Copyright © 2024 Kaseya Limited

CYBER HAWK®
by RapidFire Tools

USER GUIDE

Cyber Hawk Web Console

Detecting and Responding to IT Security Policy Violations

4/12/2024 4:16 PM

Kaseya®

☎ +1-678-323-1300 rapidfiretools.com support@rapidfiretools.com

Contents

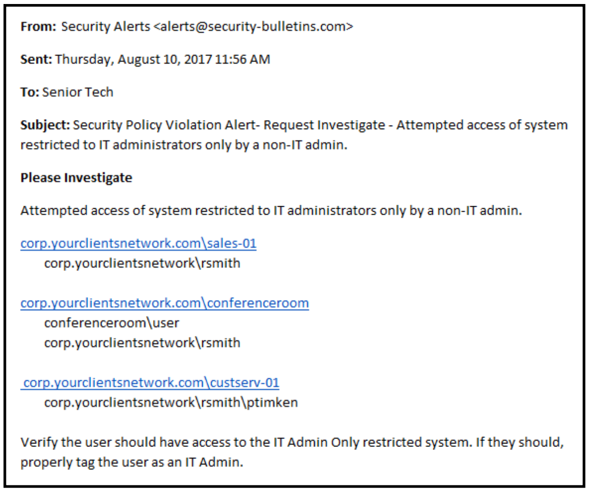
Introduction to Cyber Hawk Web Console

This section contains everything you need to know before getting started with the Cyber Hawk Web Console.

Cyber Hawk Overview

Cyber Hawk prowls an entire network each day at whatever time you determine and then sends out daily **Security Policy Violation Alerts** to notify you of any suspicious activity.

Each discovered issue listed in a Security Policy Violation Alert contains an “Alert Link” to the **RapidFire Tools Portal**. The Portal automates the process of responding to security issues by enabling your technicians to **Investigate** or **Ignore** the Alert item.



From: Security Alerts <alerts@security-bulletins.com>

Sent: Thursday, August 10, 2017 11:56 AM

To: Senior Tech

Subject: Security Policy Violation Alert- Request Investigate - Attempted access of system restricted to IT administrators only by a non-IT admin.

Please Investigate

Attempted access of system restricted to IT administrators only by a non-IT admin.

corp.yourclientsnetwork.com\sales-01
corp.yourclientsnetwork\rsmith

corp.yourclientsnetwork.com\conferenceroom
conferenceroom\user
corp.yourclientsnetwork\rsmith

corp.yourclientsnetwork.com\custserv-01
corp.yourclientsnetwork\rsmith\ptimken

Verify the user should have access to the IT Admin Only restricted system. If they should, properly tag the user as an IT Admin.

In the RapidFire Tools Portal you can:

- review the issue’s forensics
- automatically generate a service ticket in your favorite Ticketing System/PSA
- configure a **Smart-Tag** to change Cyber Hawk's behavior
- issue an **Ignore Rule** to ignore the alert or prevent it from being generated again in the future

With the Cyber Hawk **Web Console**, you can also use the RapidFire Tools Portal to set up and manage Cyber Hawk deployments for all of your sites, from beginning to end.

Cyber Hawk performs scheduled IT network assessment scans on a daily and/or weekly basis. When *Anomalies*, *Changes*, or *Threats* (ACT) are identified on the network, Cyber Hawk issues Security Policy Violation Alerts according to rules that you configure.

Anomalies, Changes, and Threats

Each time Cyber Hawk executes a pre-scheduled scan, it’s on the look-out for three classifications of internal network security issues: Anomalies, Changes, and Threats.

© 2024 RapidFire Tools, Inc. All rights reserved.

- **Anomalies** are suspicious activities and findings that are out of the ordinary and unexpected and that should be investigated. Examples of anomalies are users logging in at times outside their historical patterns, or a USB drive plugged into a computer that has been tagged as being "locked down."
- **Changes** are recorded variances from previous scans linked to specific aspects of the network environment that could represent a threat. Examples of suspicious changes are a user's security permission promoted to administrative, or a new device added to the network that wasn't there before.
- **Threats** are defined as clear and recognizable dangers to the network environment that need fast attention. Examples of threats would be a critical security hole or a machine in the "DMZ" that hasn't been patched in 30 days.

Every day Cyber Hawk looks at a broad range of assets and configurations in search of anomalies, changes and threats, including: Wireless Networks, Network Devices, User Behavior, Computers, Printers, DNS entries, Switch Port Connections (Layer 2/3), and Internal Network Vulnerabilities. It also looks at issues specifically for environments subject to HIPAA and PCI compliance.

And, on a weekly basis, Cyber Hawk will also notify you of changes in the large categories of: Access Control, Computer Security, Wireless Access, and Network Security.

Cyber Hawk Components

In order to use and get the most out of Cyber Hawk, you will need the following components:

Cyber Hawk Component	Description
Cyber Hawk Appliance	This is the **RapidFire Tools Server** that you install on the target network, where it performs daily network scans to detect anomalies, changes, and threats.
VulScan Integration	With VulScan, you can import internal vulnerability scans into your Cyber Hawk site. This allows you to generate alert notifications regarding technical vulnerabilities. You can set a schedule at which to import internal scans. The integration requires a VulScan site in the same portal organization as your Cyber Hawk site.
RapidFire Tools Portal	The RapidFire Tools Portal allows your tech team to manage all of your Cyber Hawk deployments for each Site. The RapidFire Tools Portal is also used to process Investigate Alert Action Requests and Ignore Alert Action Requests created in response to Anomalies, Changes, or Threats (ACT) detected by the Cyber Hawk Appliance. The Portal acts as an ACT "triage center" that enables technicians to view a "To-Do" list of Investigate Alert Action Requests and Ignore Alert Action Requests and to enable processing of these requests by: • transferring the requests to Ticketing/PSA Systems such as Autotask, ConnectWise, and Tigerpaw • using the Portal to modify Cyber Hawk Smart-Tags to configure the Cyber Hawk Appliance to more effectively detect Security Policy violations and address False Positives • creating Ignore Rules to address Alert False Positives • completing a given Action Request To access the RapidFire Tools Portal, visit the default web site URL of https://www.youritportal.com.
The Service Plan and Service Catalog Creator	Cyber Hawk users have access to a unique "Service Plan Creator" tool that gives you the ability to modify our starter Service Plans, or create your own

© 2024 RapidFire Tools, Inc. All rights reserved.

Cyber Hawk Component	Description
	plans from scratch. You define and name the offerings based on the security policies that you want to enforce, and the tool automatically generates a “Service Plan Catalog” (or catalogs), and “Service Plan Matrix” sheet that compares your plans to help you sell them to your clients and prospects. Once you sell one of your plans to your client, simply “apply” the plan to the Cyber Hawk assigned to that client and its Service Policy Violation detection capability is then automatically configured to deliver that exact plan.
Portal Integration with Ticketing Systems/PSAs	To set up Cyber Hawk integration of the Autotask, ConnectWise, or Tigerpaw ticketing/PSA systems with the RapidFire Tools Portal, please refer to "Set Up and Assign a Ticketing/PSA System Integration to a Site" on page 65.

© 2024 RapidFire Tools, Inc. All rights reserved.

Setting Up Cyber Hawk

This section covers how to set up and begin using Cyber Hawk.

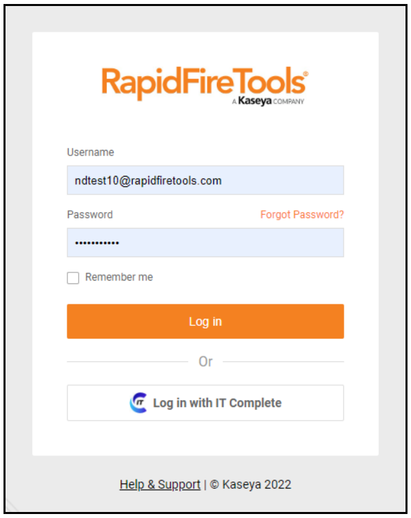
> **Note:** If you have previously set up Cyber Hawk Sites using the Network Detective app, you can access and manage those Sites in the Portal, too. This should NOT require any additional set up. See the topics in this guide for details on how to manage your Sites using the Cyber Hawk Web Console in the RapidFire Tools Portal.

Create a New Site

> **Tip:** We recommend you get started by making a "practice site" and setting up your own security service in-house. Use this practice site to familiarize yourself with Cyber Hawk and the installation and configuration process.

The first step in deploying Cyber Hawk is creating a "**Site**". Sites help you organize the security services you offer by location and/or client. To create a site:

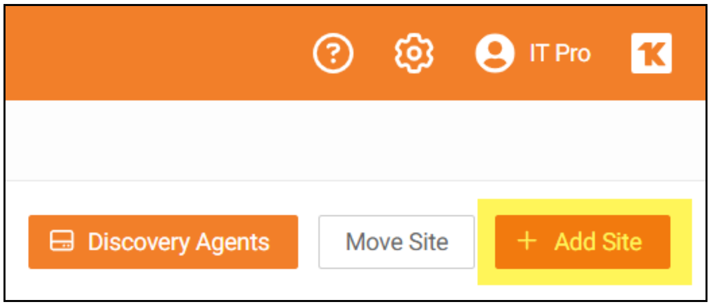
1. Access the RapidFire Tools Portal at https://www.youritportal.com and log in with your credentials.



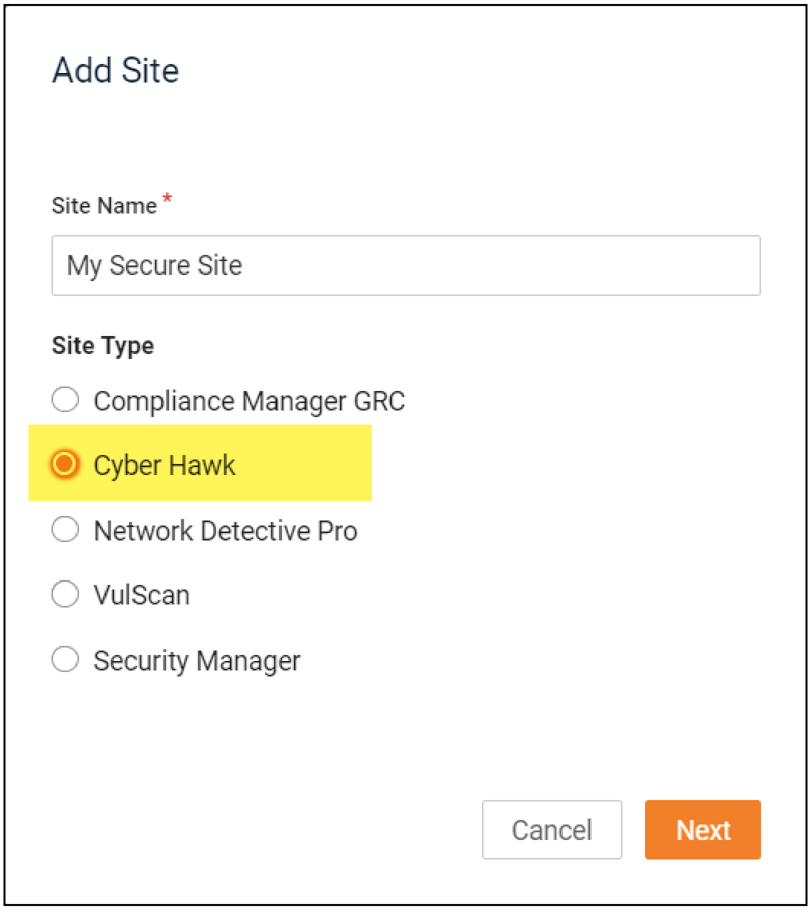
Username
ndtest10@rapidfiretools.com
Password
••••••••••

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

© 2024 RapidFire Tools, Inc. All rights reserved.



3. Enter a **Site Name**. This can be the name of the location where Cyber Hawk is being deployed, for example.
4. Under **Site Type**, select **Cyber Hawk**.



Add Site

Site Name *

My Secure Site

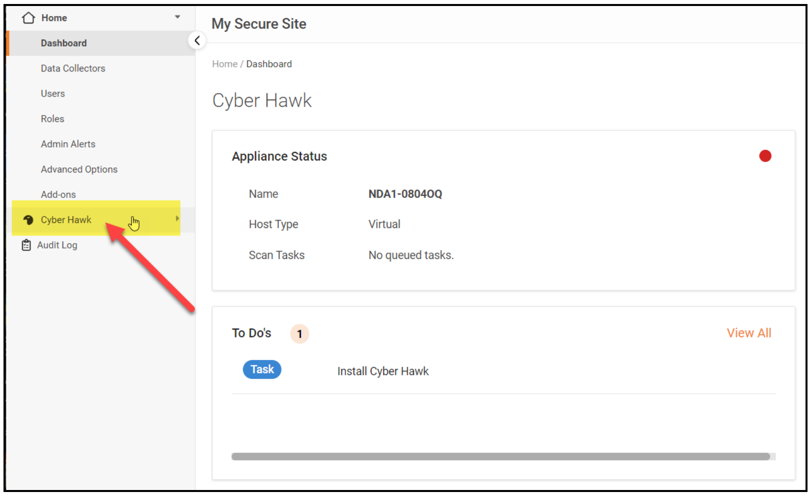
Site Type

○ Compliance Manager GRC
● Cyber Hawk
○ Network Detective Pro
○ VulScan
○ Security Manager

5. Click **Next**.

© 2024 RapidFire Tools, Inc. All rights reserved.

6. If prompted, select a subscription option. Contact your Sales Representative to review specific subscription options for your account.
7. Select an **Org Folder** for the site and click **Next**. **Confirm** your new site and subscription option.
8. The Site Home page will appear. Click the **Cyber Hawk tab**.



My Secure Site

Home / Dashboard

Cyber Hawk

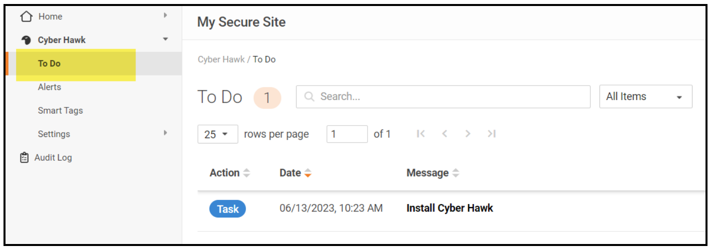
Appliance Status

Name	NDA1-08040Q
Host Type	Virtual
Scan Tasks	No queued tasks.

To Do's 1

Task Install Cyber Hawk

Then click **To Do** from the left menu.



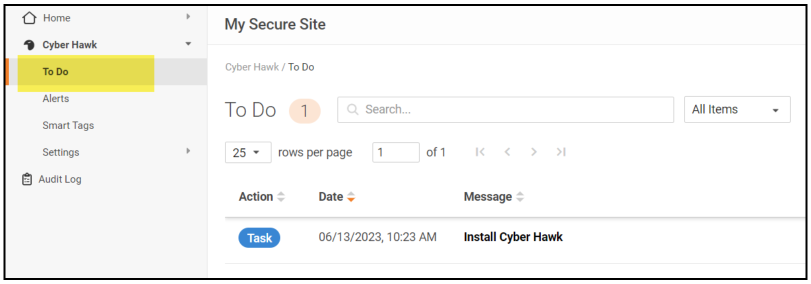
My Secure Site

Cyber Hawk / To Do

To Do 1

Action	Date	Message
Task	06/13/2023, 10:23 AM	Install Cyber Hawk

New **To Do** items will appear in the Site's To Do list.



My Secure Site

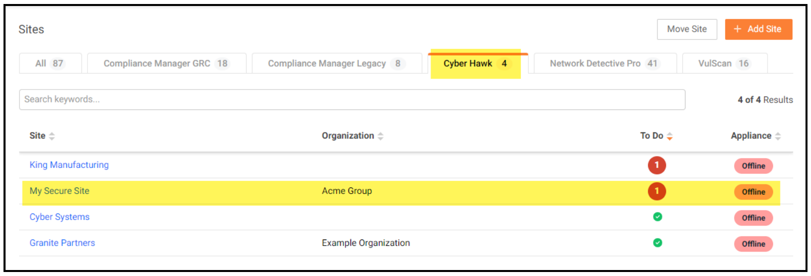
Cyber Hawk / To Do

To Do 1

Action	Date	Message
Task	06/13/2023, 10:23 AM	Install Cyber Hawk

© 2024 RapidFire Tools, Inc. All rights reserved.

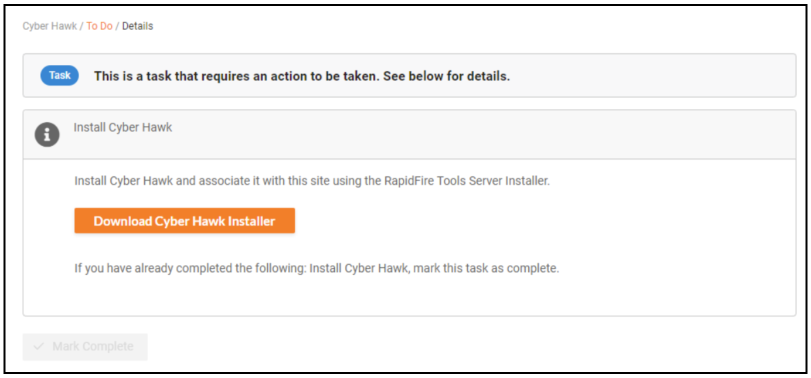
The new site will be added to the Sites home page in the RapidFire Tools Portal.



Site	Organization	To Do	Appliance
King Manufacturing		1	Offline
My Secure Site	Acme Group	1	Offline
Cyber Systems		✓	Offline
Granite Partners	Example Organization	✓	Offline

Task 1 — Install Cyber Hawk

Install the **RapidFire Tools Server** on a PC on the target network. The **server** (also called an **appliance**) collects data and performs automated scans within the assessment environment.



This is a task that requires an action to be taken. See below for details.

Install Cyber Hawk

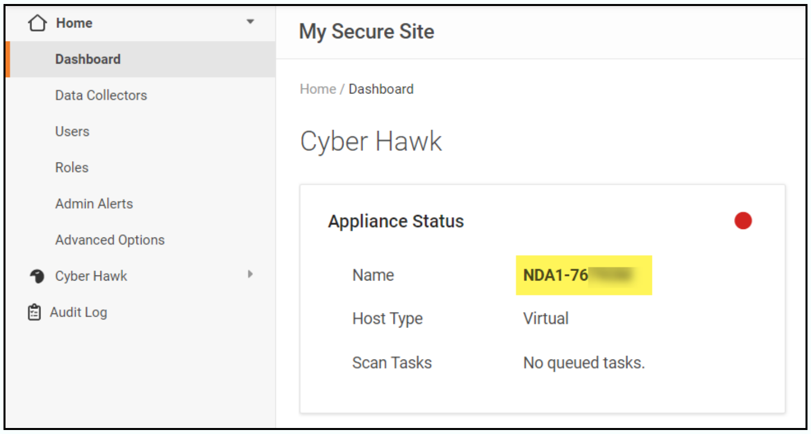
Install Cyber Hawk and associate it with this site using the RapidFire Tools Server Installer.

If you have already completed the following: Install Cyber Hawk, mark this task as complete.

See the Installation Guide for RapidFire Tools Server for Cyber Hawk for more detailed instructions on installing the appliance on the target network. The process should only take 10 minutes or less.

Important: You can only install **one** RapidFire Tools server/appliance on a PC or endpoint at a time. If you need to install multiple server(s)/appliance(s), install each one on a separate endpoint on the network.

Note: In order to install the appliance, you will need to note the **Appliance ID**. You can find this from **[Your Site]** > **Home** > **Dashboard** >**Appliance Status**.

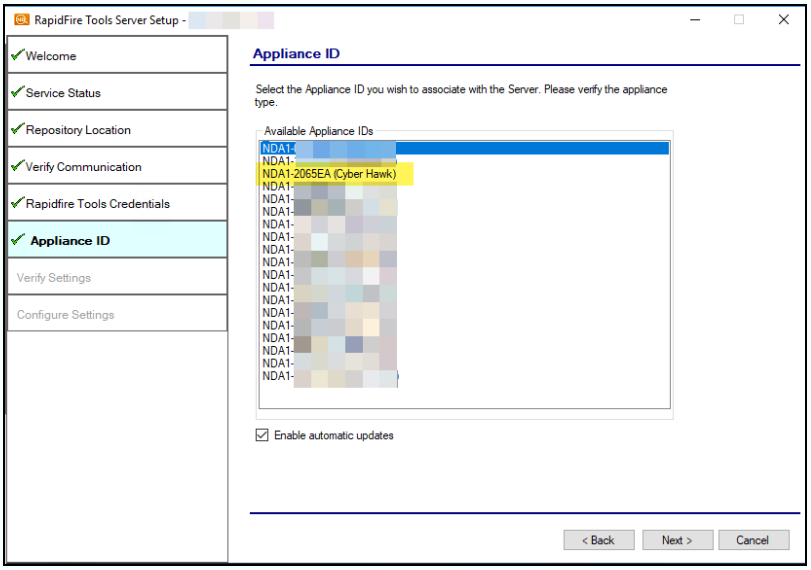


Cyber Hawk

Appliance Status

Name	NDA1-76[redacted]
Host Type	Virtual
Scan Tasks	No queued tasks.

When you install the appliance on the target network, the installer will ask you to select one of your available Appliance IDs. Select your Site's Appliance ID to "bind" your Cyber Hawk appliance to your new site.



Appliance ID

Select the Appliance ID you wish to associate with the Server. Please verify the appliance type.

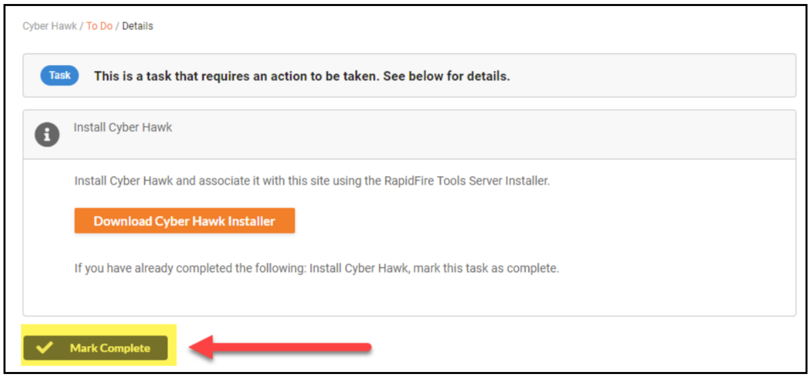
Available Appliance IDs

NDA1-[redacted]
NDA1-[redacted]
NDA1-2065EA (Cyber Hawk)
NDA1-[redacted]
NDA1-[redacted]
NDA1-[redacted]
NDA1-[redacted]
NDA1-[redacted]
NDA1-[redacted]
NDA1-[redacted]
NDA1-[redacted]
NDA1-[redacted]
NDA1-[redacted]
NDA1-[redacted]
NDA1-[redacted]
NDA1-[redacted]
NDA1-[redacted]
NDA1-[redacted]
NDA1-[redacted]

☑ Enable automatic updates

Once you finish the installation of the Cyber Hawk Appliance, return to the To Do item and click **Mark Complete**.

