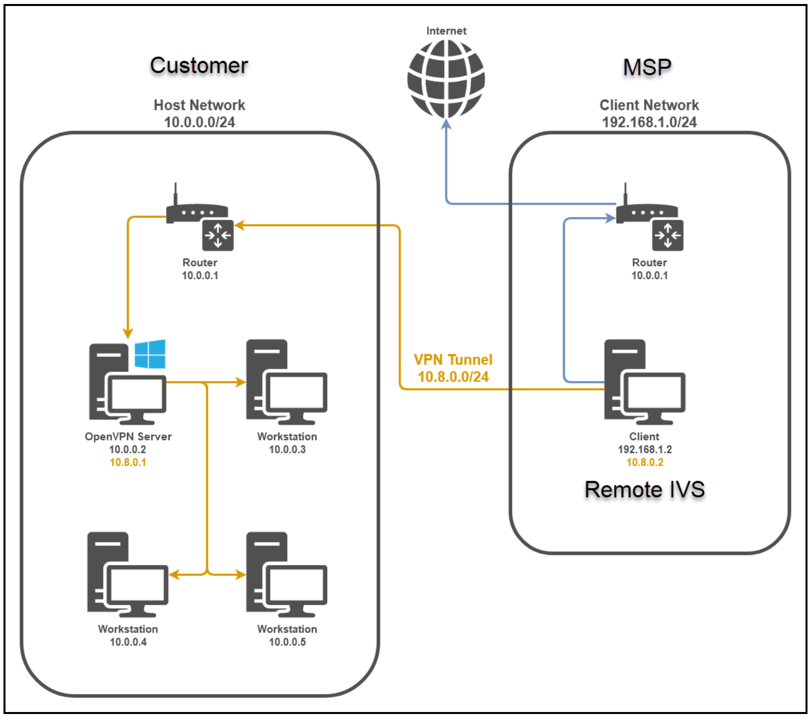
Not all customers (particularly small companies) have enough resources to maintain a separate device to perform internal vulnerability scans. The **Remote Internal Vulnerability Scanner** (Remote IVS) allows MSPs to offer a vulnerability scanning service to customers that do not have the available infrastructure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

- "Step 1 — Provision and Install Remote Internal Vulnerability Scanner" on the facing page
- "Step 2 — Setting up the OpenVPN on the server" on page 88
- "Step 3 — Create Open VPN Configuration File" on page 101
- "Step 4 — Upload Open VPN Configuration File to VulScan" on page 104
- "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.

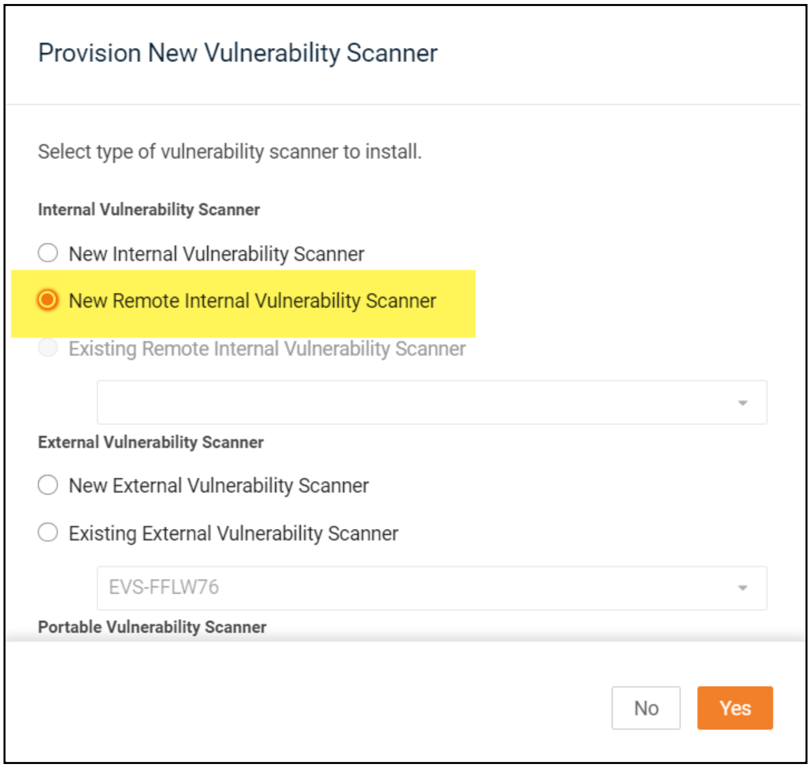


Step 1 — Provision and Install Remote Internal Vulnerability Scanner

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

1. 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 "Provision VulScan" on page 200.



2. Visit https://www.rapidfiretools.com/vs-downloads 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.

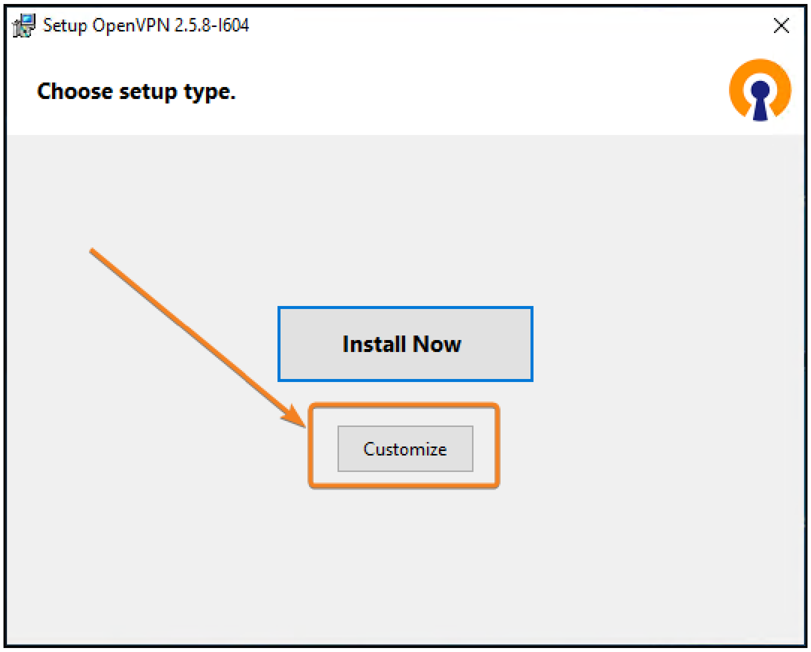
Configure Router Port Forwarding

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 this website to find detailed forwarding instructions for your specific router make and model.

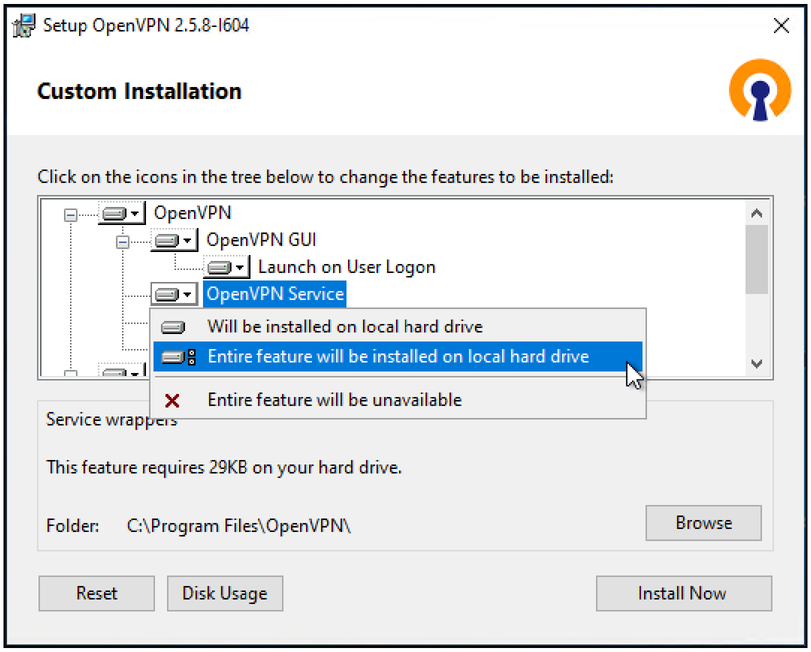
Installing the OpenVPN program on the server

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

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



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



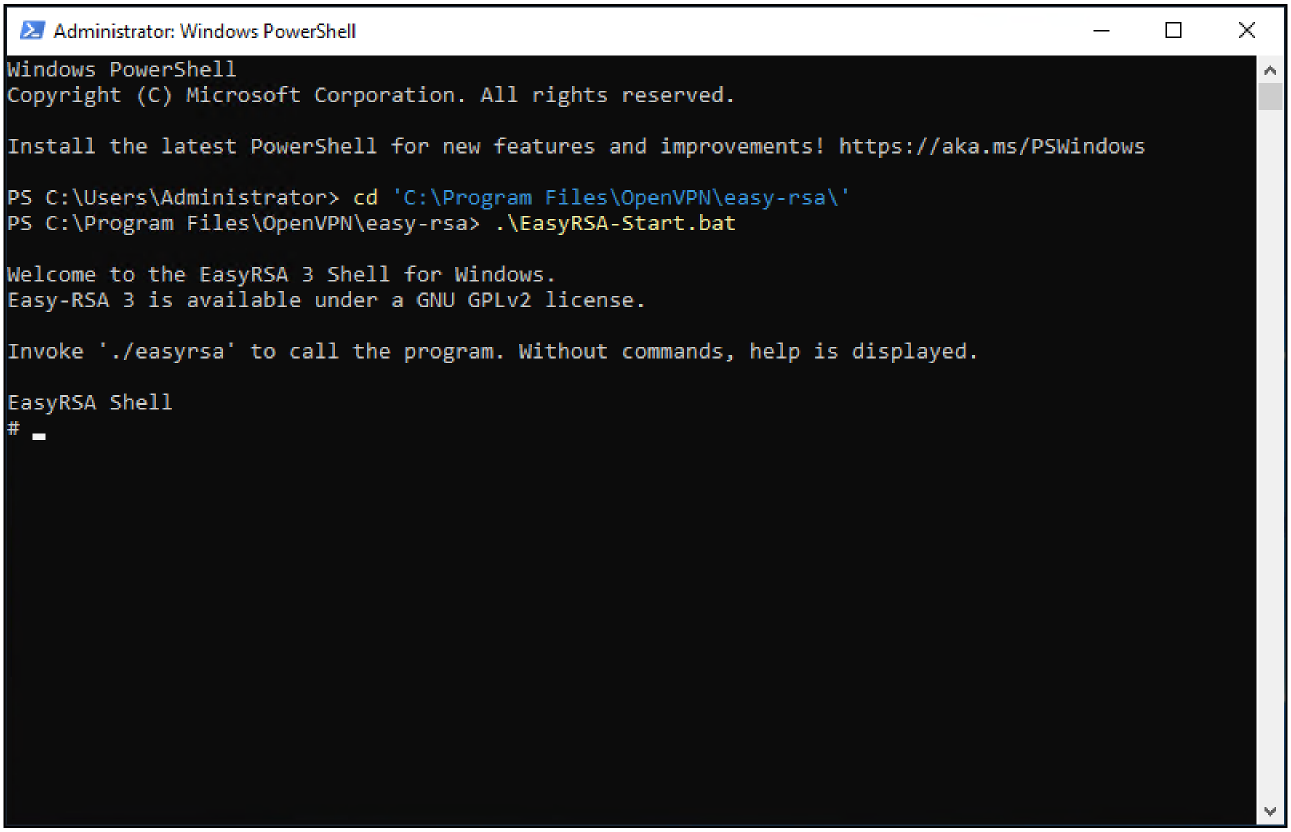
Next, click "Install Now" and wait for the client to install.

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 `EasyRSA-Start.bat` 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.

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 `auto-config` directory, create a new file called `server.ovpn`. 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

#=====================UPDATE ME=====================#
# 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"
#=====================UPDATE ME=====================#
# 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
```

```
# 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 `0.0.0.0` 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".

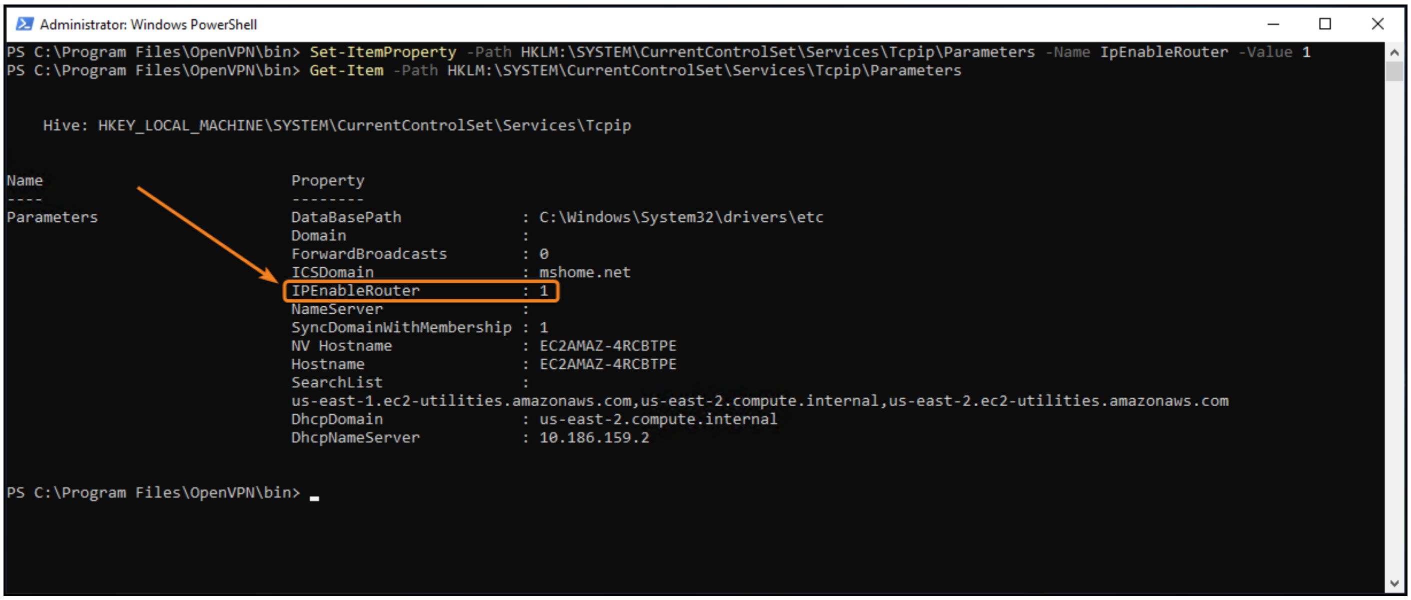
```
HKEY_LOCAL_
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\IPEnabl
eRouter
```

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

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

Verify that the key was changed with the following command:

```
Get-Item -Path
HKLM:\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
```

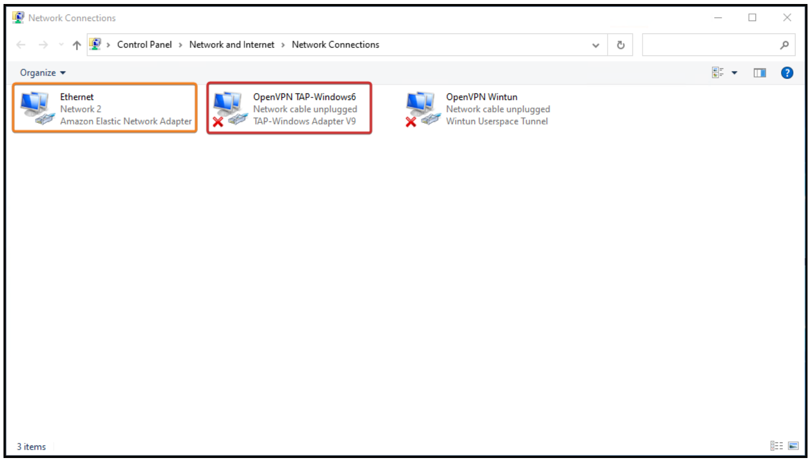


Enable internet connection sharing

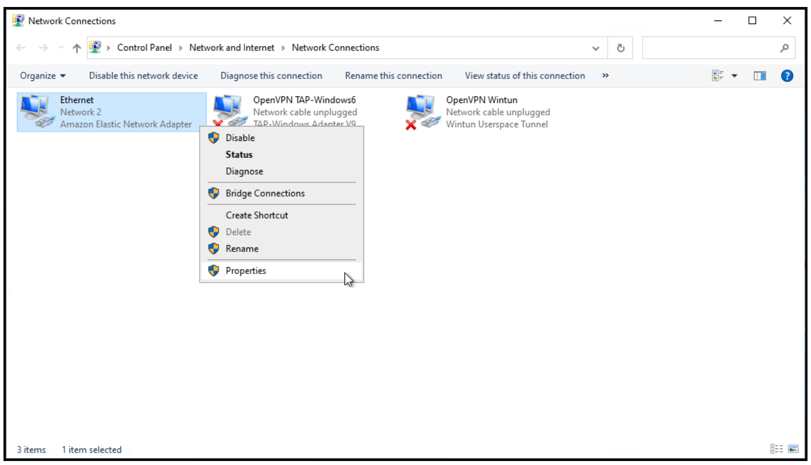
To allow the OpenVPN tunnel network adapter to access the local network, enable internet sharing on the local ethernet adapter.

Open the run dialog (⊞`Win` + `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).

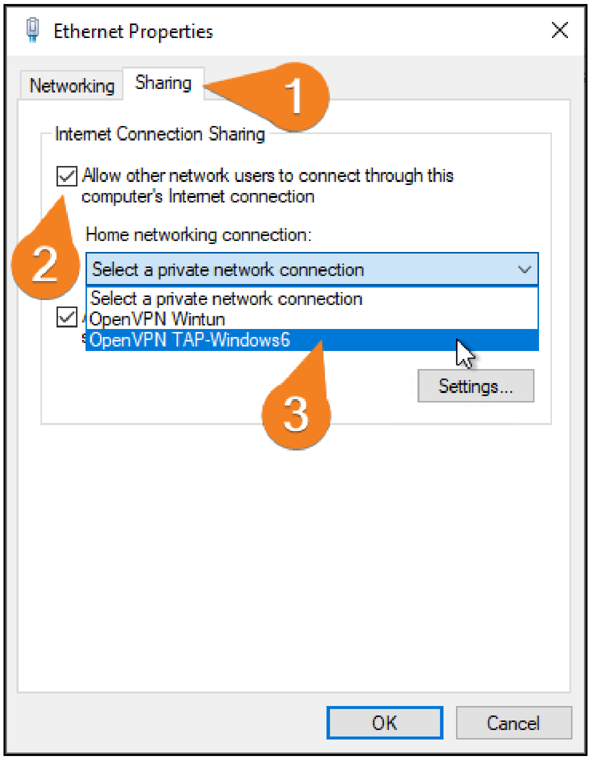


Right-click on the local network adapter and open the "Properties" menu.



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" drop-down.



Restart to apply changes

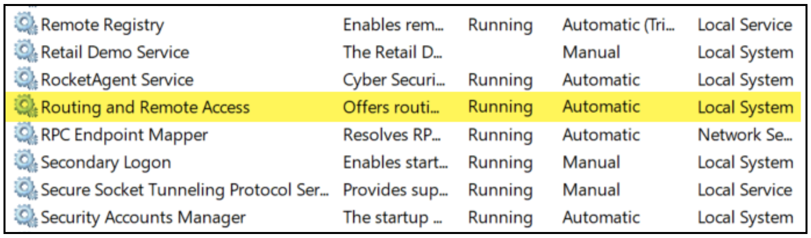
Restart the computer to apply all of the Windows network settings we changed in this section.

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

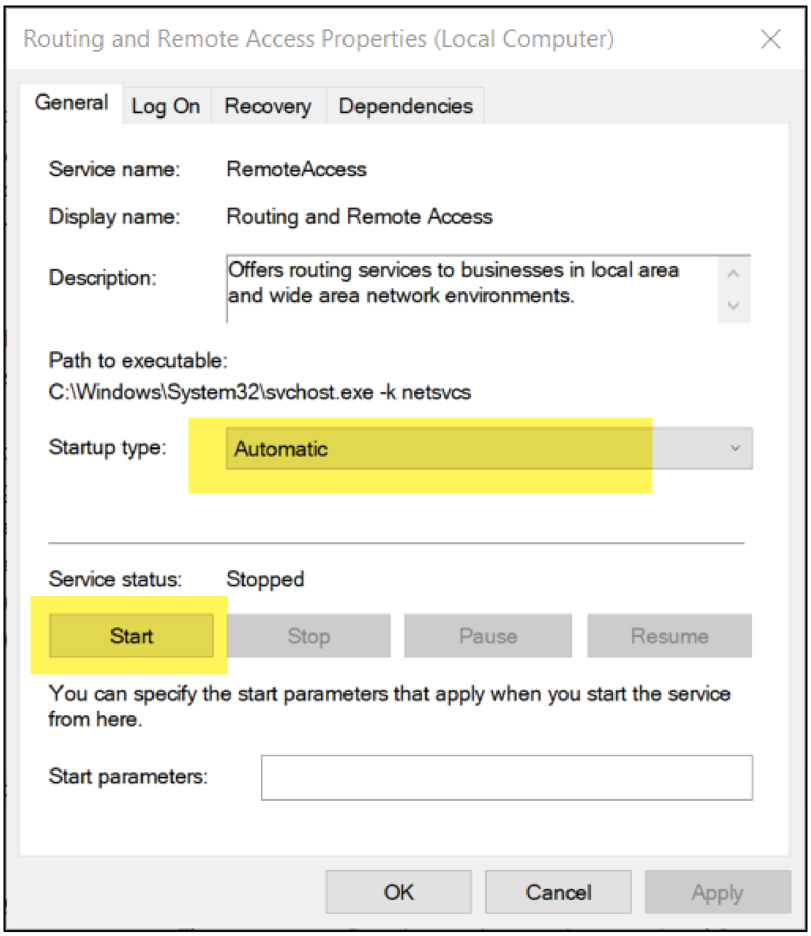
If you wish to turn off the OpenVPN server at a later time, or want to refresh configuration options, you can do so by stopping and starting the "OpenVPNService" service.

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.



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.



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 (`\\`). 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

#=====================UPDATE ME======================#
# External IP/domain of the host network
# Defines host's listening port
remote 0.0.0.0 1194
#=====================UPDATE ME=====================#

# Most clients don't need to bind to
# a specific local port number.
nobind
```

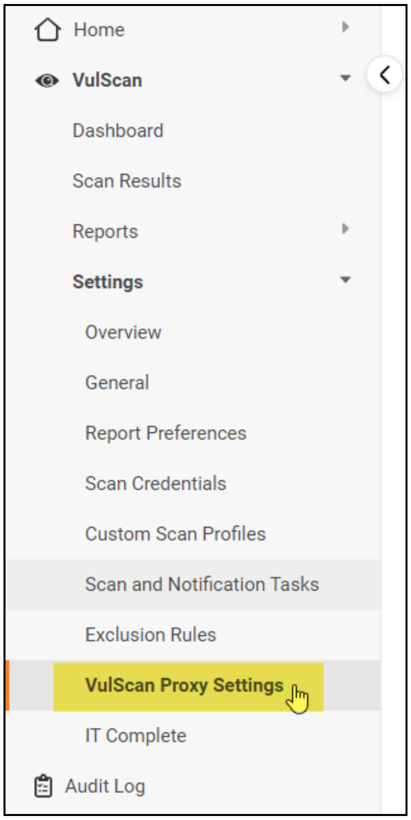
```
# Try to preserve some state across restarts.
persist-key
persist-tun

#=====================UPDATE ME=====================#
# 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>
#=====================UPDATE ME=====================#

# Verify server certificate by checking that the
# certificate has the correct key usage set.
remote-cert-tls server
key-direction 1

#=====================UPDATE ME=====================#
# 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>
#=====================UPDATE ME=====================#

# 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.

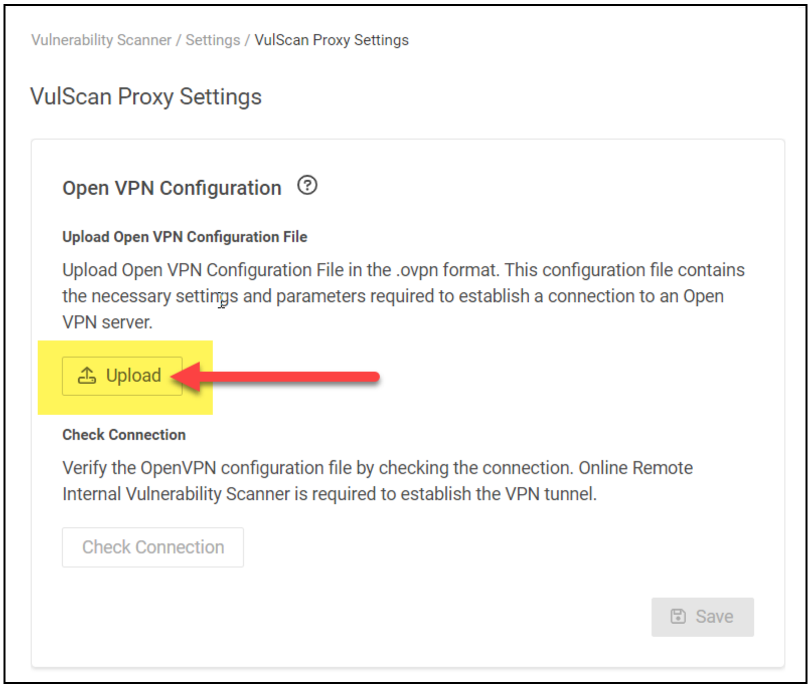
Step 4 — Upload Open VPN Configuration File to VulScan

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

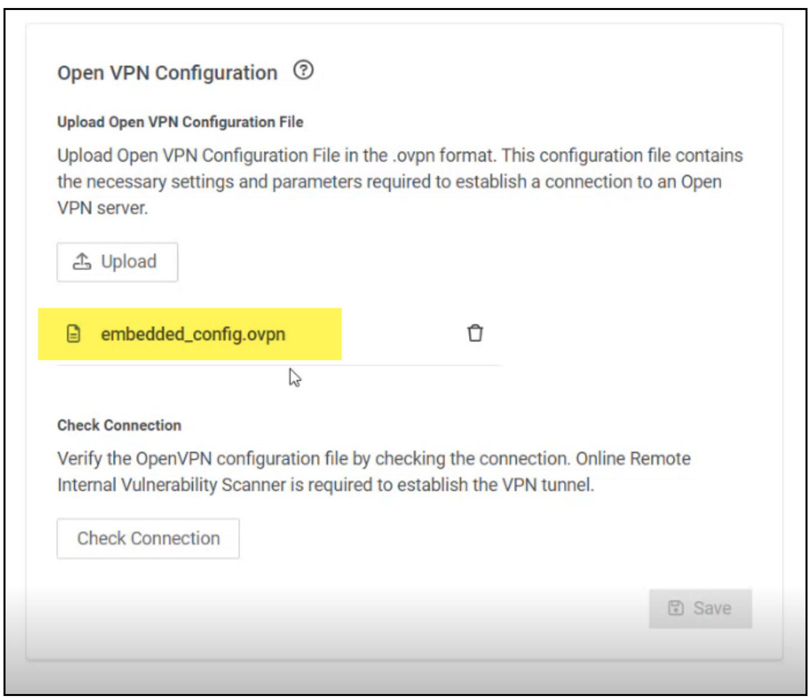
1. From your site, navigate to **VulScan** > **Settings** > **VulScan Proxy Settings**.



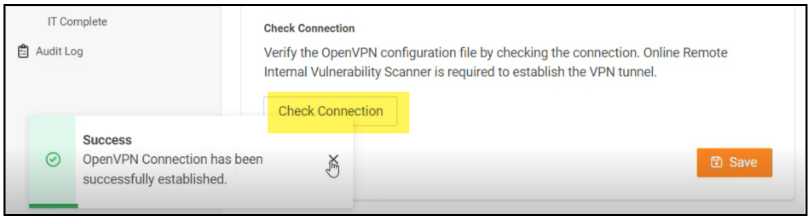
2. Under **Upload Open VPN Configuration File**, click **Upload** and select the configuration file you created earlier.



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



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

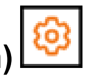
You are now ready to perform scans using the Remote IVS.

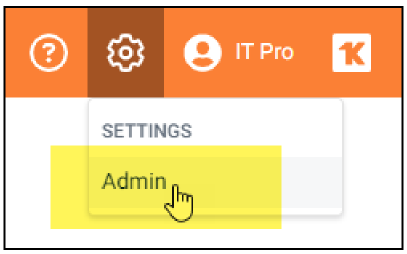
See "Create Scan and Notification Tasks" on page 20 for a complete walkthrough.

Manage Portal Users and Access

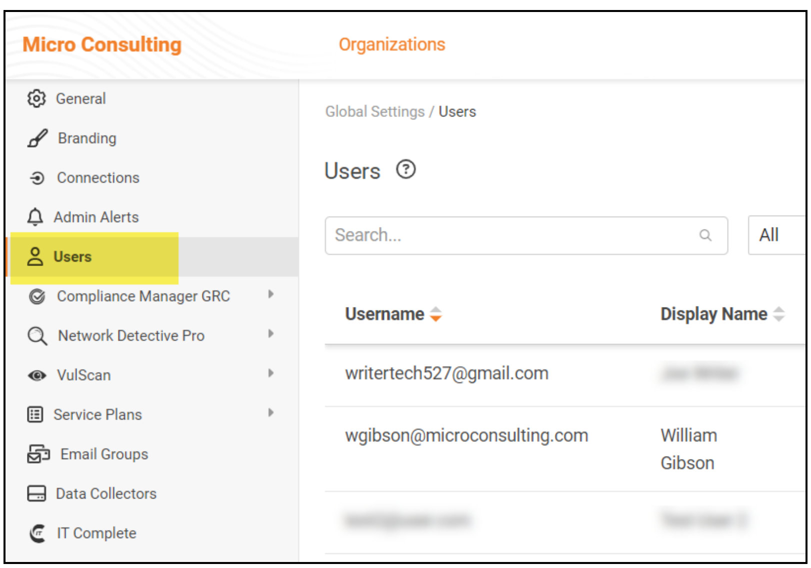
This section covers how portal admins can create and manage users. This includes assigning users the appropriate level of access for their intended roles. Likewise, here you can review how individual users can manage how they authenticate their access to the portal.

Manage Users (Global Level)

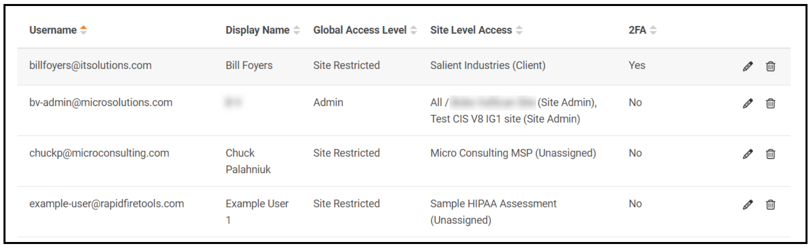
You can manage users associated with your account from global **Settings (Admin)**  > **Users**.



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



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.



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

Users and Global Access Roles

> **Note: Global Access Level vs. Site Level Access**
>
> • *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 *Site Settings* and *Global Settings*. 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

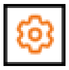
Global Access Role	Description
	Global Settings. **Who should I assign this level to?** • Users you trust within your operation to be "secondary" admins for the RapidFire Tools Portal • Users you trust with sensitive data for all of your clients • Users you trust to create and assign the appropriate 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:

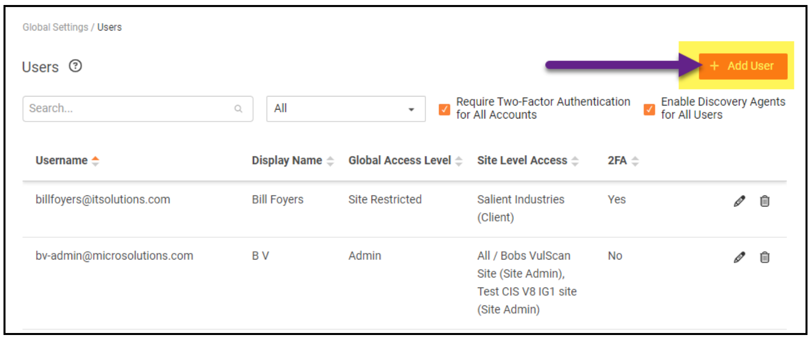
- "Add User at Global Level" on the next page
- "Edit User at Global Level" on page 113

Add User at Global Level

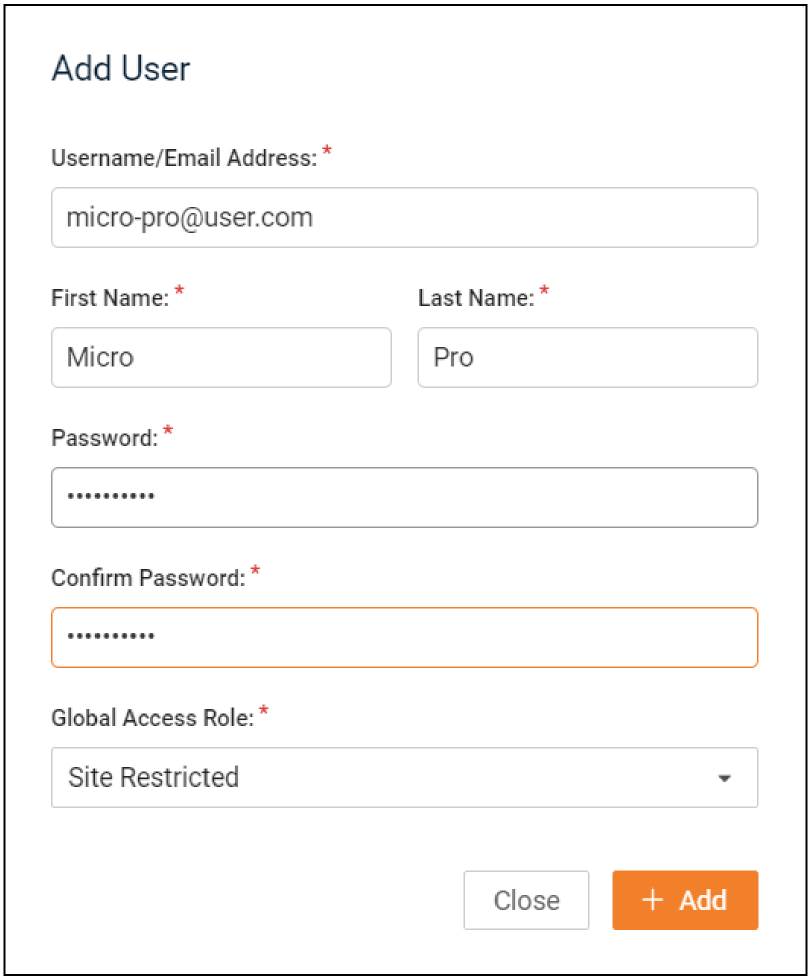
Note: When you create a user from Global Settings, you will still need to 1) associate that user with a Site, and 2) add that user to a Project Role in your Site. This will allow the new user to access the Site.