© 2024 RapidFire Tools, Inc. All rights reserved.


Cyber Hawk / To Do / Details

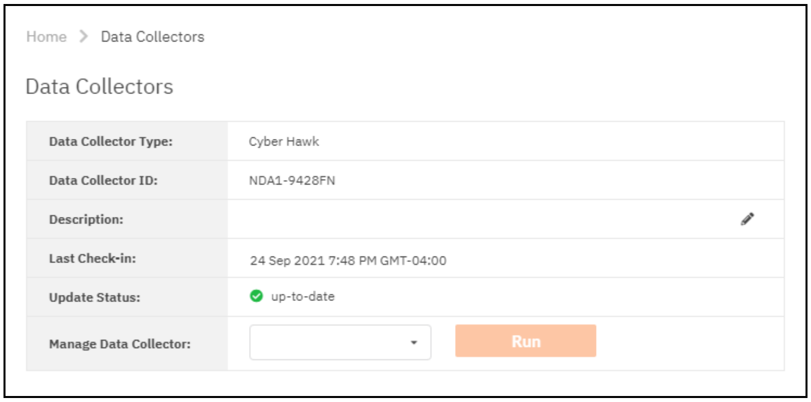
Task This is a task that requires an action to be taken. See below for details.

Install Cyber Hawk

Install Cyber Hawk and associate it with this site using the RapidFire Tools Server Installer.

If you have already completed the following: Install Cyber Hawk, mark this task as complete.

After waiting 5-15 minutes, you can verify that the appliance is online and functioning by looking at the **Last Check-In** log from **[Your Site]** > **Home** > **Data Collectors**.

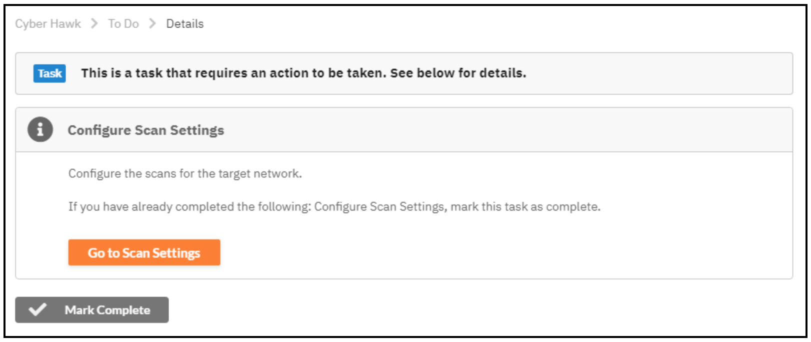

Home > Data Collectors

Data Collectors

Data Collector Type:	Cyber Hawk
Data Collector ID:	NDA1-9428FN
Description:	
Last Check-in:	24 Sep 2021 7:48 PM GMT-04:00
Update Status:	✓ up-to-date
Manage Data Collector:	

Task 2 — Configure Scan Settings

In this step you will configure the Scan Settings for the RapidFire Tools Server for Cyber Hawk.


Cyber Hawk > To Do > Details

Task This is a task that requires an action to be taken. See below for details.

Configure Scan Settings

Configure the scans for the target network.

If you have already completed the following: Configure Scan Settings, mark this task as complete.

© 2024 RapidFire Tools, Inc. All rights reserved.

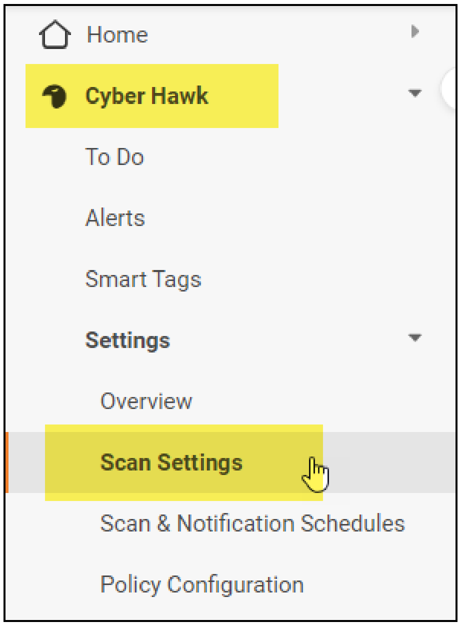
Before you configure scan settings, first determine if the target network is an **Active Directory Domain** OR a **Workgroup**. Then refer to the instructions below.

- Look here to "Configure Scan Settings for Active Directory Domain" below
- Look here to "Configure Scan Settings for Workgroup" on page 27

Important: For best results, the target network must be configured to allow for successful scans on all network endpoints. See "Pre-Scan Network Configuration Checklist" on page 219 for configuration guidance for both Windows Active Directory and Workgroup environments.

Configure Scan Settings for Active Directory Domain

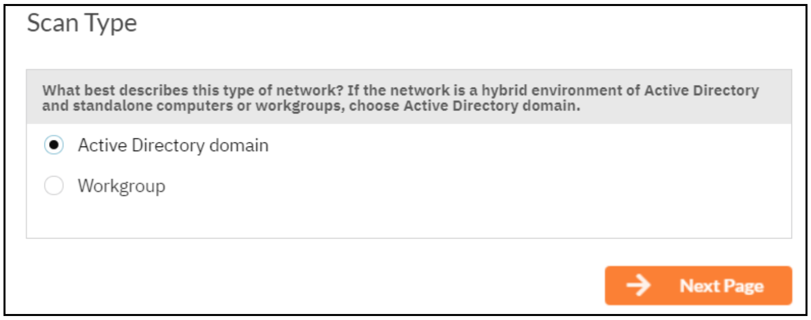
Set the **Scan Settings** from the **[Your Site]** > **Cyber Hawk** > **Settings** > **Scan Settings** page. Complete all required prompts.



Follow the steps below to configure the Scan Settings for the Cyber Hawk Appliance:

© 2024 RapidFire Tools, Inc. All rights reserved.

1. Select the Scan Type: **Active Directory Domain**. Click **Next Page**.



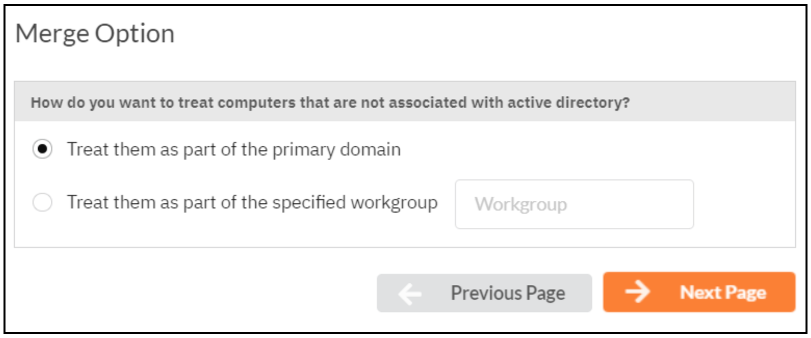
Scan Type

What best describes this type of network? If the network is a hybrid environment of Active Directory and standalone computers or workgroups, choose Active Directory domain.

● Active Directory domain

○ Workgroup

2. The **Merge Options** page will appear. Configure how you wish to treat computers that are not associated with Active Directory. You can choose to:



Merge Option

How do you want to treat computers that are not associated with active directory?

● Treat them as part of the primary domain

○ Treat them as part of the specified workgroup Workgroup

   a. Treat them as part of the primary domain
   b. Treat them as part of a specific workgroup by entering a workgroup name
   c. Don't treat them as part of a domain (non-domain assets will appear separately in alerts and reports)

> **Tip:** Use this feature to tell Cyber Hawk how to handle computers that are not connected to the domain. This affects how they appear in alerts and reports.

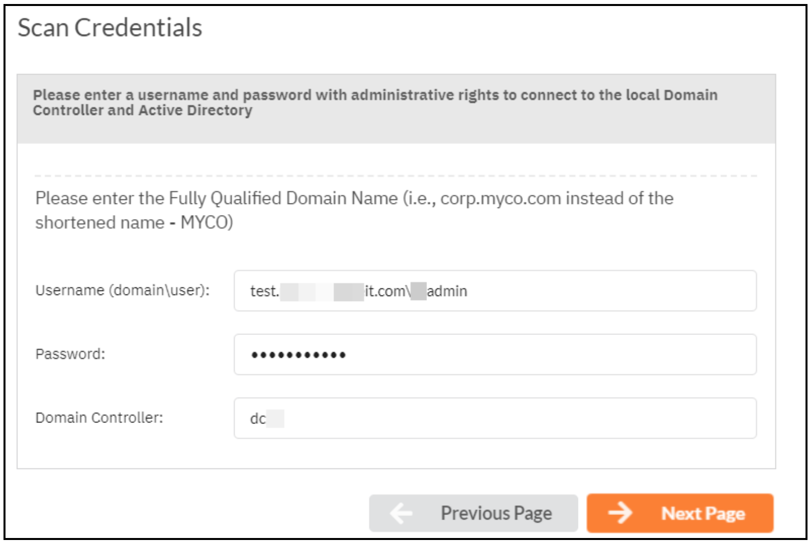
Select a merge option and click **Next Page**.

3. Enter a username and password with administrative rights to connect to the local Domain Controller and Active Directory.

> **Note:** Be sure to enter the **Fully Qualified Domain Name (FQDN)** name before the username. Example: **corp.myco.com\username**.

© 2024 RapidFire Tools, Inc. All rights reserved.

4. Also enter the **name or IP address of the Domain Controller**. Click **Next Page** to test a connection to the local Domain Controller and Active Directory to verify your credentials.



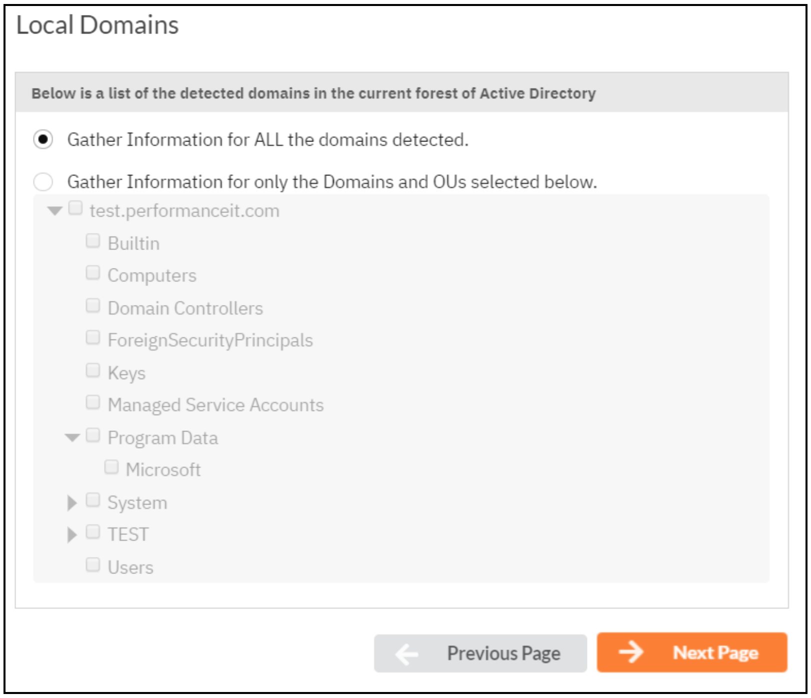
Scan Credentials

Please enter a username and password with administrative rights to connect to the local Domain Controller and Active Directory

Please enter the Fully Qualified Domain Name (i.e., corp.myco.com instead of the shortened name - MYCO)

Username (domain\user):	test.[redacted]it.com\[redacted]admin
Password:	•••••••••••
Domain Controller:	dc[redacted]

5. The **Local Domains** window will appear. If you wish to scan only specific domains or OUs, select those here. Click **Next Page**.



Local Domains

Below is a list of the detected domains in the current forest of Active Directory

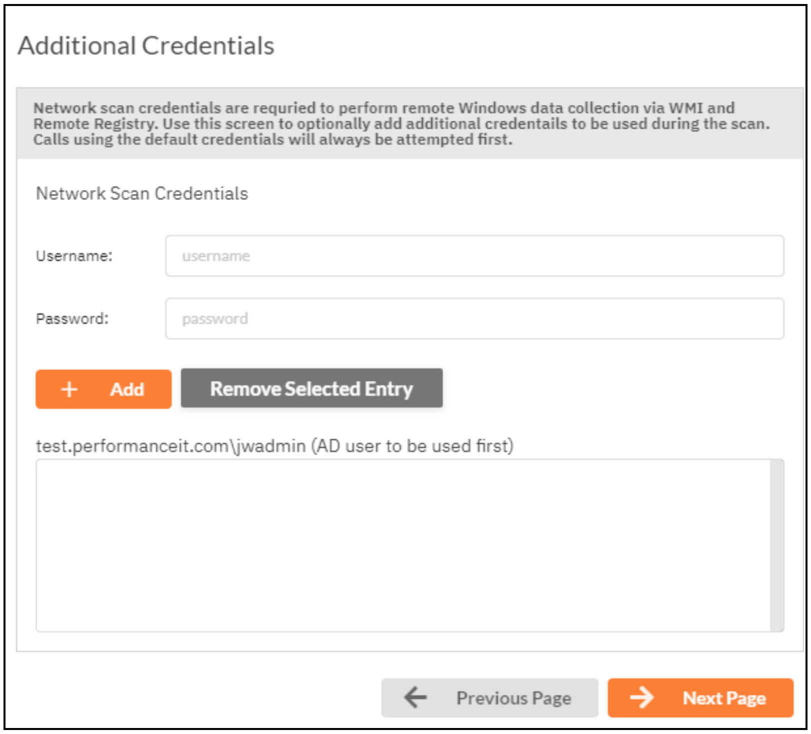
● Gather Information for ALL the domains detected.

○ Gather Information for only the Domains and OUs selected below.

- □ test.performanceit.com
  - □ Builtin
  - □ Computers
  - □ Domain Controllers
  - □ ForeignSecurityPrincipals
  - □ Keys
  - □ Managed Service Accounts
  - □ Program Data
    - □ Microsoft
  - □ System
  - □ TEST
  - □ Users

© 2024 RapidFire Tools, Inc. All rights reserved.

6. The **Additional Credentials** screen will appear. Enter any additional credentials to be used during the scan. Click **Next**.



Additional Credentials

Network scan credentials are requried to perform remote Windows data collection via WMI and Remote Registry. Use this screen to optionally add additional credentails to be used during the scan. Calls using the default credentials will always be attempted first.

Network Scan Credentials

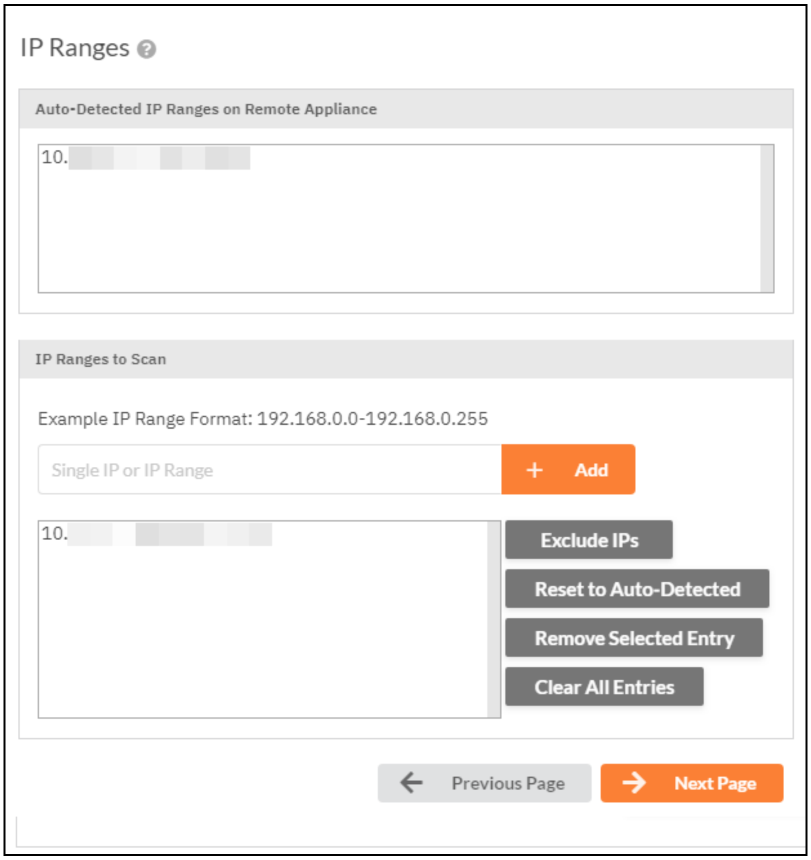
Username: username

Password: password

test.performanceit.com\jwadmin (AD user to be used first)

7. The **IP Ranges** screen will then appear. The Cyber Hawk 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**.

© 2024 RapidFire Tools, Inc. All rights reserved.



IP Ranges

Auto-Detected IP Ranges on Remote Appliance

10.[redacted]

IP Ranges to Scan

Example IP Range Format: 192.168.0.0-192.168.0.255

Single IP or IP Range

10.[redacted]

From this screen you can also:

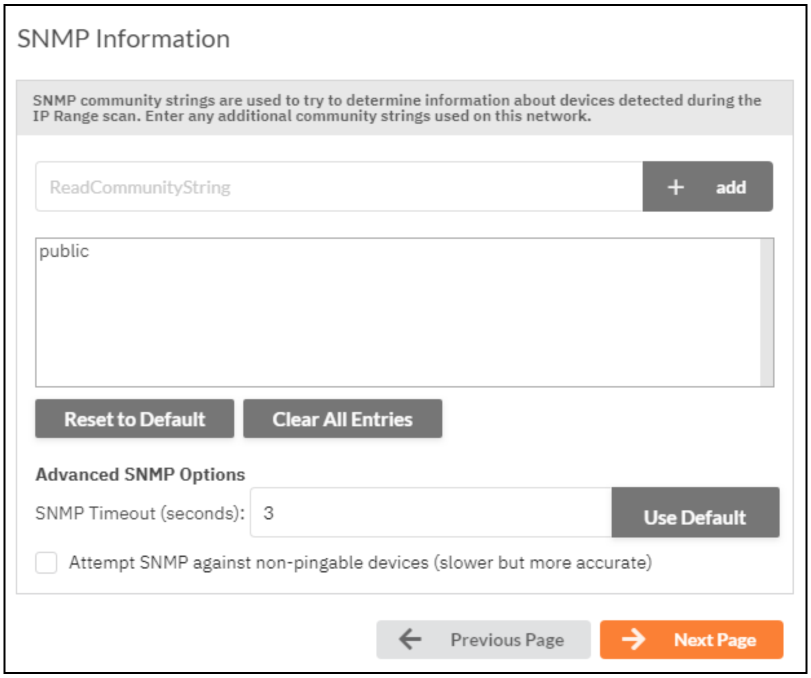
- Click **Reset to Default** to reset to the automatically suggested IP Range.
- **Exclude IPs** or IP ranges from the scan.

> **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.

Click **Next Page** once you have configured the IP ranges for the scan.

8. The **SNMP Information** window will appear. Enter any additional SNMP community strings used on the network. Click **Next Page**.

© 2024 RapidFire Tools, Inc. All rights reserved.



SNMP Information

SNMP community strings are used to try to determine information about devices detected during the IP Range scan. Enter any additional community strings used on this network.

public

Advanced SNMP Options

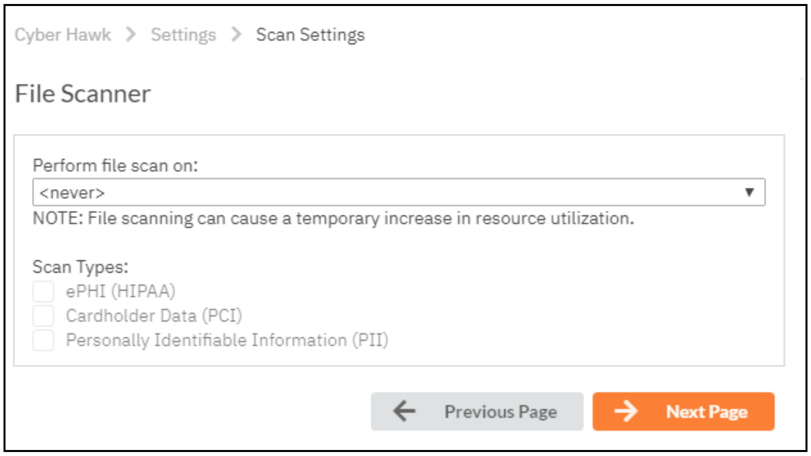
SNMP Timeout (seconds): 3

□ Attempt SNMP against non-pingable devices (slower but more accurate)

9. The **File Scanner** window will appear. Choose what day of the week to perform the file scan. Select a day of the week from the drop-down menu. Next, select the Scan Types that will be performed:
    - **ePHI** (HIPAA) will scan for Electronic Protected Health Information
    - **Cardholder Data** (PCI) will scan for payment card numbers and other related information
    - **Personally Identifiable Information** (PII) will scan for information such as a

© 2024 RapidFire Tools, Inc. All rights reserved.

person's name or social security number



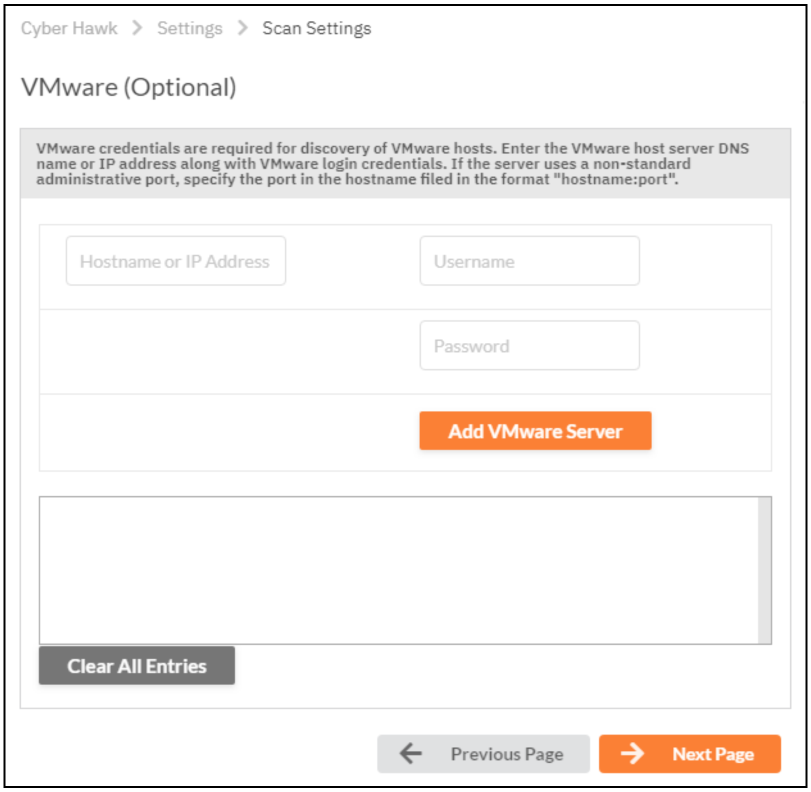
Cyber Hawk > Settings > Scan Settings

File Scanner

Perform file scan on:
<never>
NOTE: File scanning can cause a temporary increase in resource utilization.

Scan Types:
□ ePHI (HIPAA)
□ Cardholder Data (PCI)
□ Personally Identifiable Information (PII)

10. The optional **VMware** credentials window will appear. Enter the hostnames or IP Addresses of any VMware hosts that you wish to include in the scan. Likewise enter credentials needed to access the VMware hosts. Click **Next Page**.



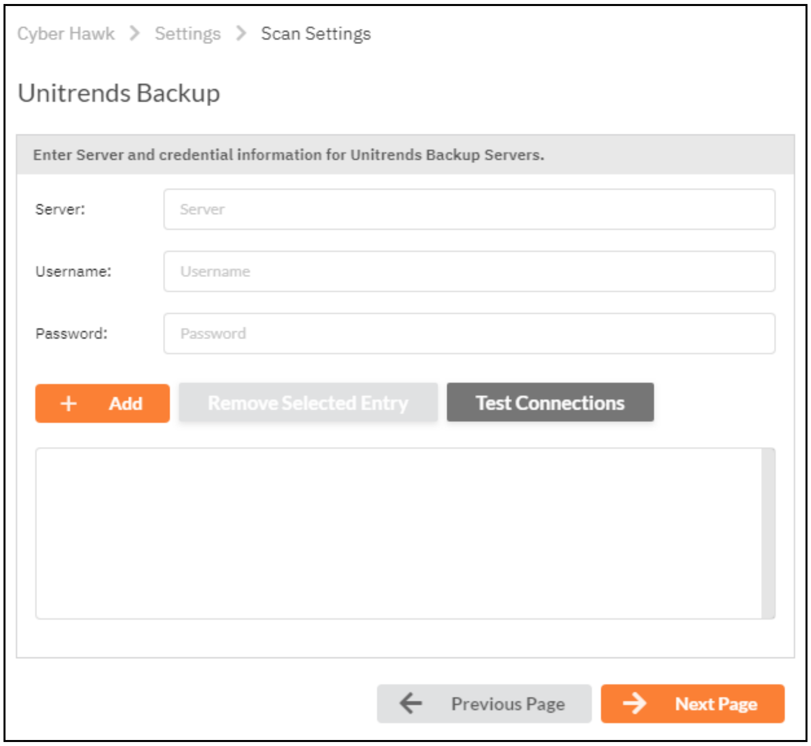
Cyber Hawk > Settings > Scan Settings

VMware (Optional)

VMware credentials are required for discovery of VMware hosts. Enter the VMware host server DNS name or IP address along with VMware login credentials. If the server uses a non-standard administrative port, specify the port in the hostname filed in the format "hostname:port".

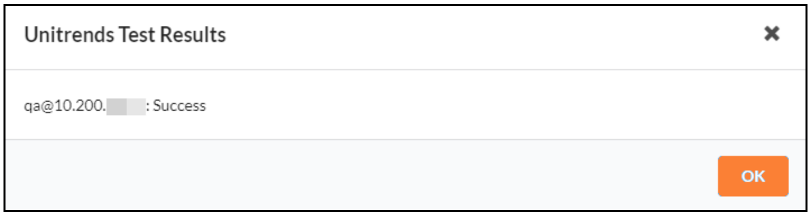
© 2024 RapidFire Tools, Inc. All rights reserved.

11. The **Unitrends Backup** screen will appear. Enter the Unitrends Backup server name and login credentials.



Enter Server and credential information for Unitrends Backup Servers.

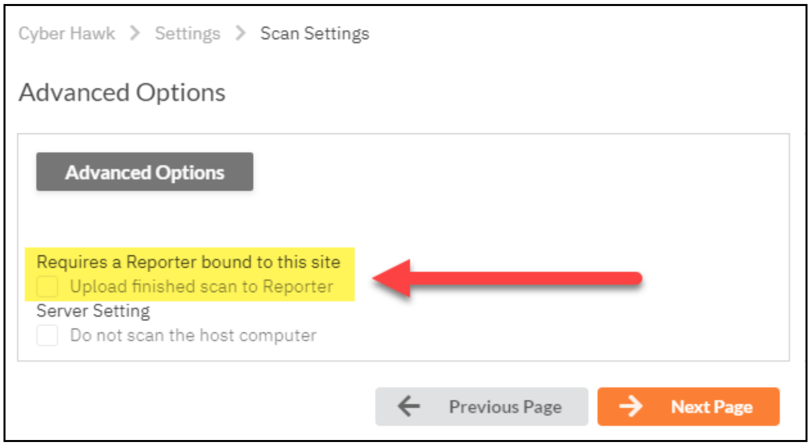
12. Click **Test Connection** to verify your Unitrends scan configuration.



qa@10.200.[redacted]: Success

13. If you are using a **Reporter** appliance, you can also choose whether to upload the finished scans to the Reporter. Click **Next Page**.

© 2024 RapidFire Tools, Inc. All rights reserved.



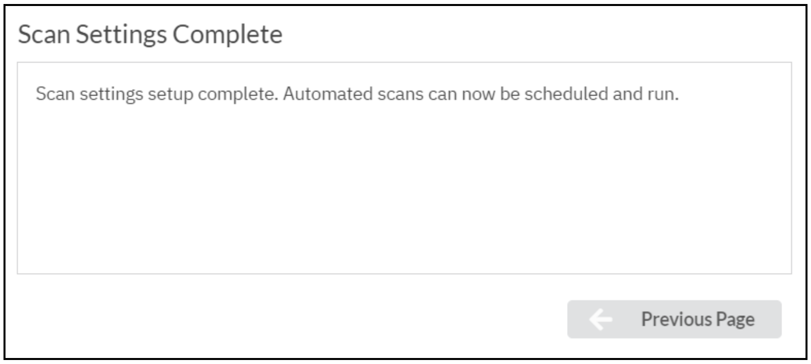
Requires a Reporter bound to this site

□ Upload finished scan to Reporter

Server Setting

□ Do not scan the host computer

14. Your scan settings will then be complete.



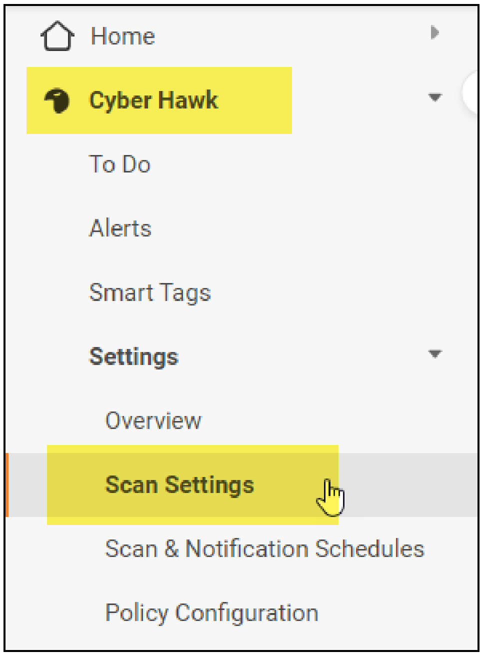
Scan settings setup complete. Automated scans can now be scheduled and run.

When you have finished entering the scan settings, return to the To Do list and click **Mark Complete** for the **Configure Scan Settings** To Do task.

© 2024 RapidFire Tools, Inc. All rights reserved.

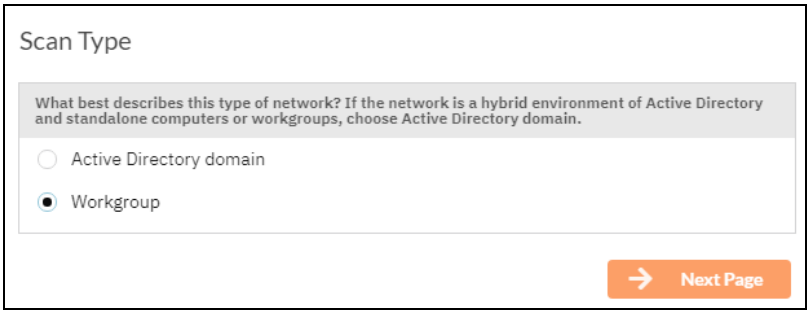
Configure Scan Settings for Workgroup

Set the **Scan Settings** from the **[Your Site]** > **Cyber Hawk** > **Settings** > **Scan Settings** page. Complete all required prompts.



Follow the steps below to configure the Scan Settings for the Cyber Hawk Appliance:

1. From the Scan Settings screen, select the Scan Type: **Workgroup**. Click **Next Page**.



Scan Type

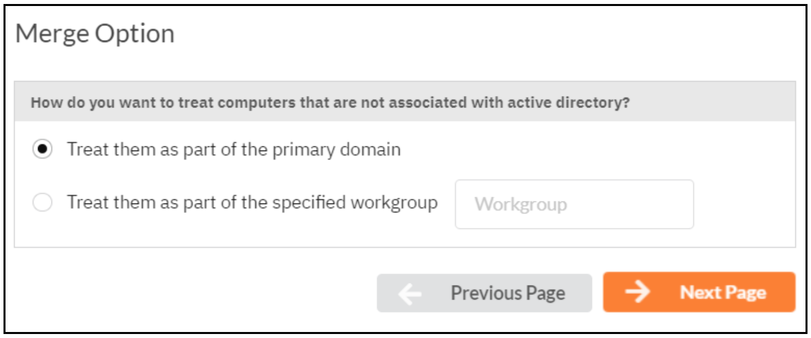
What best describes this type of network? If the network is a hybrid environment of Active Directory and standalone computers or workgroups, choose Active Directory domain.

○ Active Directory domain

● Workgroup

2. The **Merge Options** page will appear. Configure how you wish to treat computers that are not associated with Active Directory. You can choose to:

© 2024 RapidFire Tools, Inc. All rights reserved.



Merge Option

How do you want to treat computers that are not associated with active directory?

● Treat them as part of the primary domain

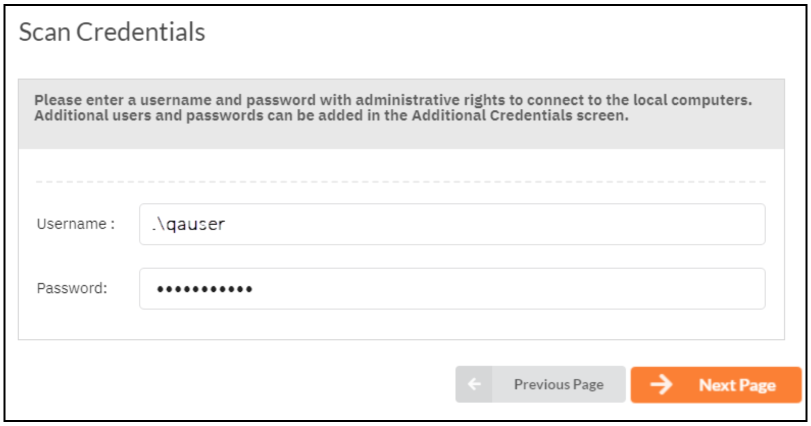
○ Treat them as part of the specified workgroup Workgroup

a. Treat them as part of the primary domain
b. Treat them as part of a specific workgroup by entering a workgroup name
c. Don't treat them as part of a domain (non-domain assets will appear separately in alerts and reports)

> **Tip:** Use this feature to tell Cyber Hawk how to handle computers that are not connected to the domain. This affects how they appear in alerts and reports.

Select a merge option and click **Next Page**.

3. Enter scan credentials with administrative rights to connect to the local computers in the workgroup.



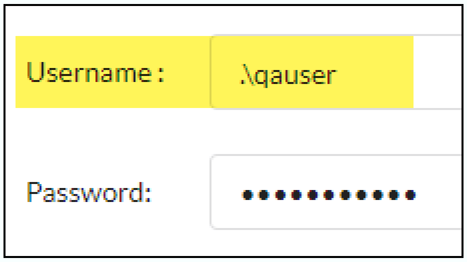
Scan Credentials

Please enter a username and password with administrative rights to connect to the local computers. Additional users and passwords can be added in the Additional Credentials screen.

Username : .\qauser

Password: •••••••••••

Note: For Workgroups, enter the characters ".\" (without quotation marks) immediately before the username, as in the image below.



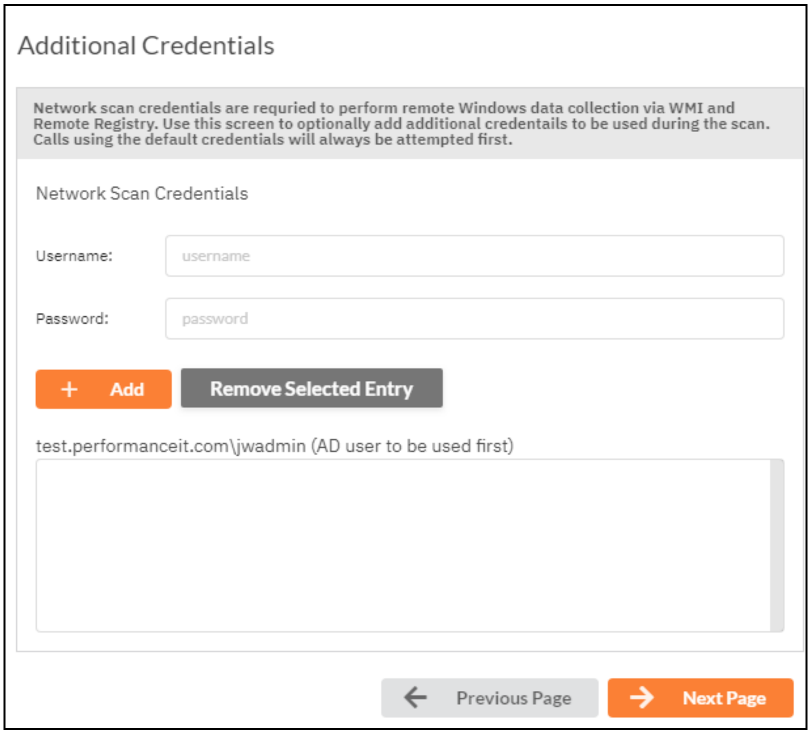
Username : .\qauser

Password: ••••••••••••

Click **Next Page** to test the connection and verify your credentials.

4. The **Additional Credentials** screen will appear. Enter any additional credentials to be used during the scan. Click **Next**.

Important: If each workgroup PC has its own unique Admin username and password credentials, you will need to enter each set of credentials here in order to scan these PCs.



Additional Credentials

Network scan credentials are requried to perform remote Windows data collection via WMI and Remote Registry. Use this screen to optionally add additional credentails to be used during the scan. Calls using the default credentials will always be attempted first.

Network Scan Credentials

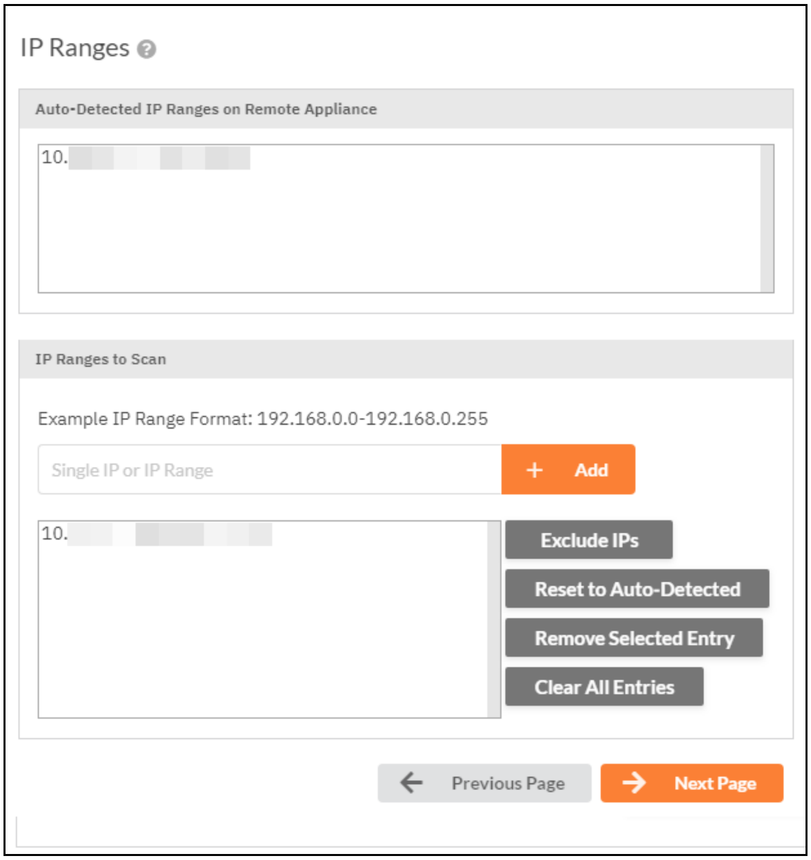
Username: username

Password: password

test.performanceit.com\jwadmin (AD user to be used first)

© 2024 RapidFire Tools, Inc. All rights reserved.

5. The **IP Ranges** screen will then appear. The **Cyber Hawk** 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**.



10.[redacted]

Example IP Range Format: 192.168.0.0-192.168.0.255

10.[redacted]

From this screen you can also:

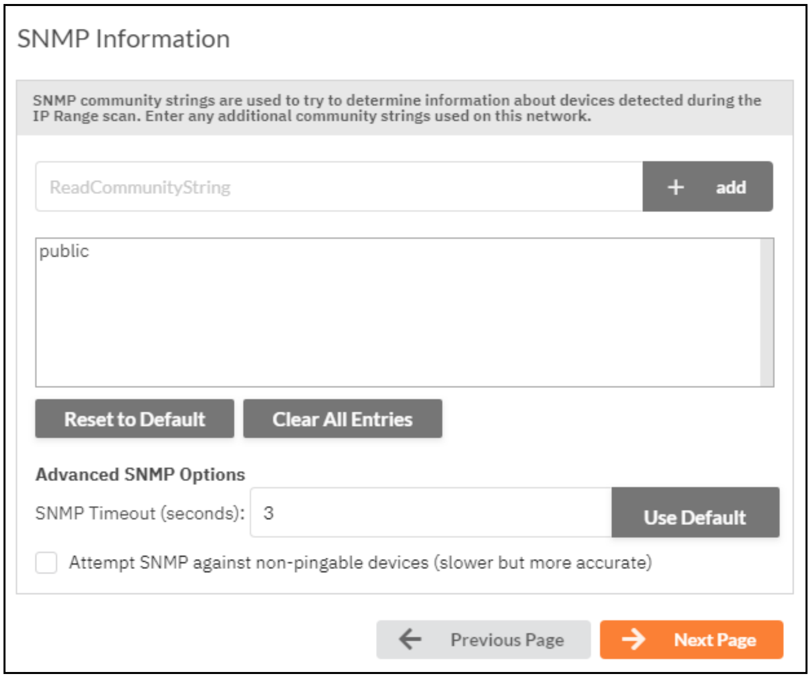
- Click **Reset to Default** to reset to the automatically suggested IP Range.
- **Exclude IPs** or IP ranges from the scan.

> **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.

© 2024 RapidFire Tools, Inc. All rights reserved.

Click **Next Page** once you have configured the IP ranges for the scan.

6. The **SNMP Information** window will appear. Enter any additional SNMP community strings used on the network. Click **Next Page**.



SNMP Information

SNMP community strings are used to try to determine information about devices detected during the IP Range scan. Enter any additional community strings used on this network.