You can add users to your account at the global level from the global **Settings (Admin)**  > **Users** page. To do this:

1. Click **Add User**.

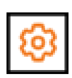


2. Enter the user's information, including password.



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 *Site Settings* and *Global Settings*. Can access API Keys from Global Settings.

<table>
<tr><th>Global Access Role</th><th>Description</th></tr>
<tr><td></td><td>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</td></tr>
<tr><td>ADMIN</td><td>Has global access to multiple sites. Has access to Site Settings and 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</td></tr>
<tr><td>RESTRICTED</td><td>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</td></tr>
</table>

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

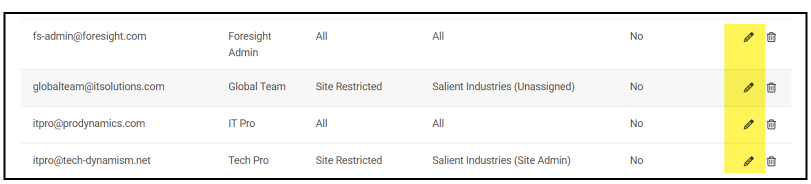
4. Click **Add**. The user will be added.

Edit User at Global Level

Note: Only *Master* and *Admin* users can edit users. And only Master users can edit other Master users. See "Manage Users (Global Level)" on page 107 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
globalteam@itsolutions.com	Global Team	Site Restricted	Salient Industries (Unassigned)	No
itpro@prodynamics.com	IT Pro	All	All	No
itpro@tech-dynamism.net	Tech Pro	Site Restricted	Salient Industries (Site Admin)	No

3. Click **Save**.

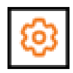
Enable Log In with KaseyaOne

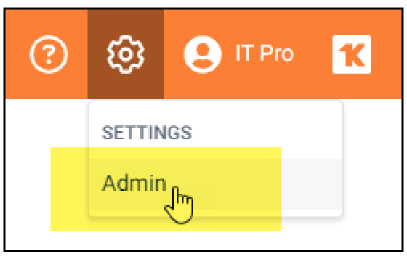
Once you are logged in with KaseyaOne, you can jump to any other IT Complete product without having to log in separately for each app. This provides a seamless workflow for IT Complete integrations. Follow these steps to enable users to log in with KaseyaOne.

Enable Log in with KaseyaOne at Account Level from Global Settings

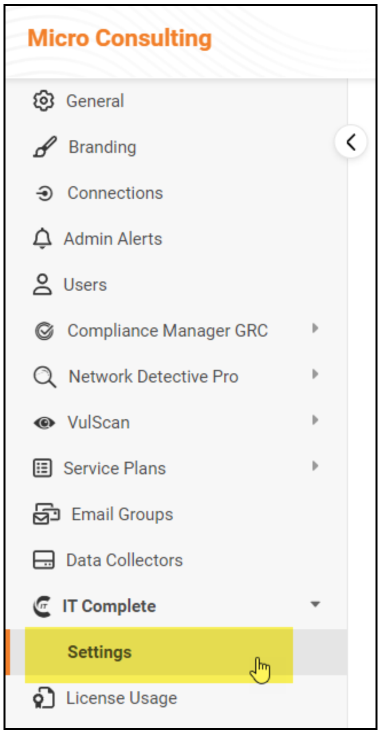
Before users can access the log in with KaseyaOne feature, a **GLOBAL ADMIN USER** must first enable the feature at the account level.

To do this:

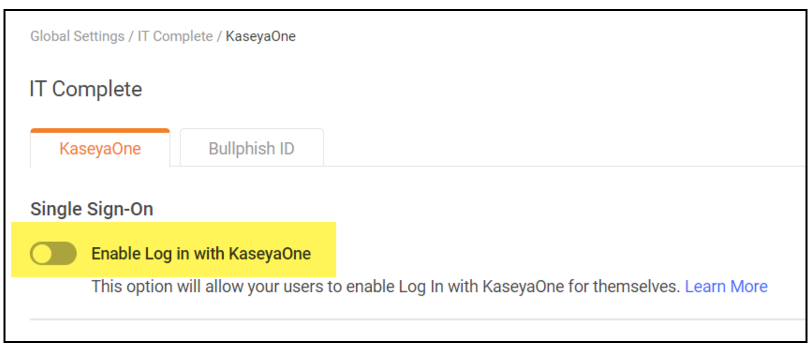
1. Open global **Settings (Admin)**  from the RapidFire Tools Portal top menu.



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

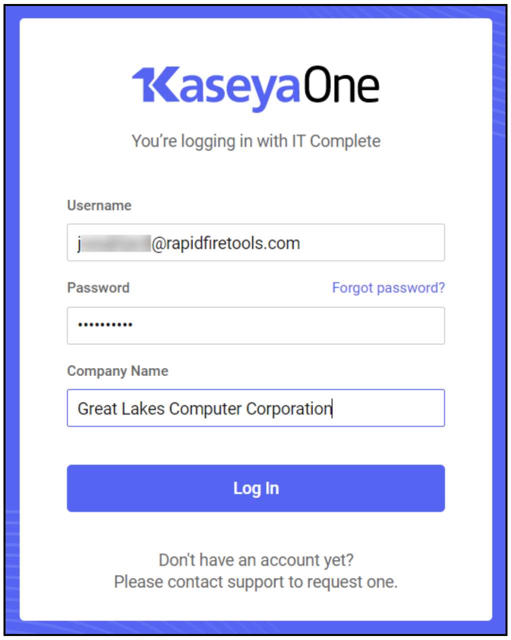


3. Activate the **Log in with IT Complete** slider.

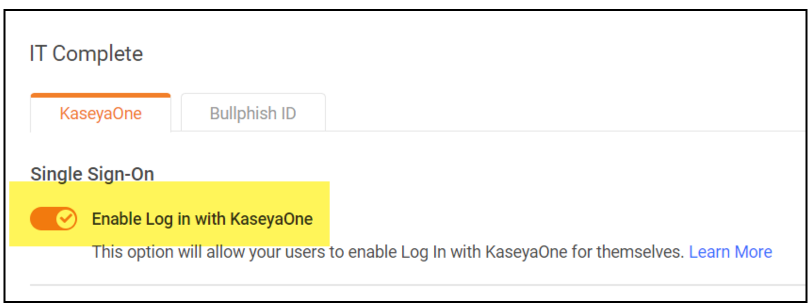


4. The KaseyaOne portal will open in your browser. Enter your KaseyaOne login credentials.

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

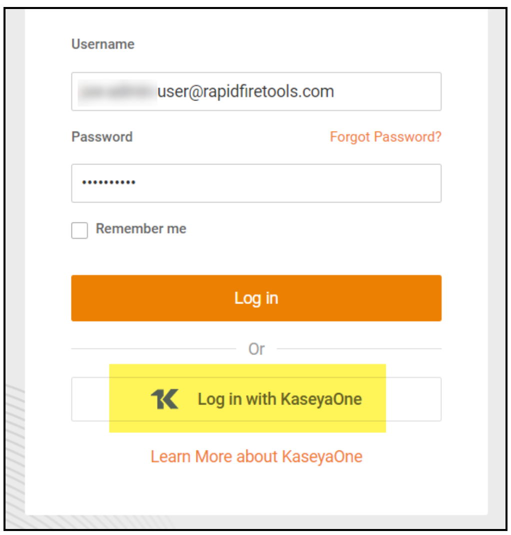


5. If prompted, **enable two-factor authentication** for your KaseyaOne account.
6. Once you log in to KaseyaOne, your browser will return to the RapidFire Tools Portal. The **Log in with KaseyaOne** feature will be activated for all portal users.

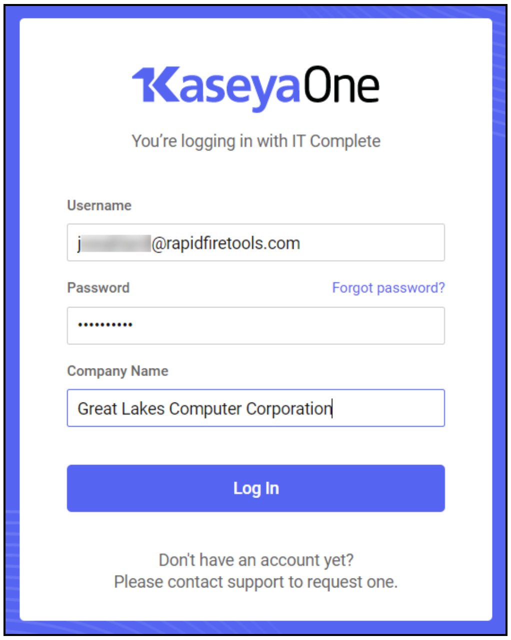


Log in with your KaseyaOne user

1. Once you "Enable Log in with KaseyaOne at Account Level from Global Settings" 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 "User Matching Criteria" on the next page. You can also "Enable Automatic User Creation for RapidFire Tools Portal" on page 121 – 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.



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



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

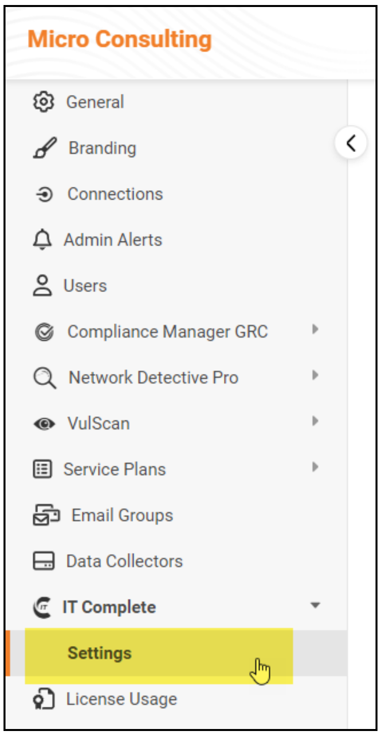
The following table describes what happens when you configure the Require Log In with KaseyaOne setting from global **Settings (Admin)** > **ITComplete** > **Settings**.

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.

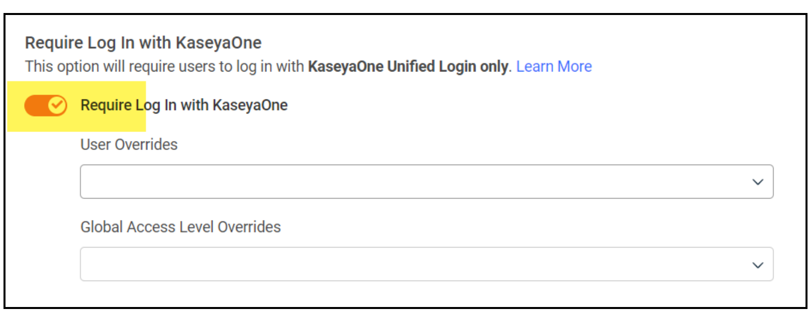
Toggle	Setting	Action / Description
Require Log In with KaseyaOne	Disabled	Allows users to log into the module with either their KaseyaOne Unified Login credentials (if "Enable Log In with KaseyaOne" on page 114 is turned on) or their local RapidFire Tools Portal credentials.

To Enable Require Log in with KaseyaOne:

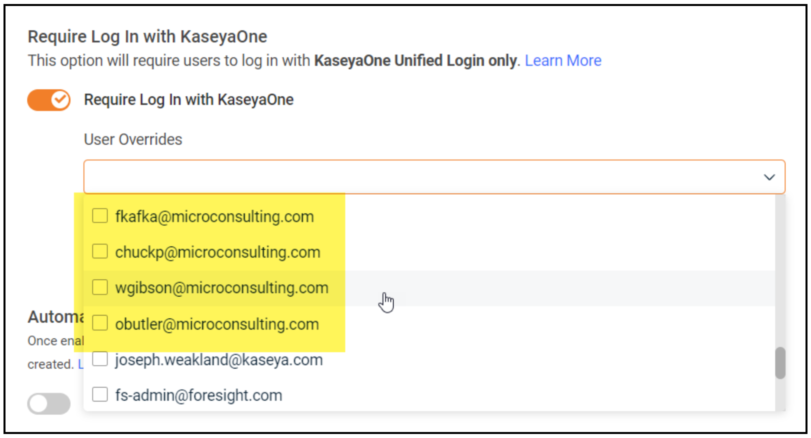
1. From the RapidFire Tools Portal, open **IT Complete** > **Settings** from the left-hand settings menu.



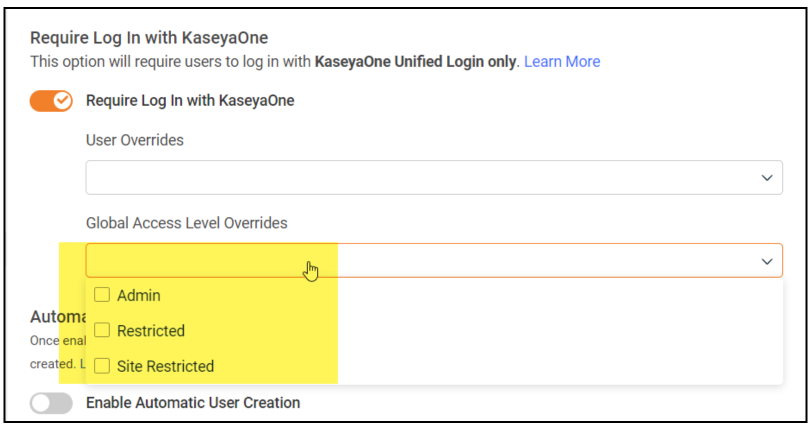
2. In the Require Log in with Kaseya One section, **select the Require Log In with KaseyaOne toggle switch** to enable the setting. Note that selecting the toggle switch again disables the setting.



- **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.



- **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.



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.

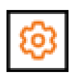
Once you first Enable Log in with KaseyaOne, users can log in to the RapidFire Tools Portal using KaseyaOne, but must already have a unique matching email address or username in the RapidFire Tools Portal. However, if you then **enable Automatic User Creation**, your users in KaseyaOne who log in to 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.

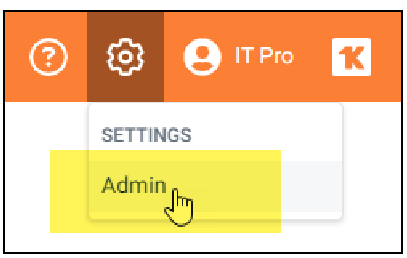
Here's how to enable Automatic User Creation for KaseyaOne users who will access the RapidFire Tools Portal:

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

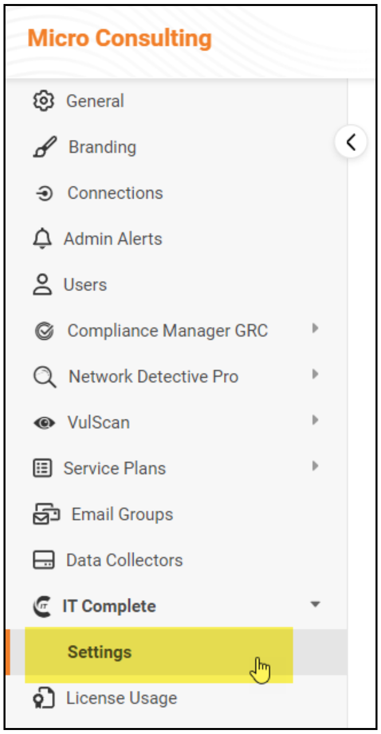
Before users can access the log in with KaseyaOne feature, a **GLOBAL ADMIN USER** must first enable the feature at the account level.

To do this:

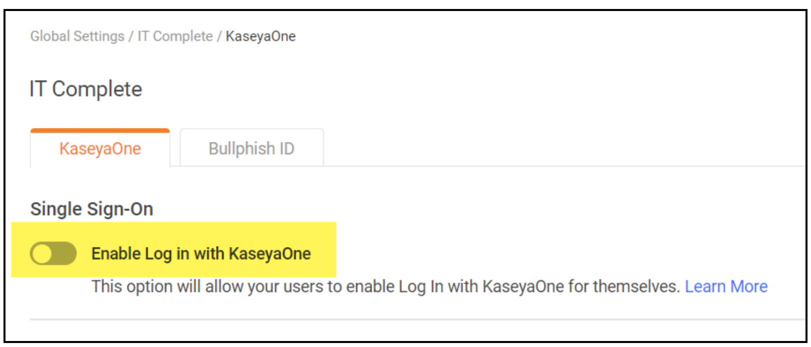
1. Open global **Settings (Admin)**  from the RapidFire Tools Portal top menu.



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

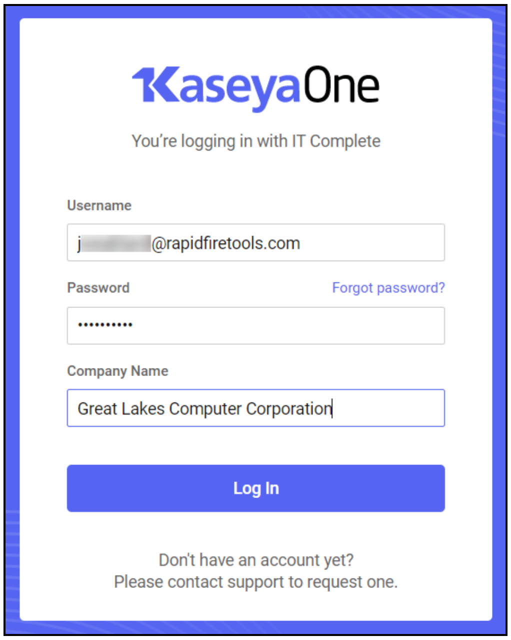


3. Activate the **Log in with IT Complete** slider.

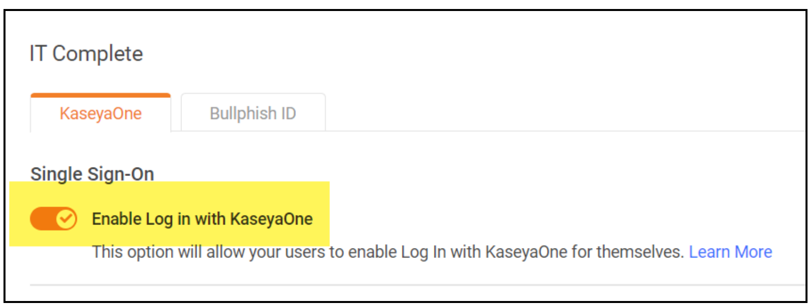


4. The KaseyaOne portal will open in your browser. Enter your KaseyaOne login credentials.

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

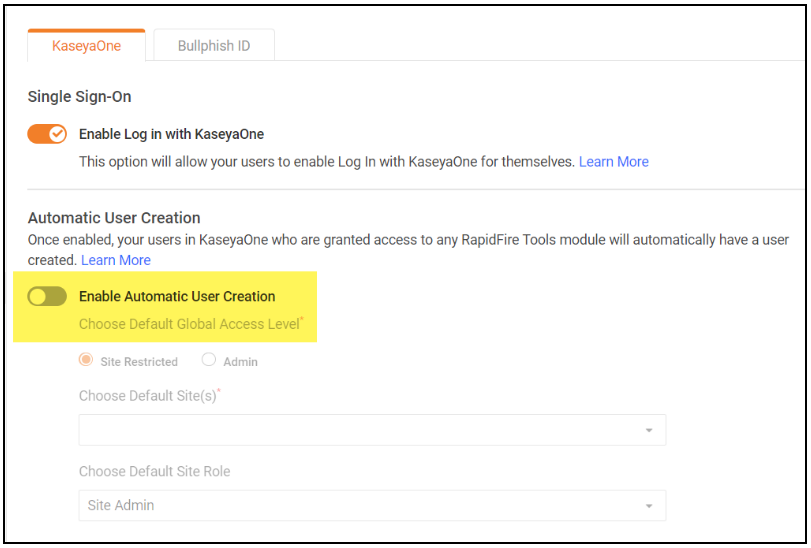


5. If prompted, **enable two-factor authentication** for your KaseyaOne account.
6. Once you log in to KaseyaOne, your browser will return to the RapidFire Tools Portal. The **Log in with KaseyaOne** feature will be activated for all portal users.

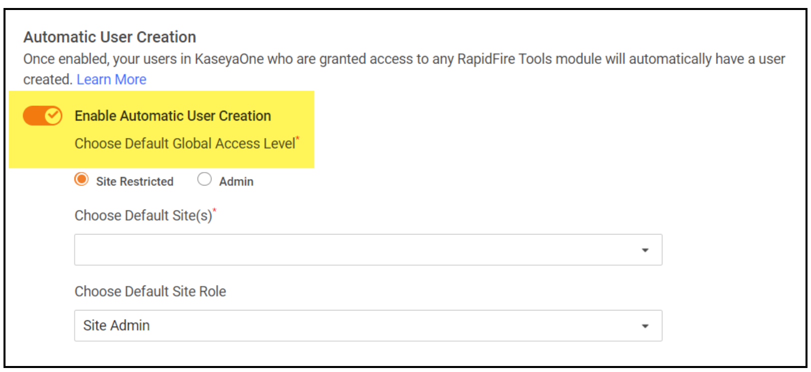


Step 2 – Enable Automatic User Creation

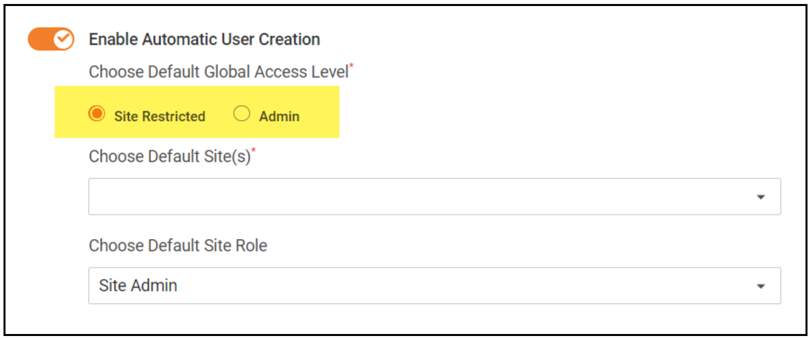
Once you enable log in with KaseyaOne, the Enable Automatic User Creation option will become available. Here's how to set it up:



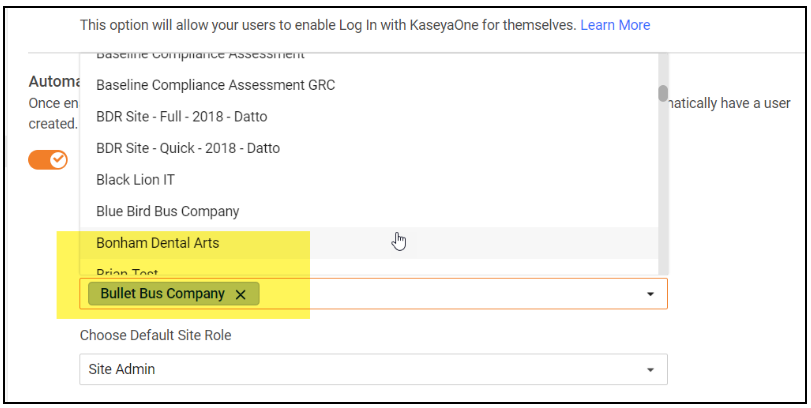
1. From **Enable Automatic User Creation**, activate the slider.



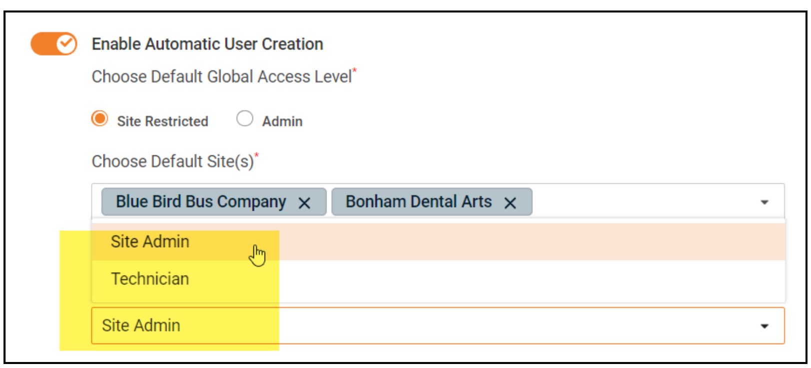
2. Choose the **Default Global Access Level**. This determines the user's level of access to the portal. There are two options:
   - **Site Restricted**: User can only access the Default Site(s) and organizations they are assigned. The Site Restricted user must also be assigned a Default Site Role.
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



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.



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



Step 3 – KaseyaOne User Logs into RapidFire Tools Portal

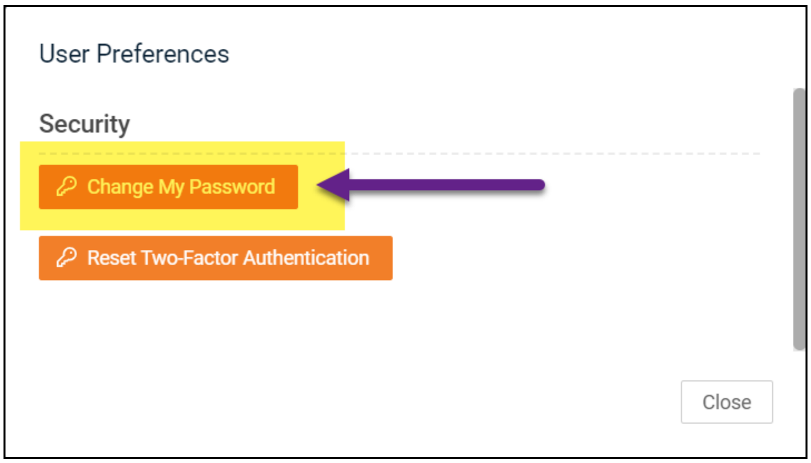
Once the Portal Admin enables Automatic User Creation for the KaseyaOne account, KaseyaOne users can log into the RapidFire Tools Portal from My IT Complete.

- 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.

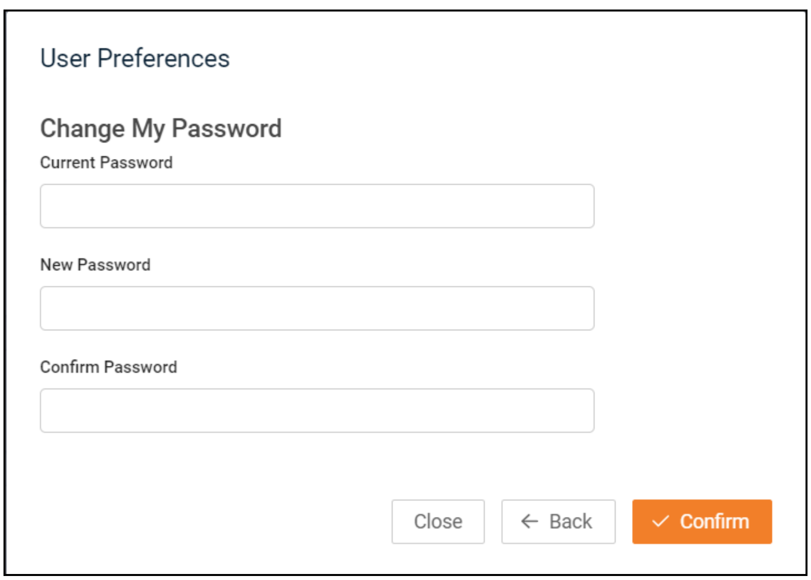
Change your Password

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.



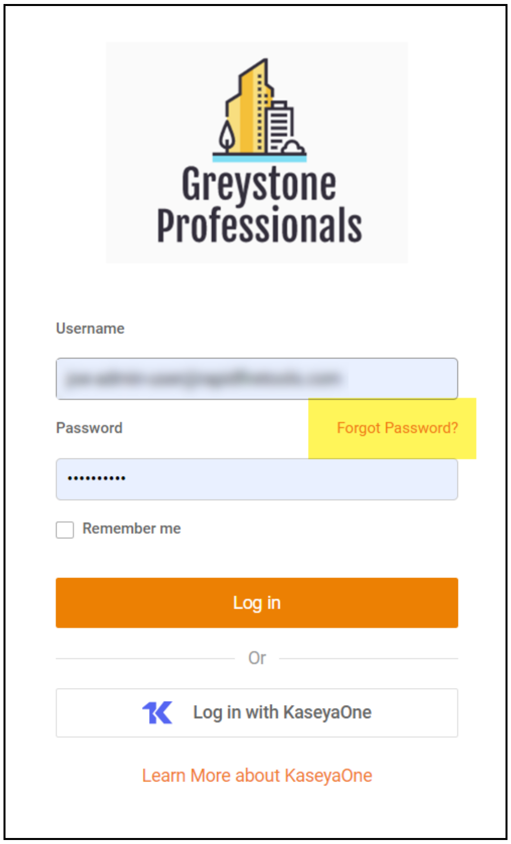
6. Click **Confirm**.

Your password will then be changed.

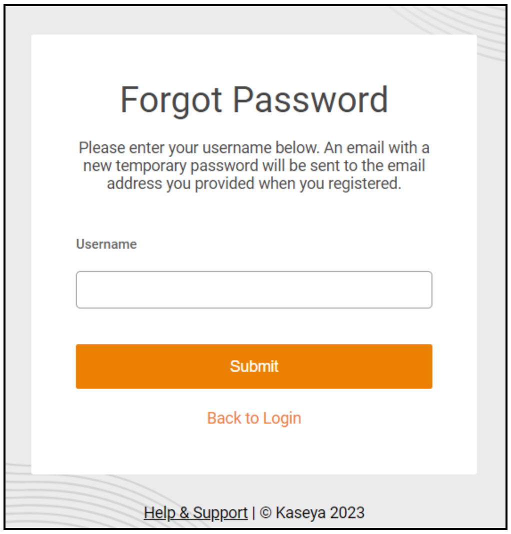
Recover Forgotten Password

To recover a forgotten password:

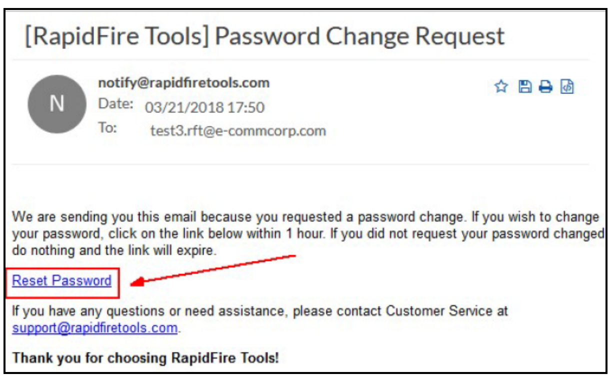
1. Open the RapidFire Tools Portal at https://www.youritportal.com.



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



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.

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.

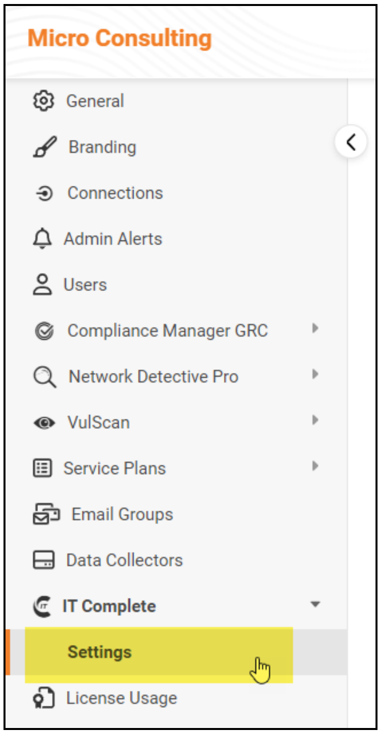
Note: In order to set up Access Groups for KaseyaOne and the RapidFire Tools Portal, you must first "Enable Log In with KaseyaOne" on page 114.

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

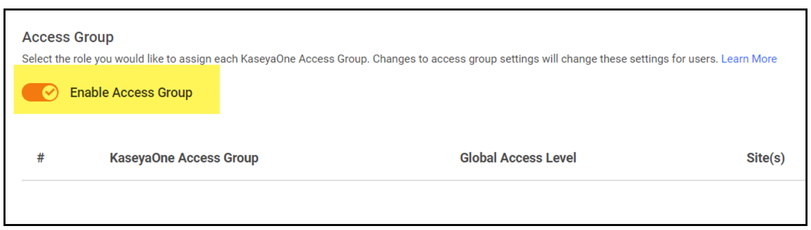
Toggle	Setting	Action / Description
Enable Access Groups	Enabled	Enables Access Groups for KaseyaOne users to the RapidFire Tools Portal whereby KaseyaOne Access Groups are mapped to Portal Global Access Levels. This will ensure new logins to the RapidFire Tools Portal have the privileges relevant to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

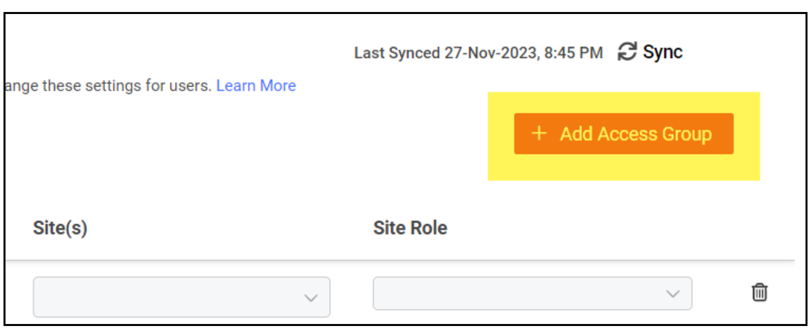
1. From the RapidFire Tools Portal, open global **Settings (Admin)** . Then open **IT Complete** > **Settings** from the left-hand settings menu.