ReadCommunityString

public

Advanced SNMP Options

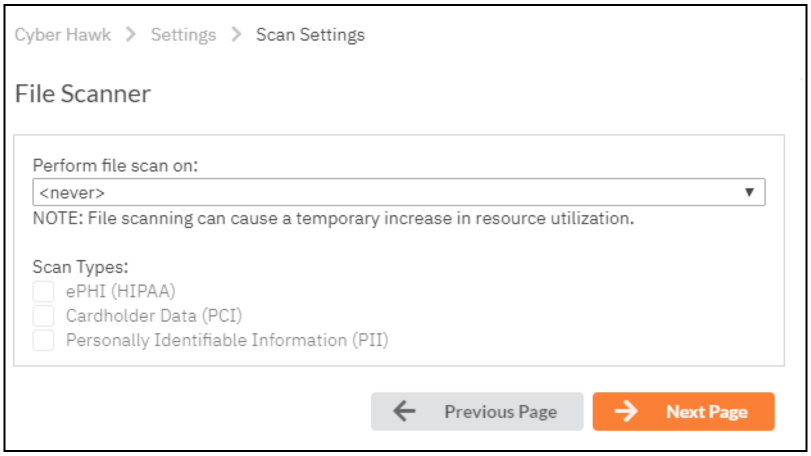
SNMP Timeout (seconds): 3

□ Attempt SNMP against non-pingable devices (slower but more accurate)

7. The **File Scanner** window will appear. Choose what day of the week to perform the file scan. Select a day of the week from the drop-down menu. Next, select the Scan Types that will be performed:

   - **ePHI** (HIPAA) will scan for Electronic Protected Health Information
   - **Cardholder Data** (PCI) will scan for payment card numbers and other related information
   - **Personally Identifiable Information** (PII) will scan for information such as a

person’s name or social security number



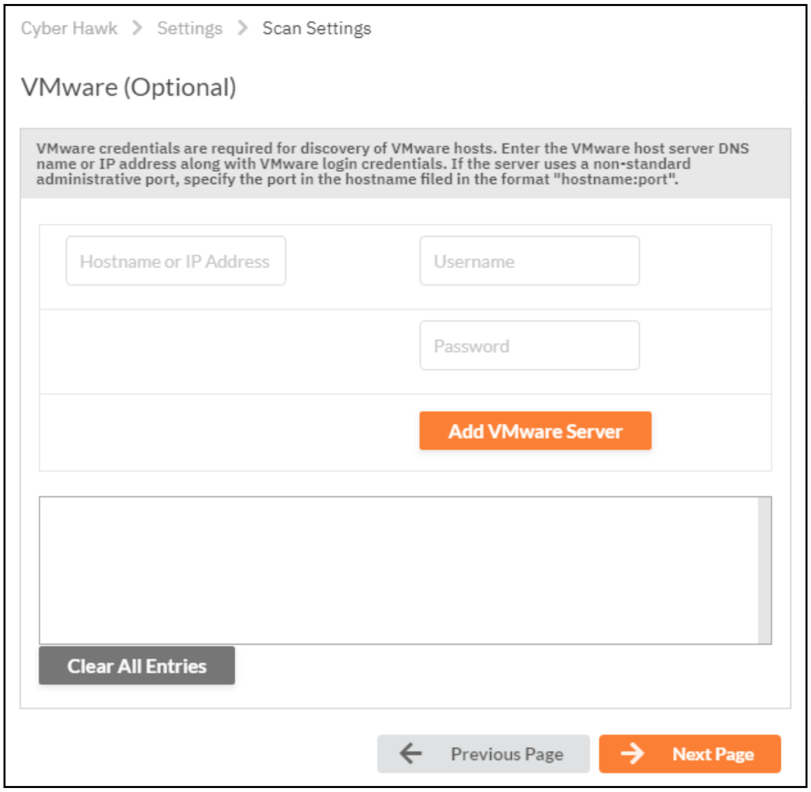
Cyber Hawk > Settings > Scan Settings

File Scanner

Perform file scan on:
<never>
NOTE: File scanning can cause a temporary increase in resource utilization.

Scan Types:
□ ePHI (HIPAA)
□ Cardholder Data (PCI)
□ Personally Identifiable Information (PII)

8. The optional **VMware** credentials window will appear. Enter the hostnames or IP Addresses of any VMware hosts that you wish to include in the scan. Likewise enter credentials needed to access the VMware hosts. Click **Next Page**.

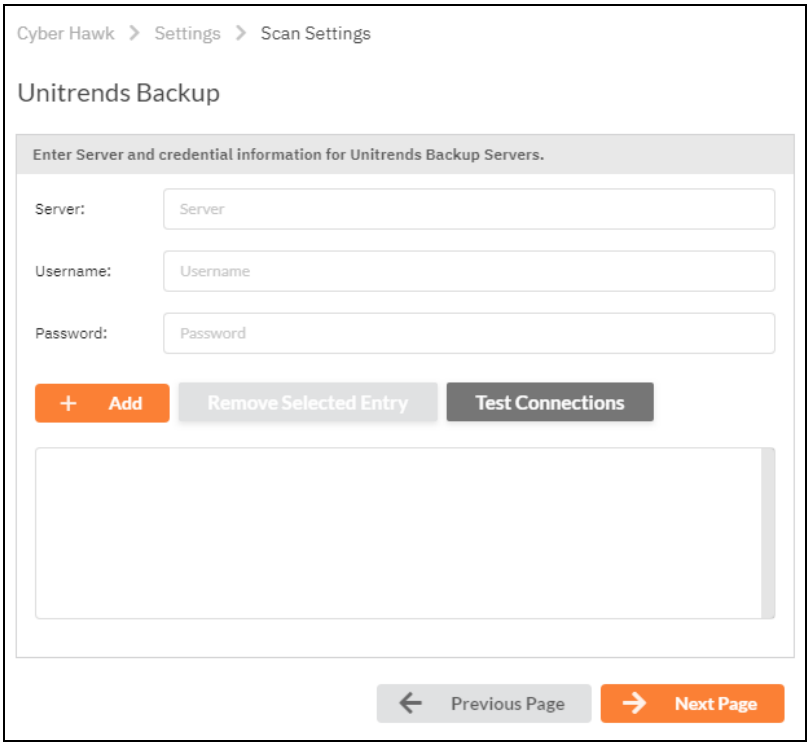


Cyber Hawk > Settings > Scan Settings

VMware (Optional)

VMware credentials are required for discovery of VMware hosts. Enter the VMware host server DNS name or IP address along with VMware login credentials. If the server uses a non-standard administrative port, specify the port in the hostname filed in the format "hostname:port".

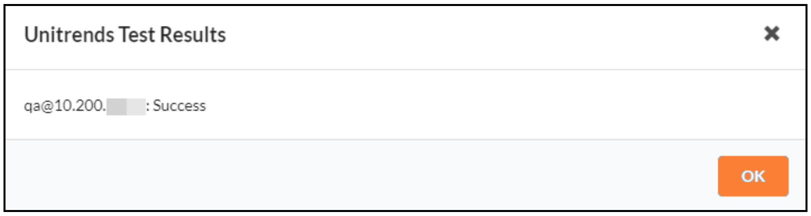
9. The **Unitrends Backup** screen will appear. Enter the Unitrends Backup server name and login credentials.



Unitrends Backup

Enter Server and credential information for Unitrends Backup Servers.

10. Click **Test Connection** to verify your Unitrends scan configuration.

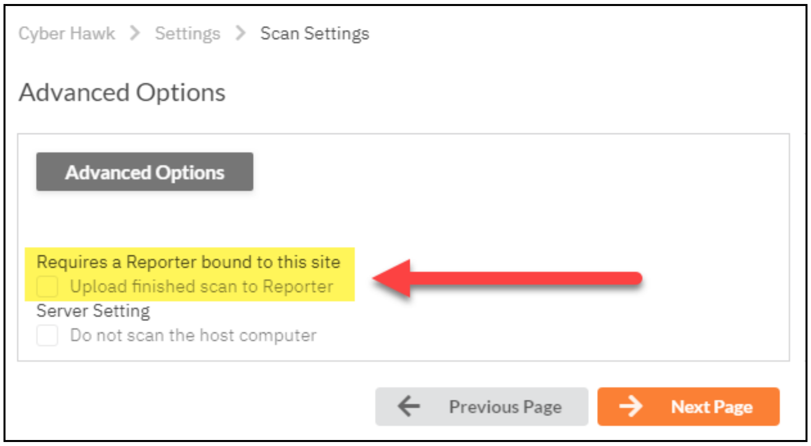


Unitrends Test Results

qa@10.200.[redacted]: Success

11. If you are using a **Reporter** appliance, you can also choose whether to upload the finished scans to the Reporter. Click **Next Page**.

© 2024 RapidFire Tools, Inc. All rights reserved.



Cyber Hawk > Settings > Scan Settings

Advanced Options

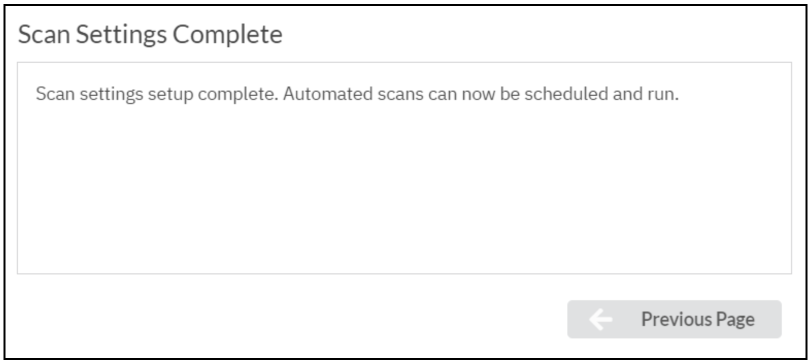
Requires a Reporter bound to this site

□ Upload finished scan to Reporter

Server Setting

□ Do not scan the host computer

12. Your scan settings will then be complete.



Scan Settings Complete

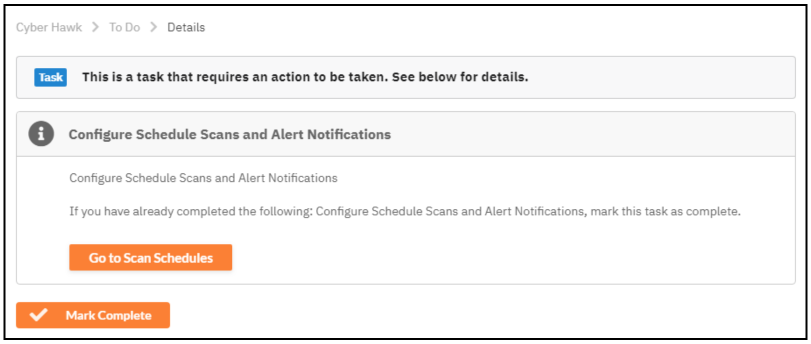
Scan settings setup complete. Automated scans can now be scheduled and run.

When you have finished entering the scan settings, return to the To Do list and click **Mark Complete** for the **Configure Scan Settings** To Do task.

Task 3 — Configure Schedule Scans and Alert Notifications

In this To Do task, you will configure the scanning and alert schedules for Cyber Hawk.

© 2024 RapidFire Tools, Inc. All rights reserved.



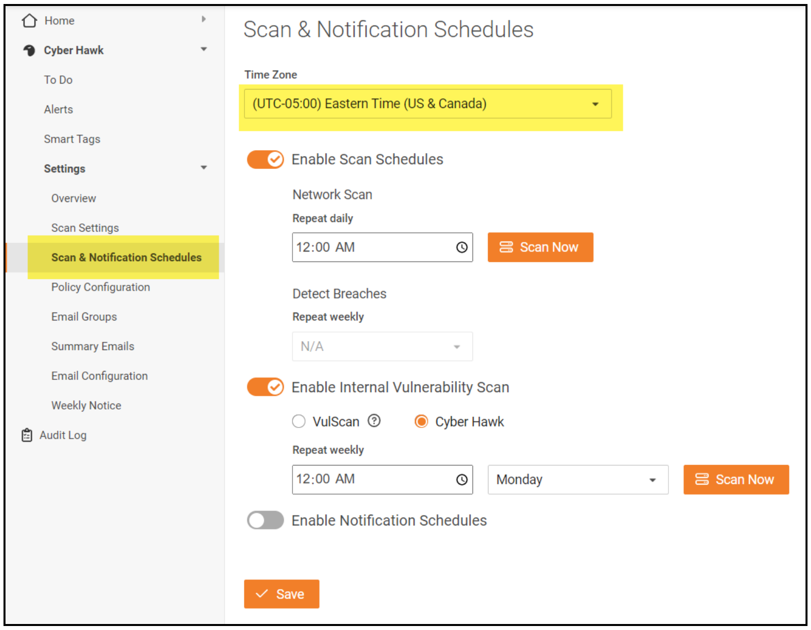
This is a task that requires an action to be taken. See below for details.

Configure Schedule Scans and Alert Notifications

Configure Schedule Scans and Alert Notifications

If you have already completed the following: Configure Schedule Scans and Alert Notifications, mark this task as complete.

First, go to **Cyber Hawk tab** > **Settings** > **Scan & Notification Schedules**. Set the **Time Zone** for scans and alerts for this Site. Then configure your scan and alert notifications as below:



Scan & Notification Schedules

Time Zone: (UTC-05:00) Eastern Time (US & Canada)

☑ Enable Scan Schedules

Network Scan
Repeat daily: 12:00 AM

Detect Breaches
Repeat weekly: N/A

☑ Enable Internal Vulnerability Scan

○ VulScan ● Cyber Hawk

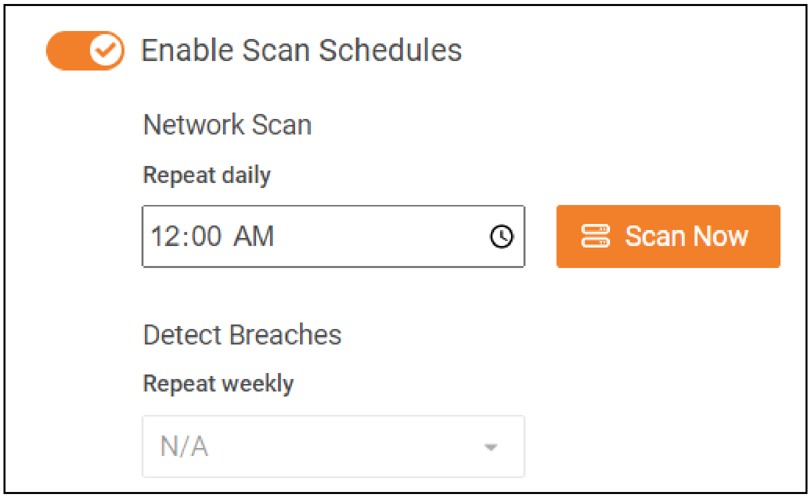
Repeat weekly: 12:00 AM Monday

□ Enable Notification Schedules

Enable Scan Schedules

Activate the slider to enable the daily (Level 1) **Network Scan**.

© 2024 RapidFire Tools, Inc. All rights reserved.



Enable Scan Schedules

Network Scan

Repeat daily

12:00 AM

Detect Breaches

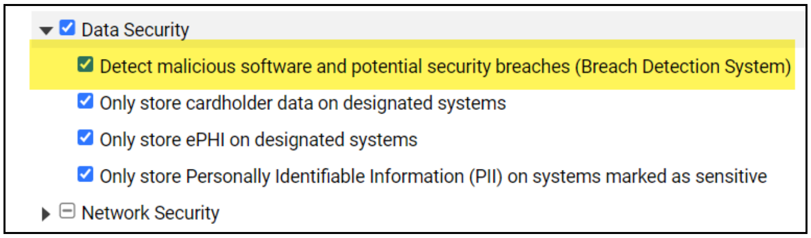
Repeat weekly

N/A

1. **Network Scan**: Set the time for the daily Cyber Hawk (Level 1) Network Scan. This scan will check for anomalies, changes, and threats as per your settings in "Task 8 — Configure Policies and Notifications" on page 48. You can also click **Scan Now** to begin a scan immediately.

   Important: The Level 1 scan employs **User Control Tests** to analyze the security of potential web browsing activity on a device. As part of the test, the data collector will attempt to access certain risk-prone websites directly from a device. If you are using an anti-virus or other tool that monitors suspicious web browsing, note that you may receive alerts from such systems related to this activity. See "User Control Tests" on page 278 for complete details.

2. **Detect Breaches**: Set the time for a malicious software and breach detection scan. This requires that you first activate the **Breach Detection System** policy from **Policy Configuration** > **Data Security**.



☑ Data Security
- ☑ Detect malicious software and potential security breaches (Breach Detection System)
- ☑ Only store cardholder data on designated systems
- ☑ Only store ePHI on designated systems
- ☑ Only store Personally Identifiable Information (PII) on systems marked as sensitive

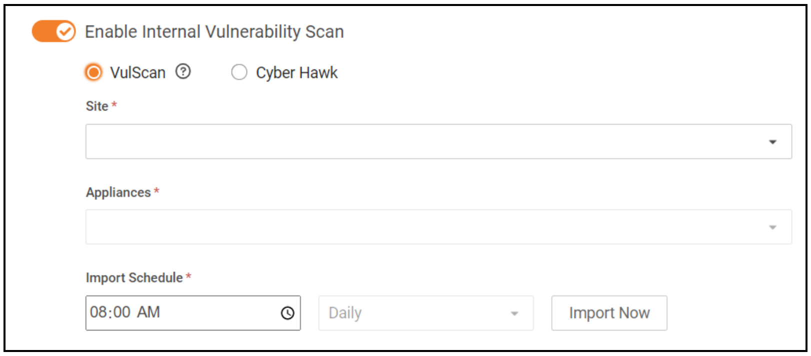
⊟ Network Security

© 2024 RapidFire Tools, Inc. All rights reserved.

Enable Internal Vulnerability Scan

Activate the slider to enable and configure Internal Vulnerability Scans (Level 2). This requires that you have 1) **a VulScan subscription**, OR 2) **an existing Cyber Hawk Virtual Appliance**.

Important: The Cyber Hawk Virtual Appliance for performing internal vulnerability scans has been deprecated. New users are encouraged to use the VulScan integration for internal vulnerability scanning.



Enable Internal Vulnerability Scan

● VulScan ○ Cyber Hawk

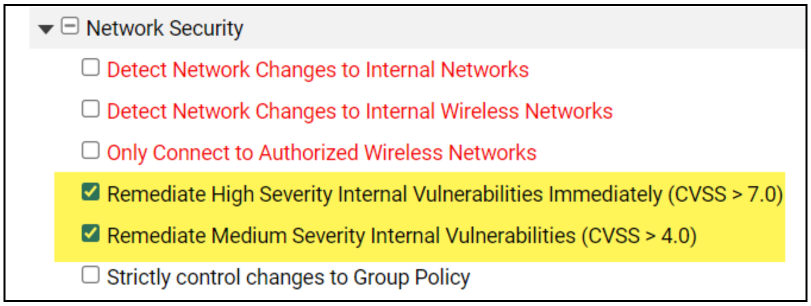
Site *

Appliances *

Import Schedule *

08:00 AM

In order to generate alerts regarding internal vulnerabilities, ensure you have selected these policies from **Settings** > **Policy Configuration** > **Network Security**. You will set up these policies later in "Task 8 — Configure Policies and Notifications" on page 48.



Network Security

- □ Detect Network Changes to Internal Networks
- □ Detect Network Changes to Internal Wireless Networks
- □ Only Connect to Authorized Wireless Networks
- ☑ Remediate High Severity Internal Vulnerabilities Immediately (CVSS > 7.0)
- ☑ Remediate Medium Severity Internal Vulnerabilities (CVSS > 4.0)
- □ Strictly control changes to Group Policy

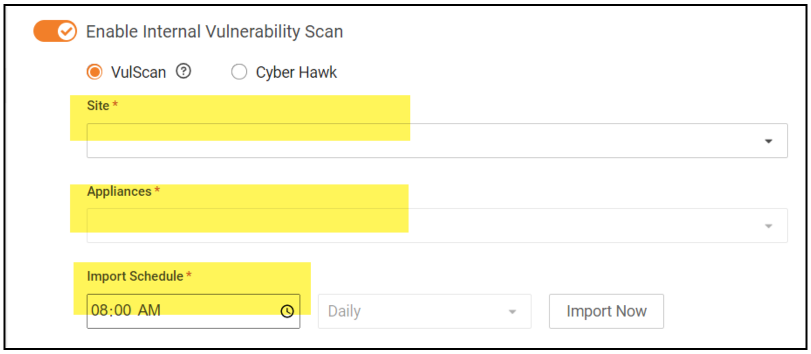
Enable Internal Vulnerability Scanning using VulScan Import

By default, **new Cyber Hawk sites** will prompt you to use **VulScan to import internal vulnerability scans**. However, if you have an existing Cyber Hawk Virtual Appliance associated with your site, you can choose between the Cyber Hawk Virtual Appliance and VulScan for internal vulnerability scanning.

© 2024 RapidFire Tools, Inc. All rights reserved.

- This topic demonstrates how to use VulScan to import internal vulnerability scans.
- If you wish instead to use your existing Cyber Hawk Virtual Appliance to perform internal vulnerability scans, see "Enable Cyber Hawk Internal Vulnerability Scan" on the facing page.

1. First, select **Vulscan**. (This step is only required if you also have a Cyber Hawk Virtual Appliance associated with your site.)
2. From **Site**, select your VulScan site from the drop-down menu. Your VulScan site **must be in the same organization** as your Cyber Hawk site.



☑ Enable Internal Vulnerability Scan

● VulScan ○ Cyber Hawk

Site *

Appliances *

Import Schedule *

08:00 AM

Daily

Import Now

3. From **Appliances**, select the VulScan appliance(s) from which to import internal vulnerability scans. **Be sure you have a scheduled internal vulnerability scan task set up for your VulScan site.**
4. From **Import Schedule**, set the time and interval to import the results of VulScan internal vulnerability scans.

   Note: Set the import time to occur **after** your VulScan internal vulnerability scans will have completed.

   You can also click **Import Now** to import scans immediately.

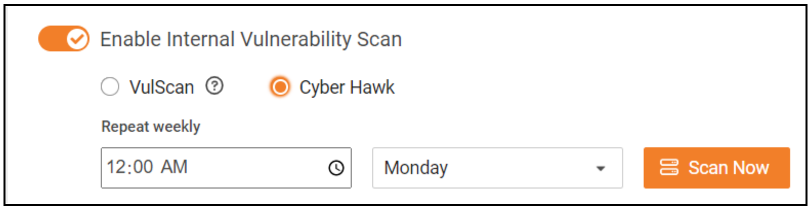
   Tip: For more information regarding VulScan, see the VulScan User Guide here.

© 2024 RapidFire Tools, Inc. All rights reserved.

Enable Cyber Hawk Internal Vulnerability Scan

1. If you wish to use an existing Cyber Hawk Virtual Appliance, select **Cyber Hawk**.

   > **Note:** This option will only appear if you have an existing Cyber Hawk **Virtual Appliance** associated with your site. New Cyber Hawk sites will use the RapidFire Tools Server for the daily network scan (Level 1), and VulScan for internal vulnerability scanning (Level 2) by default. See also "Migrate Cyber Hawk Virtual Appliance to Scan Server" on page 224.



Enable Internal Vulnerability Scan

○ VulScan ● Cyber Hawk

Repeat weekly

12:00 AM | Monday

2. From **Repeat Weekly**, set the time and interval. Your Cyber Hawk scan will occur at the assigned interval using the deprecated Virtual Appliance.

Tips for Scheduling the Internal Vulnerability Scan

Internal Network Vulnerability scans are intentionally designed to be aggressive and comprehensive in nature. At Internal Network Vulnerability scan run time, there are instances where these scans can impact network performance and access to computer endpoints by network users during the time a scheduled Internal Network Vulnerability scan is being performed.

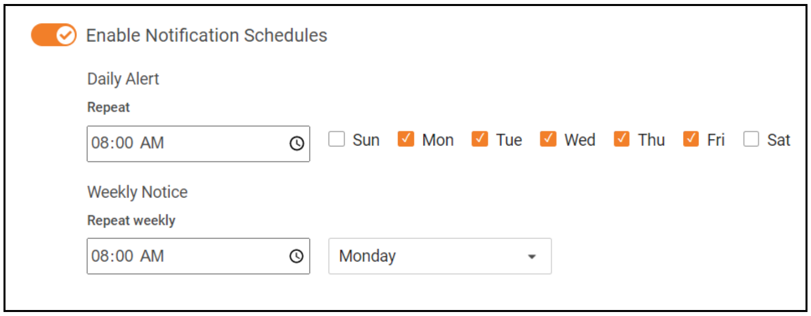
It is recommended that:

- scans are scheduled and performed at times when the network is not in use by network users, back-up processes, or any other system or process that requirements unimpeded network access.
- any routers, switches, computers, industrial devices connected to the network, security devices, and other network devices that should not be interfered with in any way during day to day network operation or must be operational and accessible to network systems and users on a 24x7x365 basis, that these IP addresses of the aforementioned devices should be excluded from the Cyber Hawk's IP Range settings contained within the Cyber Hawk's Scan Settings.

© 2024 RapidFire Tools, Inc. All rights reserved.

Enable Notification Schedules

Activate the slider to enable Notification Schedules.



Enable Notification Schedules

Daily Alert

Repeat

08:00 AM ☐ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☐ Sat

Weekly Notice

Repeat weekly

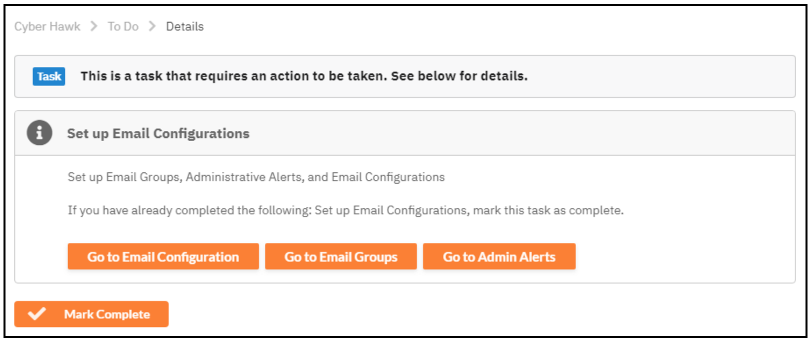
08:00 AM Monday

- **Daily Alert**: This is the time that Cyber Hawk will send out Daily Alert notifications to End Users and the Tech Group. You can also configure the days of the week that the Notifications will be sent (default is Monday through Friday).
- **Weekly Notice**: This is the time that Cyber Hawk will send out a weekly notice to recipients (default is Monday at 8:00am).

When you are finished configuring Scan & Notification Schedules, click **Save**.

Task 4 — Set up Email Configurations

In this task you will configure email alerts for your **Tech Group**, and, if you choose, **End Users** at the Site who can direct your techs to investigate or ignore alerts.



Task This is a task that requires an action to be taken. See below for details.

Set up Email Configurations

Set up Email Groups, Administrative Alerts, and Email Configurations

If you have already completed the following: Set up Email Configurations, mark this task as complete.

- **Email Groups**: Set up/select the groups who should receive Cyber Hawk Alerts; includes Tech Group and End Users
- **Admin Alerts**: Choose who will receive Admin Alerts, such as status of network

© 2024 RapidFire Tools, Inc. All rights reserved.

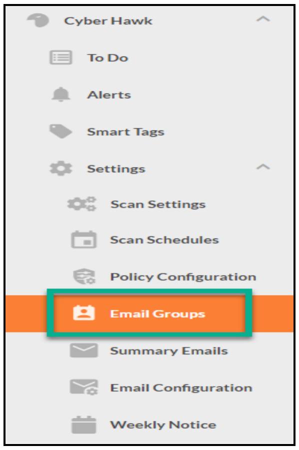
scans

- **Email Configuration**: Set up any custom email options for the Site

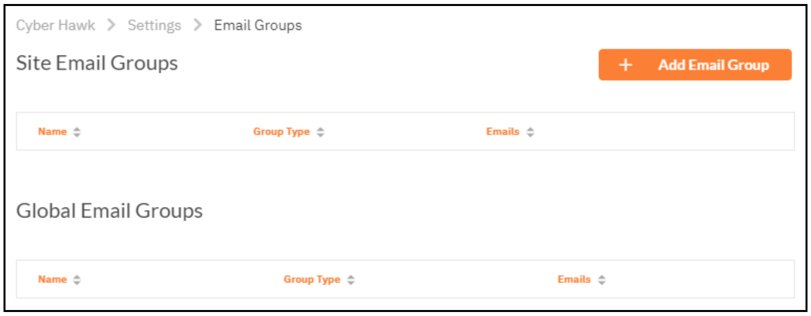
Set Up Email Groups

To set up Email Groups:

1. From the To Do item, click **Go to Email Groups** or go to the **Cyber Hawk tab** > **Settings**.
2. Click **Email Groups** from the Settings options on the left-hand side of the screen.

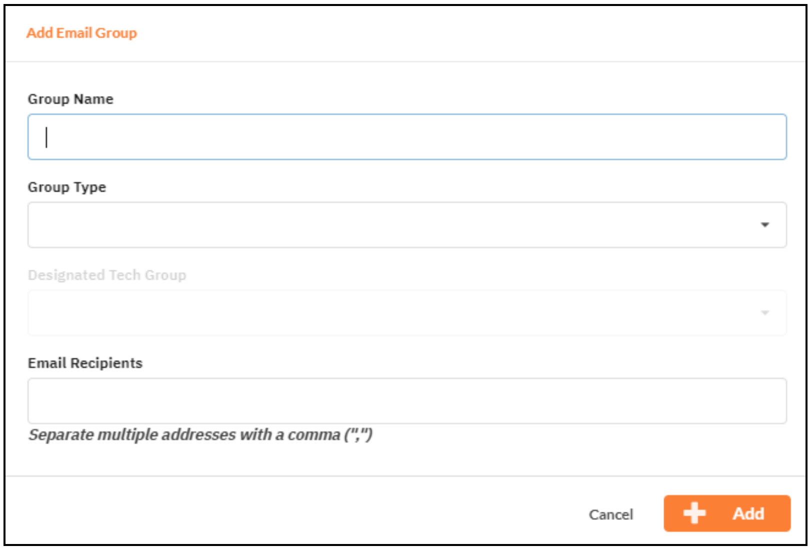


3. Click **Add Email Group**.



4. Enter a *Group Name*, *Group Type*, and then the *Email Recipients*. Separate individual email addresses with a comma.

© 2024 RapidFire Tools, Inc. All rights reserved.



Add Email Group

Group Name

Group Type

Designated Tech Group

Email Recipients

Separate multiple addresses with a comma (",")

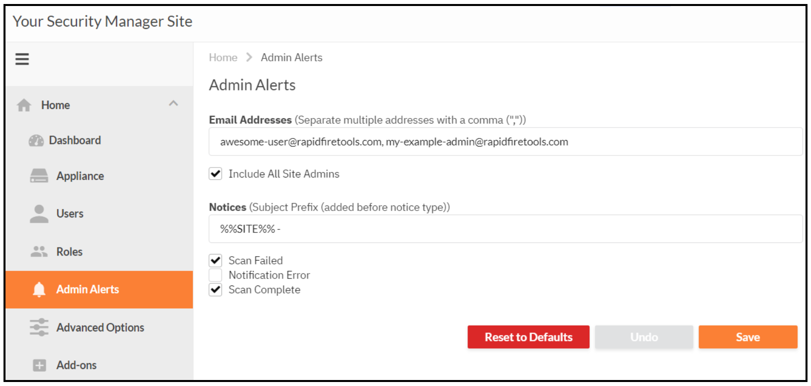
Note: For *Group Type*:
- Select **Tech** for Alerts that will be sent to your Technicians.
- Select **End User** for Alerts that you wish to send to on-site users for feedback before involving your Technicians.

You will configure which Alerts go to which Group Type later in the Policy Configuration set up process.

5. Click **Add**. The group will be added to the list.

Set Up Admin Alerts

1. Next set up **Admin Alerts**. Go to **Home tab** > **Admin Alerts**.



Admin Alerts

Email Addresses (Separate multiple addresses with a comma (","))

awesome-user@rapidfiretools.com, my-example-admin@rapidfiretools.com

☑ Include All Site Admins

Notices (Subject Prefix (added before notice type))

%%SITE%% -

☑ Scan Failed
□ Notification Error
☑ Scan Complete

© 2024 RapidFire Tools, Inc. All rights reserved.

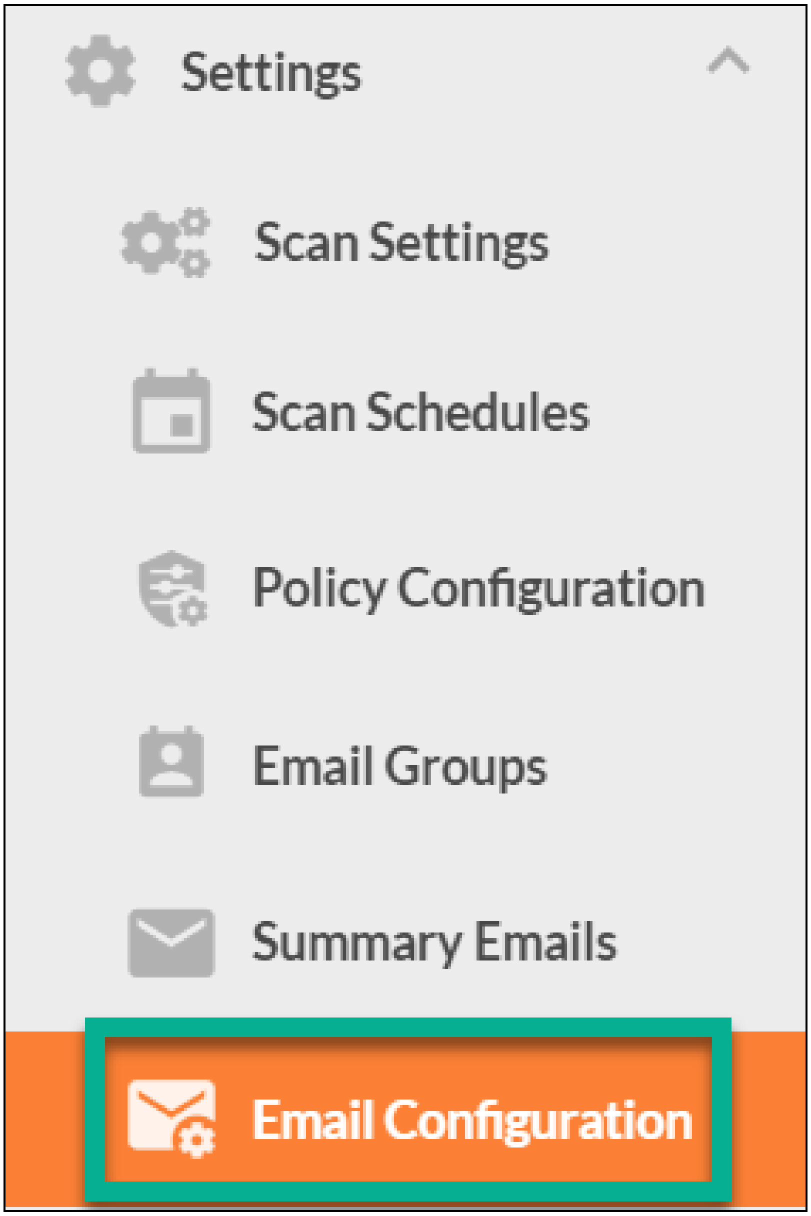
2. Enter and separate individual email addresses with a comma.
3. Enter a subject prefix for admin alerts.
4. Configure how Cyber Hawk will handle Administrative emails. This includes errors related to scans or notifications. Click **Save**.

   > **Note:** The Administrative Emails recipient will receive the results of the pre-scan analysis, so make sure you enter the email address of one of your tech group members who can use this information to address any issues with the scan configuration.

Set Up Email Configuration

1. Finally, configure your emails for the Site. Go to **Cyber Hawk tab** > **Settings** > **Email Configuration**.
2. Enter the configuration information for the email server. Choose whether to use the default configuration or your own custom SMTP server information. Click **Save**.
3. Under Email Subjects, choose whether to change the subject lines for Cyber Hawk emails. Click **Save**.

© 2024 RapidFire Tools, Inc. All rights reserved.

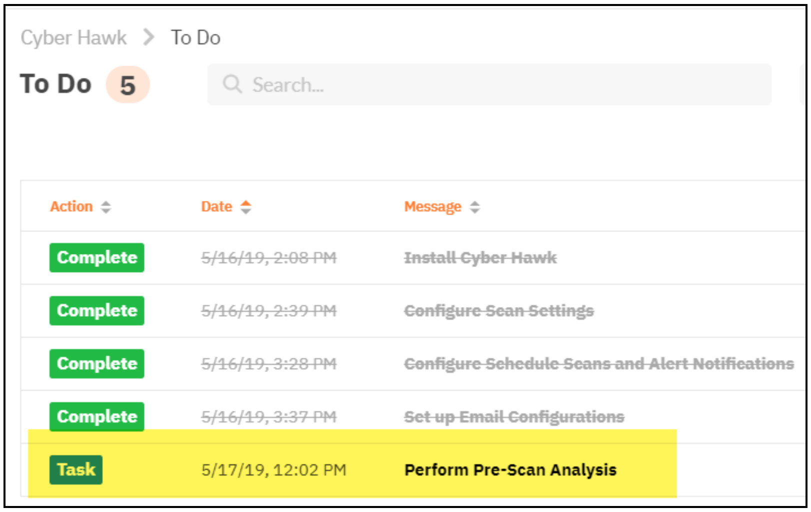


4. When you are finished, return to the To Do item and click **Mark Complete**.

The **Perform Pre-Scan Analysis** To Do item will then be added to the To Do list.

Task 5 — Perform Pre-Scan Analysis

Next the Cyber Hawk appliance will perform a **Pre-Scan Analysis** on the target network. This will show you any set-up issues with your Cyber Hawk scan configuration before the final client deployment.



Action	Date	Message
Complete	~~5/16/19, 2:08 PM~~	~~Install Cyber Hawk~~
Complete	~~5/16/19, 2:39 PM~~	~~Configure Scan Settings~~
Complete	~~5/16/19, 3:28 PM~~	~~Configure Schedule Scans and Alert Notifications~~
Complete	~~5/16/19, 3:37 PM~~	~~Set up Email Configurations~~
Task	5/17/19, 12:02 PM	Perform Pre-Scan Analysis

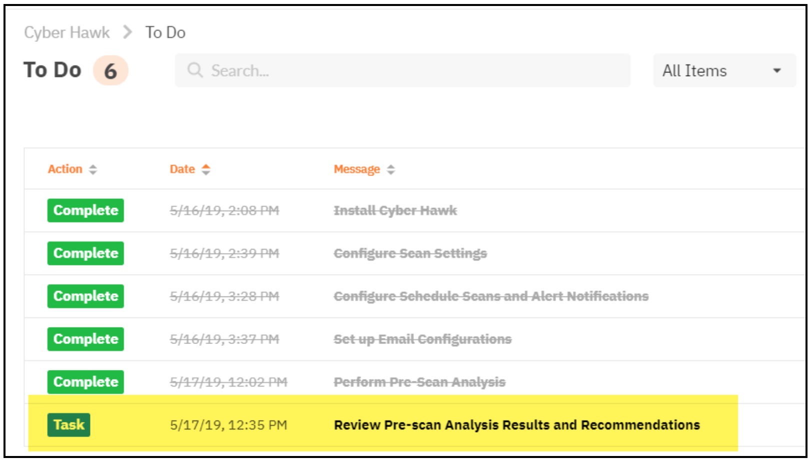
When the pre-scan analysis finishes, the administrator(s) will receive an email summarizing any issues identified with your Cyber Hawk scan settings.

Important: For best results, the target network must be configured to allow for successful scans on all network endpoints. See "Pre-Scan Network Configuration Checklist" on page 219 for configuration guidance for both Windows Active Directory and Workgroup environments.

Task 6 — Review Pre-Scan Analysis Results and Recommendations

When the pre-scan analysis finishes, an item will also appear in your To Do list that contains a summary of any potential set-up issues with the Cyber Hawk deployment. Usually, you can resolve most all of these issues by making sure the target network is configured to allow successful scanning.

© 2024 RapidFire Tools, Inc. All rights reserved.



Cyber Hawk > To Do

To Do 6

Search...

All Items

Action	Date	Message
Complete	~~5/16/19, 2:08 PM~~	~~Install Cyber Hawk~~
Complete	~~5/16/19, 2:39 PM~~	~~Configure Scan Settings~~
Complete	~~5/16/19, 3:28 PM~~	~~Configure Schedule Scans and Alert Notifications~~
Complete	~~5/16/19, 3:37 PM~~	~~Set up Email Configurations~~
Complete	~~5/17/19, 12:02 PM~~	~~Perform Pre-Scan Analysis~~
Task	5/17/19, 12:35 PM	Review Pre-scan Analysis Results and Recommendations

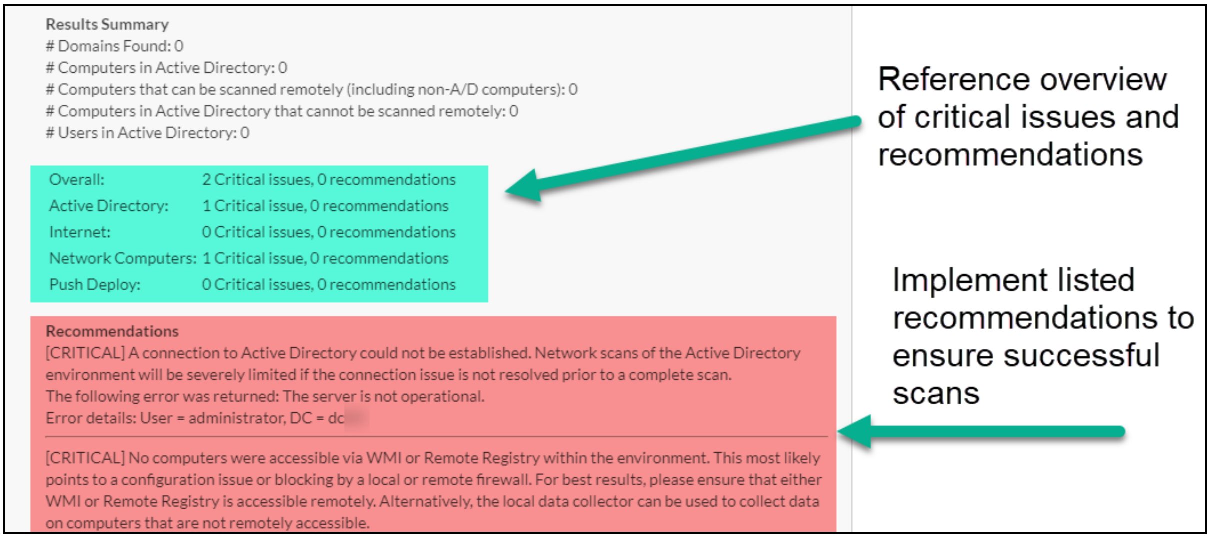
The **Results Summary** from the pre-scan analysis will appear on the task details page. Use this information to remediate any identified network configuration issues before continuing the assessment.

Important: For best results, the target network must be configured to allow for successful scans on all network endpoints. See "Pre-Scan Network Configuration Checklist" on page 219 for configuration guidance for both Windows Active Directory and Workgroup environments.

Note: A 100% successful scan may not be possible in some cases due to network restrictions. Before opening ports or allowing protocols, please consult with your network and system administrator.

Below the Results Summary, refer to the **Recommendations** for specific suggestions for mitigating the issues that were identified.

© 2024 RapidFire Tools, Inc. All rights reserved.



Results Summary
Domains Found: 0
Computers in Active Directory: 0
Computers that can be scanned remotely (including non-A/D computers): 0
Computers in Active Directory that cannot be scanned remotely: 0
Users in Active Directory: 0

Overall:	2 Critical issues, 0 recommendations
Active Directory:	1 Critical issue, 0 recommendations
Internet:	0 Critical issues, 0 recommendations
Network Computers:	1 Critical issue, 0 recommendations
Push Deploy:	0 Critical issues, 0 recommendations

Recommendations
[CRITICAL] A connection to Active Directory could not be established. Network scans of the Active Directory environment will be severely limited if the connection issue is not resolved prior to a complete scan.
The following error was returned: The server is not operational.
Error details: User = administrator, DC = dc[redacted]

[CRITICAL] No computers were accessible via WMI or Remote Registry within the environment. This most likely points to a configuration issue or blocking by a local or remote firewall. For best results, please ensure that either WMI or Remote Registry is accessible remotely. Alternatively, the local data collector can be used to collect data on computers that are not remotely accessible.

Reference overview of critical issues and recommendations

Implement listed recommendations to ensure successful scans

Tip: If the Analysis reveals CRITICAL issues:

a) Review recommendations and address any identified network restriction issues, and

b) Resolve identified issues before proceeding with marking the Review Pre-scan Analysis Results and Recommendations task complete.

Specifically:
- Also be sure that the Cyber Hawk appliance successfully connected to the **Domain Controller**.
- If you still have issues, work with your Technician to be sure the target network meets the "Pre-Scan Network Configuration Checklist" on page 219.

When you have reviewed the pre-scan analysis and are finished making any recommended changes to the target network, click **Mark Complete**. The **Internal Scan** will then begin automatically.