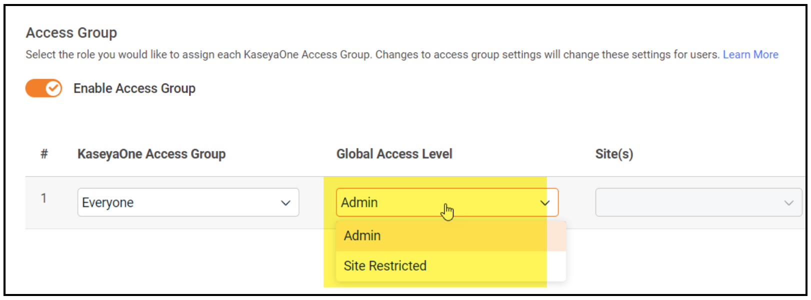
2. In the Access Groups section, select the **Enable Access Groups** toggle switch to enable the setting. Note that selecting the toggle switch again disables the setting.



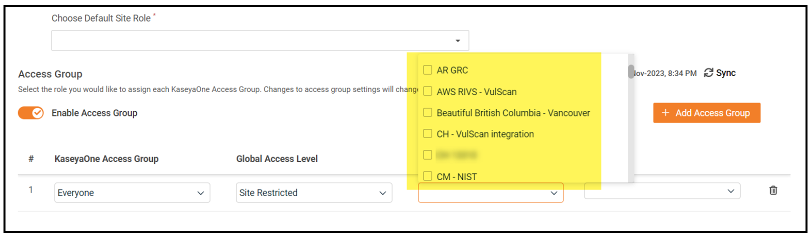
3. Click **Add Access Group** to create a new KaseyaOne Group-to-RapidFire Tools Portal Role mapping.



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



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.



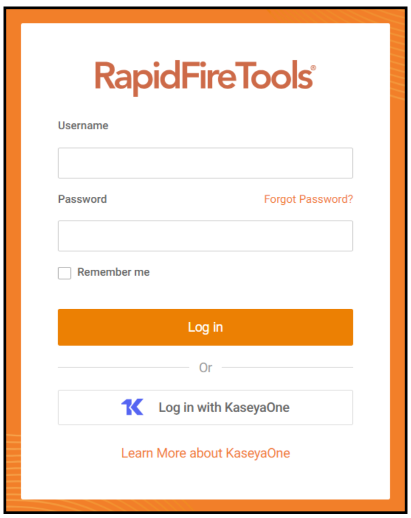
Once you set up Access Groups for the RapidFire Tools Portal, new users who log in with their KaseyaOne credentials will enter the Portal with the permissions that you specify.

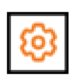
Set Up Portal Branding

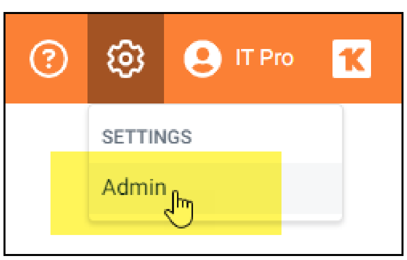
The RapidFire Tools Portal allows you to customize many elements to fit with your organization's brand and identity. This topic covers how you can modify the Portal's look and feel.

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

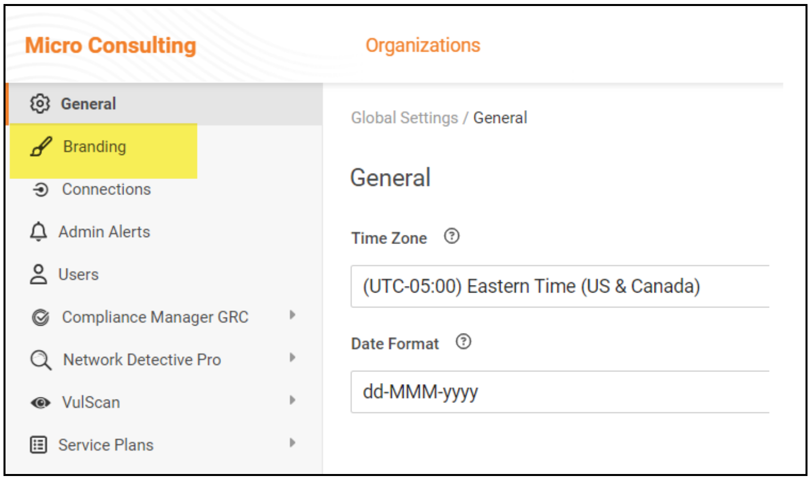
   Note: In order to configure the settings in the Portal, the login credentials you use to access the Portal will require the Master User rights.



2. Click global **Settings (Admin)**  > **Users**.



3. Click **Branding**.



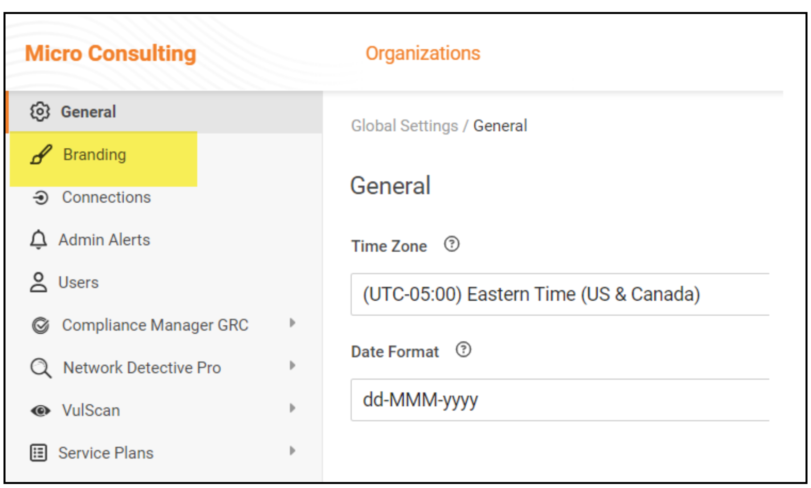
From this page, you can then:

- "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

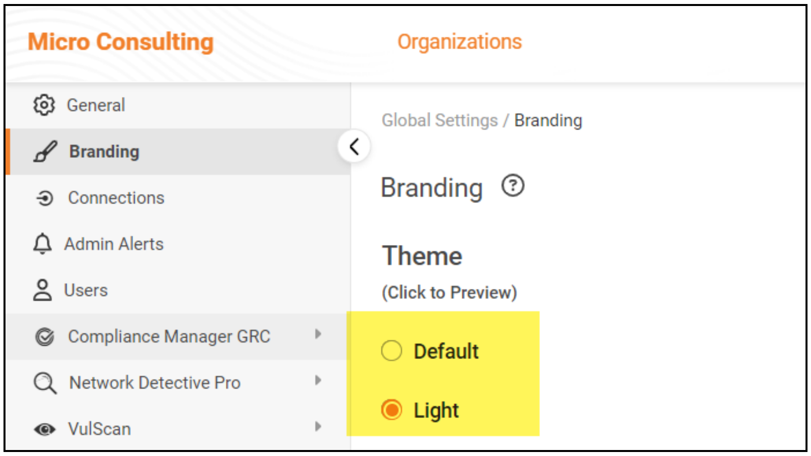
Set Custom Portal Theme

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.



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

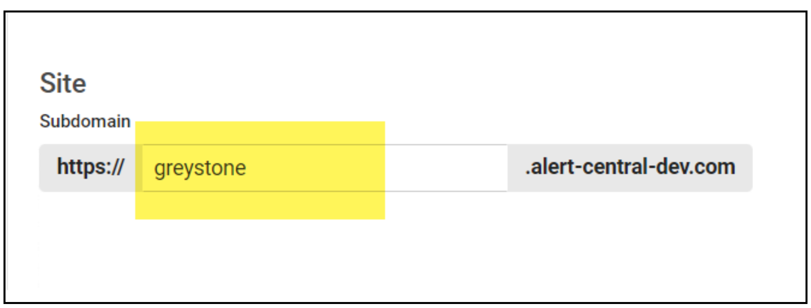


3. When you select the theme, you can click around the Portal and preview it. You must click **Save** from global **Settings (Admin)** > **Branding** to apply your changes. This change will apply to all users.

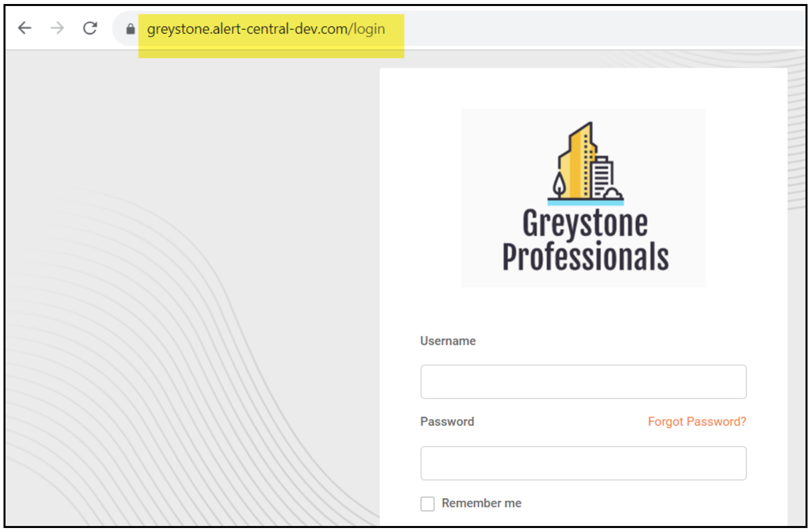
Set Custom Portal Subdomain

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.



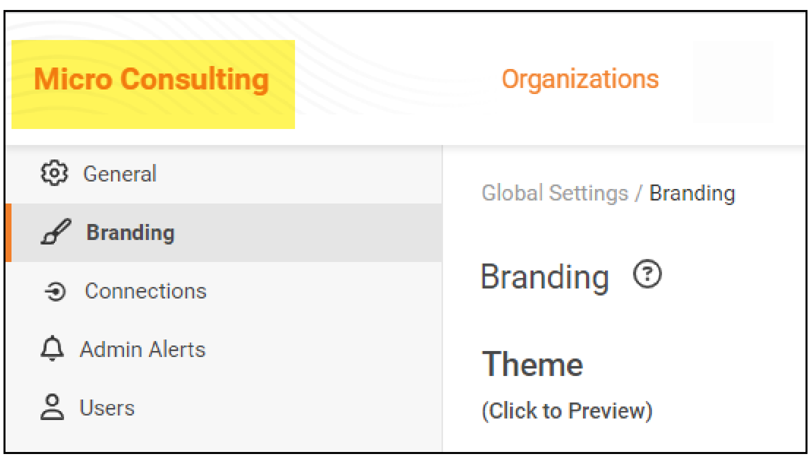
2. Click **Save**.
3. Log out of the RapidFire Tools Portal.
4. Next, access the RapidFire Tools Portal by using the URL for the new Subdomain you configured to access the Portal's login screen.



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.

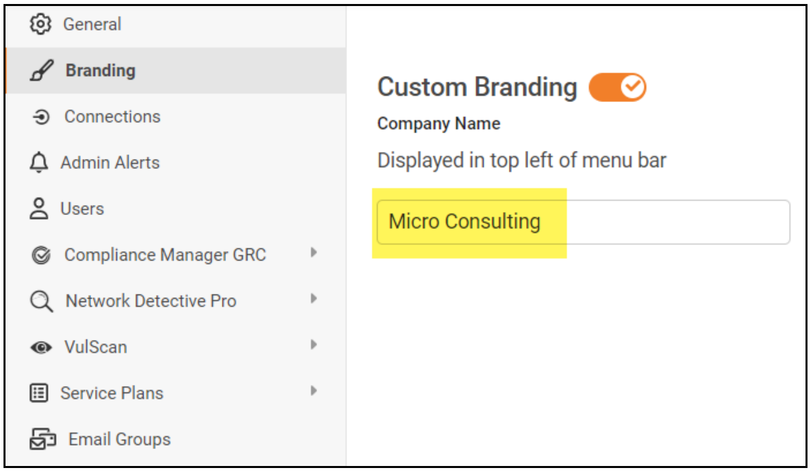
Set Custom Company Name

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



To do this:

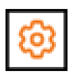
1. From global **Settings (Admin)** > **Branding**, enter your custom company name under Custom Branding.

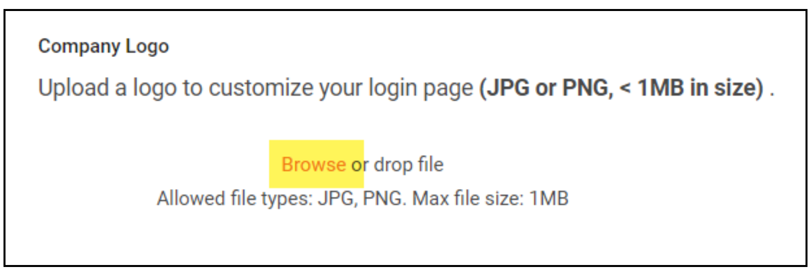


2. Click **Save**. Your custom name will then appear in the top-left corner of the portal for all users to see.

Set Custom Company Logo

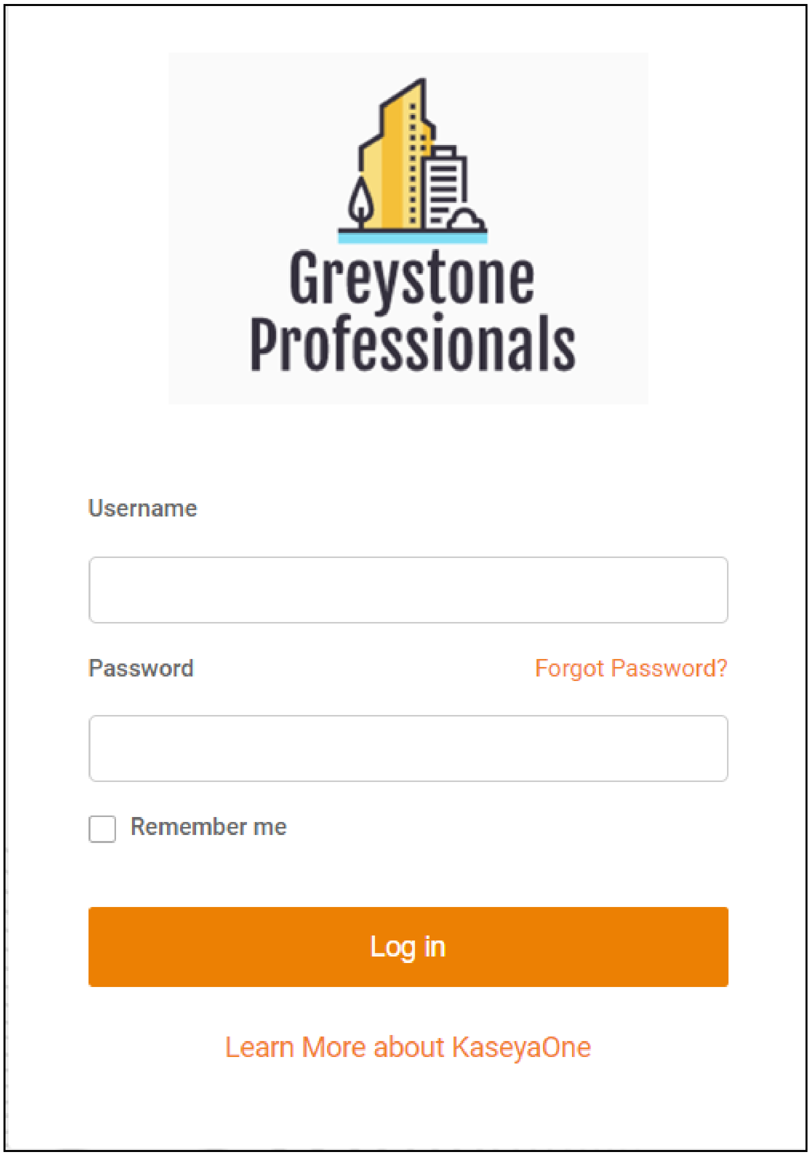
You can set a custom company logo on the Portal login screen to communicate your brand to users. To do this:

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

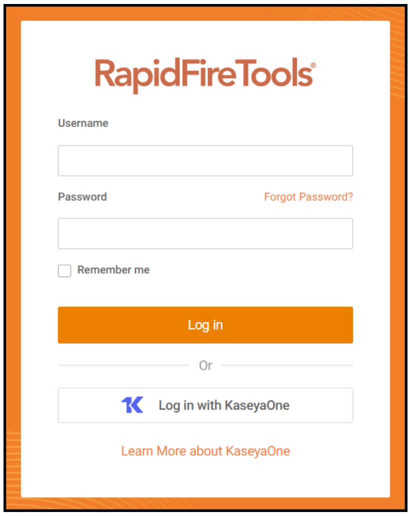
login screen.

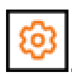


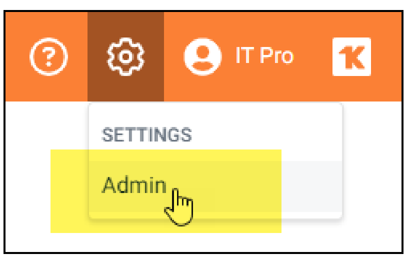
Set Up a Custom Subdomain to Access the RapidFire Tools Portal

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

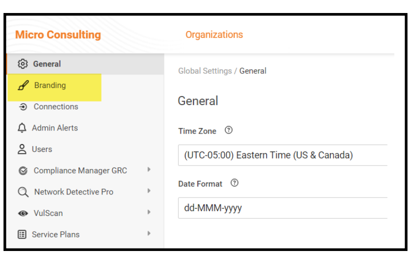
> **Note:** In order to configure the settings in the Portal, the login credentials you use to access the Portal will require the Master User rights.



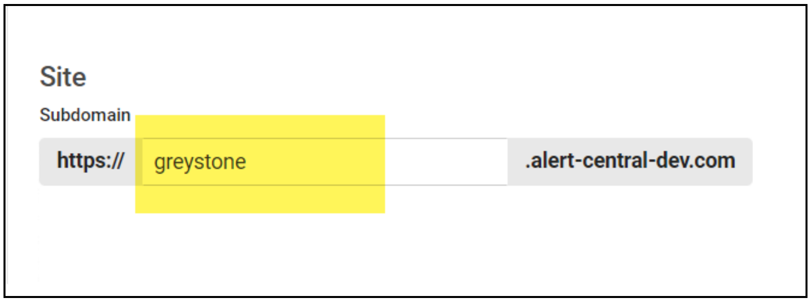
2. Click global **Settings (Admin)** .



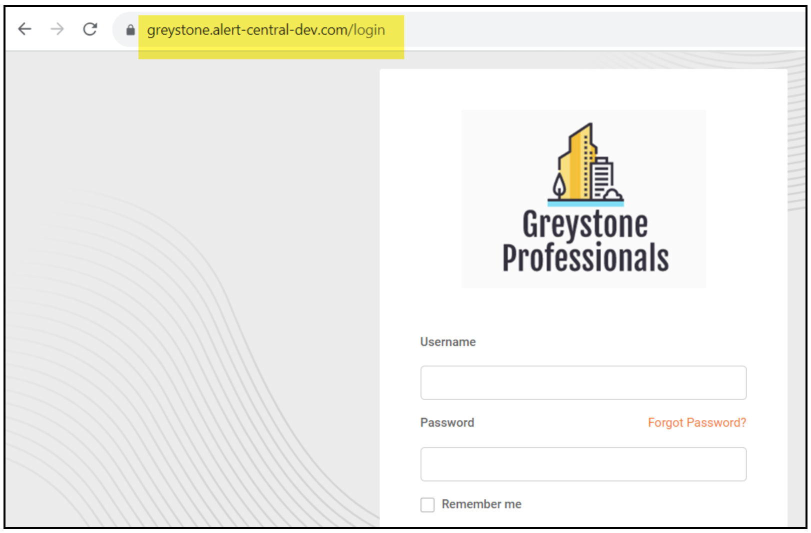
3. Click **Branding**.



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



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.



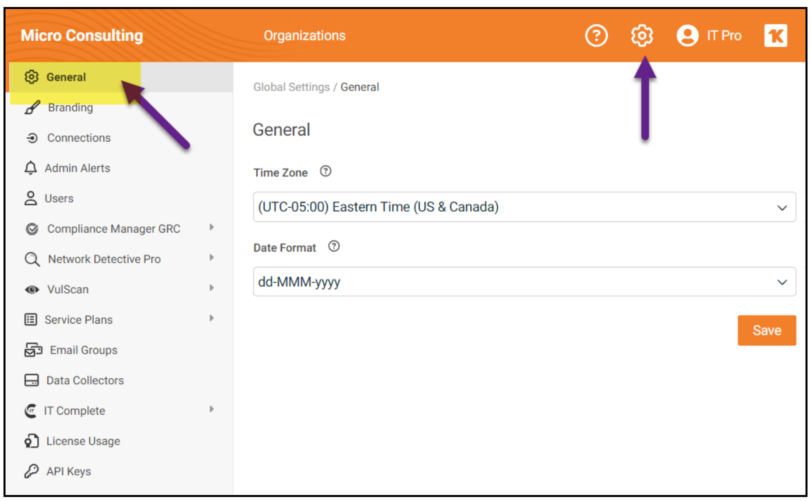
Portal Administration

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

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:

1. Go to global **Settings (Admin)** > **General**.



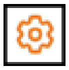
2. Select your time zone from the drop down menu.
3. Click **Save**.

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:

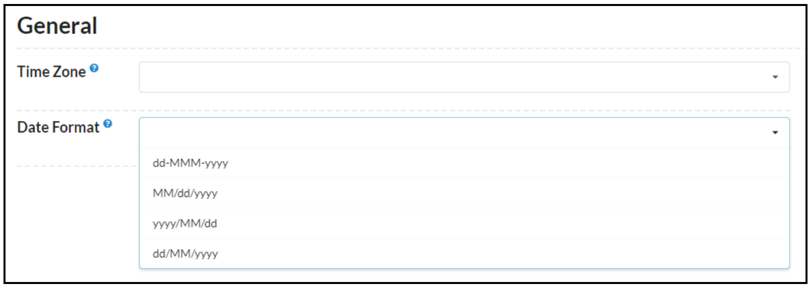
- start time for scans when using the limit scan start time feature for a site
- last modified date of risk update reports
- last sync date and time for Kaseya BMS billing integration

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)**

 > **General** settings.

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



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

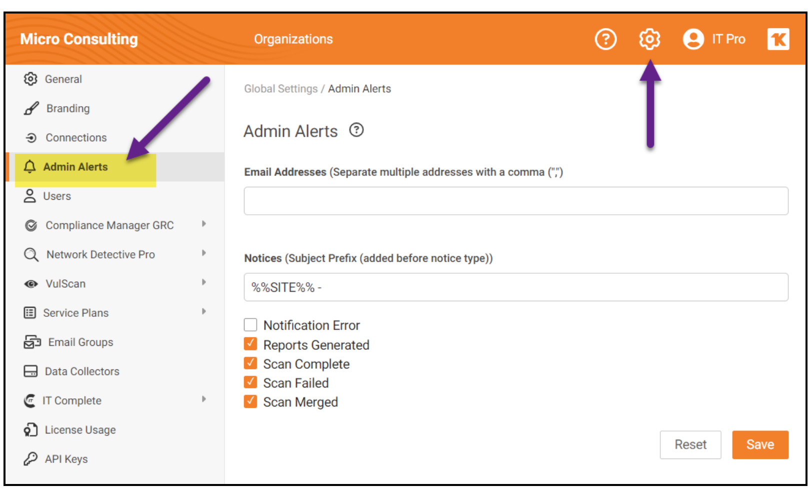
To configure Admin Alerts:

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.

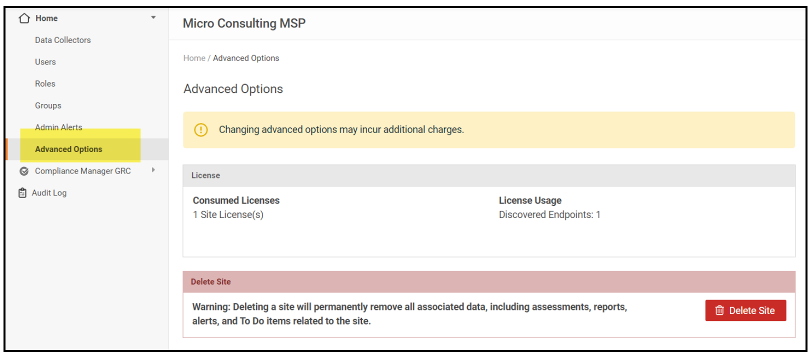


3. Add a Subject Prefix that will be included in email's subject line before the notice type.
4. Select which types of alerts to send to the listed users.
5. Click **Save**. You can also choose to **Reset** to Global Settings.

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**.

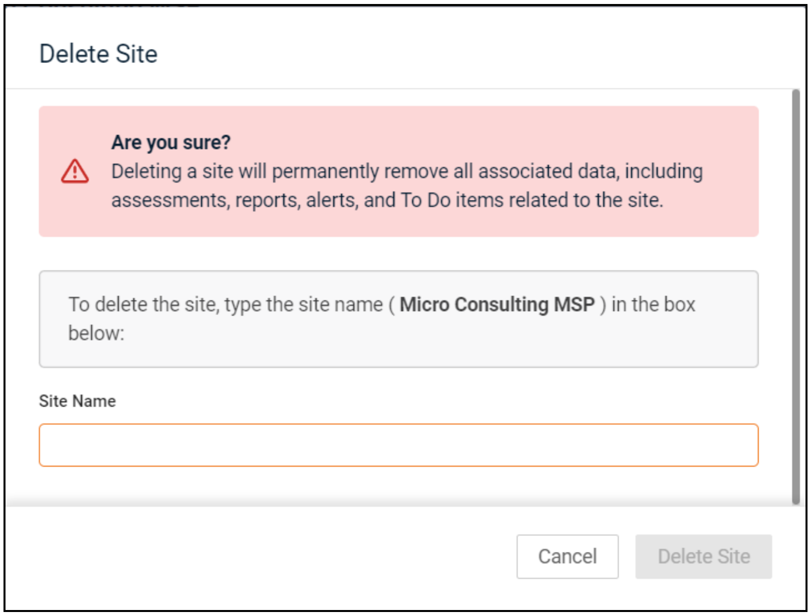


3. Click **Delete Site**.

> **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**.

The site will then be removed from the system.



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.

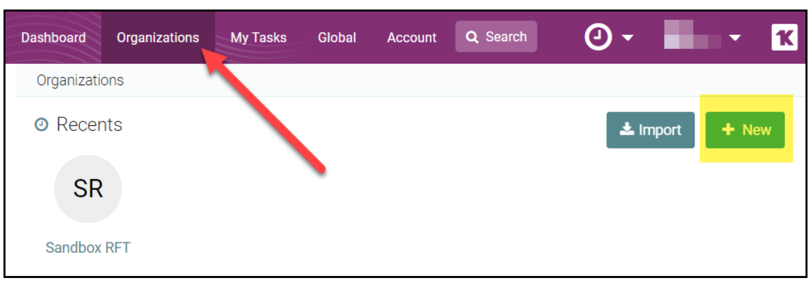
> **Note:** You must subscribe to IT Glue Enterprise to access this feature.

Here's how to enable this feature:

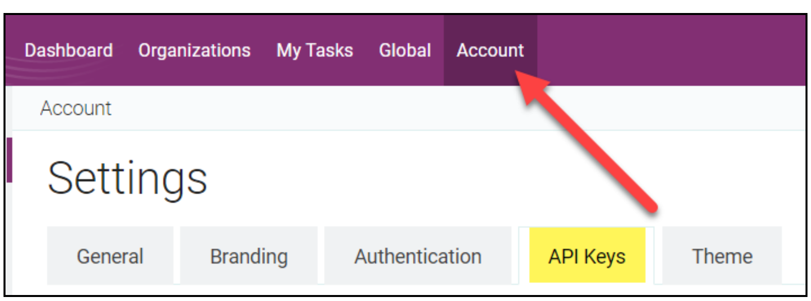
Step 1 — Create and Copy API Key in IT Glue

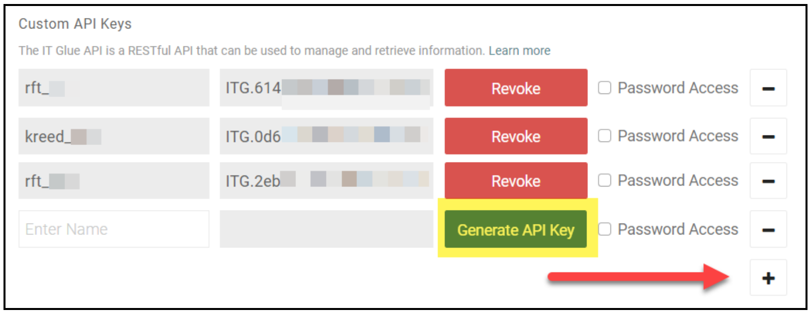
First, you need to set up an API Key in IT Glue.

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.



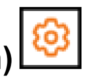
2. Create an IT Glue API Key for your use during integration and set up. You can do this from **Account** > **API Keys**.

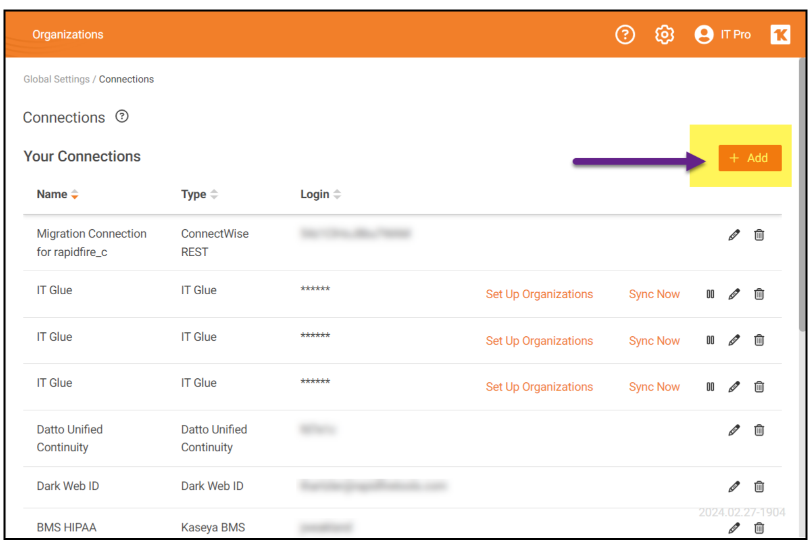




Important: For your reference, save a copy of the API key outside of IT Glue.

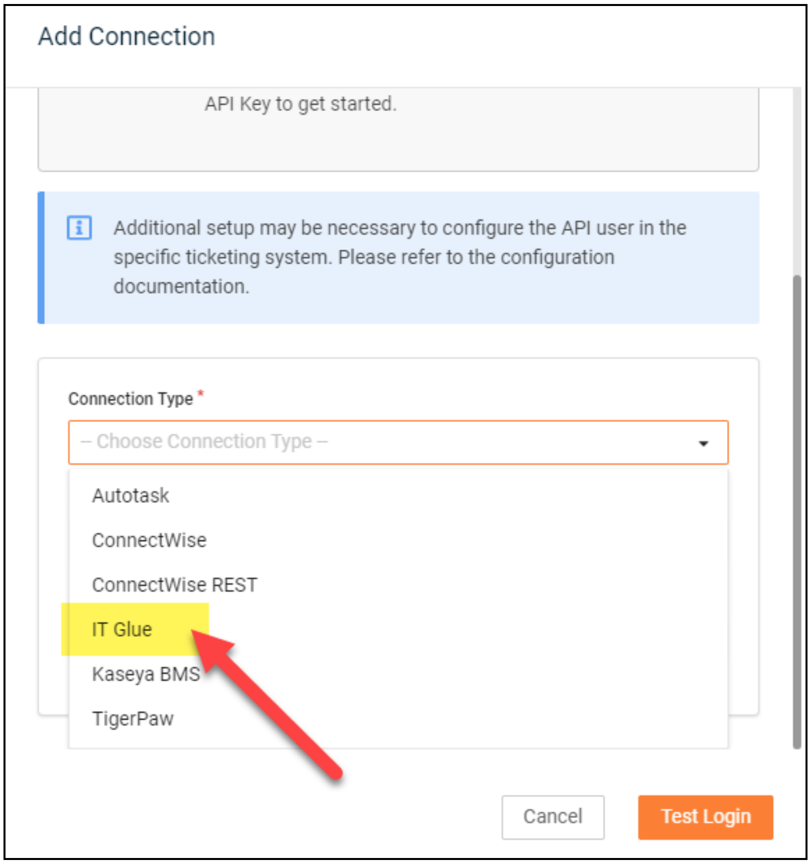
Step 2 — Enable Connection to IT Glue from Portal Global Settings

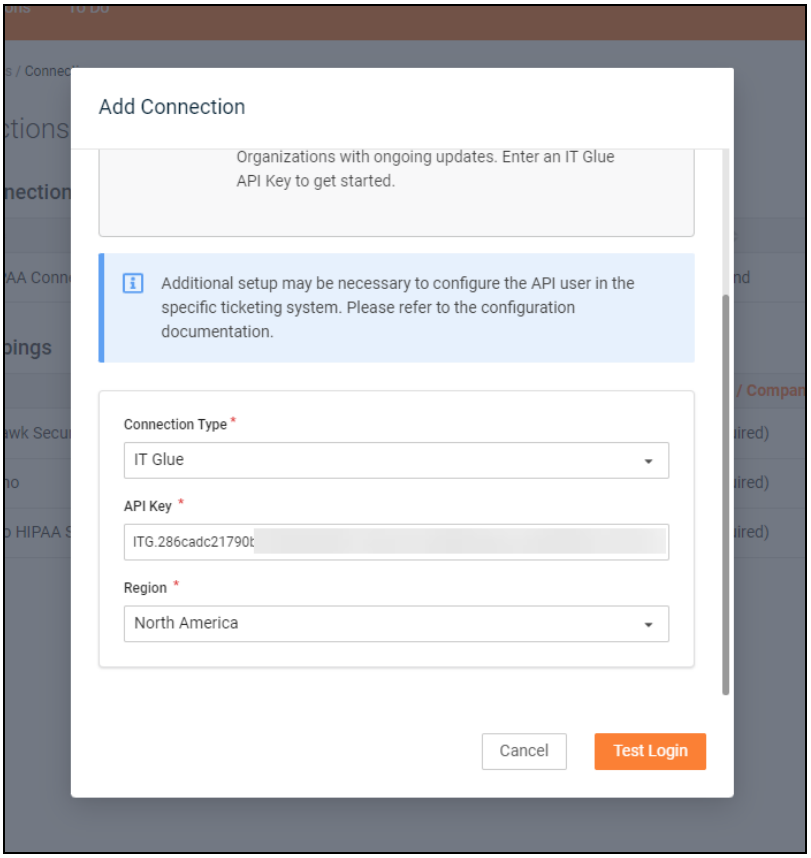
1. Next, from the RapidFire Tools Portal, navigate to global **Settings (Admin)**  > **Connections**.
2. From **Your Connections**, click **Add**.



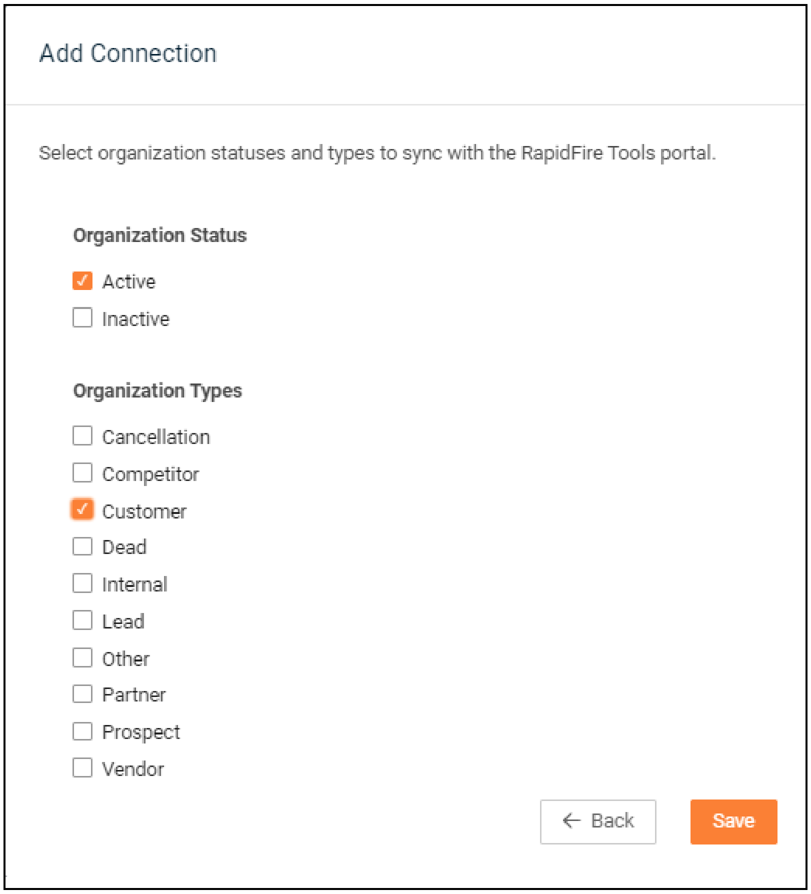
3. **Select IT Glue** from the drop-down menu and **enter the API Key**.

4. Click **Test Login**.





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



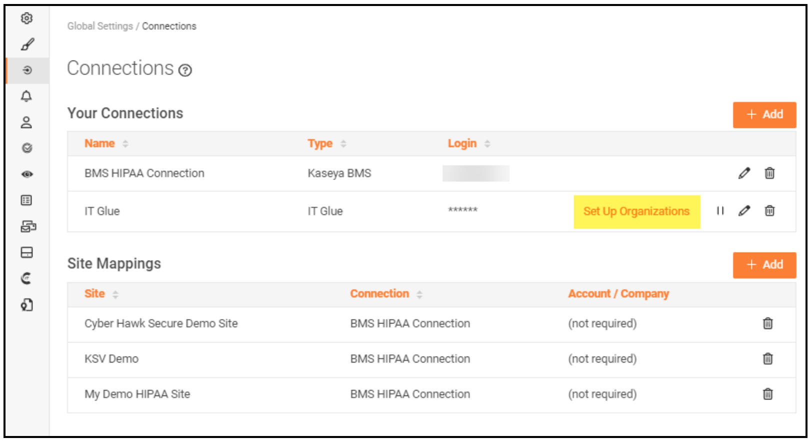
Note: These fields are configured in IT Glue.

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

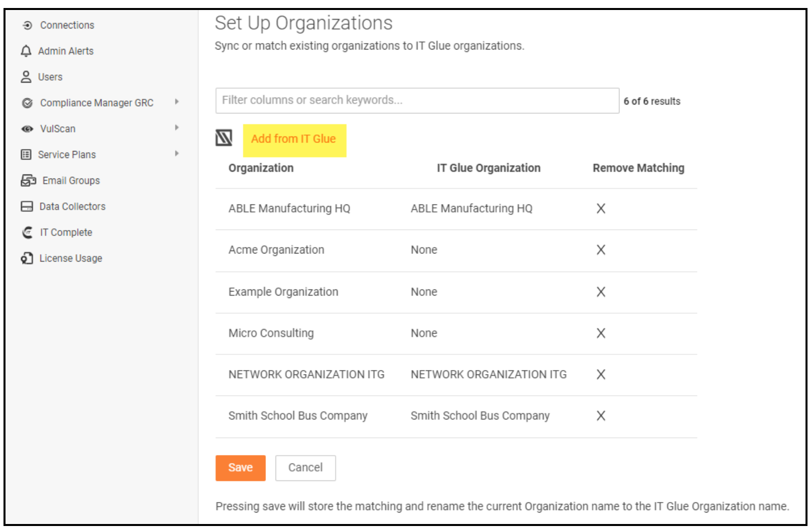
Step 3 — Set Up Organizations

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.

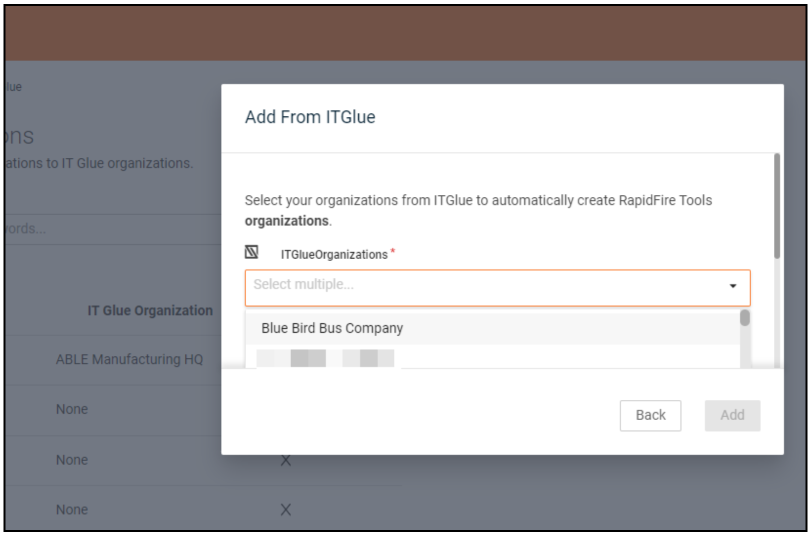
1. From My Connections, click **Set Up Organizations**.



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.



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**.



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

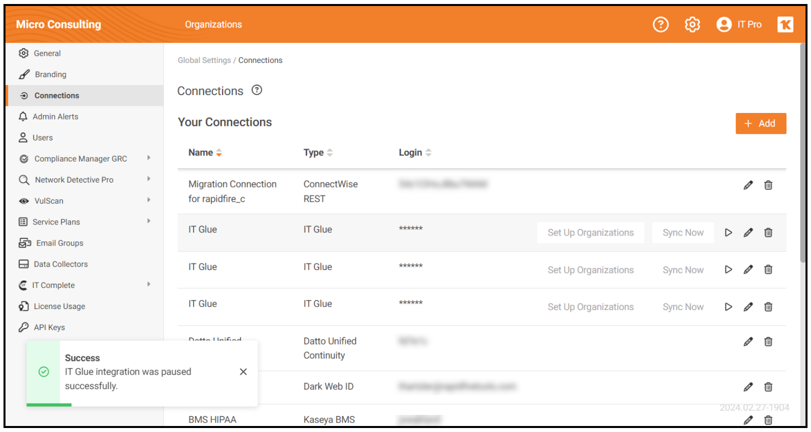
Once you import orgs from IT Glue into the RFT Portal, the org names will be synchronized; changes to org names in IT Glue will regularly update the corresponding org names in the RFT Portal.

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

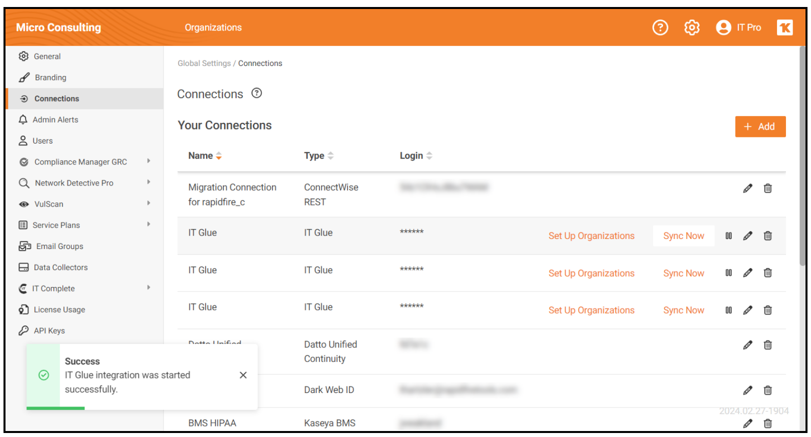
> **Note:** The sync is limited to org names and works one way from ITGlue into the RFT Portal. Note also that deleting orgs in the RFT Portal will not delete orgs in IT Glue.

Pause Org Name Synchronization

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



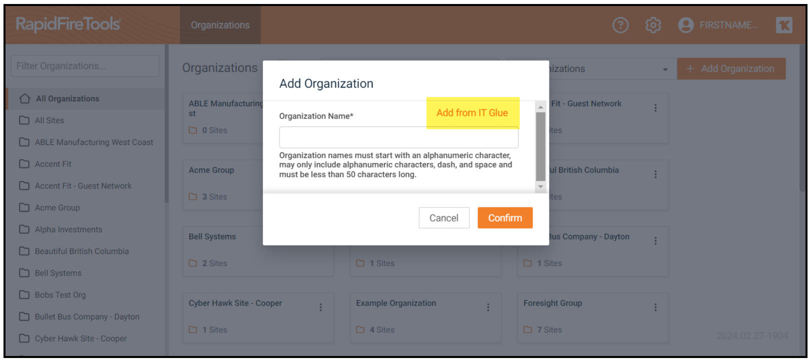
To resume synchronizing org names, find the ITGlue connection and click the **play** button.



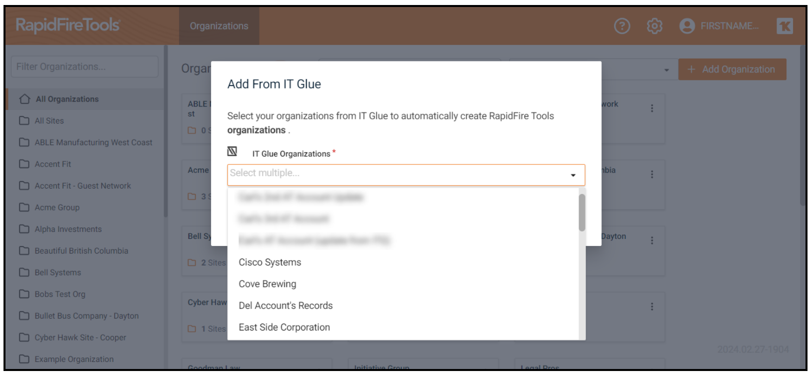
Import IT Glue Orgs when Creating New Organizations

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**.



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

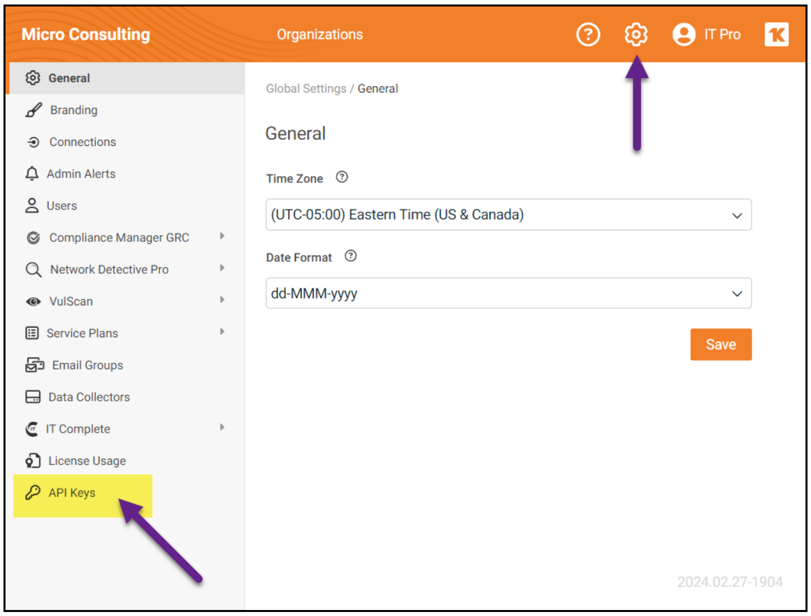


Create an API Key

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.

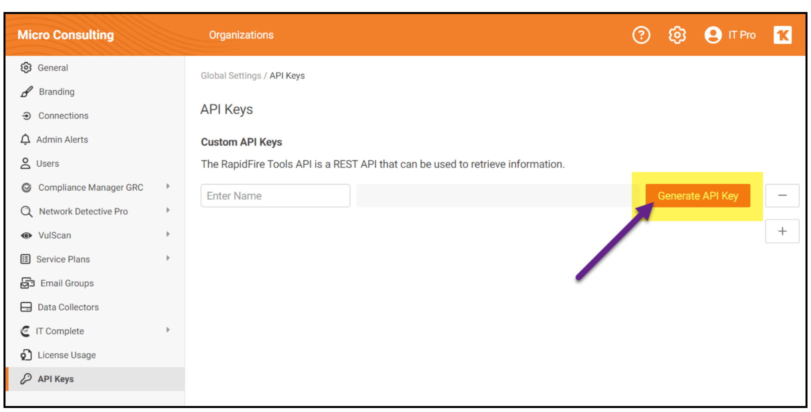
Here's how to generate an API key:

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

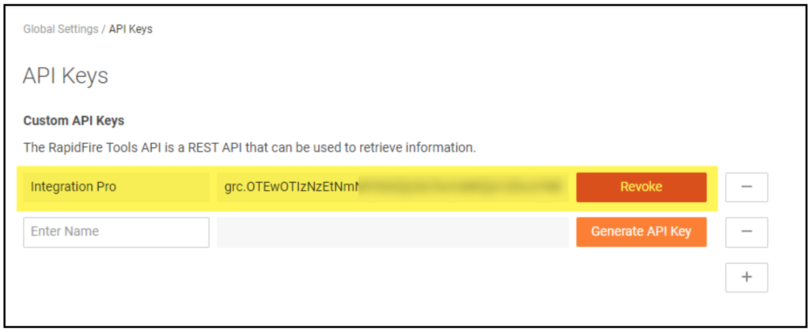


Note: Your user must have Global Access Role "**All**" (master user) to access this feature.

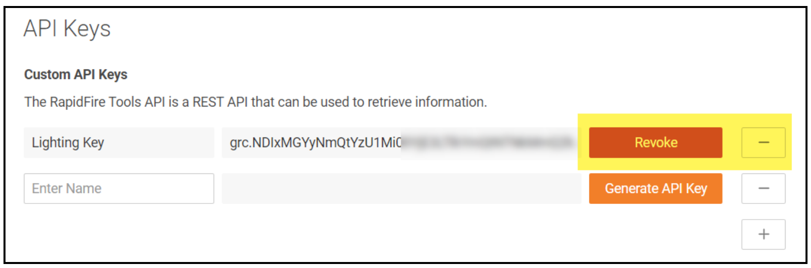
2. From Custom API Keys, **enter a name** for your key, then click **Generate API Key**.



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.



Appendices

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

VulScan Integration with Network Detective

Migrate Inspector 2 to VulScan

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

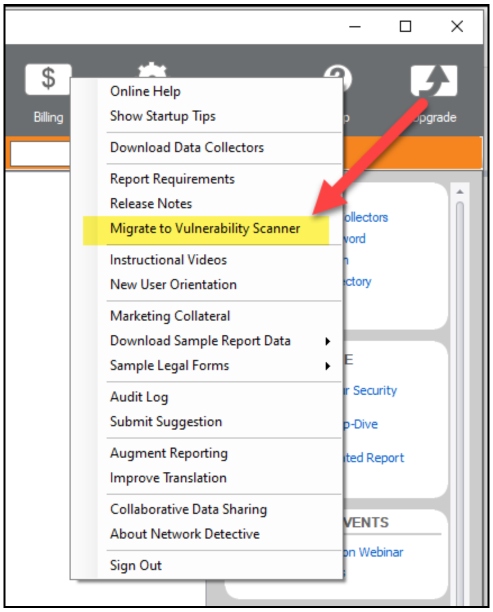
As of Monday, January 26, 2021, **Inspector 2** will be deprecated and replaced by **VulScan**.

- 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 "Generate Internal Vulnerability Reports in Network Detective using VulScan" on page 164.)

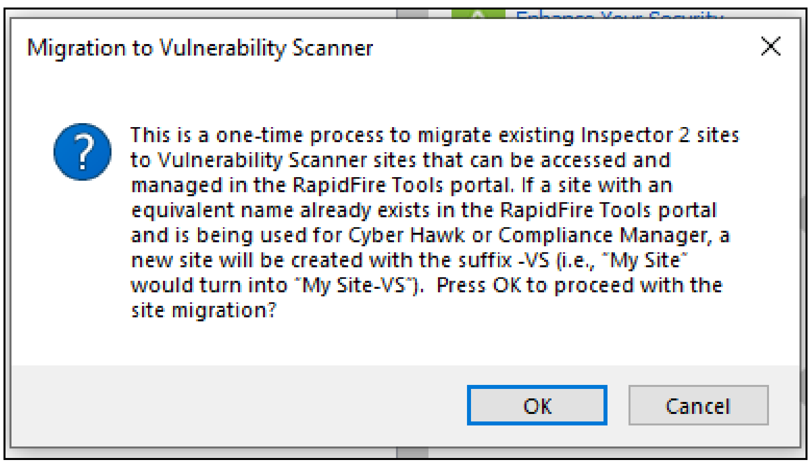
Inspector 2 users should follow these steps to upgrade to VulScan.

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**.



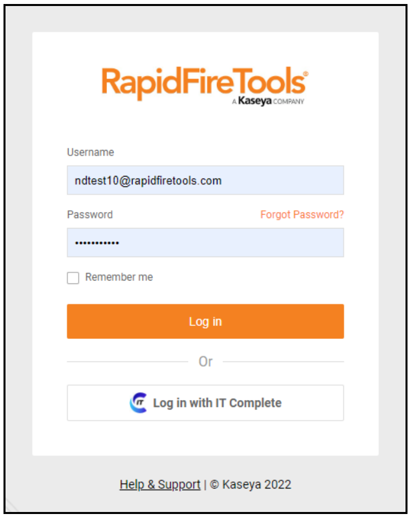
Note: This is a one-time process to migrate existing Inspector 2 sites to VulScan sites that can be accessed and managed in the RapidFire Tools portal.

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").

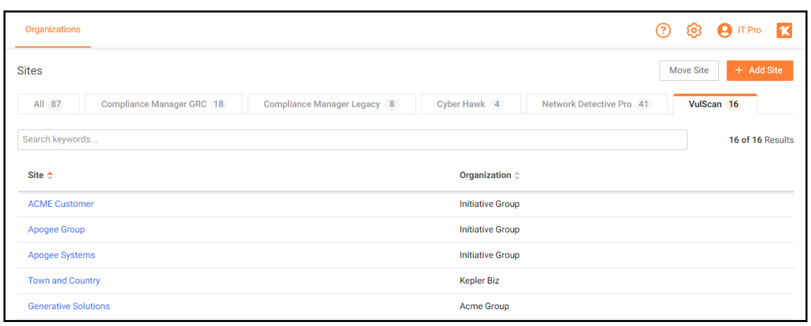
4. All of your existing Inspector 2 sites will be migrated to VulScan **sites in the RapidFire Tools Portal**.
5. The **Queued Scan Tasks** for your Inspector 2 sites will be carried over as scan tasks that can be managed from your VulScan site in the RapidFire Tools Portal. **Unscheduled Scan Tasks 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.

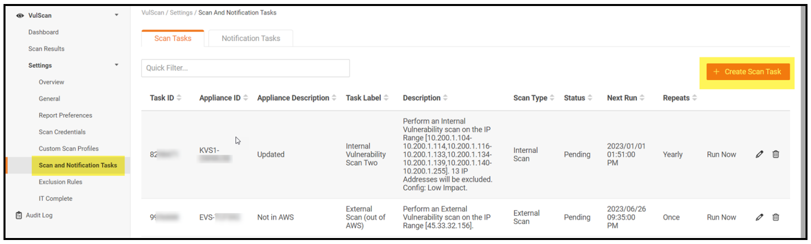


2. Select your new site from the Site page. You can then begin using VulScan.



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

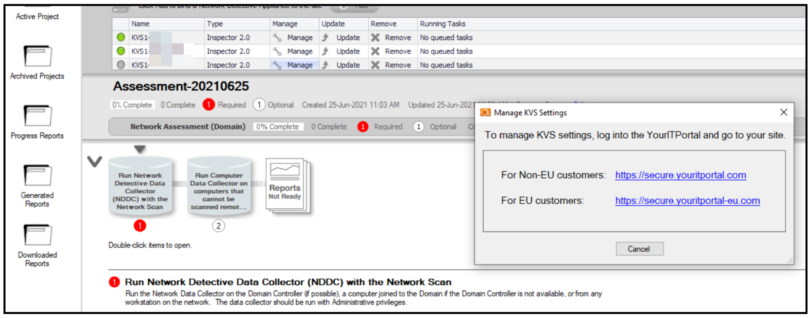
MORE INFO:

- **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

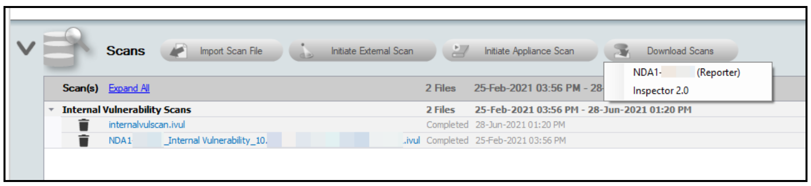
Generate Internal Vulnerability Reports in Network Detective using VulScan

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:

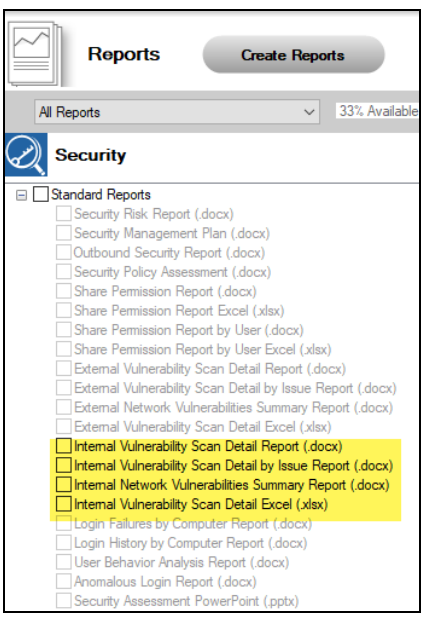
1. First, you need to set up and manage VulScan scan tasks from the RapidFire Tools Portal. From Network Detective, when you right click **Manage** for a VulScan appliance from the site options, you will be prompted to access the portal.



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**.



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

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 Reporter User 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)

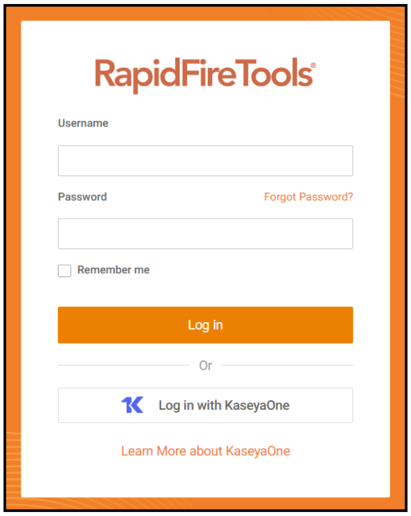
PSA System	PSA Prerequisites
Autotask	The Autotask SOAP integration has been deprecated (see below). To use the new integration, all you need is a username and password for a non-API user. **Important:** The new Autotask integration is not supported by Network Detective or Network Detective on the web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

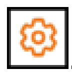
PSA System	PSA Prerequisites
Autotask SOAP (Deprecated)	• Autotask API Username • Autotask API Password
REST ConnectWise	• ConnectWise REST Public Key • ConnectWise REST Private Key • ConnectWise Company ID • ConnectWise PSA URL
SOAP ConnectWise	• ConnectWise Username • ConnectWise Password • ConnectWise Company ID • ConnectWise PSA URL
Tigerpaw Software	• 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.

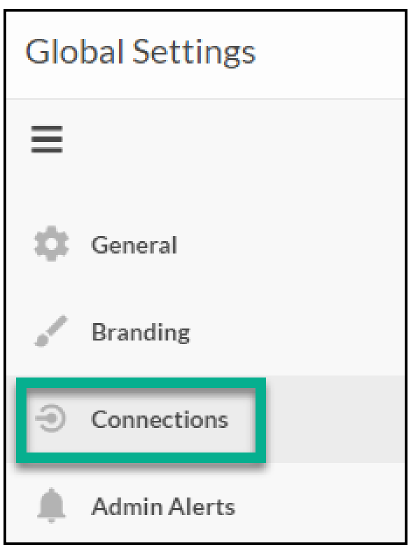
1. Visit https://www.youritportal.com and log into the RapidFire Tools Portal.



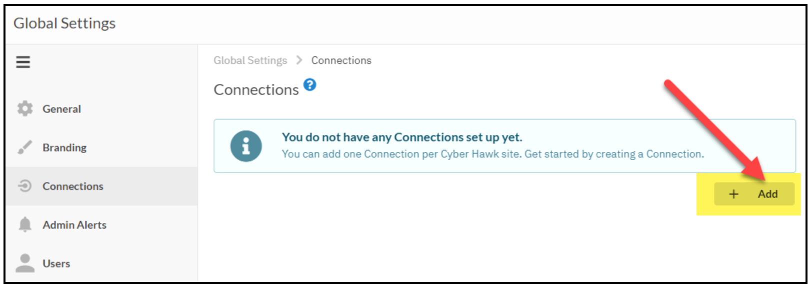
2. Click global **Settings (Admin)** .

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

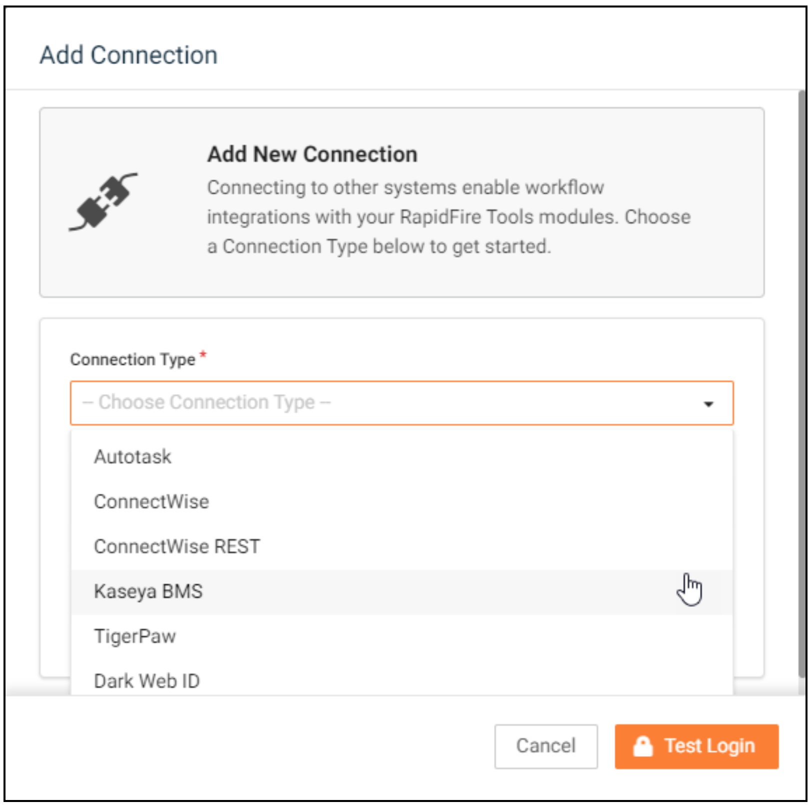
3. Click **Connections**.



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



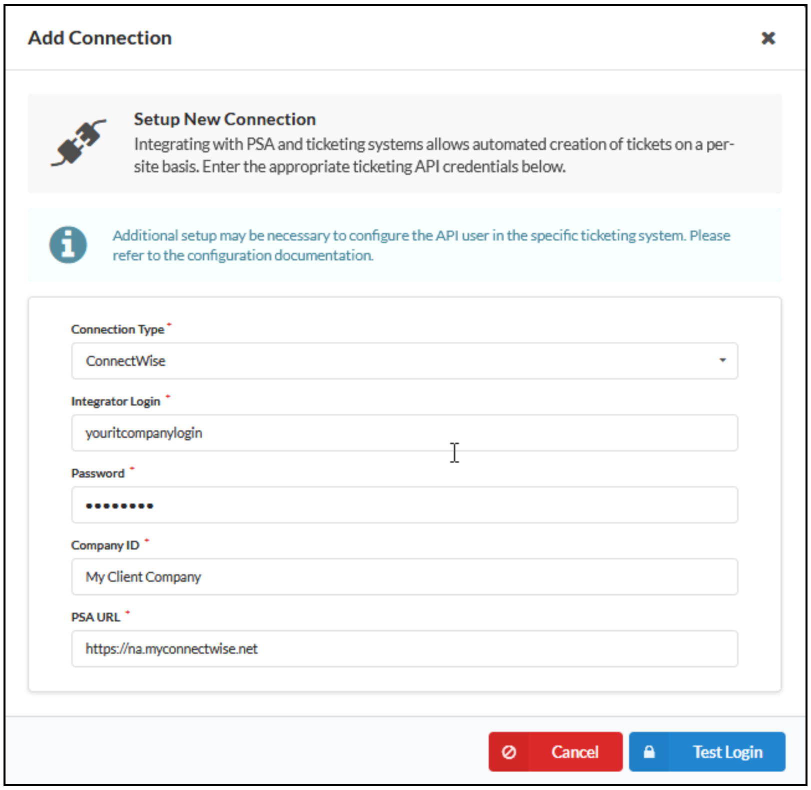
5. In the Setup New Connection window, configure the **Connection Type** by selecting the PSA/Ticketing system.



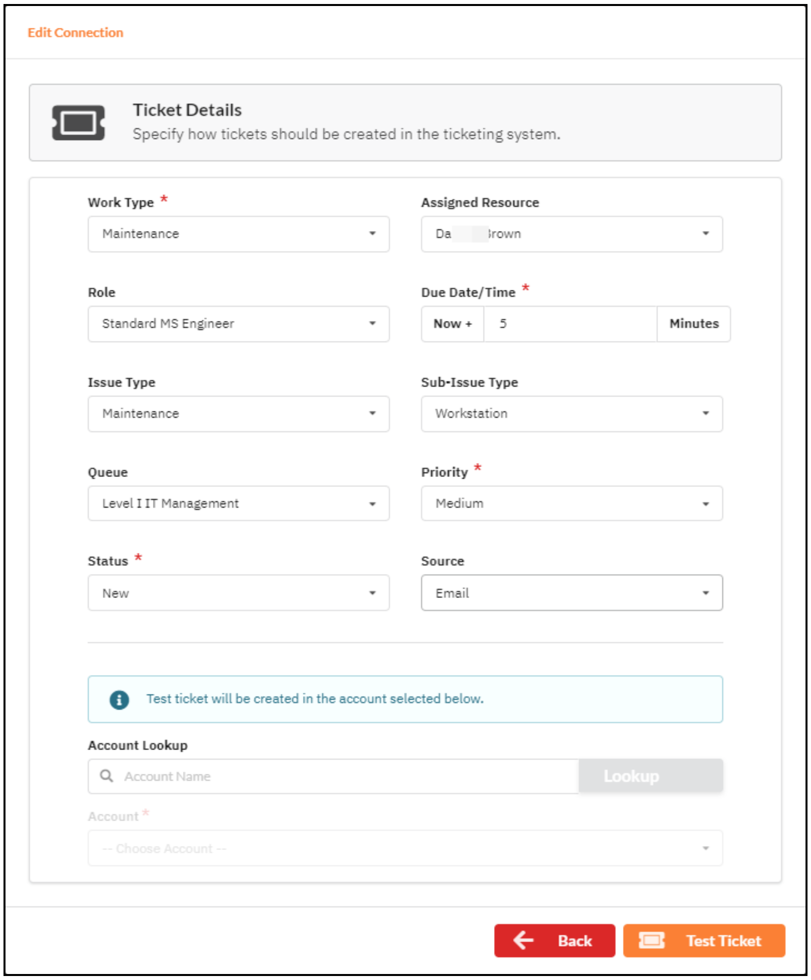
6. Then enter the information required to set up the Connection.