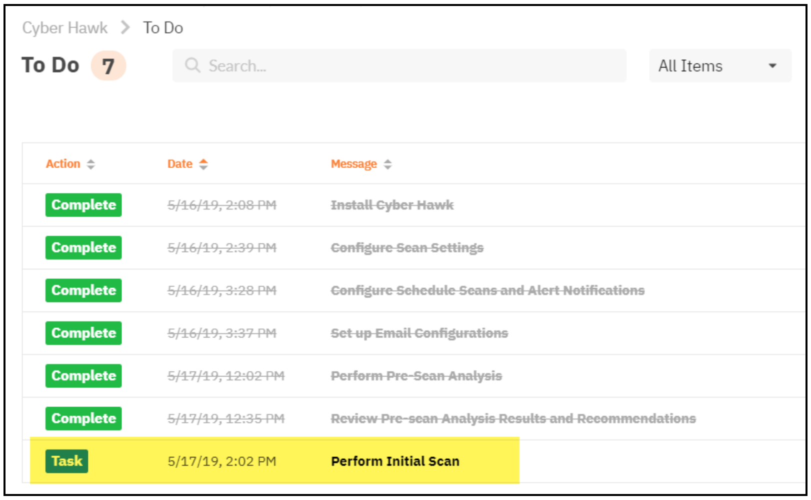
Task 7 — Perform Initial Cyber Hawk Scan

Before you can continue setting up Cyber Hawk, you need to perform an *initial scan* in order to gather more information about the target network. The initial scan will begin as

© 2024 RapidFire Tools, Inc. All rights reserved.

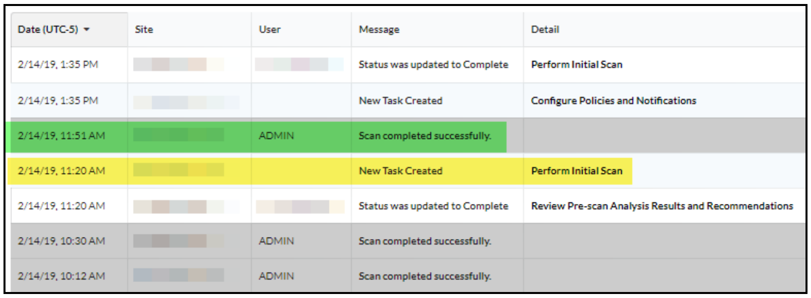
soon as you click Mark Complete on the previous task, "Review Pre-scan Analysis Results and Recommendations."

The task **Perform Initial Scan** will then appear in your To Do list. At this point in the process, a Cyber Hawk network scan and a local computer scan will have been initiated on the network.



Action	Date	Message
Complete	~~5/16/19, 2:08 PM~~	~~Install Cyber Hawk~~
Complete	~~5/16/19, 2:39 PM~~	~~Configure Scan Settings~~
Complete	~~5/16/19, 3:28 PM~~	~~Configure Schedule Scans and Alert Notifications~~
Complete	~~5/16/19, 3:37 PM~~	~~Set up Email Configurations~~
Complete	~~5/17/19, 12:02 PM~~	~~Perform Pre-Scan Analysis~~
Complete	~~5/17/19, 12:35 PM~~	~~Review Pre-scan Analysis Results and Recommendations~~
Task	5/17/19, 2:02 PM	Perform Initial Scan

The Admin user assigned to receive Admin Notifications should receive an email when the scan is complete. You can also check whether the scan is complete by referring to the Audit Log, as pictured below:



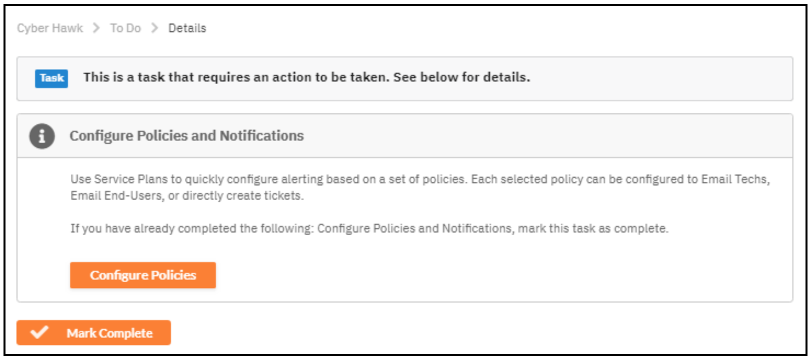
Date (UTC-5)	Site	User	Message	Detail
2/14/19, 1:35 PM	[redacted]	[redacted]	Status was updated to Complete	Perform Initial Scan
2/14/19, 1:35 PM	[redacted]		New Task Created	Configure Policies and Notifications
2/14/19, 11:51 AM	[redacted]	ADMIN	Scan completed successfully.	
2/14/19, 11:20 AM	[redacted]		New Task Created	Perform Initial Scan
2/14/19, 11:20 AM	[redacted]	[redacted]	Status was updated to Complete	Review Pre-scan Analysis Results and Recommendations
2/14/19, 10:30 AM	[redacted]	ADMIN	Scan completed successfully.	
2/14/19, 10:12 AM	[redacted]	ADMIN	Scan completed successfully.	

Once the scan is complete, return to the *Perform Initial Scan* To Do item and click **Mark Complete**.

Task 8 — Configure Policies and Notifications

© 2024 RapidFire Tools, Inc. All rights reserved.

In this To Do item, you will configure Cyber Hawk Security Policies and Notifications.



This is a task that requires an action to be taken. See below for details.

Configure Policies and Notifications

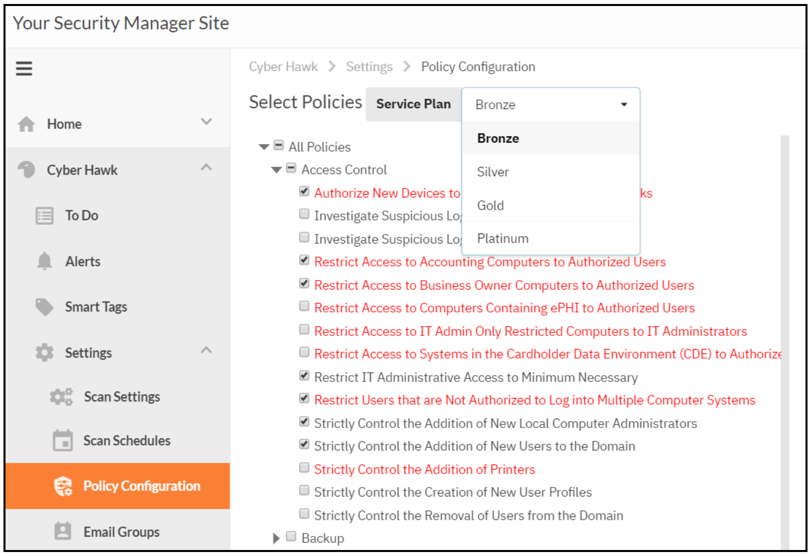
Use Service Plans to quickly configure alerting based on a set of policies. Each selected policy can be configured to Email Techs, Email End-Users, or directly create tickets.

If you have already completed the following: Configure Policies and Notifications, mark this task as complete.

In short, this is where you create the "Service Plan" of Security Policies that will be enforced on the target network. To do this:

1. When you are ready to configure policies, click **Configure Policies**. The **Policy Configuration** page will appear.
2. Select a **Service Plan** from the drop-down menu. You can select from several default Service Plans "out of the box" and modify them for use with the Site.

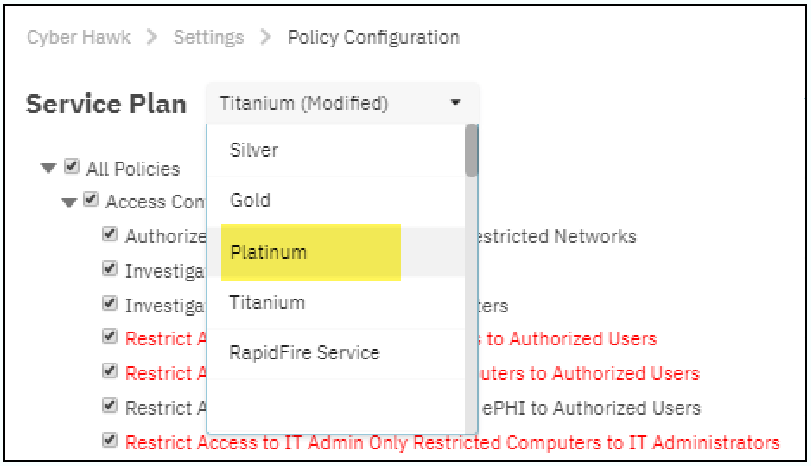
   > **Tip:** If you wish to create a "global" Service Plan that you can apply to multiple sites, see "Create Global Service Plans for Cyber Hawk" on page 97, then return to this step and apply your global policy to this site.



- ▼ ⊟ All Policies
  - ▼ ⊟ Access Control
    - ☑ Authorize New Devices to … ks
    - ☐ Investigate Suspicious Lo…
    - ☐ Investigate Suspicious Lo…
    - ☑ Restrict Access to Accounting Computers to Authorized Users
    - ☑ Restrict Access to Business Owner Computers to Authorized Users
    - ☐ Restrict Access to Computers Containing ePHI to Authorized Users
    - ☐ Restrict Access to IT Admin Only Restricted Computers to IT Administrators
    - ☐ Restrict Access to Systems in the Cardholder Data Environment (CDE) to Authorize
    - ☑ Restrict IT Administrative Access to Minimum Necessary
    - ☑ Restrict Users that are Not Authorized to Log into Multiple Computer Systems
    - ☑ Strictly Control the Addition of New Local Computer Administrators
    - ☑ Strictly Control the Addition of New Users to the Domain
    - ☐ Strictly Control the Addition of Printers
    - ☐ Strictly Control the Creation of New User Profiles
    - ☐ Strictly Control the Removal of Users from the Domain
  - ▶ ☐ Backup

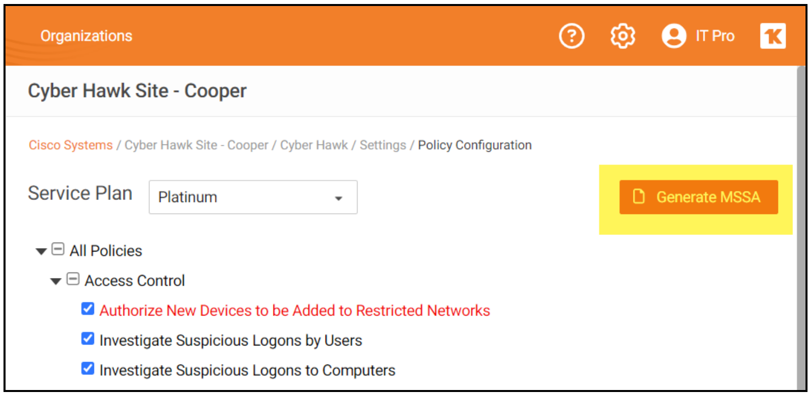
© 2024 RapidFire Tools, Inc. All rights reserved.

3. If you wish to modify the Service Plan for this Site, check or uncheck any specific security policies. Then click **Next**.

> **Note:** When you make changes to a Service Plan at the site-level, *the plan will be modified for this Site only*. If a Service Plan has been modified for a Site, it will show "**modified**" next the Service Plan name in the drop-down menu.
>
> 
>
> Cyber Hawk > Settings > Policy Configuration
>
> Service Plan: Titanium (Modified)
>
>
>
> - ☑ All Policies
>   - ☑ Access Con
>   - ☑ Authorize … estricted Networks
>   - ☑ Investiga
>   - ☑ Investiga … ers
>   - ☑ Restrict A … to Authorized Users
>   - ☑ Restrict A … uters to Authorized Users
>   - ☑ Restrict A … ePHI to Authorized Users
>   - ☑ Restrict Access to IT Admin Only Restricted Computers to IT Administrators

4. Before you click **Next**, you can optionally generate a **Managed Security Services Agreement (MSSA)** from the drop down menu. This will create an agreement between you and the client. To do this:

   a. Click **Generate MSSA**.



Cyber Hawk Site - Cooper

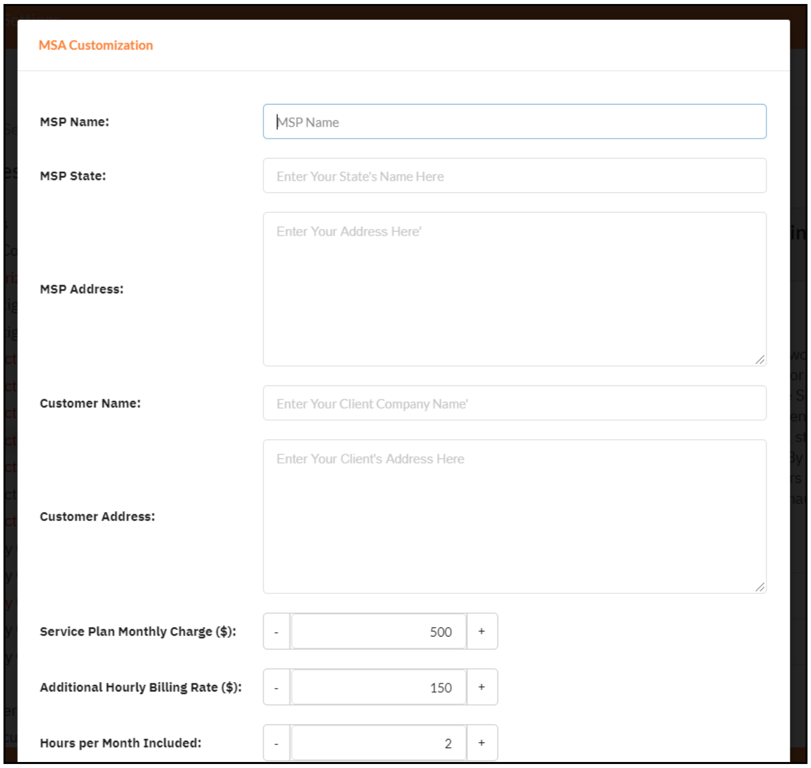
Cisco Systems / Cyber Hawk Site - Cooper / Cyber Hawk / Settings / Policy Configuration

Service Plan: Platinum

- ⊟ All Policies
  - ⊟ Access Control
    - ☑ Authorize New Devices to be Added to Restricted Networks
    - ☑ Investigate Suspicious Logons by Users
    - ☑ Investigate Suspicious Logons to Computers

   b. Enter your custom information for the MSSA.

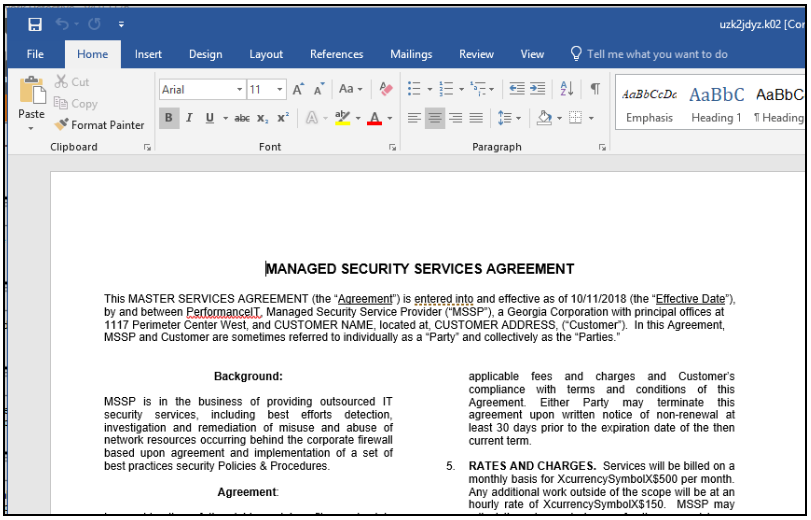
© 2024 RapidFire Tools, Inc. All rights reserved.



MSA Customization

MSP Name:	MSP Name
MSP State:	Enter Your State's Name Here
MSP Address:	Enter Your Address Here'
Customer Name:	Enter Your Client Company Name'
Customer Address:	Enter Your Client's Address Here
Service Plan Monthly Charge ($):	- 500 +
Additional Hourly Billing Rate ($):	- 150 +
Hours per Month Included:	- 2 +

c. A Word doc version of the MSSA will open. You can provide this to the client when and how you see fit.



MANAGED SECURITY SERVICES AGREEMENT

This MASTER SERVICES AGREEMENT (the "Agreement") is entered into and effective as of 10/11/2018 (the "Effective Date"), by and between PerformanceIT, Managed Security Service Provider ("MSSP"), a Georgia Corporation with principal offices at 1117 Perimeter Center West, and CUSTOMER NAME, located at, CUSTOMER ADDRESS, ("Customer"). In this Agreement, MSSP and Customer are sometimes referred to individually as a "Party" and collectively as the "Parties."

Background:

MSSP is in the business of providing outsourced IT security services, including best efforts detection, investigation and remediation of misuse and abuse of network resources occurring behind the corporate firewall based upon agreement and implementation of a set of best practices security Policies & Procedures.

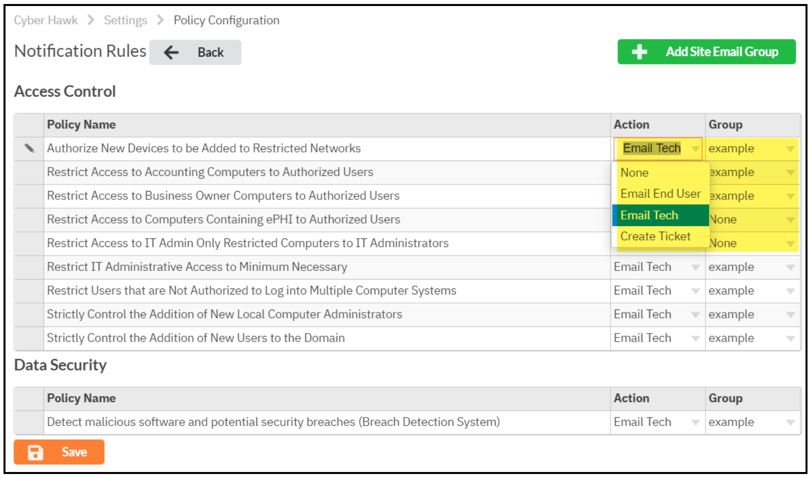
Agreement:

applicable fees and charges and Customer's compliance with terms and conditions of this Agreement. Either Party may terminate this agreement upon written notice of non-renewal at least 30 days prior to the expiration date of the then current term.

5. **RATES AND CHARGES.** Services will be billed on a monthly basis for XcurrencySymbolX$500 per month. Any additional work outside of the scope will be at an hourly rate of XcurrencySymbolX$150. MSSP may

d. You can come back and modify the security policy at any time, as well as generate a new MSSA.

5. Once you click **Next**, the Notification Rules screen will appear. Here configure how Cyber Hawk will respond to each Security Policy. Select an **Action** for each Policy.



Cyber Hawk > Settings > Policy Configuration

Notification Rules

Access Control

Policy Name	Action	Group
Authorize New Devices to be Added to Restricted Networks	Email Tech	example
Restrict Access to Accounting Computers to Authorized Users		example
Restrict Access to Business Owner Computers to Authorized Users		example
Restrict Access to Computers Containing ePHI to Authorized Users		None
Restrict Access to IT Admin Only Restricted Computers to IT Administrators		None
Restrict IT Administrative Access to Minimum Necessary	Email Tech	example
Restrict Users that are Not Authorized to Log into Multiple Computer Systems	Email Tech	example
Strictly Control the Addition of New Local Computer Administrators	Email Tech	example
Strictly Control the Addition of New Users to the Domain	Email Tech	example

Data Security

Policy Name	Action	Group
Detect malicious software and potential security breaches (Breach Detection System)	Email Tech	example

Actions include:

- **None**: Take no action. An Alert will still be generated for the issue in the Portal.
- **Email End User**: Send an email to an end user group. The end user will then make a decision about whether to request further investigation from the Tech Team.
- **Email Tech**: Send an email to the Tech Team to investigate the issue.
- **Create a Ticket**: Automatically Create a Ticket in your favorite PSA/ticketing system

> **Note:** These Actions will generate To Do and Alert items in the RapidFire Tools Portal.

6. Select the Email **Group Name** (the email group to whom to send either an End User or Tech email notification).

7. When you have assigned *Actions* and *Groups* to all Security Policies, click **Finish**.

© 2024 RapidFire Tools, Inc. All rights reserved.

Note: To Do items and Alerts generated by Cyber Hawk will remain in the Portal for two weeks before they are automatically removed.

8. Return to the **Configure Notifications and Policies** To Do item and click **Mark Complete**.

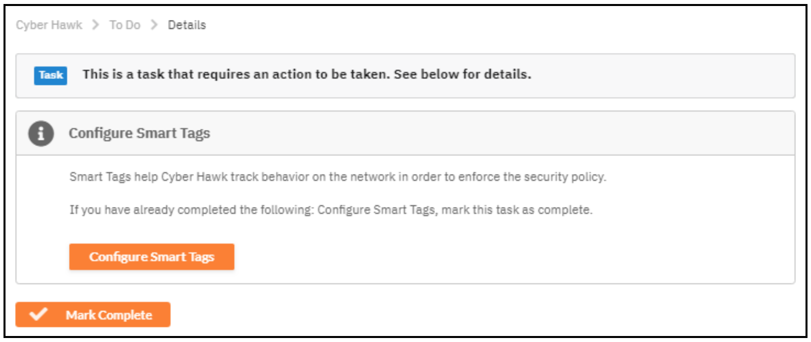
When you complete this To Do item, the **Configure Smart Tags** To Do item will appear.

Task 9 — Configure Smart Tags

Next you will deploy **Smart Tags** within the network environment. Smart Tags help Cyber Hawk better track behavior on the network in order to more effectively detect security policy violations.

Important: Note that many Cyber Hawk Security Policies REQUIRE that you assign Smart Tags to network assets such as PCs or users.

1. To get started, click **Configure Smart Tags** or go to **[Your Site]** > **Cyber Hawk** > **Smart Tags**.



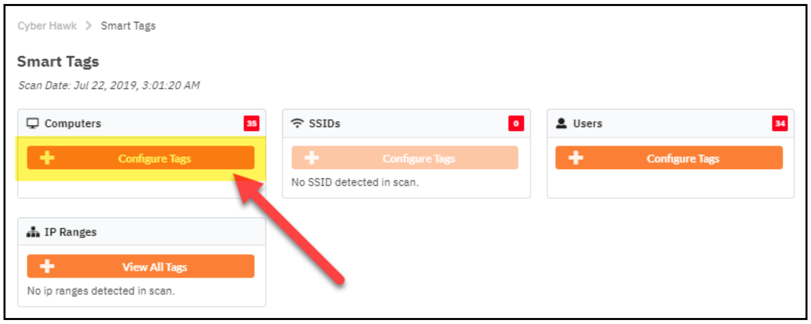
This is a task that requires an action to be taken. See below for details.