   This information will include:

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

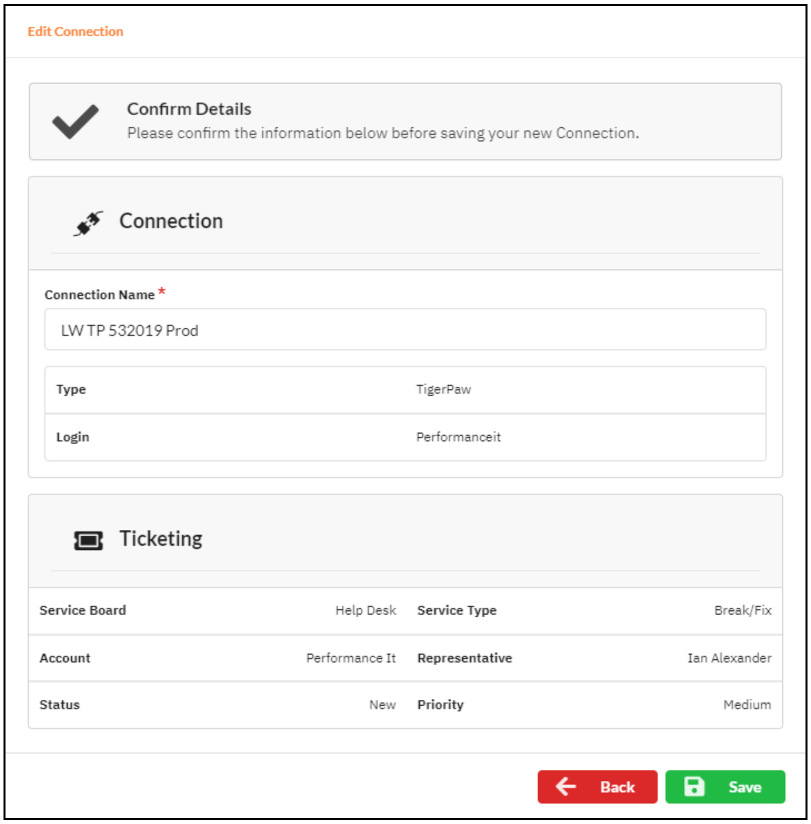


7. Click **Test Login** button to test your Connection login. After a successful test login, the second Add Connection Ticket Details window will be displayed.
8. Continue creating your Connection by entering in the necessary Ticket Details for your PSA.



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**.

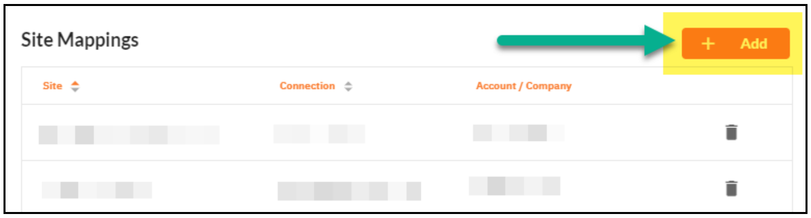


The new Connection created will be listed in the Portal's Connection list.

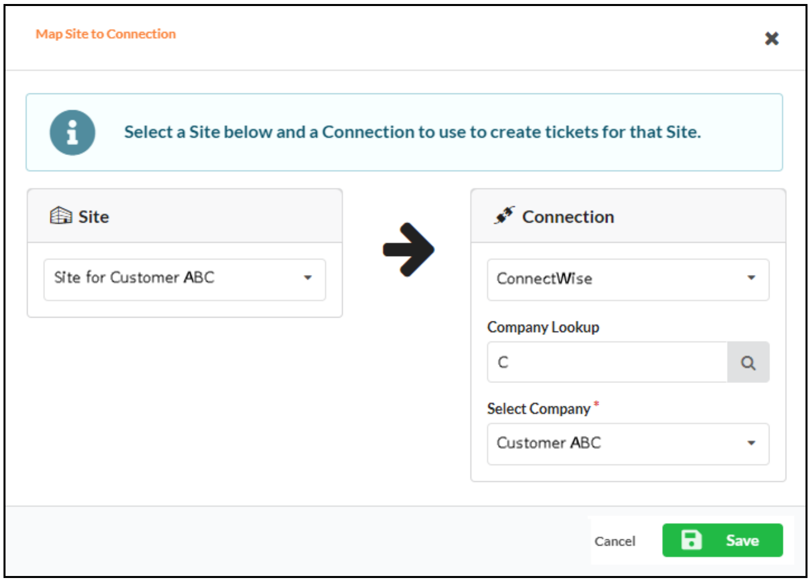
Step 3 — Map your Site to a Ticketing System/PSA Connection

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

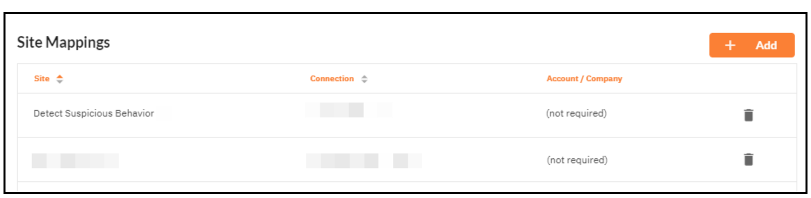
1. In the Integrations window, click **Add** under Site Mappings. The Map Site to Connection window will be displayed.



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



3. Next, **select the name of the Connection** that you want use to link the Site to your Ticketing System/PSA.
4. 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.

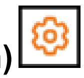


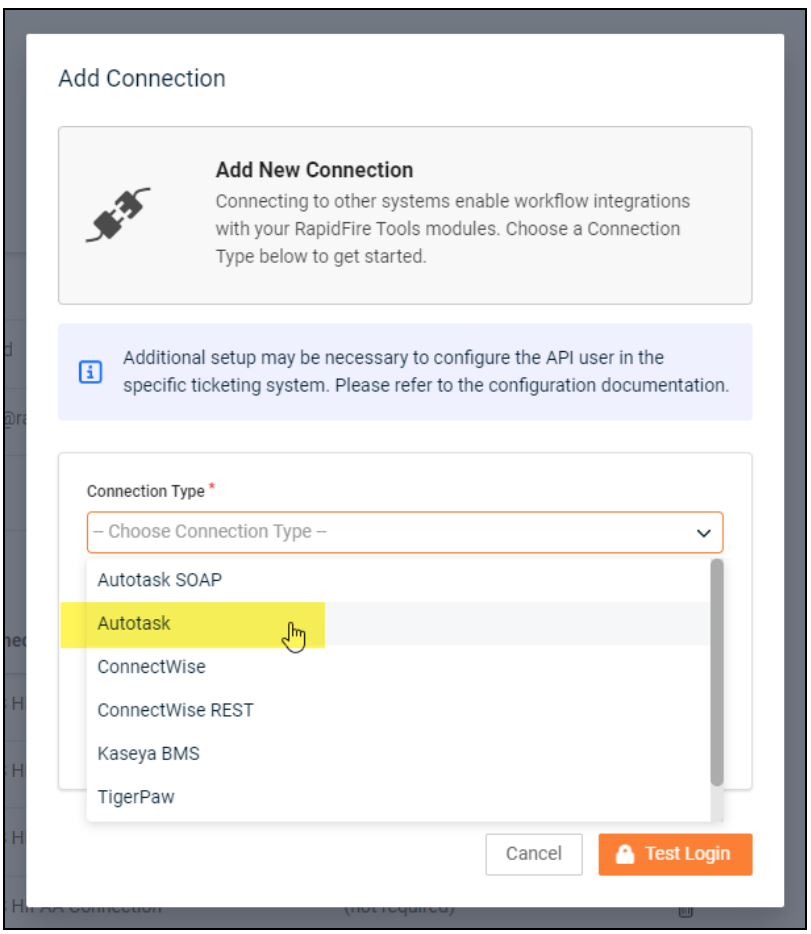
Your Portal account can now be used to create tickets for any Alerts or To Do items listed in the Portal for the RapidFire Tools Portal Site you selected.

Set Up Autotask Integration

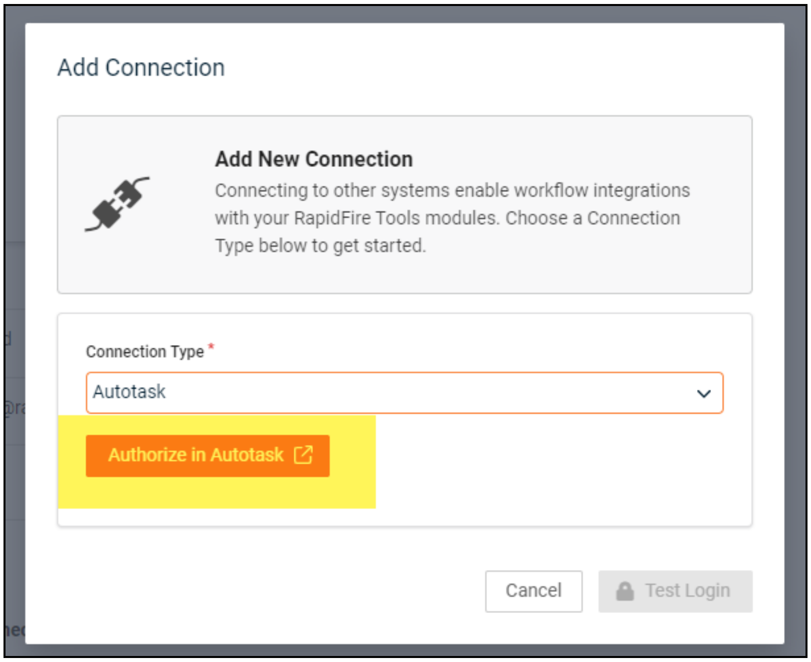
The Autotask SOAP integration has been deprecated. To use the new Autotask integration, all you need is a username and password for a non-API user. Here's how it works:

> **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.

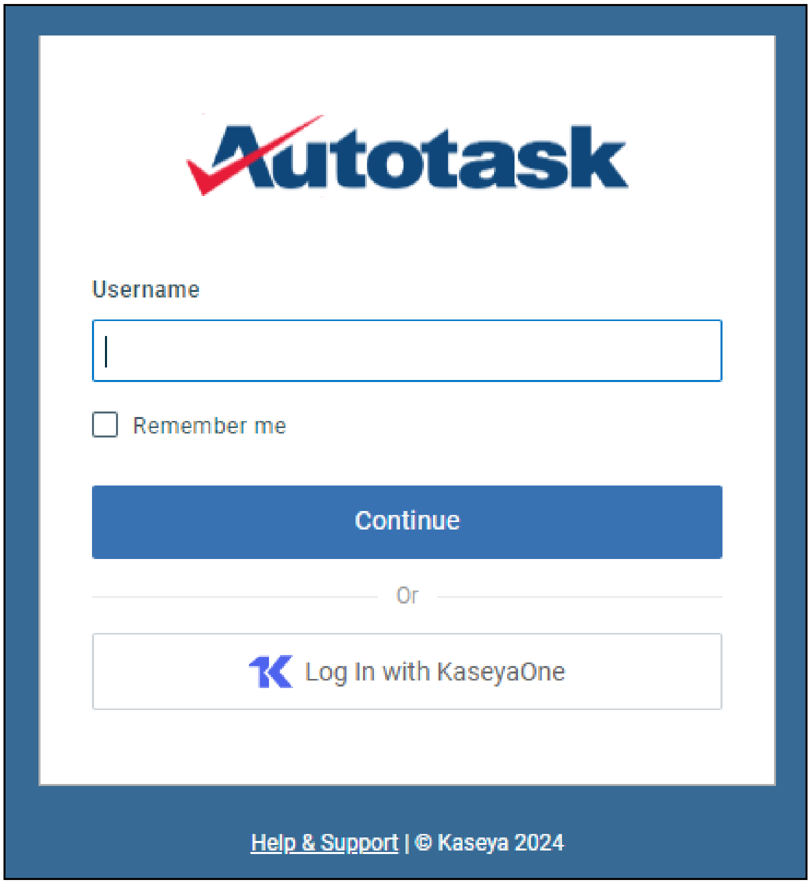
1. From the RapidFire Tools Portal, navigate to global **Settings (Admin)**  > **Connections**.
2. From **Your Connections**, click **Add**.
3. From **Connection Type**, select the **Autotask** connection type (as opposed to the deprecated Autotask SOAP connection).



4. Click **Authenticate in Autotask**.

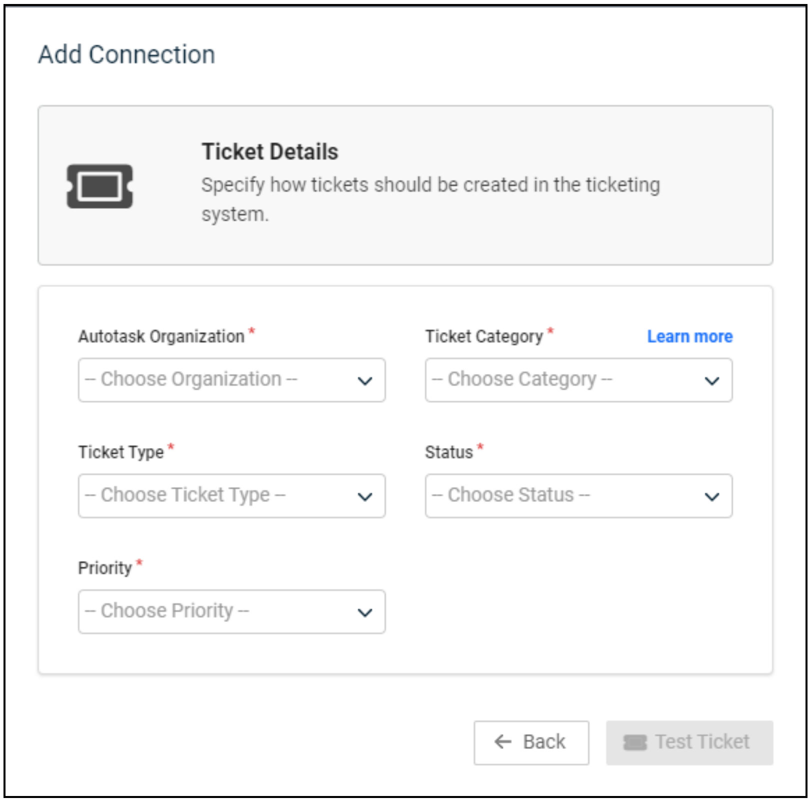


5. Log in using your Autotask username and password. We recommend that you create the connection with a user that has **Admin** privileges in Autotask.



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

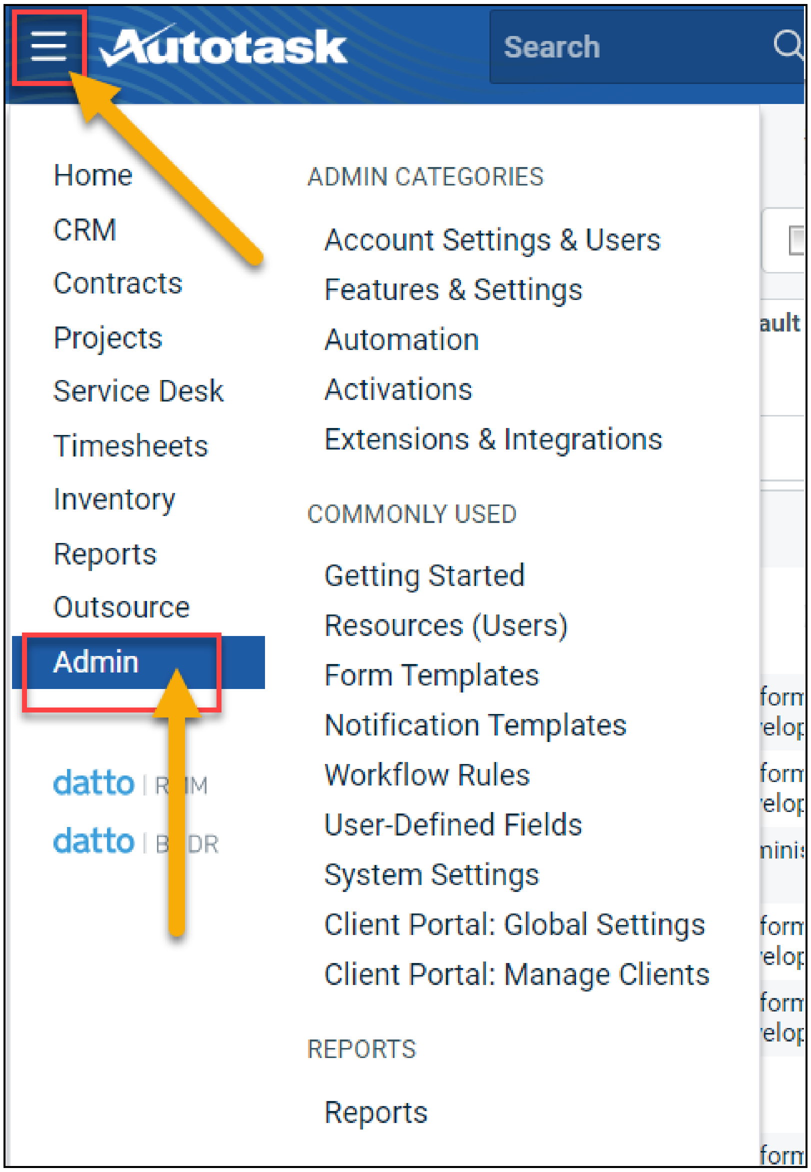
7. Configure the **Test Ticket**. When you finish, the new Autotask connection will become available, where you can map it to a site from **Site Mappings**.



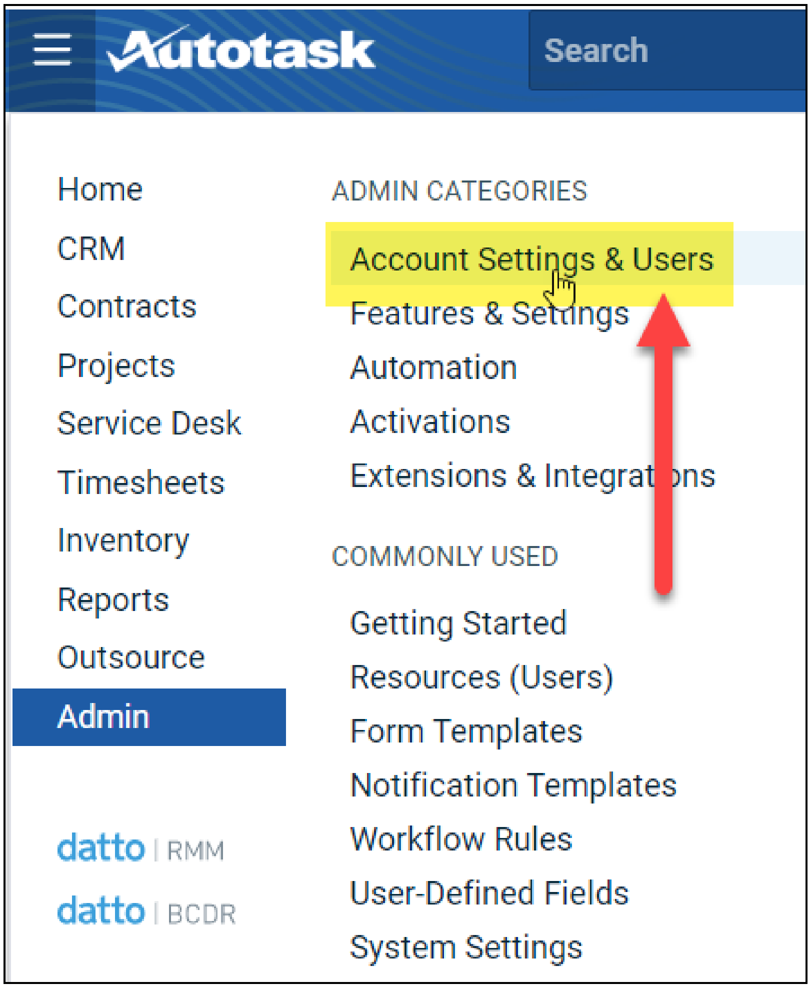
Set Up Autotask (SOAP) Integration

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

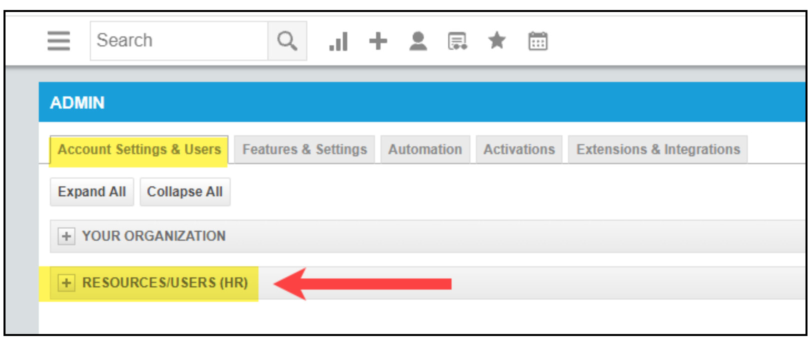
1. Log in to Autotask with your admin user credentials.
2. Click on the **Autotask home** button on the left, then click **Admin**.



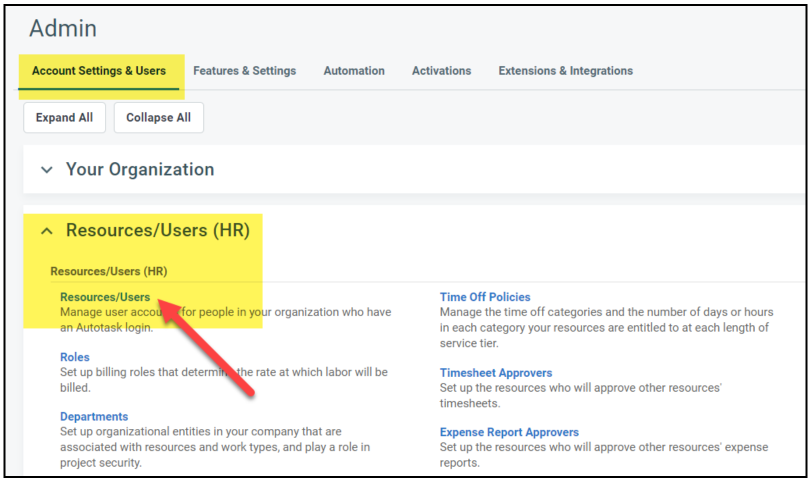
3. From the **Admin** menu, click **Account Settings & Users**.



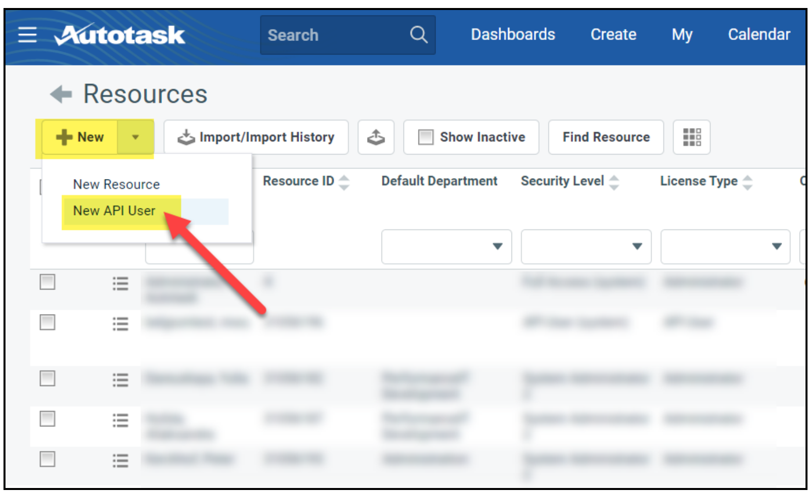
4. Next, click **Resources/Users (HR)** to expand the menu.



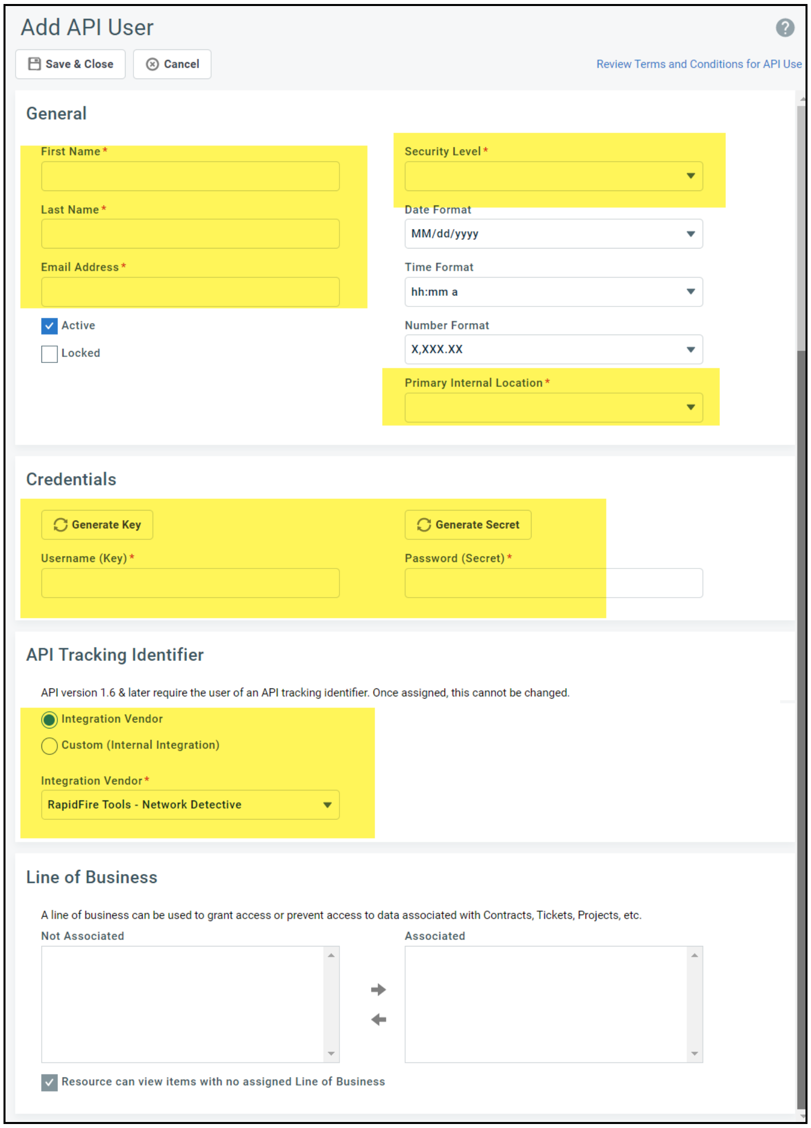
5. Then click **Resources/Users**.



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



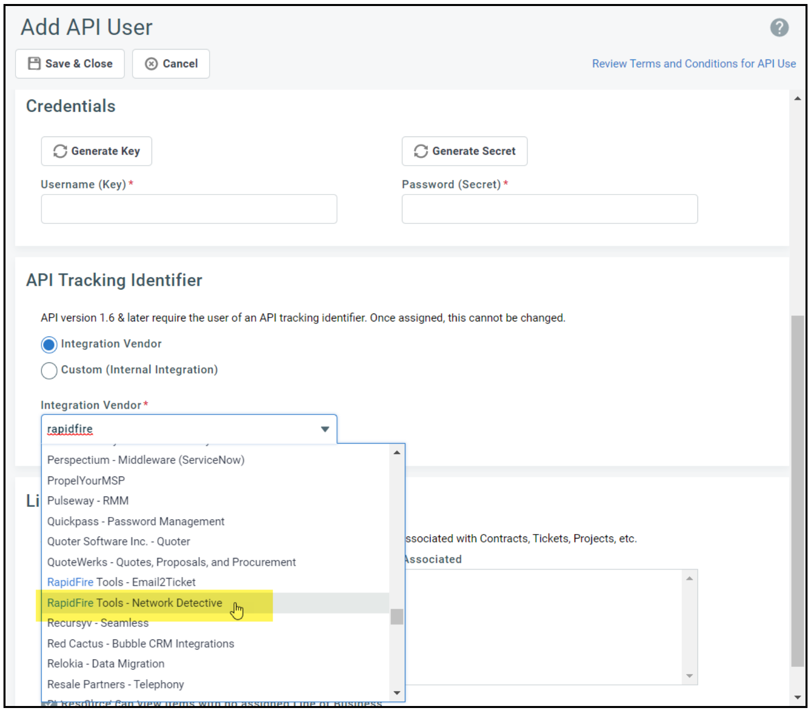
7. Enter information about the API user. Autotask will prompt you to enter the mandatory fields.



- 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**.



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:

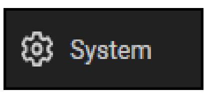
Step 1 — Download and Install the ConnectWise Manage Internet Client Application

To enable the integration, you will need to use the ConnectWise Manage Internet Client application. Download and install the app from http://university.connectwise.com/install/. 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

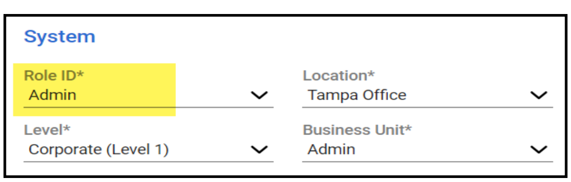
1. From the ConnectWise dashboard, click **System** from the side menu.



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**.



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 "Create Minimum Permissions 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:

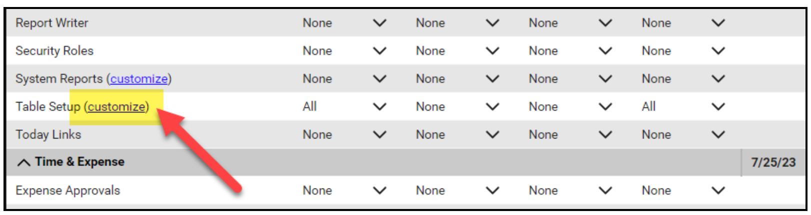
1. Go to **System** > **Security Roles**.
2. Click the [+] button to create a new security role.
3. Set the permissions for the Role as detailed in the table below and click **Save**.
4. Assign this custom Security Role to the API Member instead of full Admin.

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

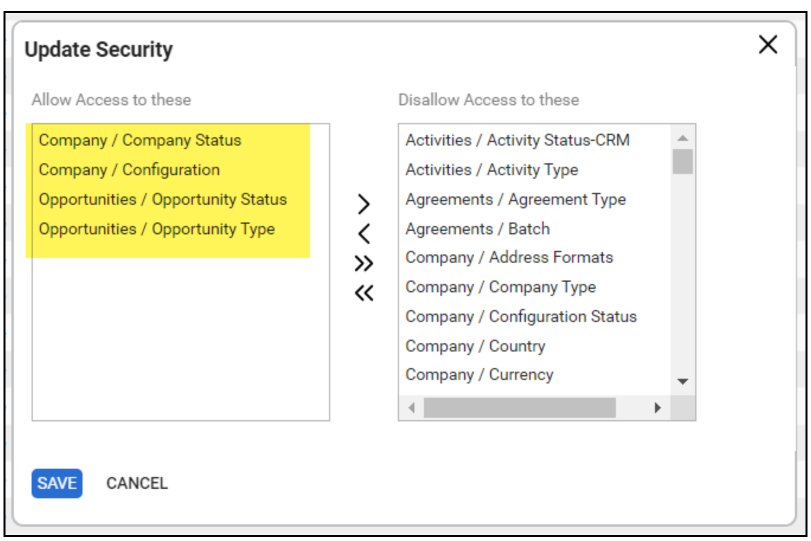
Module		Add Level	Edit Level	Delete Level	Inquire Level
	Opportunities / Opportunity Status, Opportunities / Opportunity Type (See "Table Setup Configuration" below below for an extended explanation)				

Table Setup Configuration

From Table Setup, click **customize**.



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

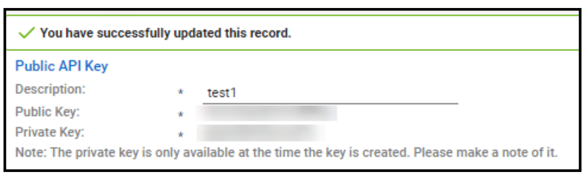


Step 3 — Create an API Key in the ConnectWise Ticketing System

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.



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.

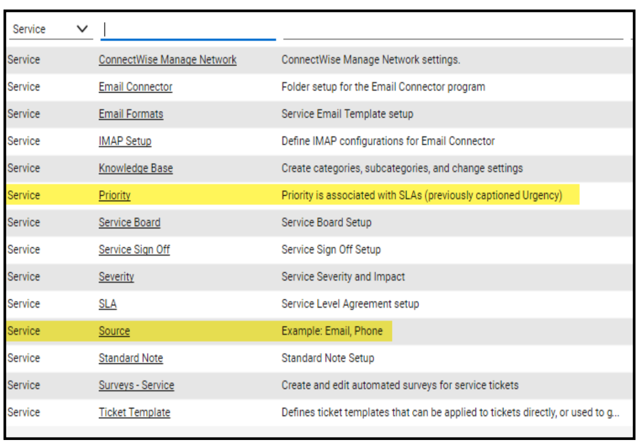
In addition, you must define values for two additional Service Tables:

2. **Source**

   You must include at least one Source.