Configure Smart Tags

Smart Tags help Cyber Hawk track behavior on the network in order to enforce the security policy.

If you have already completed the following: Configure Smart Tags, mark this task as complete.

2. Choose the type of network assets to which to assign Smart Tags (for example, *Computers* or *Users*). Click **Configure Tags**.



Cyber Hawk > Smart Tags

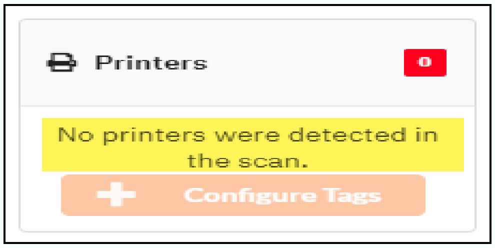
Smart Tags

Scan Date: Jul 22, 2019, 3:01:20 AM

No SSID detected in scan.

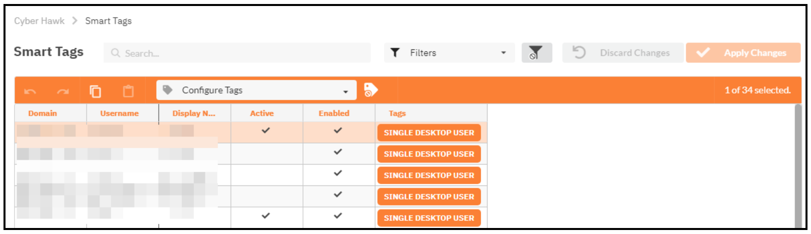
No ip ranges detected in scan.

Note: If the network scan does not uncover assets, the **Configure Tags** button will not be available.



No printers were detected in the scan.

3. A list of assets or users will appear based on the results of the network scan. From the list, select one or more assets or users to receive smart tags. You can **SHIFT + click** to select multiple assets/users at once.



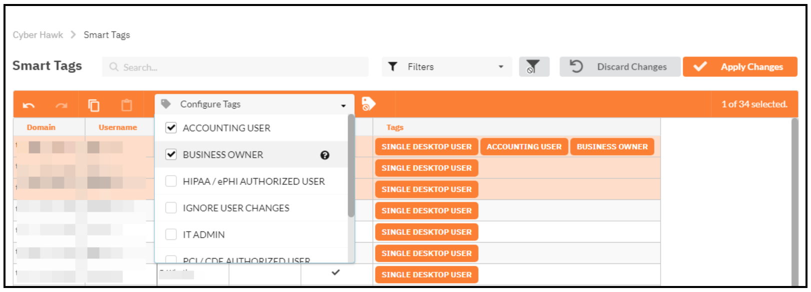
Cyber Hawk > Smart Tags

1 of 34 selected.

Domain	Username	Display N...	Active	Enabled	Tags
[redacted]	[redacted]	[redacted]	✓	✓	SINGLE DESKTOP USER
[redacted]	[redacted]	[redacted]		✓	SINGLE DESKTOP USER
[redacted]	[redacted]	[redacted]		✓	SINGLE DESKTOP USER
[redacted]	[redacted]	[redacted]		✓	SINGLE DESKTOP USER
[redacted]	[redacted]	[redacted]	✓	✓	SINGLE DESKTOP USER

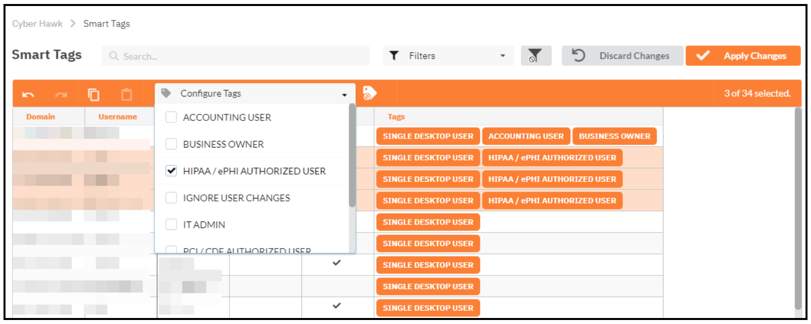
4. With the chosen assets still selected, click on one or more **Smart Tags** at the bottom of the screen.

© 2024 RapidFire Tools, Inc. All rights reserved.



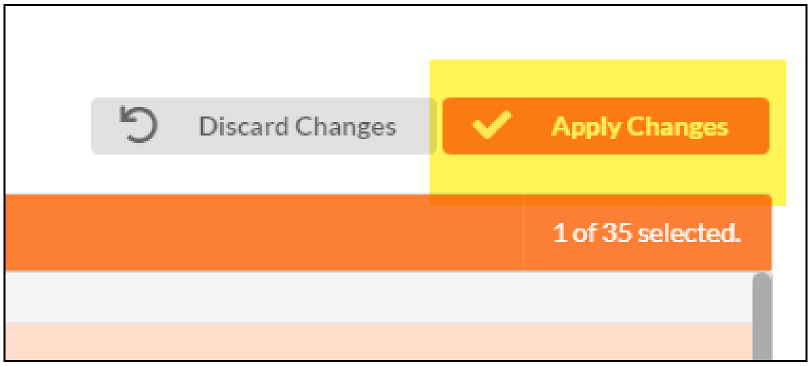
☑ ACCOUNTING USER
☑ BUSINESS OWNER
☐ HIPAA / ePHI AUTHORIZED USER
☐ IGNORE USER CHANGES
☐ IT ADMIN
☐ PCI / CDE AUTHORIZED USER

This will associate the Smart Tag(s) with the selected assets.



☐ ACCOUNTING USER
☐ BUSINESS OWNER
☑ HIPAA / ePHI AUTHORIZED USER
☐ IGNORE USER CHANGES
☐ IT ADMIN
☐ PCI / CDE AUTHORIZED USER

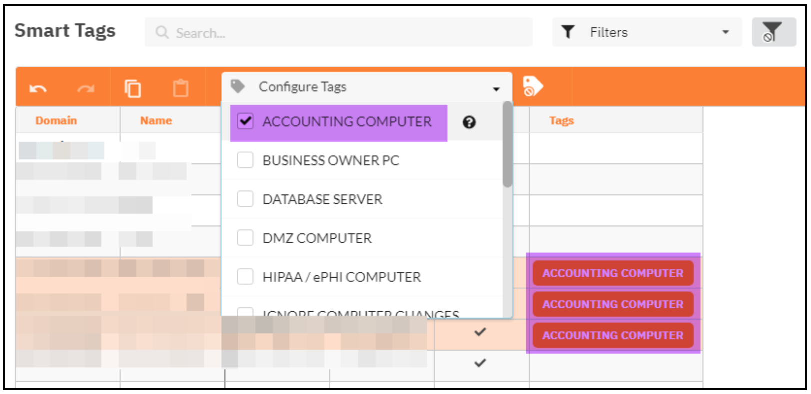
5. Click **Apply Changes** to save your **Smart Tag** configuration.



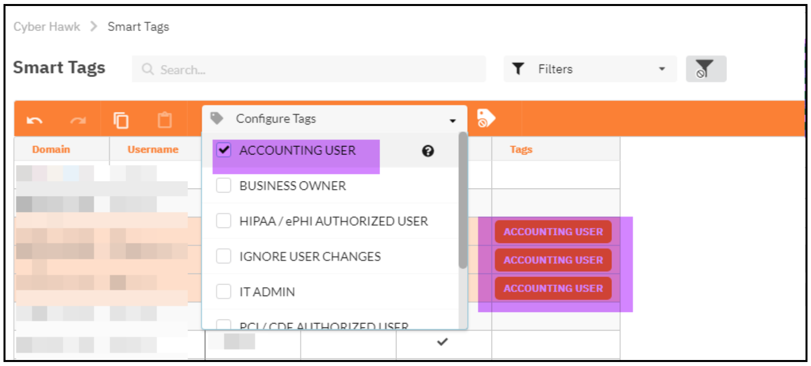
6. Return to **[Your Site]** > **Cyber Hawk** > **Smart Tags**. Continue tagging network assets (*Computers*, *Users*, *Printers*, etc.) until you have assigned all Smart Tags necessary to enforce your chosen Security Policies.

EXAMPLE: If a PC on the target network is an Accounting Computer, you can assign that PC the **Accounting Computer** Smart Tag.

© 2024 RapidFire Tools, Inc. All rights reserved.



Likewise, you can then assign authorized users the **Accounting User** Smart Tag.



This lets Cyber Hawk know that the designated accounting computers should only be accessed by authorized accounting users. If a non-accounting user attempts to access the PC, Cyber Hawk will generate an alert.

When you have assigned all recommended smart tags to network assets and users, return to the To Do item and click **Mark Complete**.

Tip: See the section "Smart Tags" on page 178 in this guide for more detailed information.

Congratulations! You've configured Cyber Hawk on the target network! Your End Users and Tech Group will now receive daily alerts whenever Cyber Hawk detects security policy violations, changes, or suspicious activity on the network.

RapidFire Tools Portal Set Up

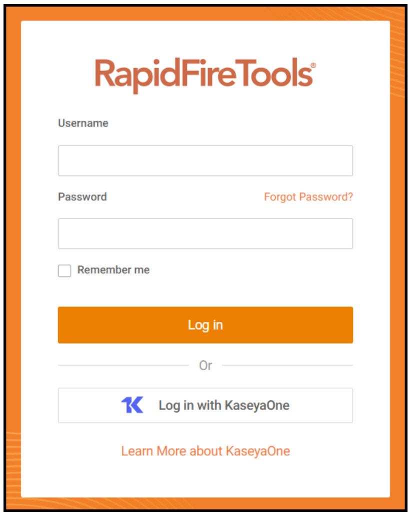
See the topics below for additional Cyber Hawk set up and help topics.

Set Up Portal Branding

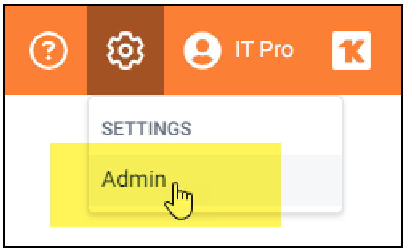
The RapidFire Tools Portal allows you to customize many elements to fit with your organization's brand and identity. This topic covers how you can modify the Portal's look and feel.

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.

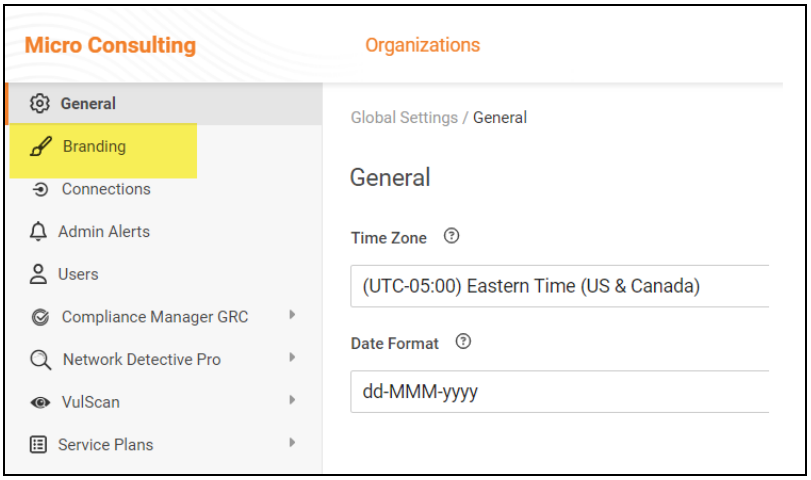


2. Click global **Settings (Admin)** ⚙ > **Users**.



3. Click **Branding**.

© 2024 RapidFire Tools, Inc. All rights reserved.



Global Settings / General

General

Time Zone: (UTC-05:00) Eastern Time (US & Canada)

Date Format: dd-MMM-yyyy

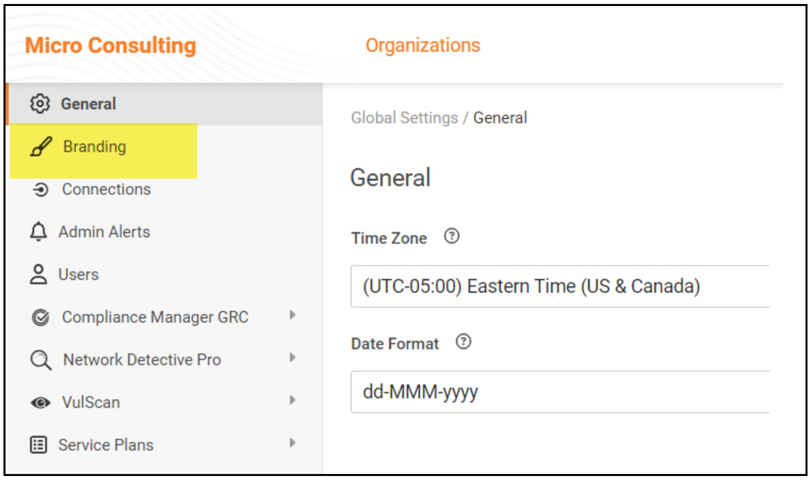
From this page, you can then:

- "Set Custom Portal Theme" below
- "Set Custom Portal Subdomain" on the facing page
- "Set Custom Company Name" on page 60
- "Set Custom Company Logo" on page 61

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.



Global Settings / General

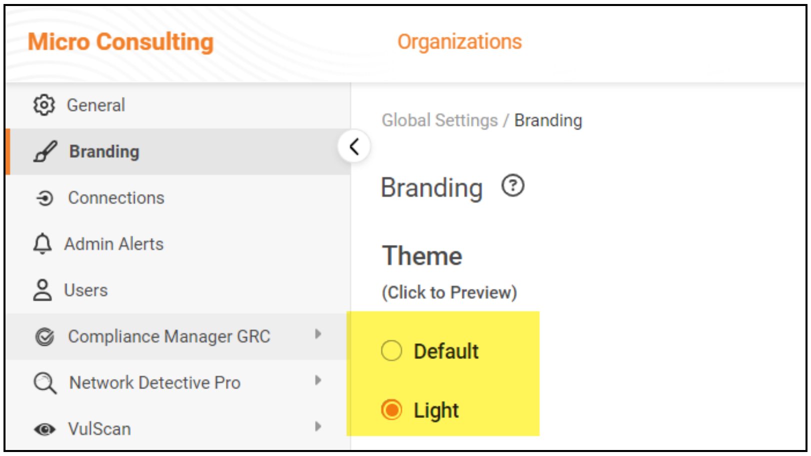
General

Time Zone: (UTC-05:00) Eastern Time (US & Canada)

Date Format: dd-MMM-yyyy

© 2024 RapidFire Tools, Inc. All rights reserved.

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



Global Settings / Branding

Branding

Theme

(Click to Preview)

○ Default

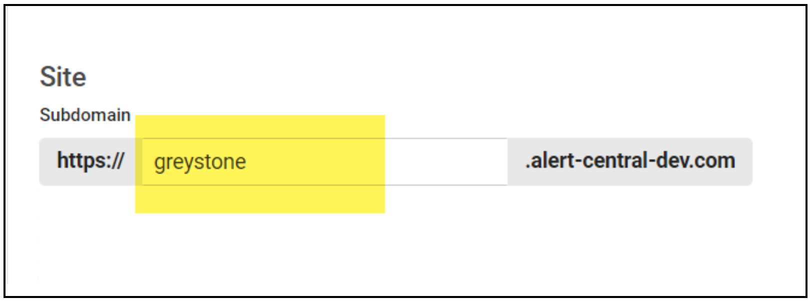
● Light

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

Set Custom Portal Subdomain

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

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



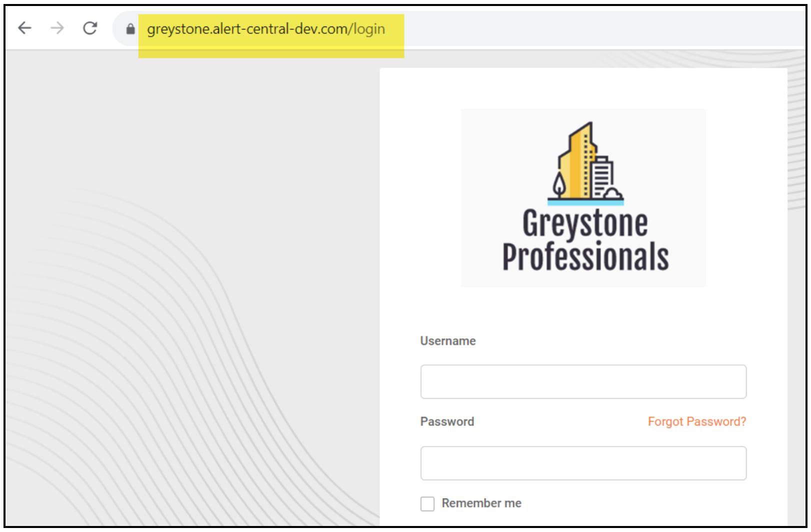
Site

Subdomain

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

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

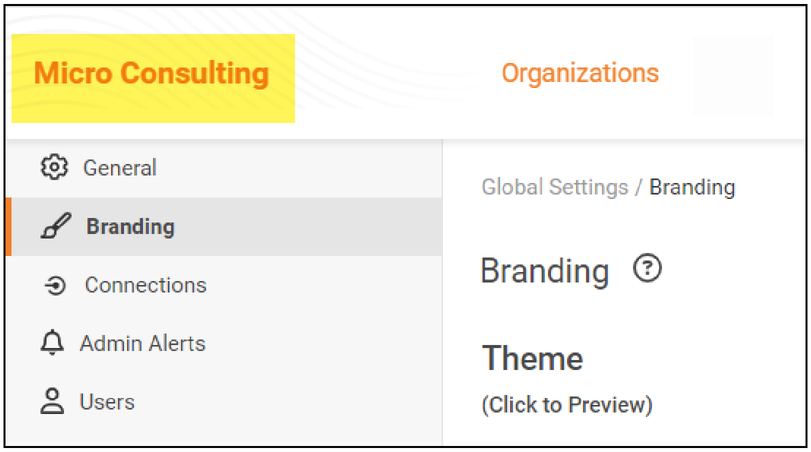
© 2024 RapidFire Tools, Inc. All rights reserved.



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.

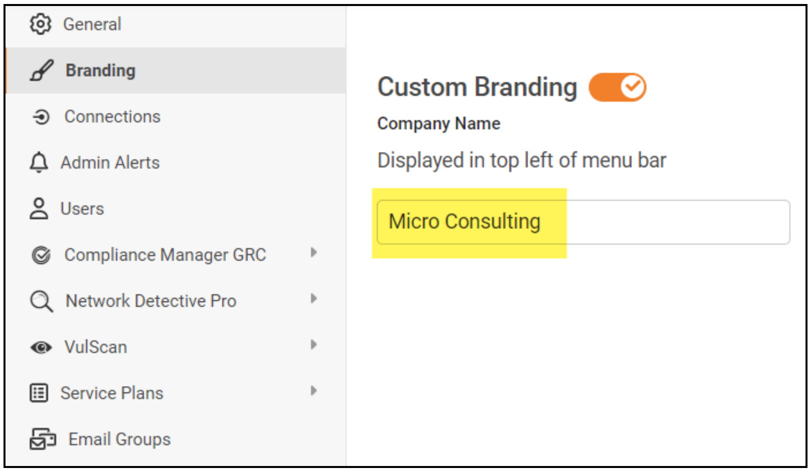
Set Custom Company Name

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.



Custom Branding

Company Name

Displayed in top left of menu bar

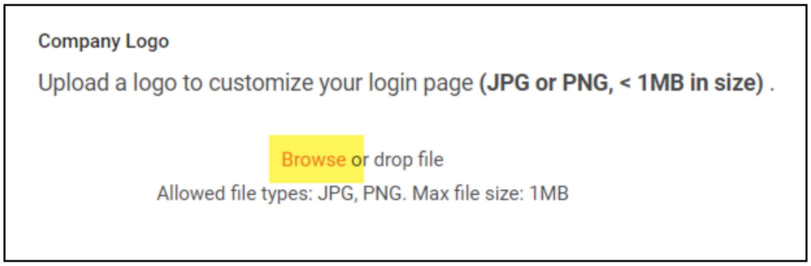
Micro Consulting

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.



Company Logo

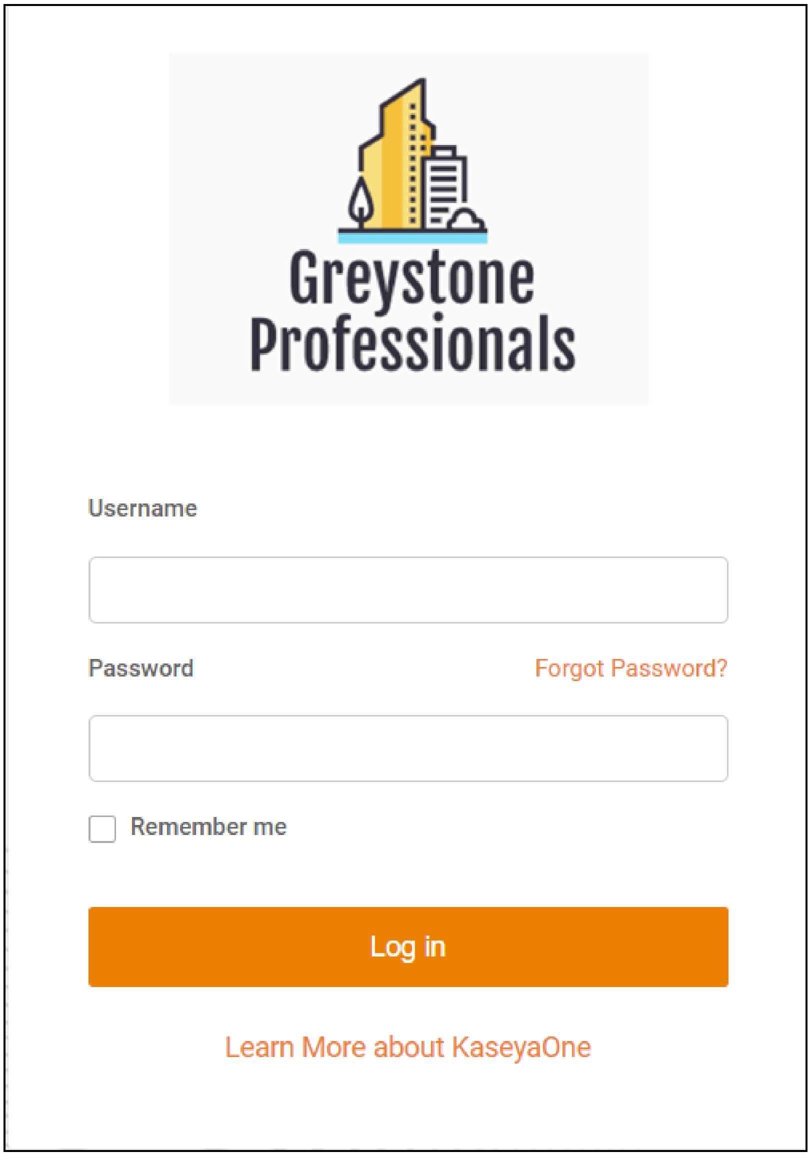
Upload a logo to customize your login page **(JPG or PNG, < 1MB in size)** .