3. **Priority**

   You must include at least one Priority level.



Service		
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...

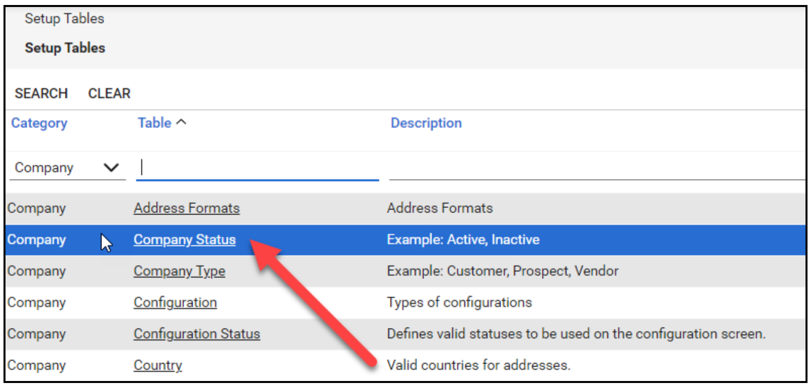
If your existing Service Tables already contain values for the fields listed above, you do not need to create new values.

Step 5 — Remove "Disallow Saving" Flag from Company

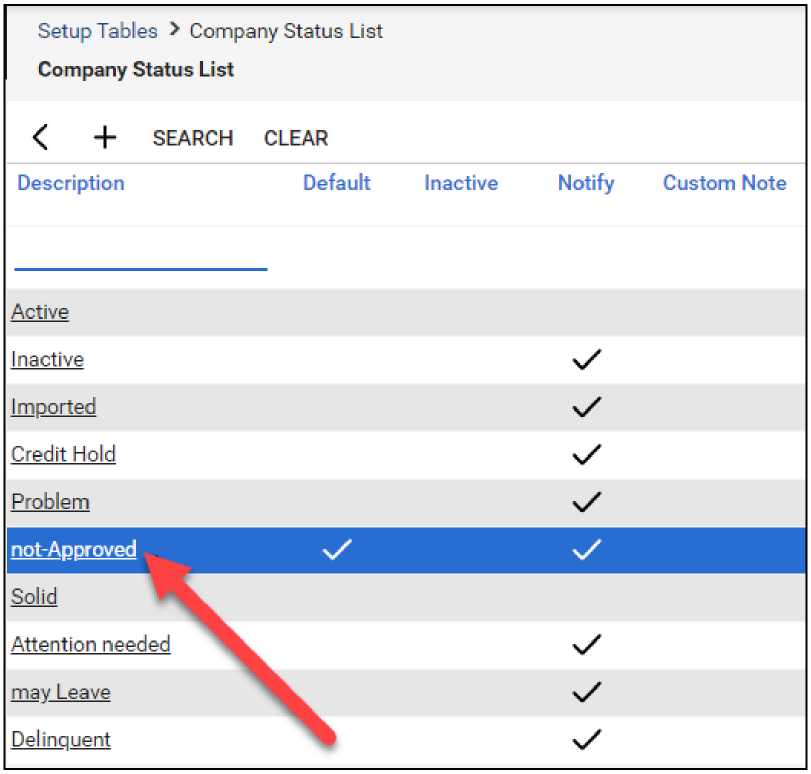
The final step is to ensure your companies are able to save data such as tickets. By default, your company may have the "**Disallow Saving**" option flag enabled; this will prevent you from exporting tickets to the company.

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

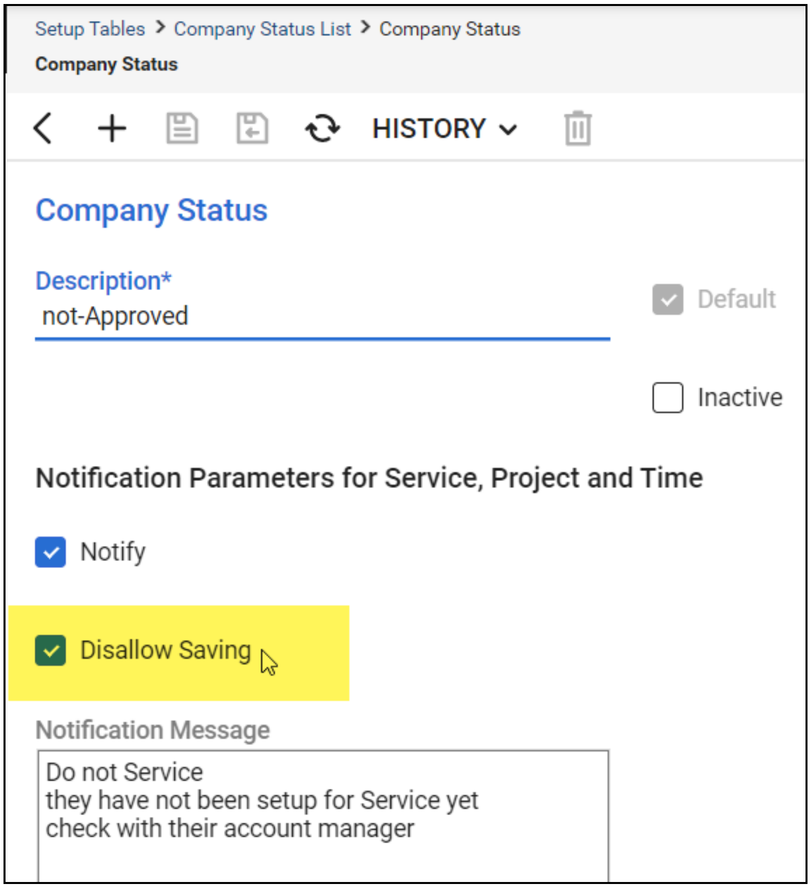
1. Navigate to **Setup Tables** > **Category** > **Company** > **Company Status**.

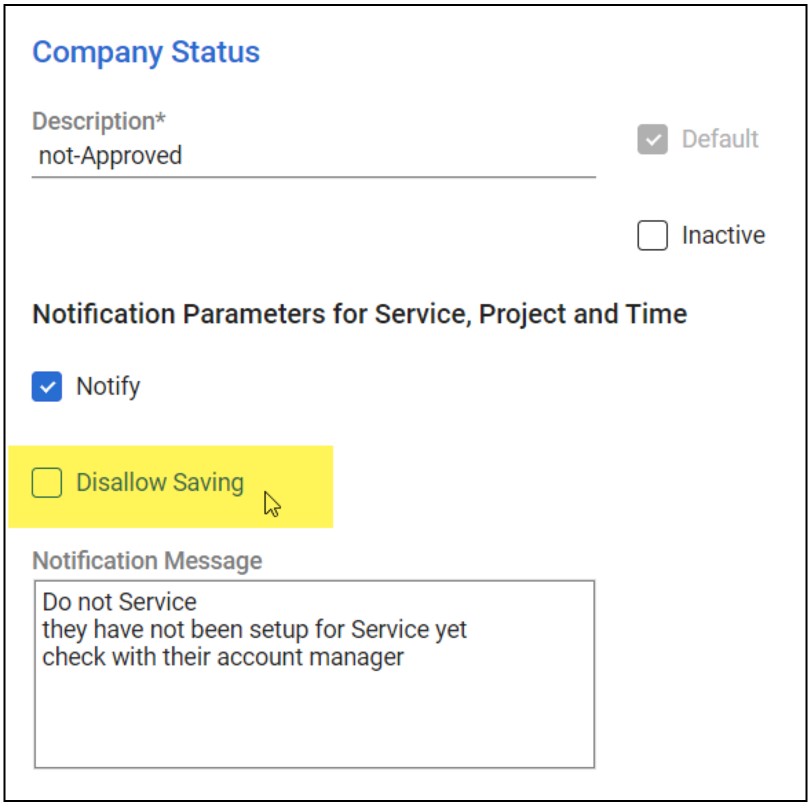


2. From Company Status, open the **not Approved** field.

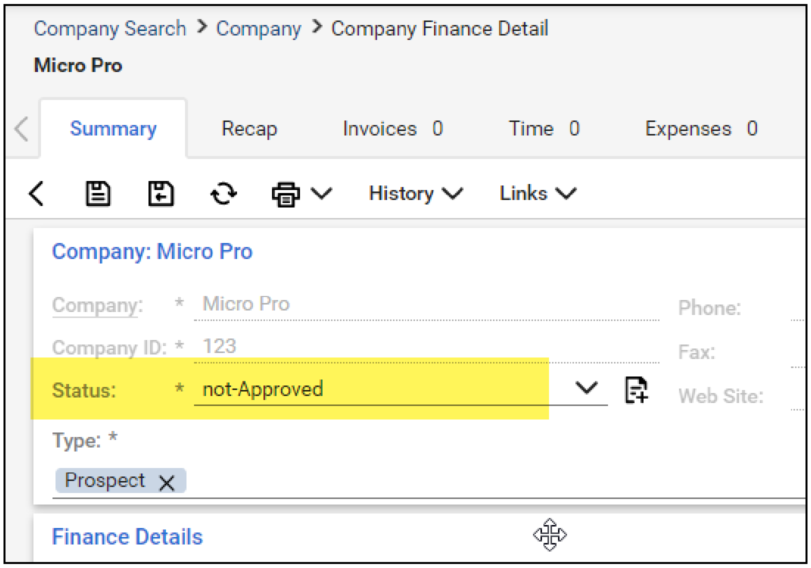


3. Uncheck the **Disallow Saving** flag.


Setup Tables > Company Status List > Company Status
Company Status
HISTORY
Company Status
Description*
not-Approved
Default
Inactive
Notification Parameters for Service, Project and Time
Notify
Disallow Saving
Notification Message
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.


Company Search > Company > Company Finance Detail
Micro Pro
Summary
Recap
Invoices 0
Time 0
Expenses 0
History
Links
Company: Micro Pro
Company: * Micro Pro
Phone:
Company ID: * 123
Fax:
Status: * not-Approved
Web Site:
Type: *
Prospect
Finance Details

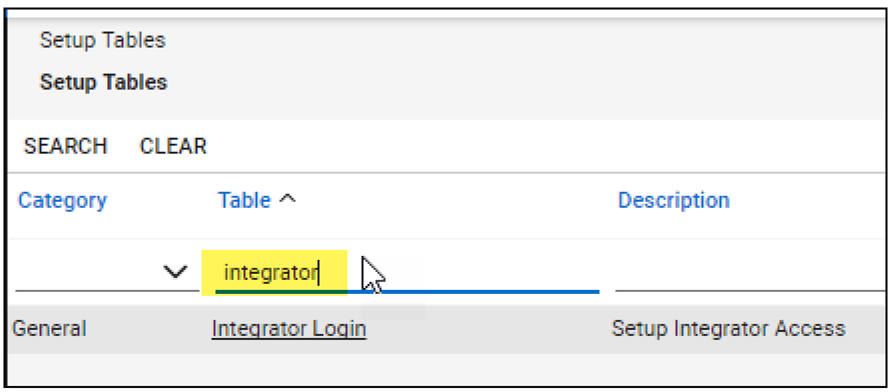
Set Up ConnectWise SOAP Integration

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 ConnectWise REST API instead.

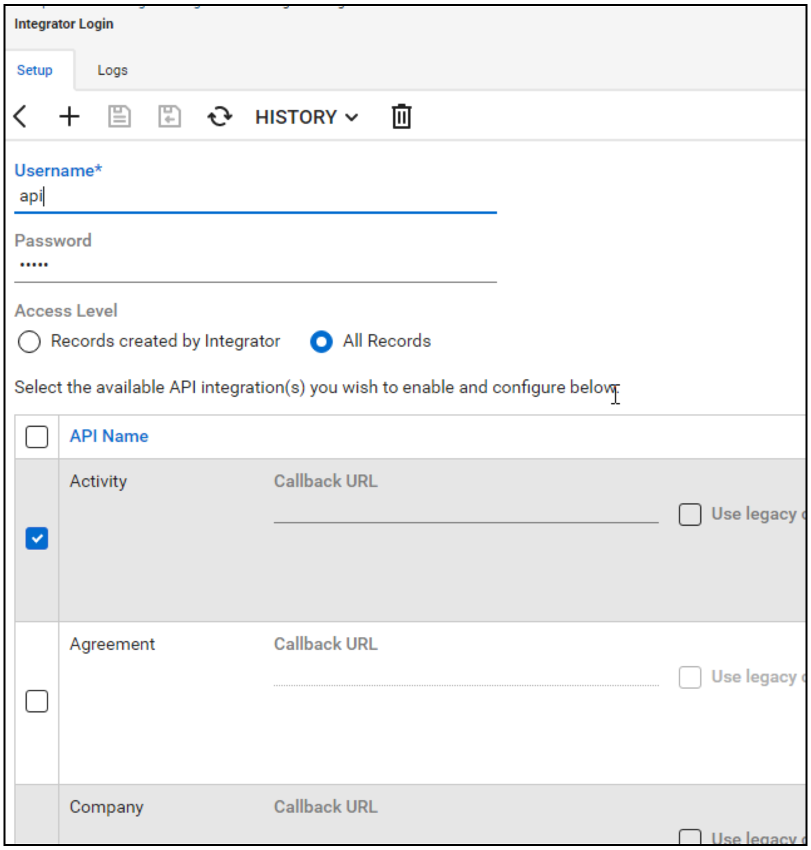
To set up the ConnectWise SOAP integration:

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



4. Click the "**New**" Icon 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

- MemberApi
- ReportingApi
- SystemApi
- ConfigurationApi



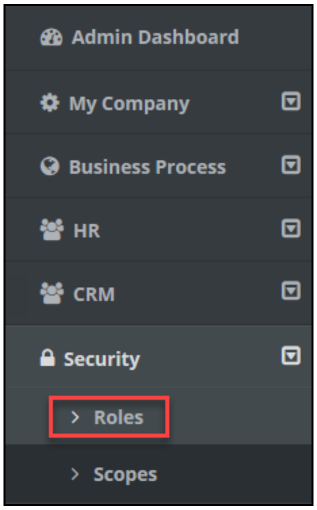
8. Click the **Save** icon to save this Integrator Login.

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

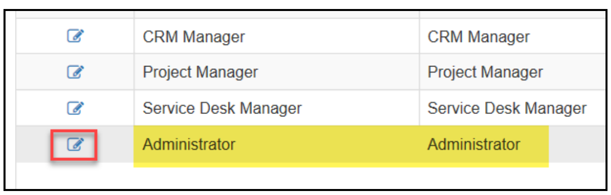
Set Up Kaseya BMS Integration

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:

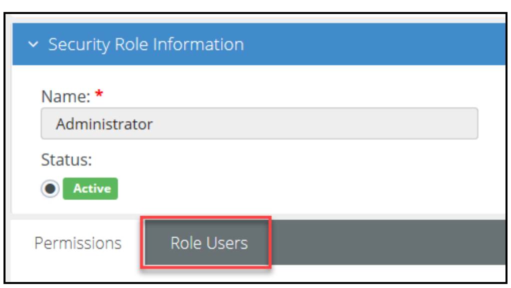
1. Log in to Kaseya BMS.
2. Go to **Security** > **Roles**.



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



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

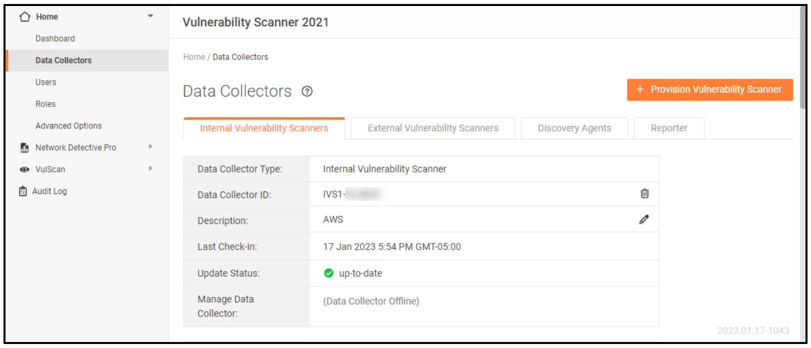


5. Click **Add**.

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**.



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

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 "Create Internal Scan Task" on page 20.

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 "Provision VulScan" on the next page.

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 "Portable VulScan Set Up" on page 228.

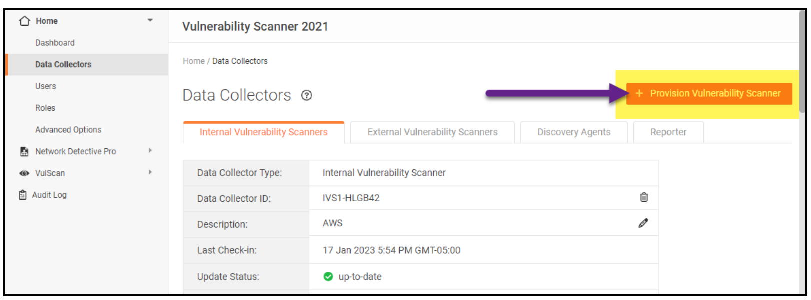
Remote Internal Vulnerability Scanner

- 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 "Set Up Remote Internal Vulnerability Scanner" on page 86.

Provision VulScan

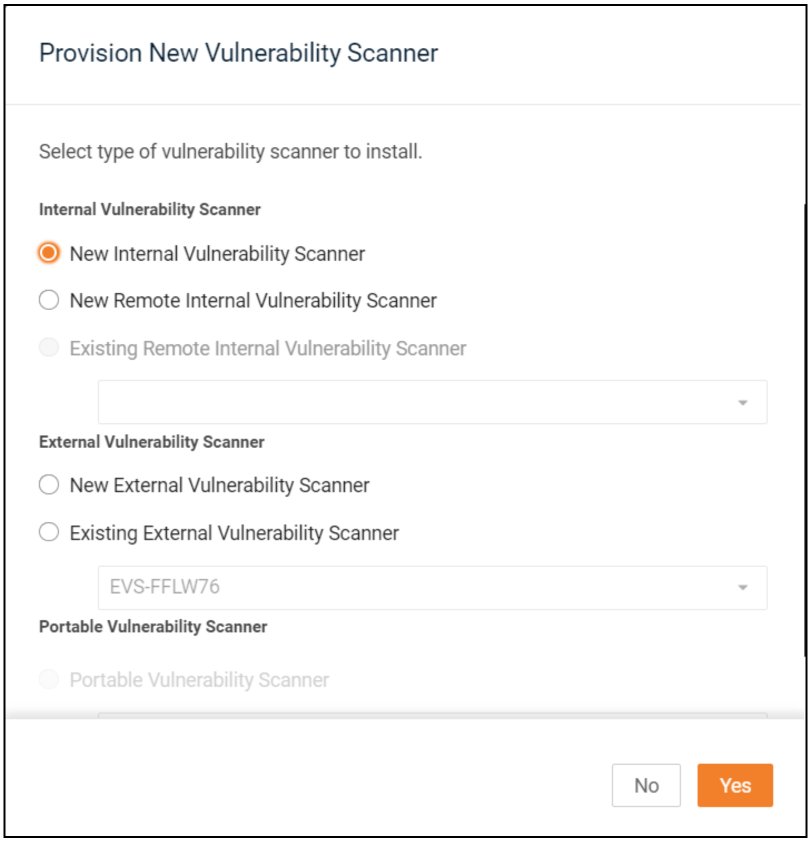
When you create a new VulScan site, a single data collector/appliance will be provisioned for the site automatically. However, you have the option to provision additional vulnerability scanner data collectors to a site. This allows you to break up larger scan jobs across two or more appliances that can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

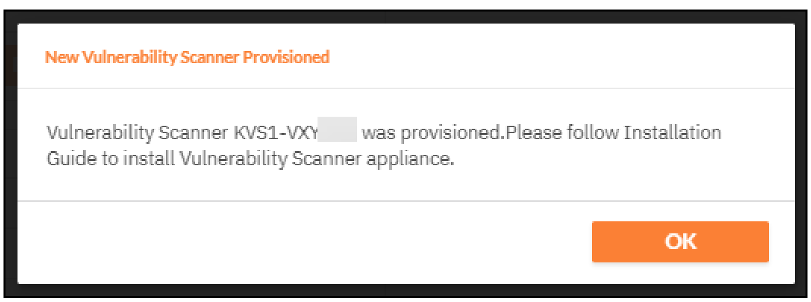


3. Select whether to provision an **internal**, **external**, **portable** or **remote** vulnerability scanner. See "Function of VulScan Data Collectors" on the previous page for a breakdown of each appliance type.

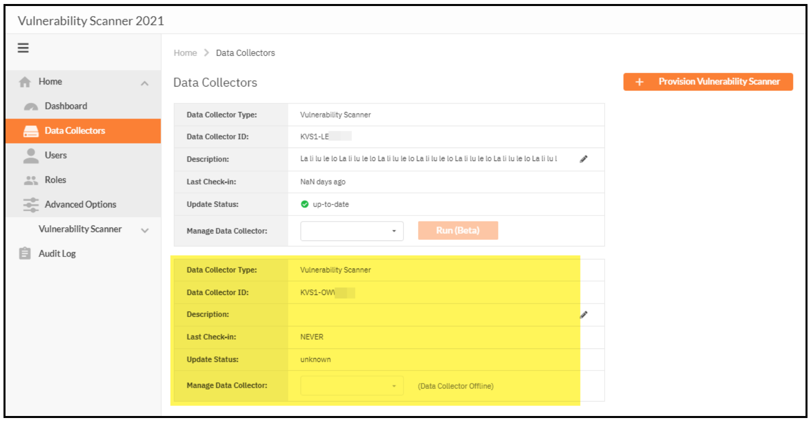
> **Note:** Some appliance types, such as the **external**, **portable**, and **remote** scanners, allow you to select from among existing appliances. In this way you can use one appliance to service multiple sites where you want to perform scans.



4. Confirm your selection.



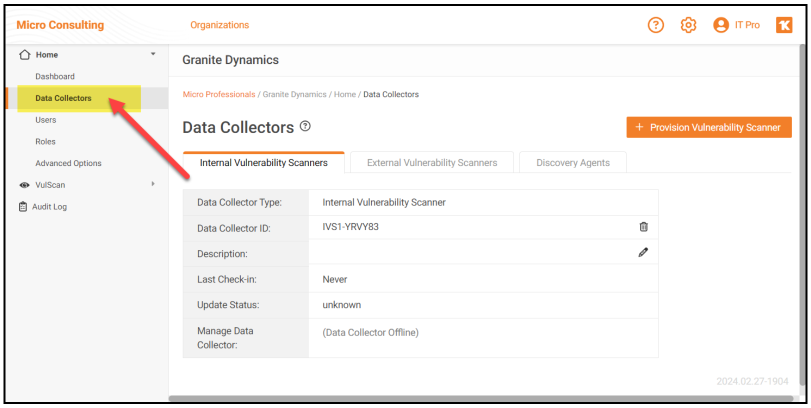
5. The new appliance will appear in the list of appliances.



6. 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 Virtual Appliance Installation Guide for VulScan 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 "Create Scan and Notification Tasks" on page 20.

Manage Site Data Collectors

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

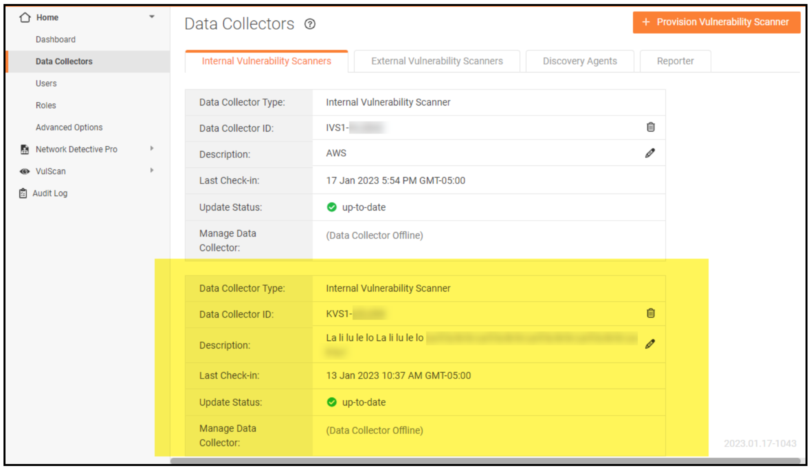


The **Data Collectors** page presents each "data collector" – also known as an *appliance* or *server* - deployed on the Site network. This includes data collectors for the various managed services: Cyber Hawk, Compliance Manager, Reporter, and other product types.

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.

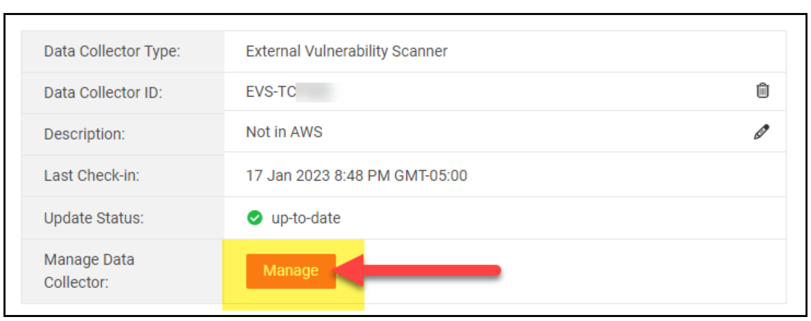


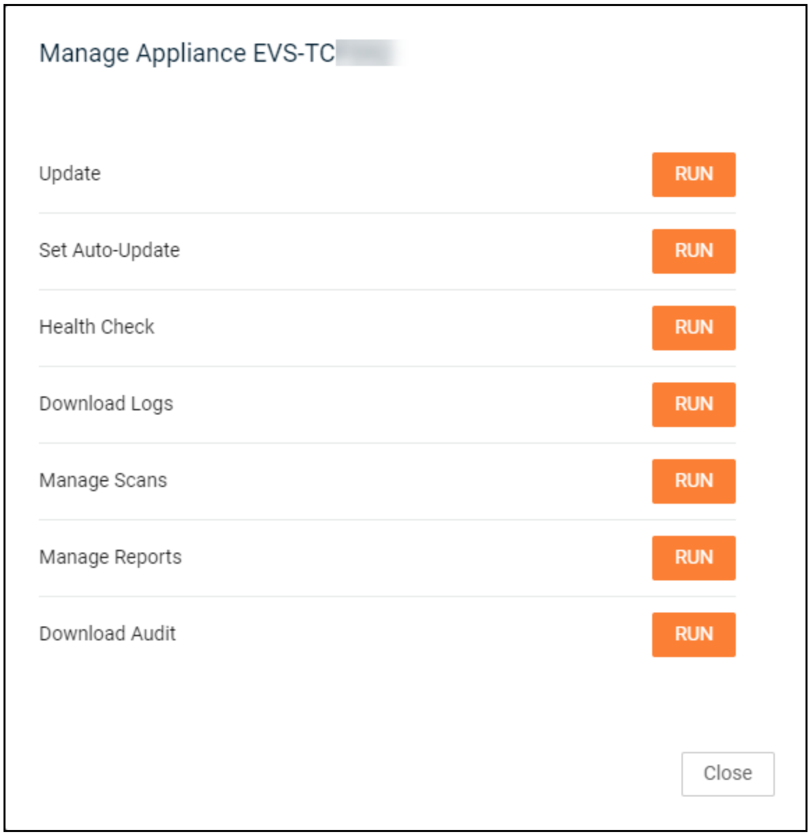
For each data collector, you can quickly see:

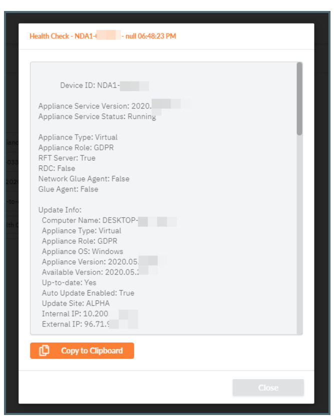
Data Collector Type	For example: Compliance Manager, Reporter, Cyber Hawk
Data Collector ID	Useful for troubleshooting purposes
Last check-in	Useful for troubleshooting purposes and indicates active status
Update status	Indicates whether the data collector has the latest update. In most cases the data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

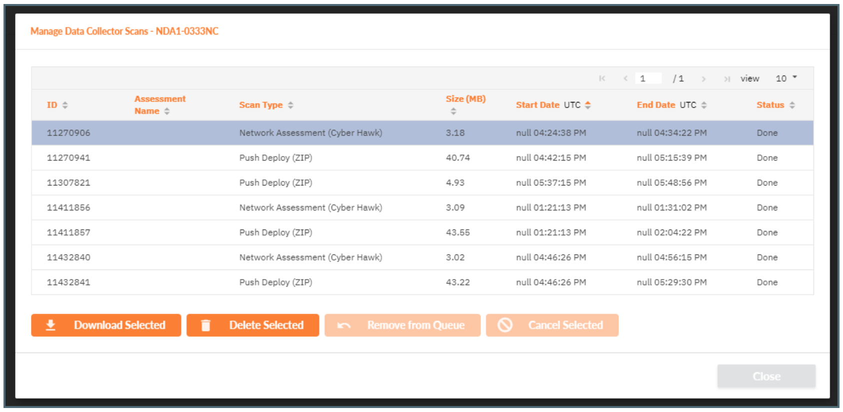
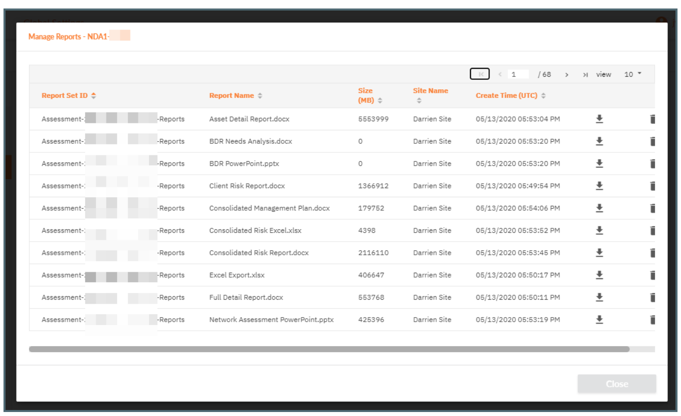
Data Collector Commands

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.





<table>
<tr><td>Update</td><td>Update the data collector to the latest version. Note that this will cancel all current scans.</td></tr>
<tr><td>Set Auto-Update</td><td>Order the data collector to automatically update itself when a new version becomes available.</td></tr>
<tr><td>Health Check</td><td>Access technical information about the data collector's current status. Can be copied as a text file for troubleshooting.

</td></tr>
<tr><td>Download Logs</td><td>Download log files for troubleshooting purposes.</td></tr>
</table>

Manage Scans	View and manage all scans assigned to the appliance.  Here you can: • Download scan files • Delete completed scans and their associated files • Remove queued scans • Cancel scans in progress
Manage Reports (Reporter only)	Access and manage reports stored on the Reporter appliance. 
Download Audit	Download the audit log for the appliance.

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.

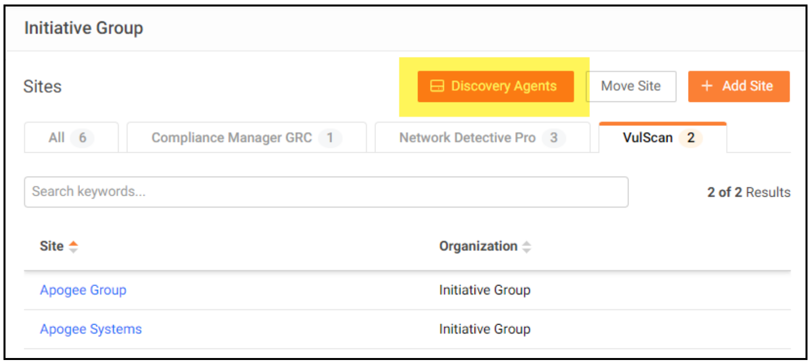
- gatekeeper.rapidfiretools.com
- go.rapidfiretools.com
- au.rapidfiretools.com
- go-eu.rapidfiretools.com
- go-au.rapidfiretools.com
- wcflb.rapidfiretools.com
- wcflb-eu.rapidfiretools.com
- wcflb-au.rapidfiretools.com
- api.ndglue.com
- networkdetective.s3.amazonaws.com
- download.rapidfiretools.com

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

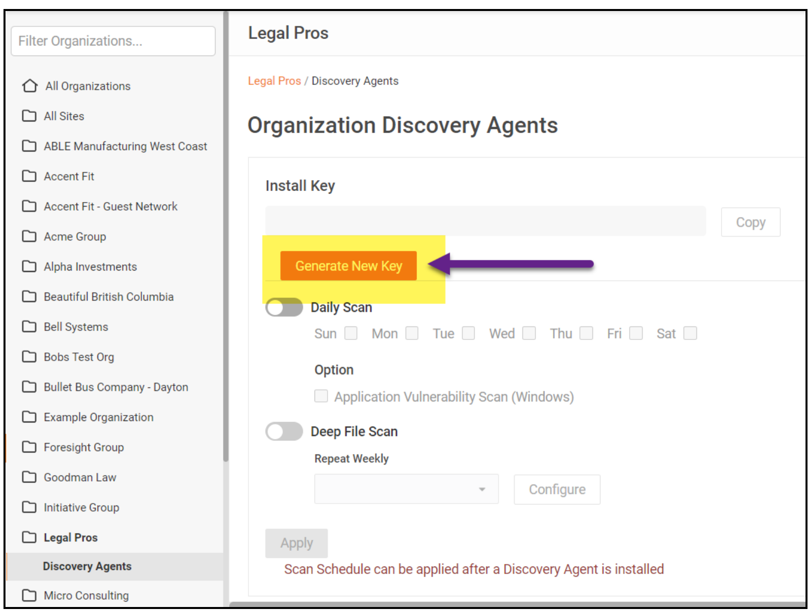
Step 1 — Enable Discovery Agents at the Organization Level

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.

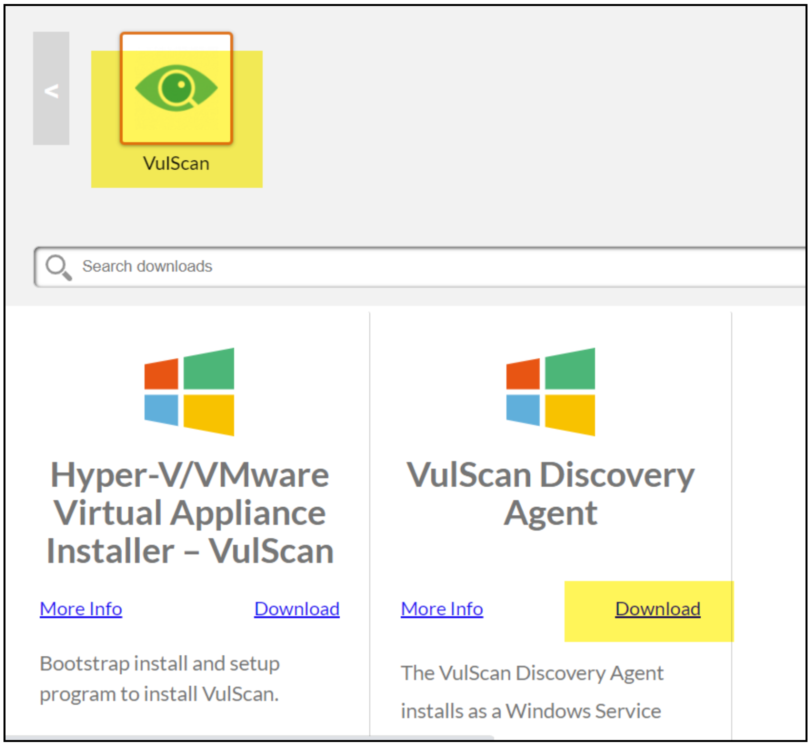
   

3. Click **Generate New Key**. **Copy the key** to your clipboard. You will use this key to authenticate the Agent to your organization.

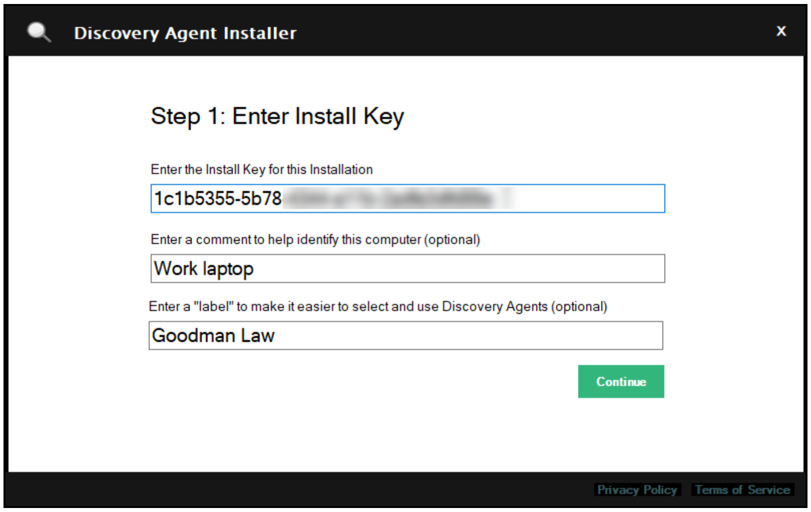
   

Step 2 — Install Windows Discovery Agent on PC on target network

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

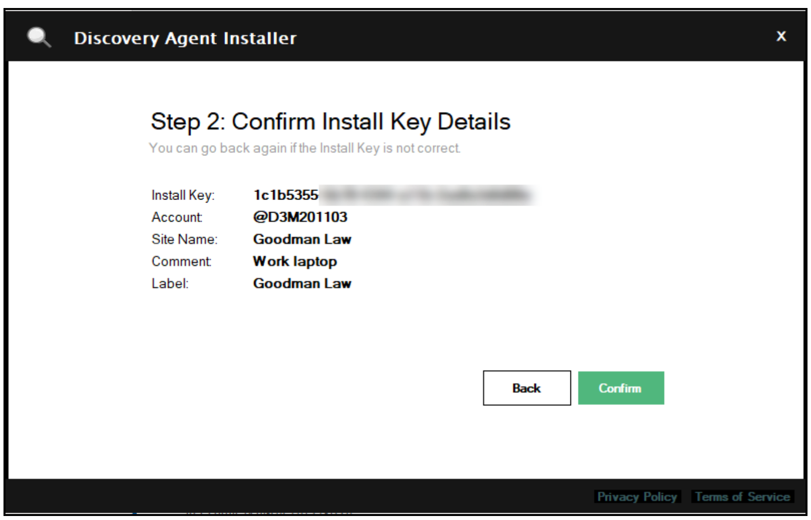


2. Open the app, proceed through the setup prompts, and click **Install**.
3. Confirm that you want to allow the Discovery Agent to make changes to your device. Once you finish the wizard, the Discovery Agents Installer will open.
4. **Enter the install key** that you generated in the previous step. 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.

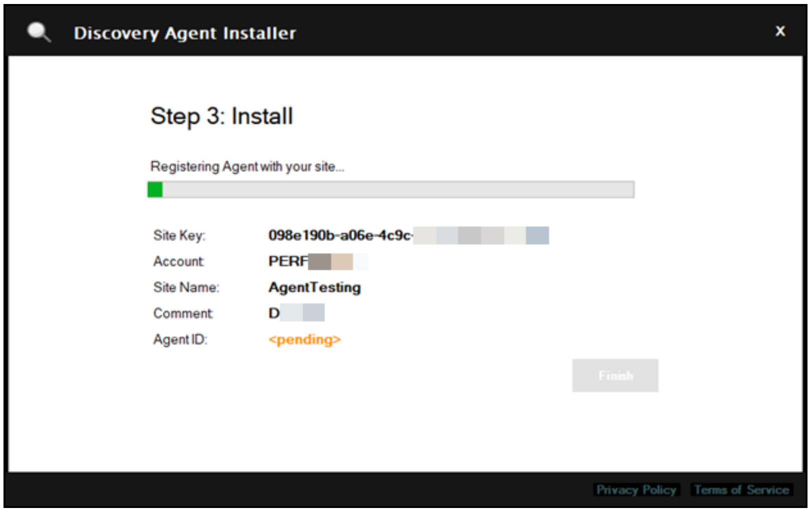


Finally, **enter an optional comment** to help identify the PC hosting the Agent.

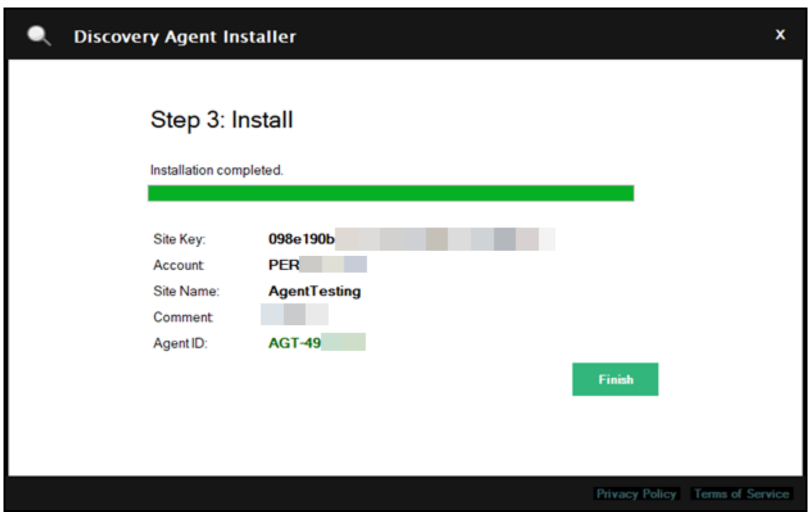
5. Next, **Confirm** the site and key details for the Discovery Agent.



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



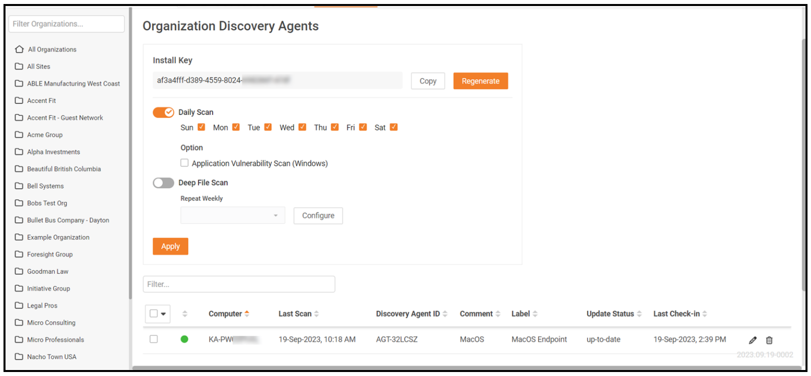
7. Click **Finish** when complete.



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

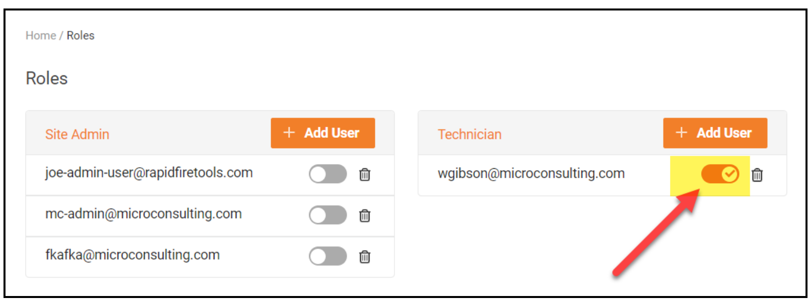
RapidFire Tools Portal.

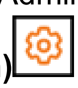


Step 4 — (Optional) Enable Access for Site Admin and Technician Users

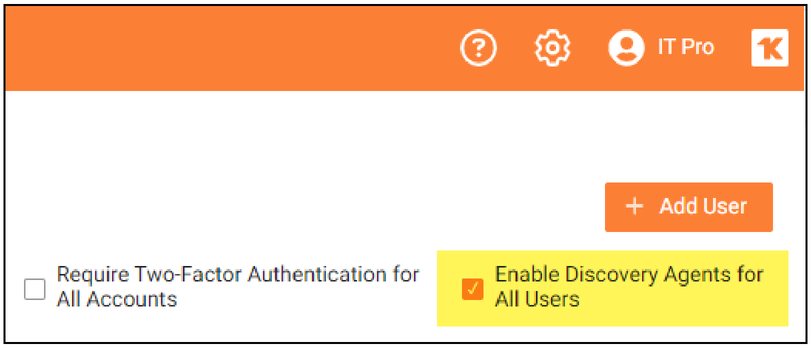
Next, you can optionally enable your Site Admin and Technician users to manage the Discovery Agents that you deploy. You can do this in two ways:

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.



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.

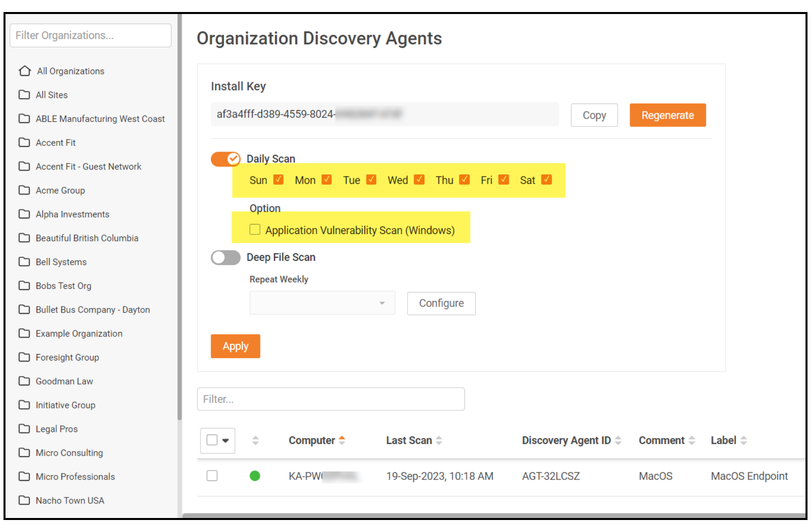


Step 5 — Schedule Scans for Discovery Agent

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 "Application Vulnerability Scan for Windows" on page 219.

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

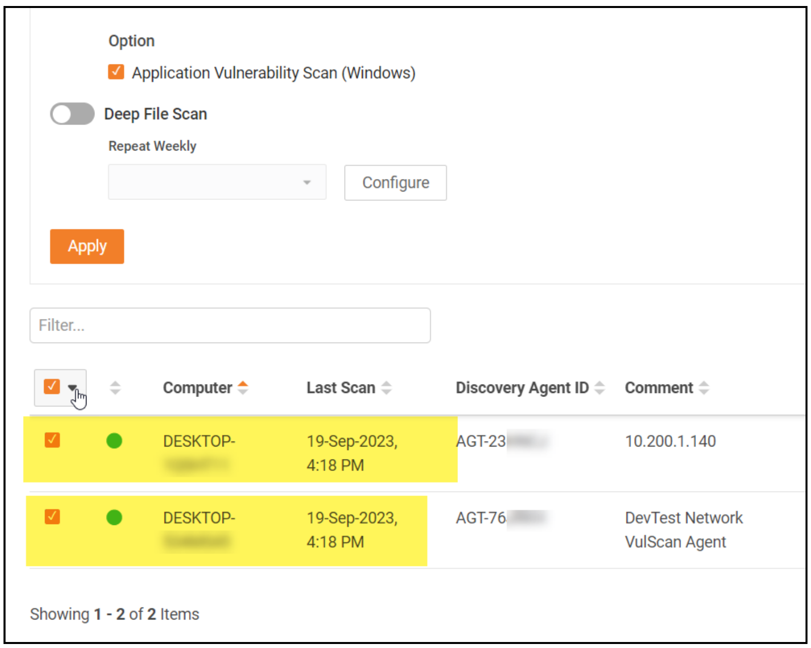


> **Note:** To avoid disruption during normal business hours, Agent scans begin at 2:00am on the selected days for the Time Zone that you set from global **Settings (Admin)** > **General** > **Time Zone**. See also "Set Time Zone" on page 142.

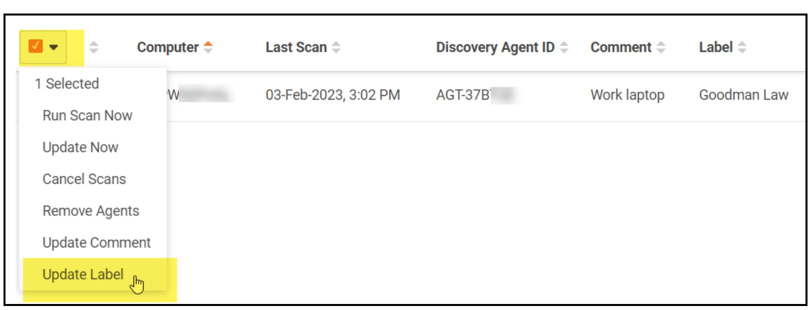
Step 6 — Assign Labels to Agents

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

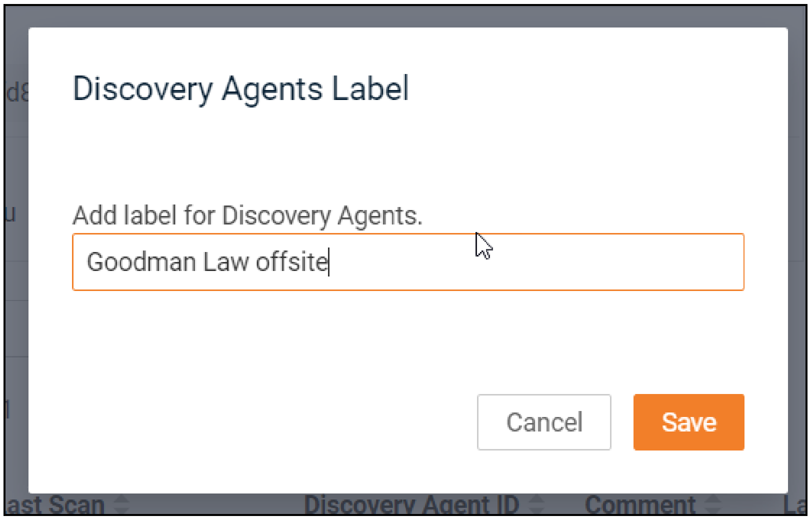
1. Navigate to **[Your Organization]** > **Discovery Agents**.
2. **Select the agents** where you want to add or edit labels.



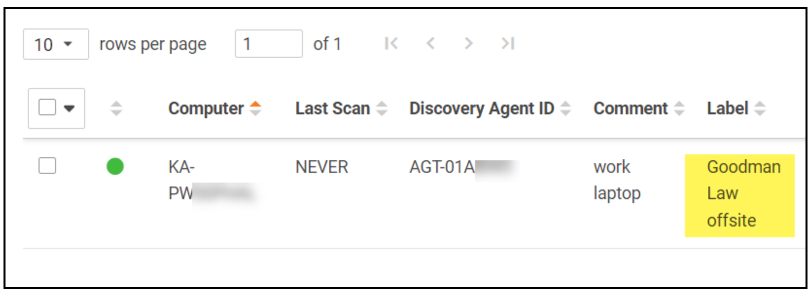
3. Click the **Select All** button, and then click **Update Label**.



4. **Enter your label** and click **Save**.



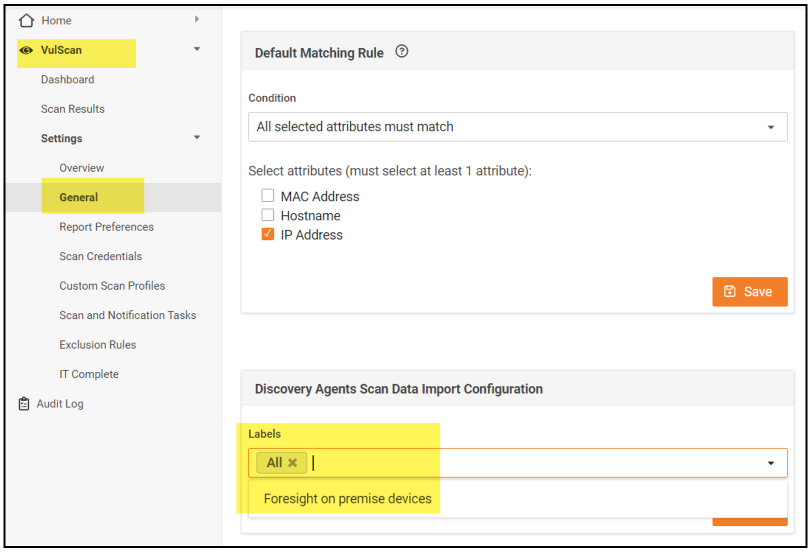
5. The label will be updated for the select agent(s).



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**.

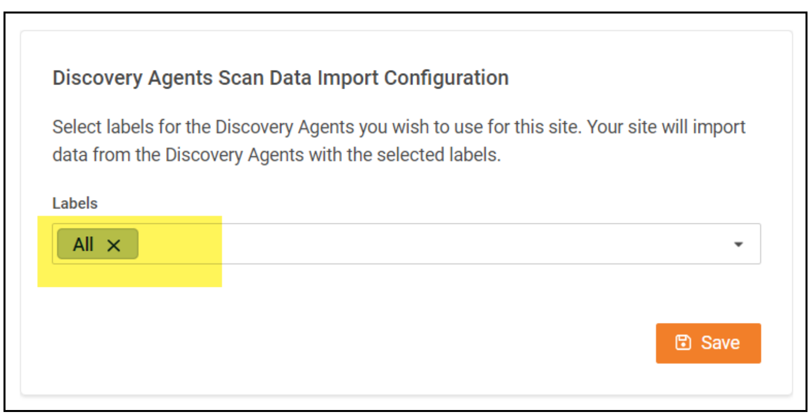


3. From **Labels**, select the labels that designate the agents you wish to use for this site. You must have first created labels for your agents. See "Step 6 — Assign Labels to Agents" on page 214.
4. Then click **Save**. Your VulScan site will then import scan data from the labeled agents. See "How Scan Data Import Configuration Works" below.

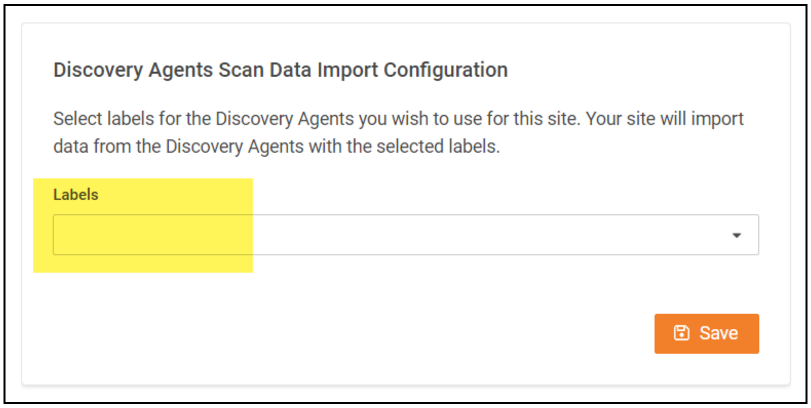
How Scan Data Import Configuration Works

When you configure VulScan Agent imports, here is what will happen:

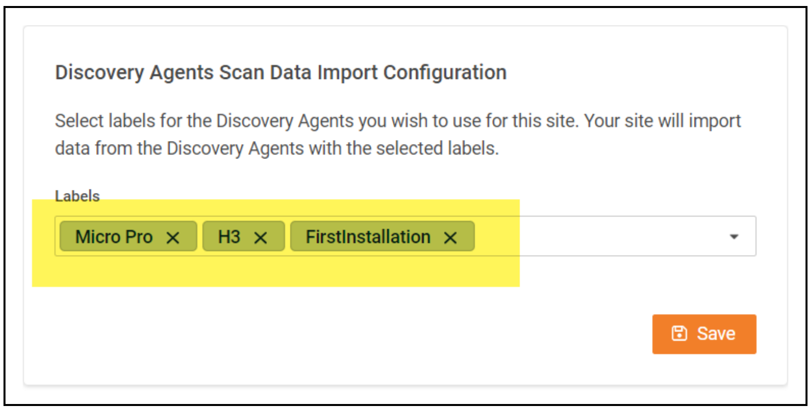
- By default, the **All** label is applied. This will import scans from **all Agents**, both with and without labels.



- If you leave the selector field **blank**, scans will be imported only from agents with **NO label**.



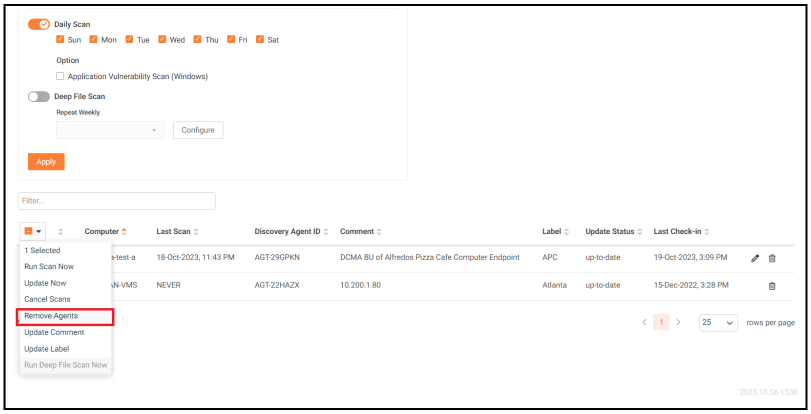
- When you select **exact labels**, only scans from agents with the **assigned labels** will be imported.



Remove Discovery Agents

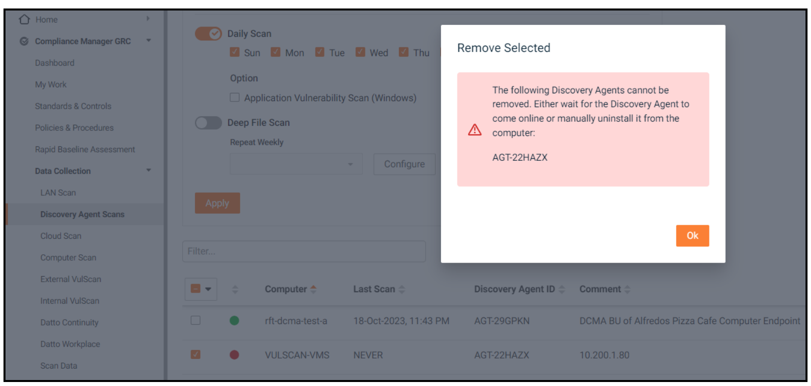
To remove Discovery Agents:

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.



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 "Uninstall Script 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.

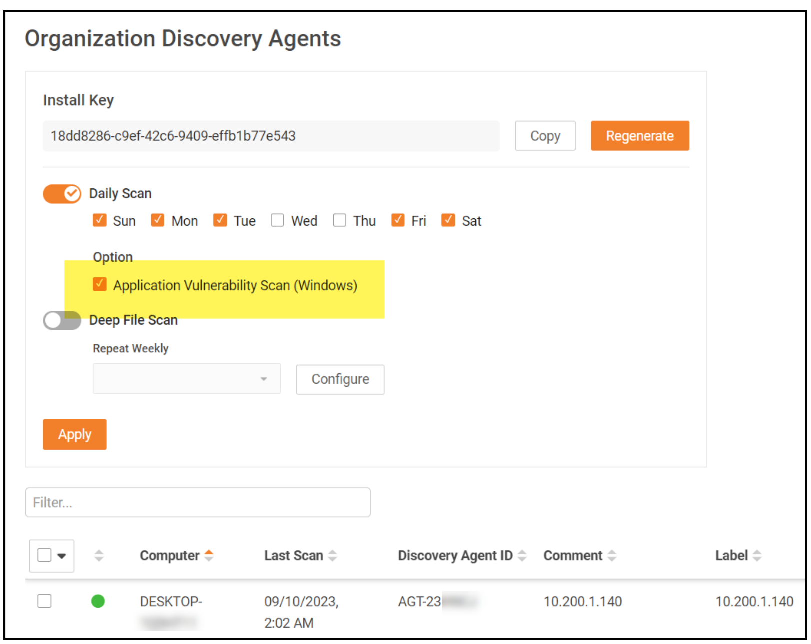
Follow these steps to enable Application Vulnerability Scanning for Windows:

Step 1 — Deploy Discovery Agents on Endpoints

First, install Discovery Agents on each endpoint that you want to scan. See "Enable Discovery Agents for Local Data Collection (VulScan)" on page 207 for complete instructions.

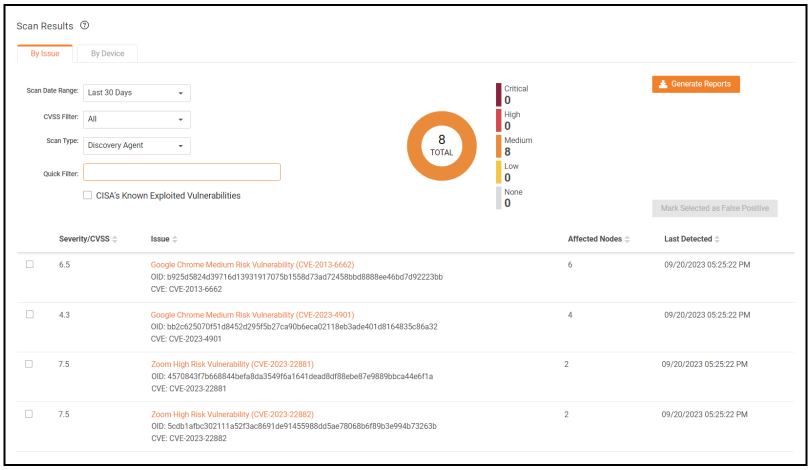
Step 2 — Enable Application Vulnerability Scan for Windows for Discovery Agents

1. From your Organization, navigate to **Discovery Agents**.
2. From the Organization Discovery Agents scan settings, enable **Application Vulnerability Scanning (Windows)**.



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**.



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.

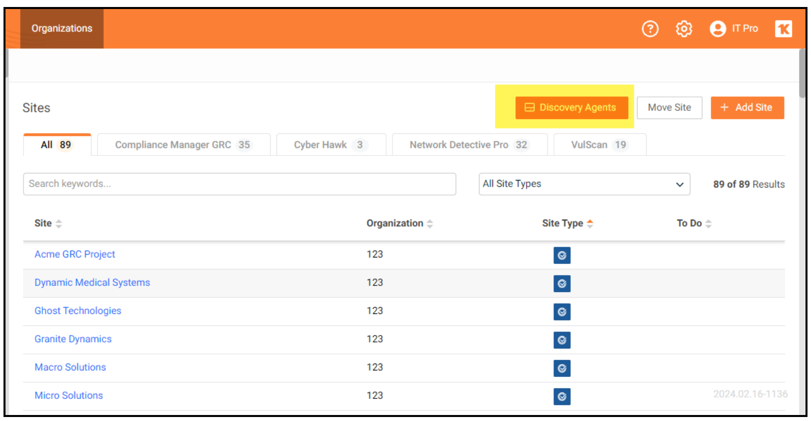
First, "Find and Copy Install Key for Discovery Agents" below. Then, run the install using the scripts below for Linux or macOS devices:

- "Default Scripted Linux Install" on the next page
- "Default Scripted macOS Install" on page 223

Find and Copy Install Key for Discovery Agents

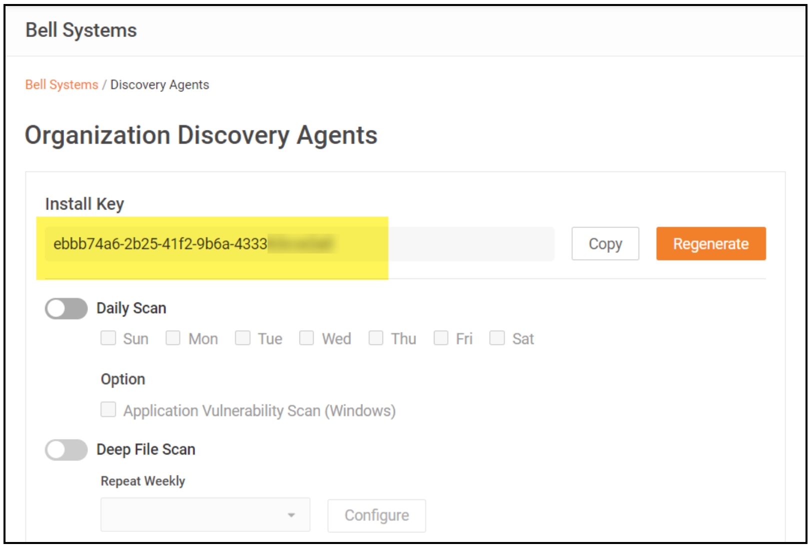
In order to deploy the Agent with the scripts below, you will first need the **Install Key** for the Discovery Agent.

1. First, find and copy the **Install Key**. From the Organization where you wish to deploy the agent, click **Discovery Agents**.



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.



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 -O
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	
Hardware	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 prereqs	**Install Key** for Discovery Agent.

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**). Refer to 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 Download .NET 6.0 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 -O
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 prereqs	**Install Key** for Discovery Agent.

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:

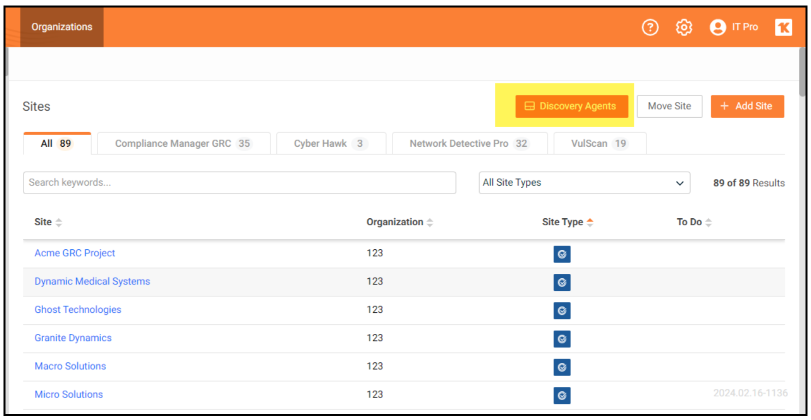
`--force`

Non-interactive mode. Does not prompt for confirmation.

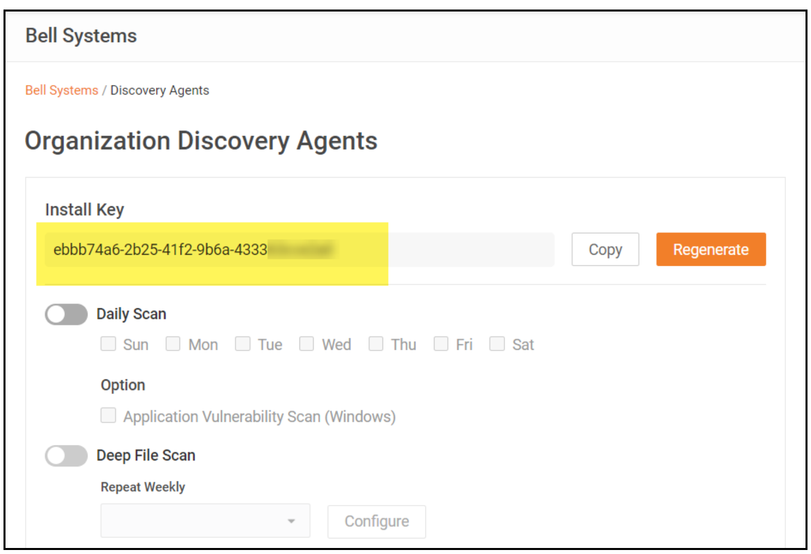
Silent Install for Discovery Agent (Windows)

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**.



2. **Generate** and **copy** the Install Key.



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\register-device.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 walk-through.

```
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.

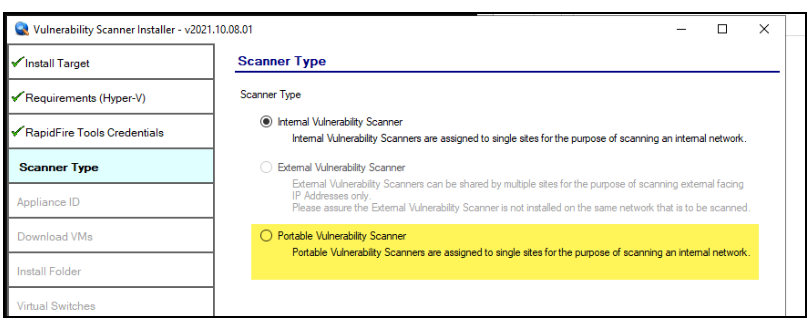
Step 1 — Provision Portable VulScan Appliance

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 https://www.rapidfiretools.com/vs-downloads.

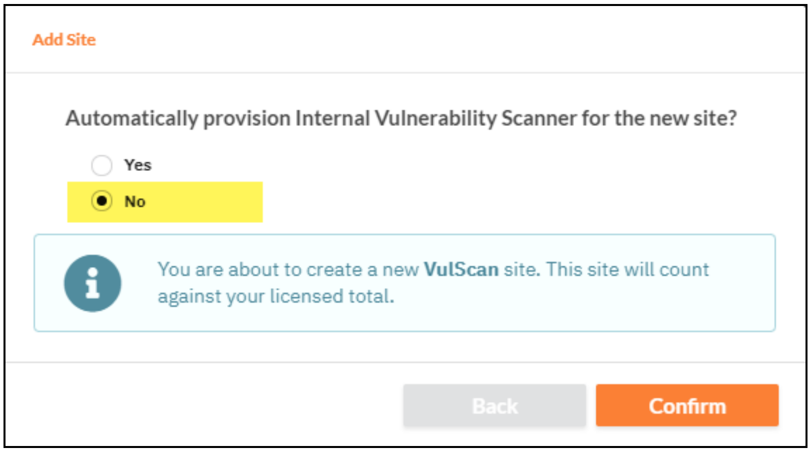
During the install process, be sure to select **Portable VulScan appliance** from the available VulScan appliance types.



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:

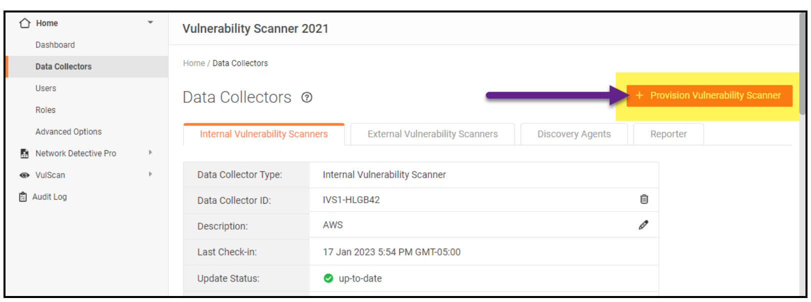
1. From the RapidFire Tools Portal, click **Add Site** and create a new VulScan Site.
2. Before you finish creating the site, select "**No**" when prompted to provision a new internal VulScan appliance for the site.



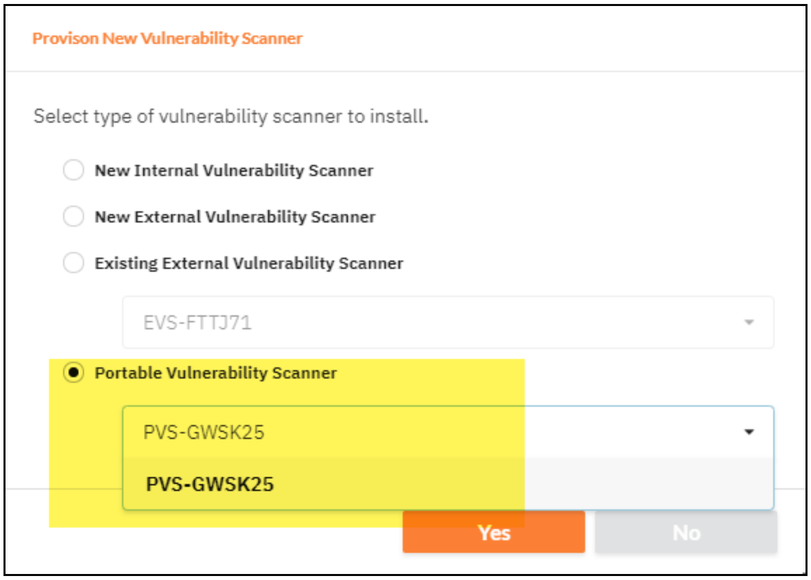
Step 4 — Assign Portable VulScan Appliance to Site

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**.



The PVS appliance will appear under the site Data Collectors.

Step 5 — Set Up and Perform Internal Scan and Notification Tasks

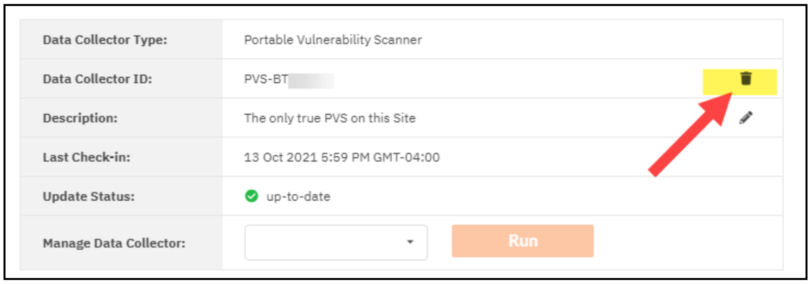
Once you install the appliance and it appears online, configure internal scan and notification tasks in exactly the same way you would with the standard internal scan appliance. See:

- "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.



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 "Step 4 — Assign Portable VulScan Appliance to Site" on page 229.

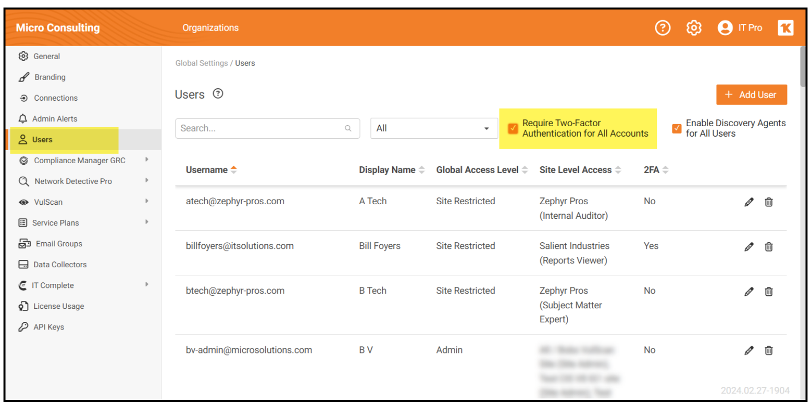
Enable Global Two-Factor Authentication (2FA) for Portal Users

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.



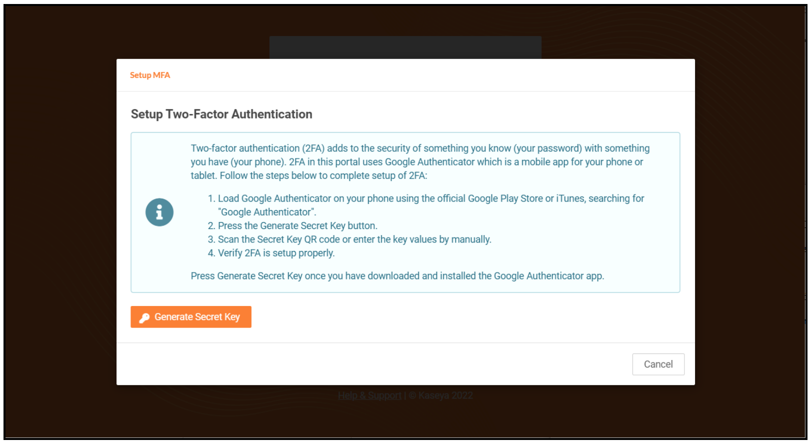
> **Note:** Site Admins, as well as Global Admin and Master users, must configure 2FA regardless of this setting.

Step 2 — Portal user logs in and sets up 2FA Access

Once the Master admin enables global 2FA, other portal users follow these steps.

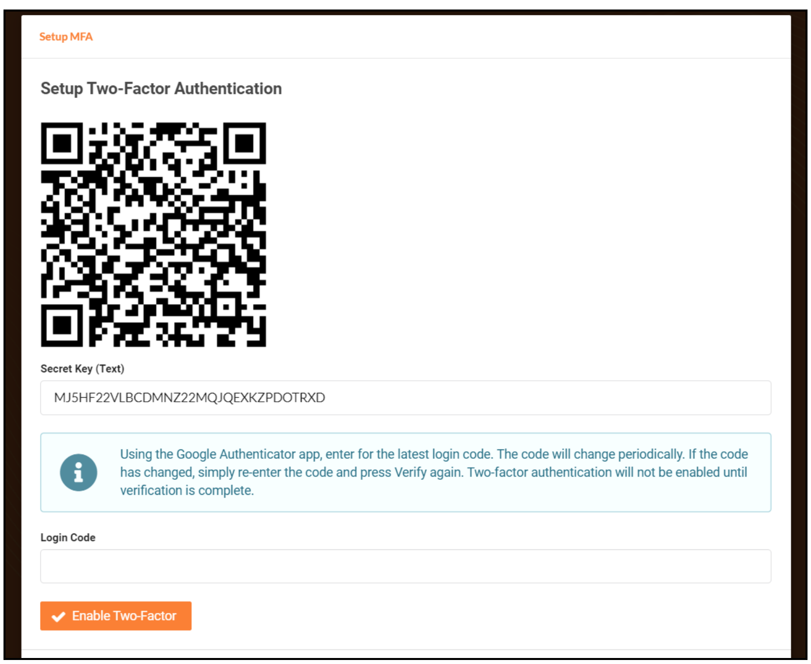
> **Note:** You will require a **mobile device** and the **Google Authenticator** app to complete this process.

1. Access the Portal and log in.
2. You will be prompted to set up 2FA. Click **Generate Secret Key**.

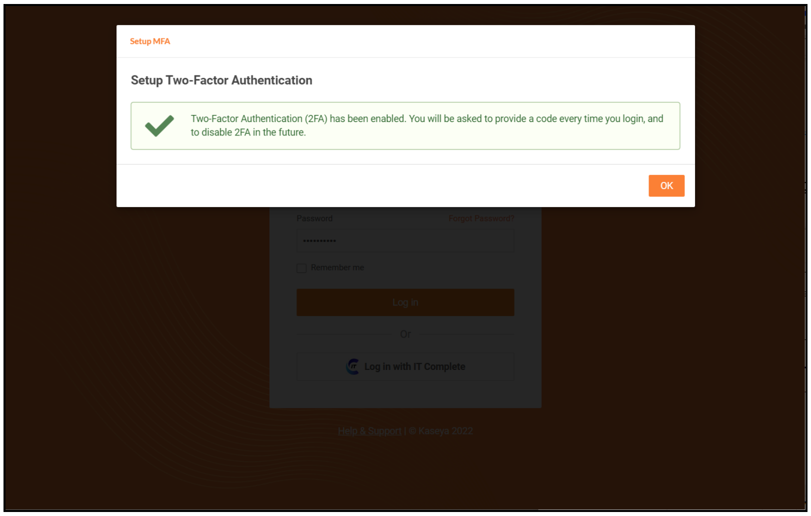


> **Note:** If you have not done so already, download and install the Google Authenticator app on your mobile device.

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.

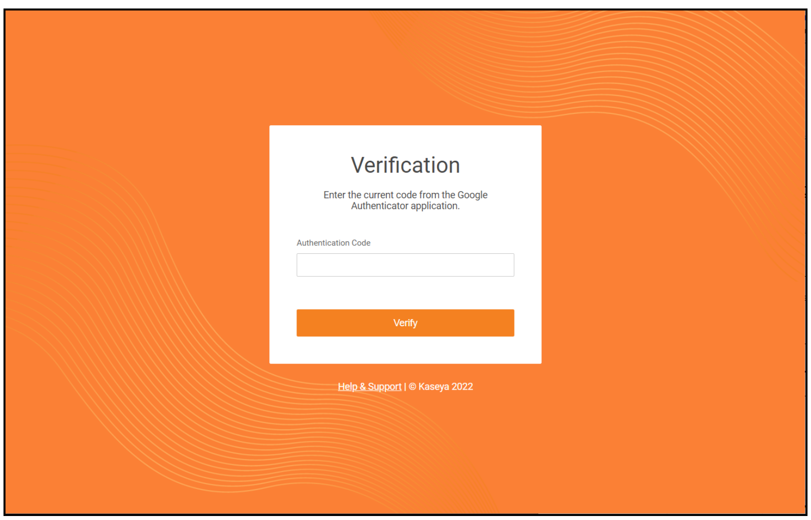


5. A setup confirmation modal will appear. Click **OK**.



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.



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.

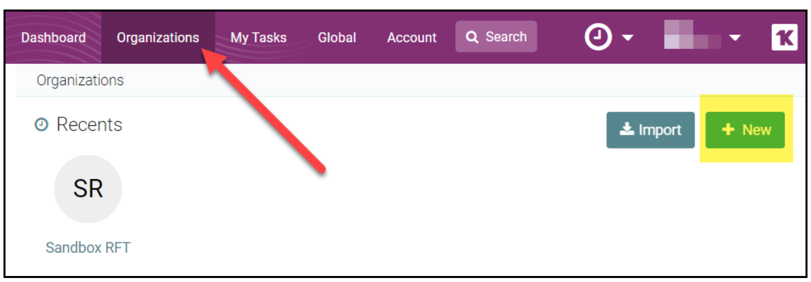
Note: You must subscribe to IT Glue Enterprise to access this feature.

Here's how to enable this feature:

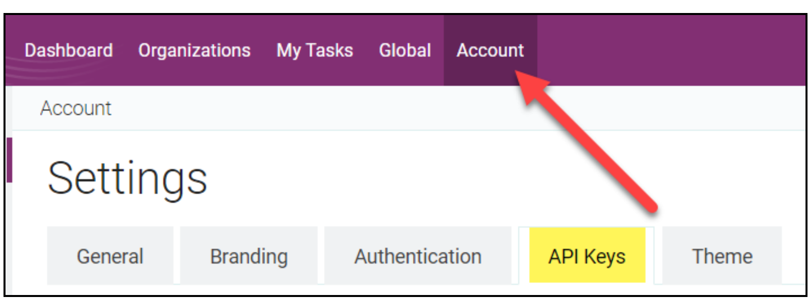
Step 1 — Create and Copy API Key in IT Glue

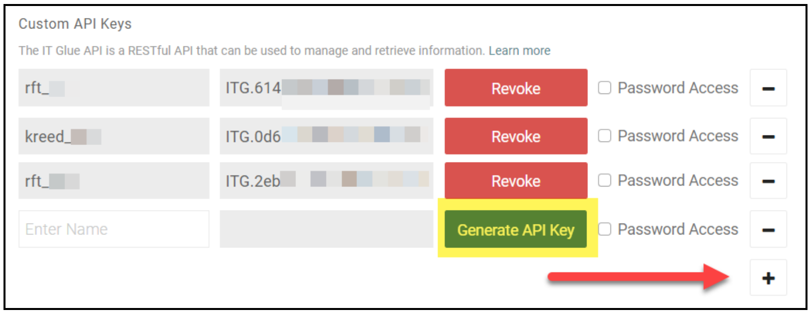
First, you need to set up an API Key in IT Glue.

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.



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

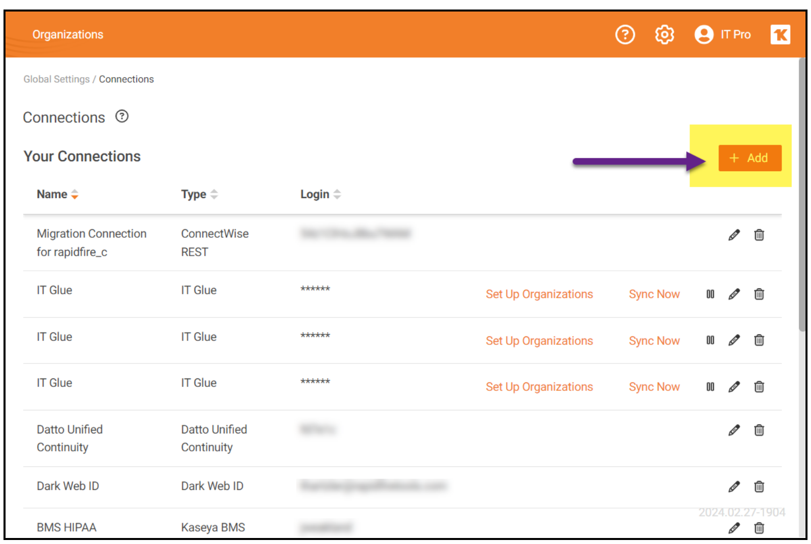




Important: For your reference, save a copy of the API key outside of IT Glue.

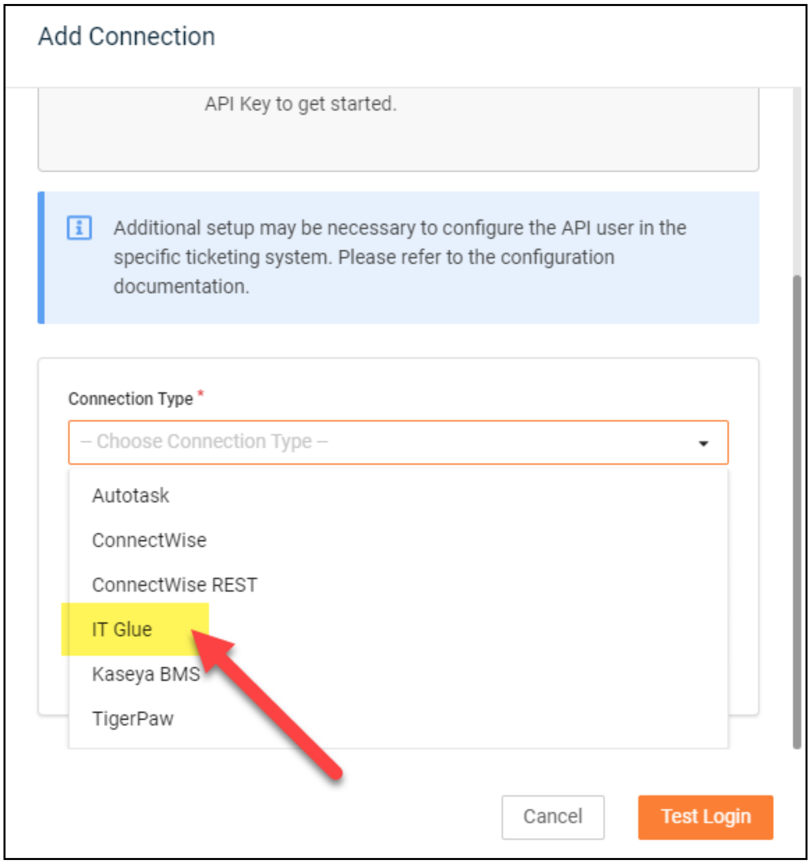
Step 2 — Enable Connection to IT Glue from Portal Global Settings

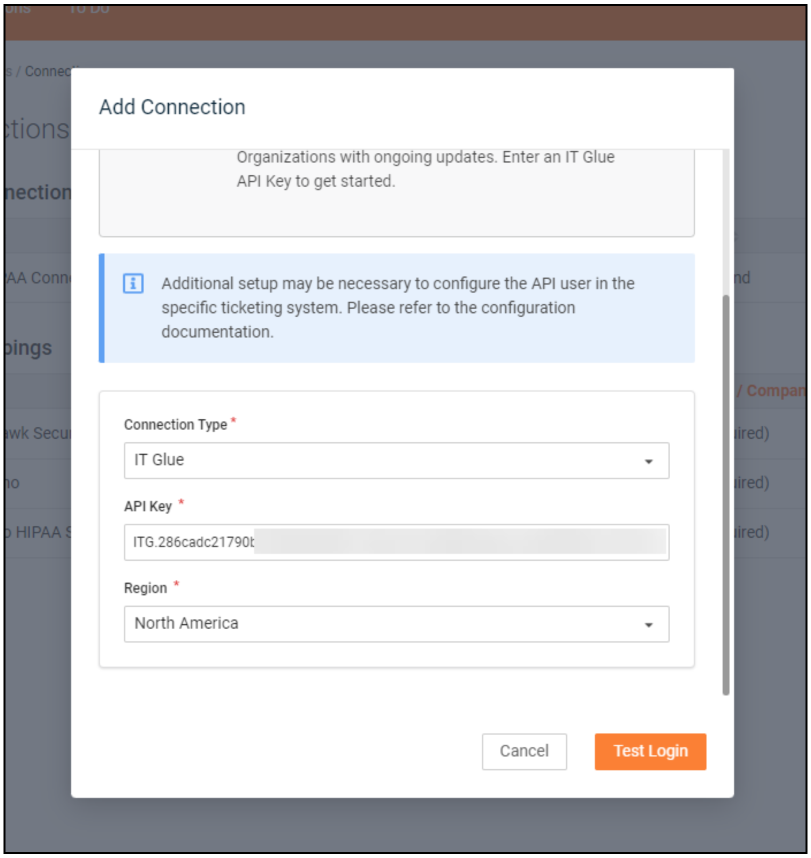
1. Next, from the RapidFire Tools Portal, navigate to global **Settings (Admin)** > **Connections**.
2. From **Your Connections**, click **Add**.



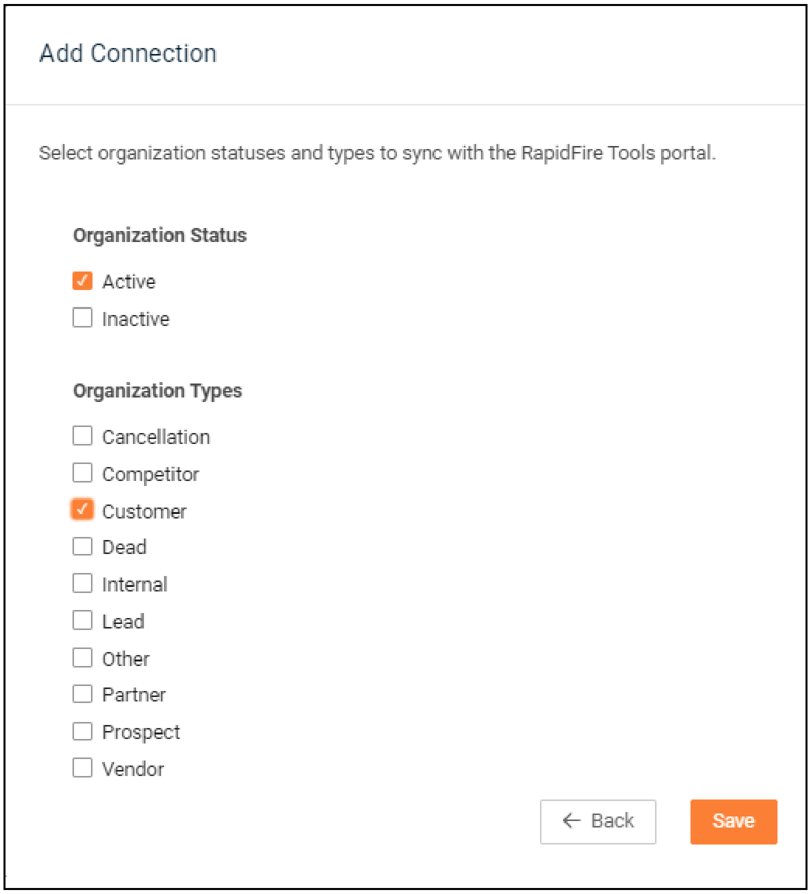
3. **Select IT Glue** from the drop-down menu and **enter the API Key**.

4. Click **Test Login**.





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



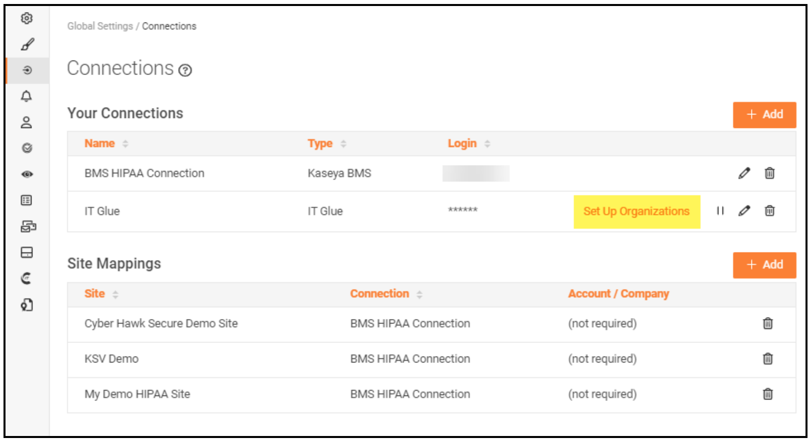
Note: These fields are configured in IT Glue.

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

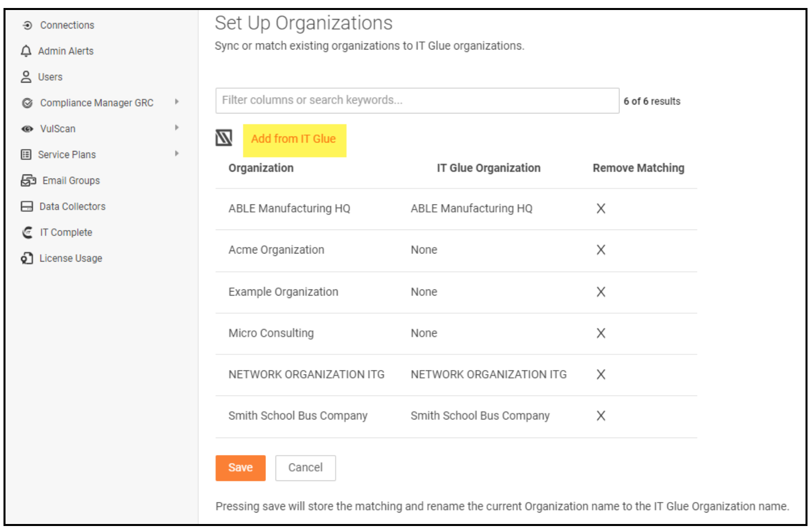
Step 3 — Set Up Organizations

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.

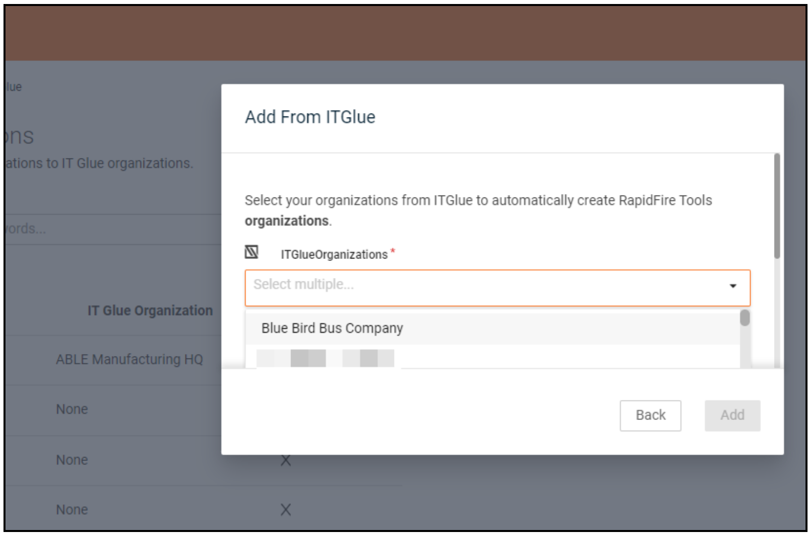
1. From My Connections, click **Set Up Organizations**.



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.



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**.



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

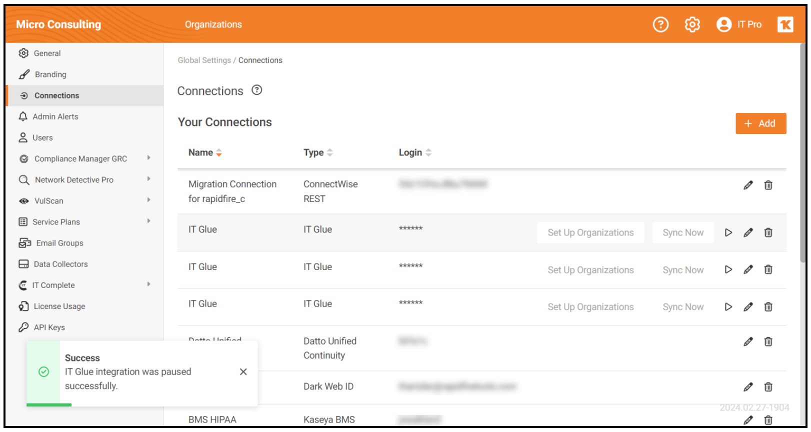
Once you import orgs from IT Glue into the RFT Portal, the org names will be synchronized; changes to org names in IT Glue will regularly update the corresponding org names in the RFT Portal.

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

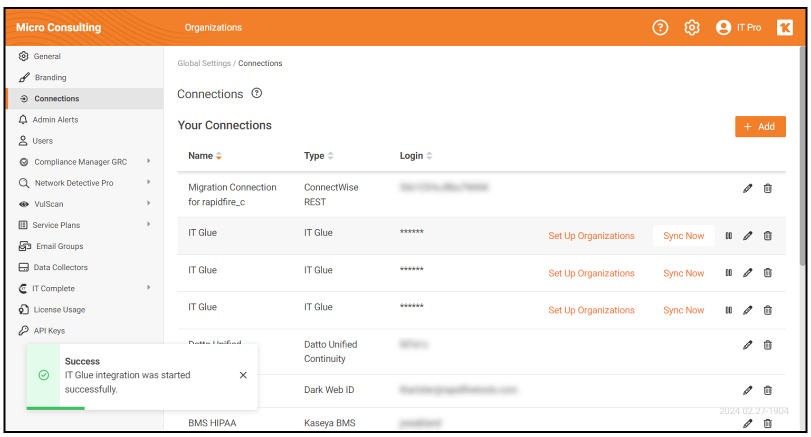
> **Note:** The sync is limited to org names and works one way from ITGlue into the RFT Portal. Note also that deleting orgs in the RFT Portal will not delete orgs in IT Glue.

Pause Org Name Synchronization

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



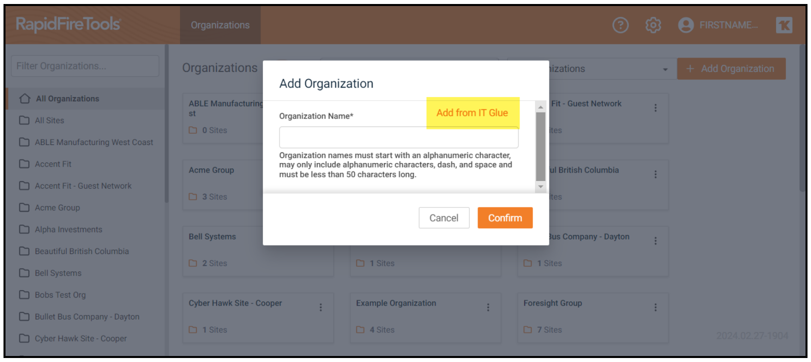
To resume synchronizing org names, find the ITGlue connection and click the **play** button.



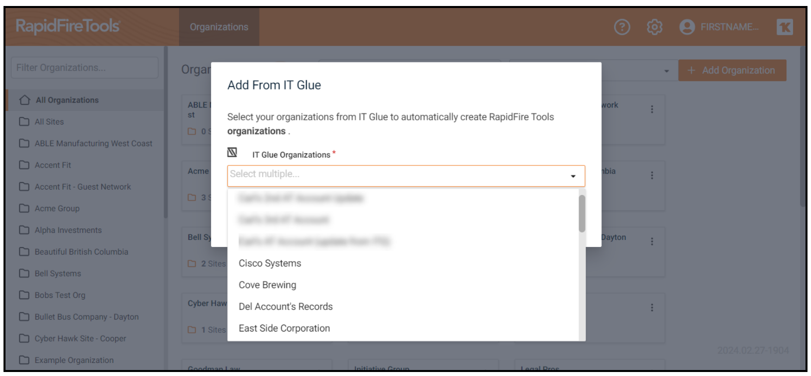
Import IT Glue Orgs when Creating New Organizations

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**.



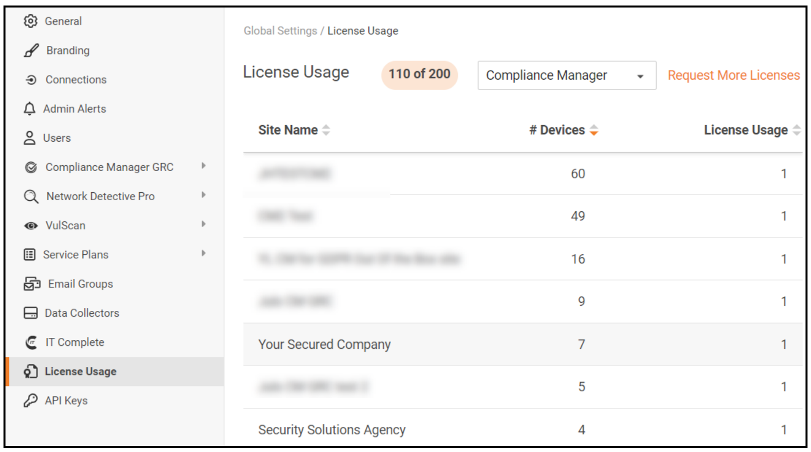
3. Select one or more IT Glue orgs from the drop-down menu and click **Add**.



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.



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.