Browse or drop file

Allowed file types: JPG, PNG. Max file size: 1MB

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

login screen.

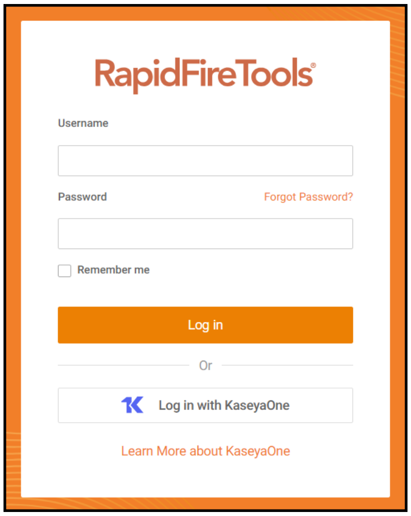


Set Up a Custom Subdomain to Access the RapidFire Tools Portal

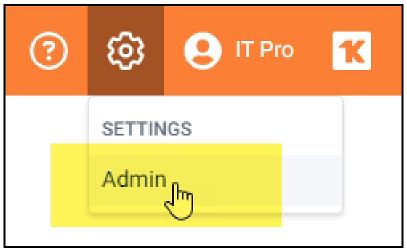
1. Visit https://www.youritportal.com and log into the RapidFire Tools Portal.

> **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.

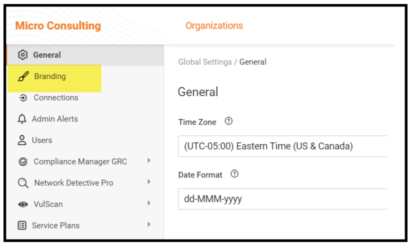
RapidFireTools® © 2024 RapidFire Tools, Inc. All rights reserved.



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



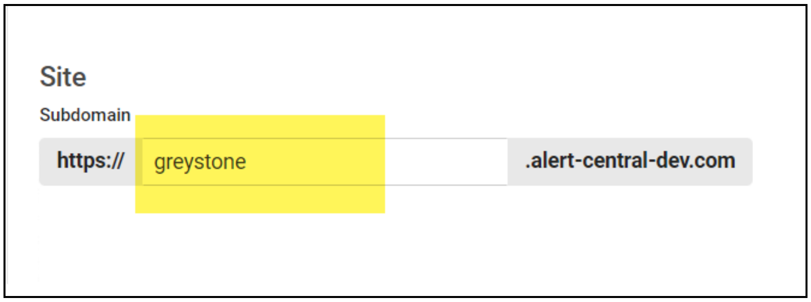
3. Click **Branding**.



Time Zone: (UTC-05:00) Eastern Time (US & Canada)

Date Format: dd-MMM-yyyy

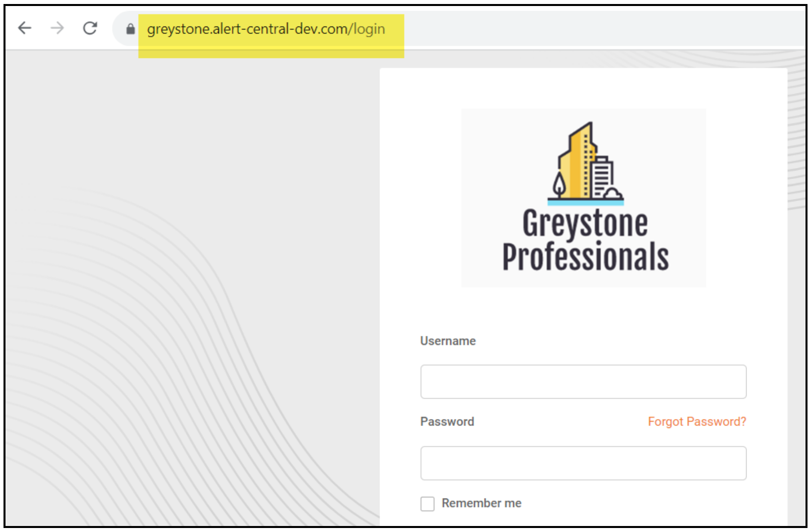
4. Enter the **Subdomain** name you desire in the Site Subdomain field.



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

© 2024 RapidFire Tools, Inc. All rights reserved.

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.



© 2024 RapidFire Tools, Inc. All rights reserved.

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

© 2024 RapidFire Tools, Inc. All rights reserved.

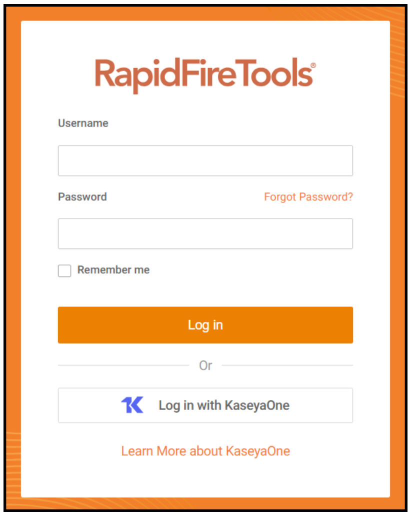
PSA System	PSA Prerequisites
Autotask® SOAP (Deprecated)	• Autotask API Username • Autotask API Password
REST ConnectWise™	• ConnectWise REST Public Key • ConnectWise REST Private Key • ConnectWise Company ID • ConnectWise PSA URL
SOAP ConnectWise™	• ConnectWise Username • ConnectWise Password • ConnectWise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

© 2024 RapidFire Tools, Inc. All rights reserved.

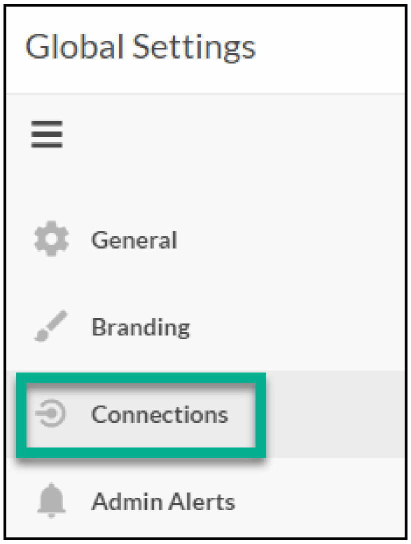
1. Visit https://www.youritportal.com and log into the RapidFire Tools Portal.



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

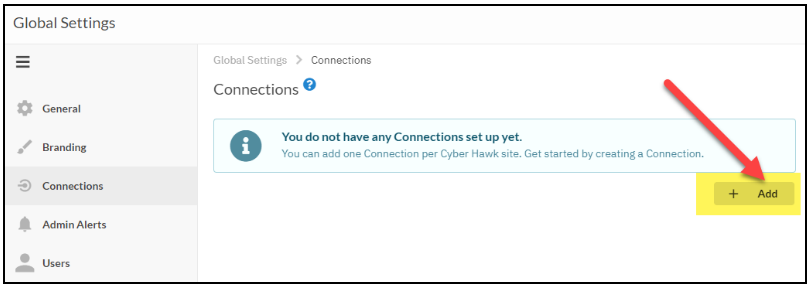
> **Note:** In order to configure the Global Settings in the Portal, you must be a global admin user.

3. Click **Connections**.



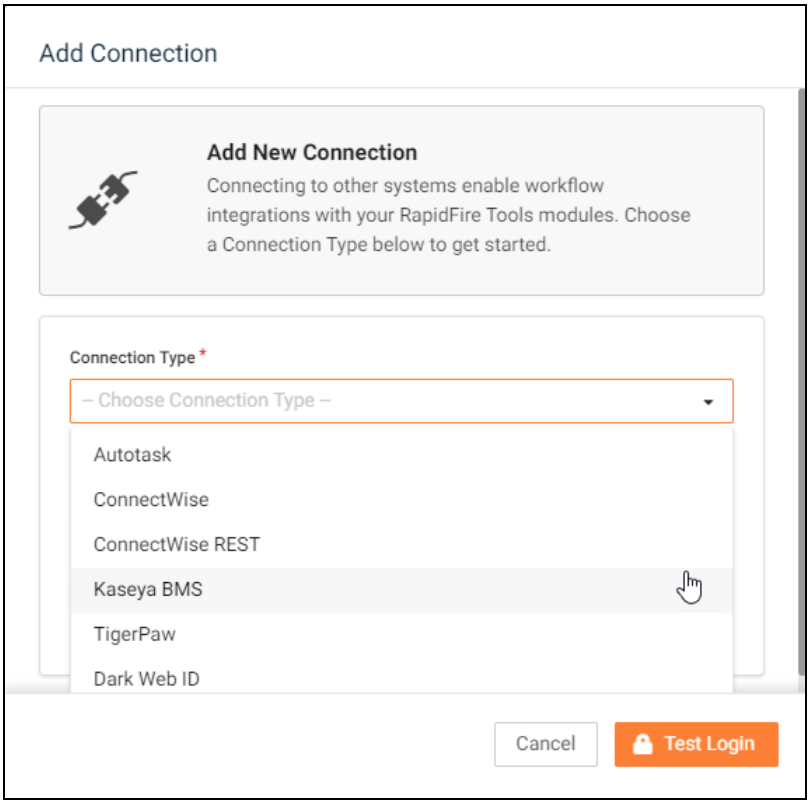
4. Click **Add** to create a new Ticketing System/PSA Connection.

© 2024 RapidFire Tools, Inc. All rights reserved.



You do not have any Connections set up yet.
You can add one Connection per Cyber Hawk site. Get started by creating a Connection.

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



Add New Connection

Connecting to other systems enable workflow integrations with your RapidFire Tools modules. Choose a Connection Type below to get started.

Connection Type *

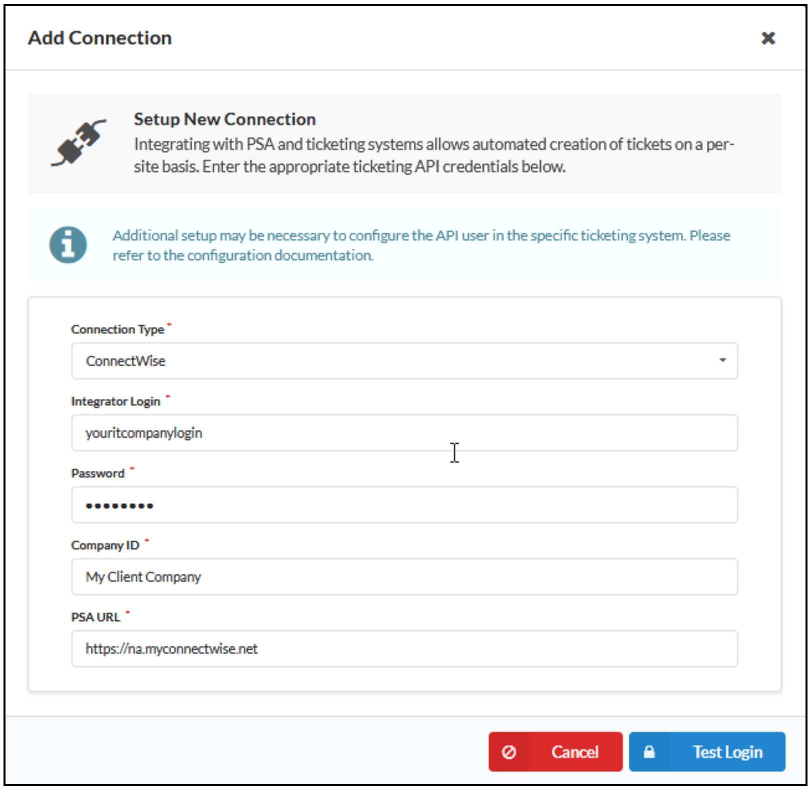
– Choose Connection Type –

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

© 2024 RapidFire Tools, Inc. All rights reserved.



Add Connection

Setup New Connection

Integrating with PSA and ticketing systems allows automated creation of tickets on a per-site basis. Enter the appropriate ticketing API credentials below.

Additional setup may be necessary to configure the API user in the specific ticketing system. Please refer to the configuration documentation.

Connection Type *: ConnectWise

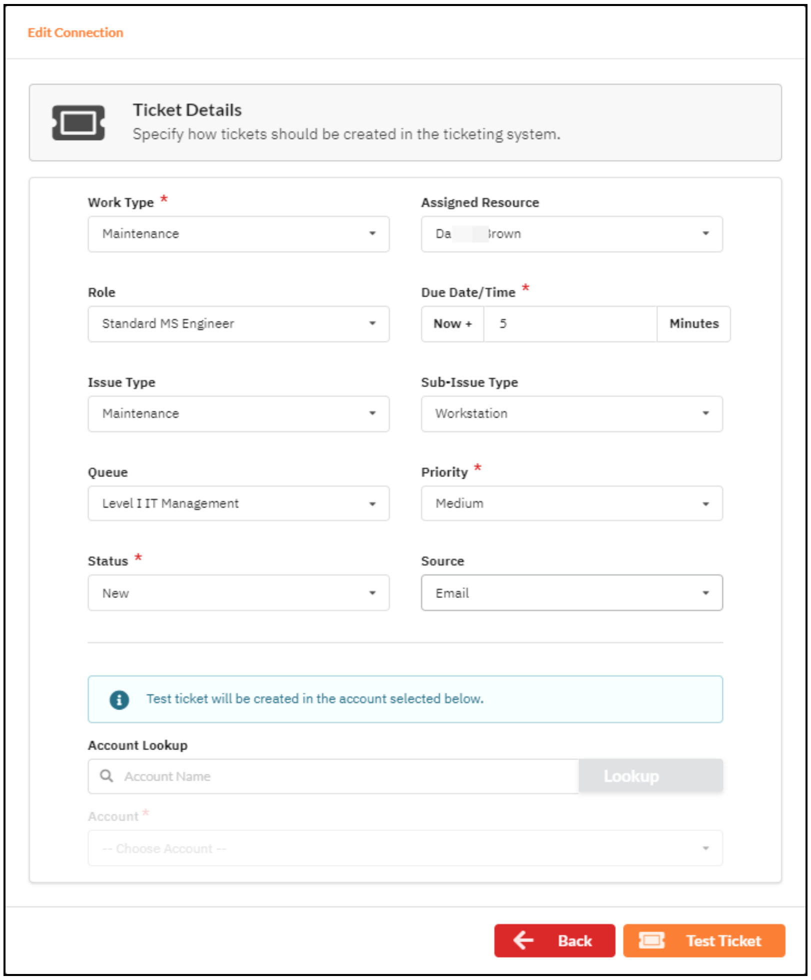
Integrator Login *: youritcompanylogin

Password *: ••••••••

Company ID *: My Client Company

PSA URL *: https://na.myconnectwise.net

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.



Edit Connection

Ticket Details

Specify how tickets should be created in the ticketing system.

Work Type * : Maintenance

Assigned Resource: Da[redacted]rown

Role: Standard MS Engineer

Due Date/Time * : Now + 5 Minutes

Issue Type: Maintenance

Sub-Issue Type: Workstation

Queue: Level I IT Management

Priority * : Medium

Status * : New

Source: Email

Test ticket will be created in the account selected below.

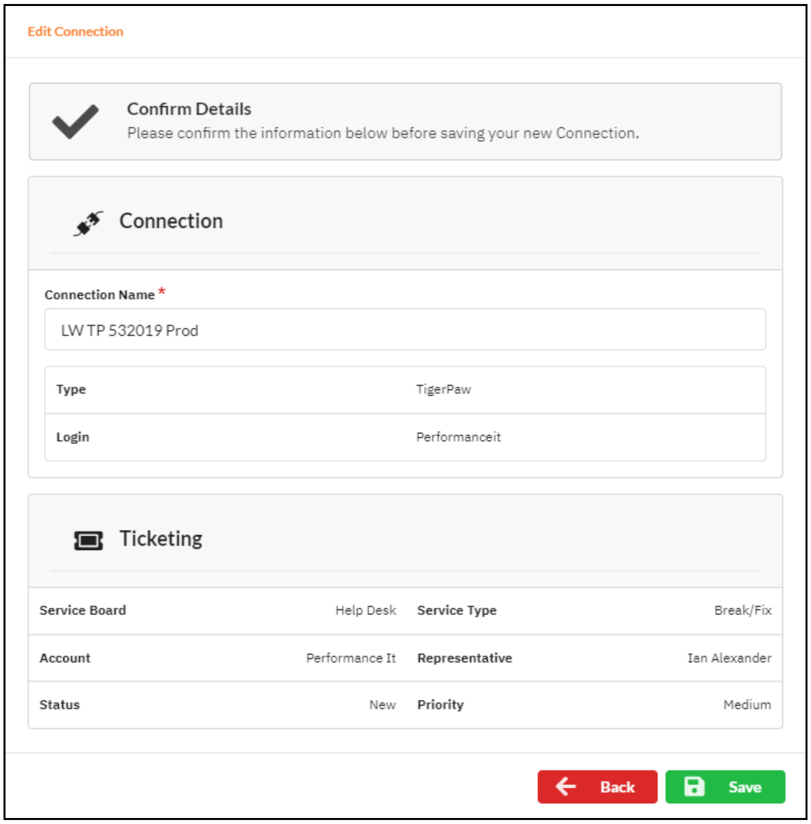
Account Lookup: Account Name

Account * : -- Choose Account --

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**.

© 2024 RapidFire Tools, Inc. All rights reserved.



Edit Connection

Confirm Details
Please confirm the information below before saving your new Connection.

Connection

Connection Name *

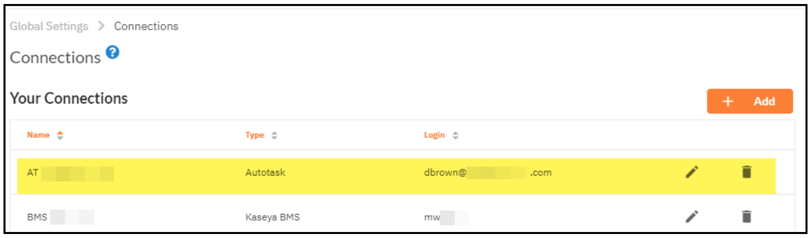
LW TP 532019 Prod

Type	TigerPaw
Login	Performanceit

Ticketing

Service Board	Help Desk	**Service Type**	Break/Fix
Account	Performance It	**Representative**	Ian Alexander
Status	New	**Priority**	Medium

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



Global Settings > Connections

Connections

Your Connections

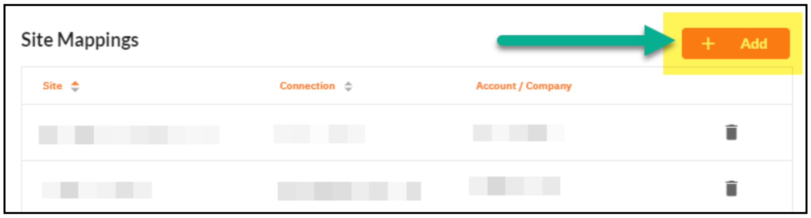
Name	Type	Login
AT [redacted]	Autotask	dbrown@[redacted].com
BMS [redacted]	Kaseya BMS	mw[redacted]

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

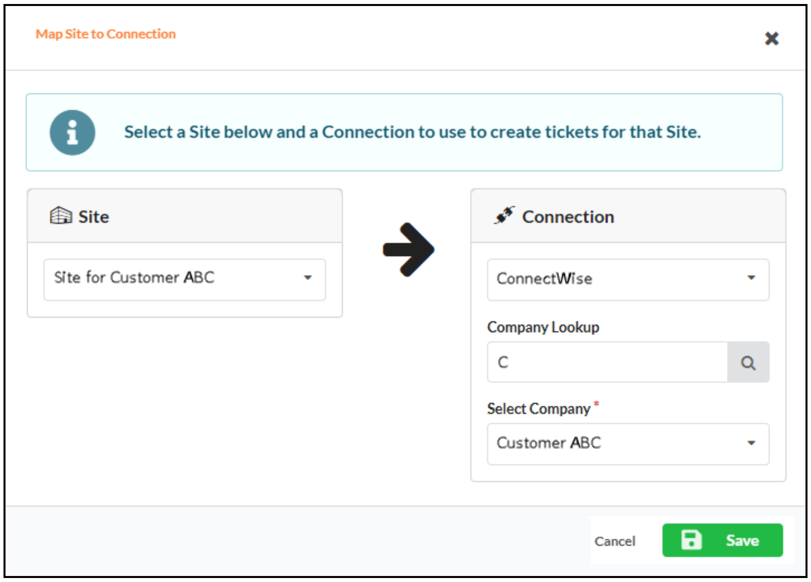
Follow these steps to map a Ticketing System/PSA Connection to the RapidFire Tools Portal Site associated with your site.

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

© 2024 RapidFire Tools, Inc. All rights reserved.



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



Select a Site below and a Connection to use to create tickets for that Site.

Site: Site for Customer ABC

Connection: ConnectWise

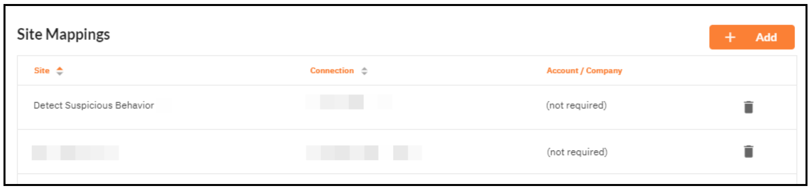
Company Lookup: C

Select Company *: Customer ABC

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.



Site	Connection	Account / Company
Detect Suspicious Behavior		(not required)
		(not required)

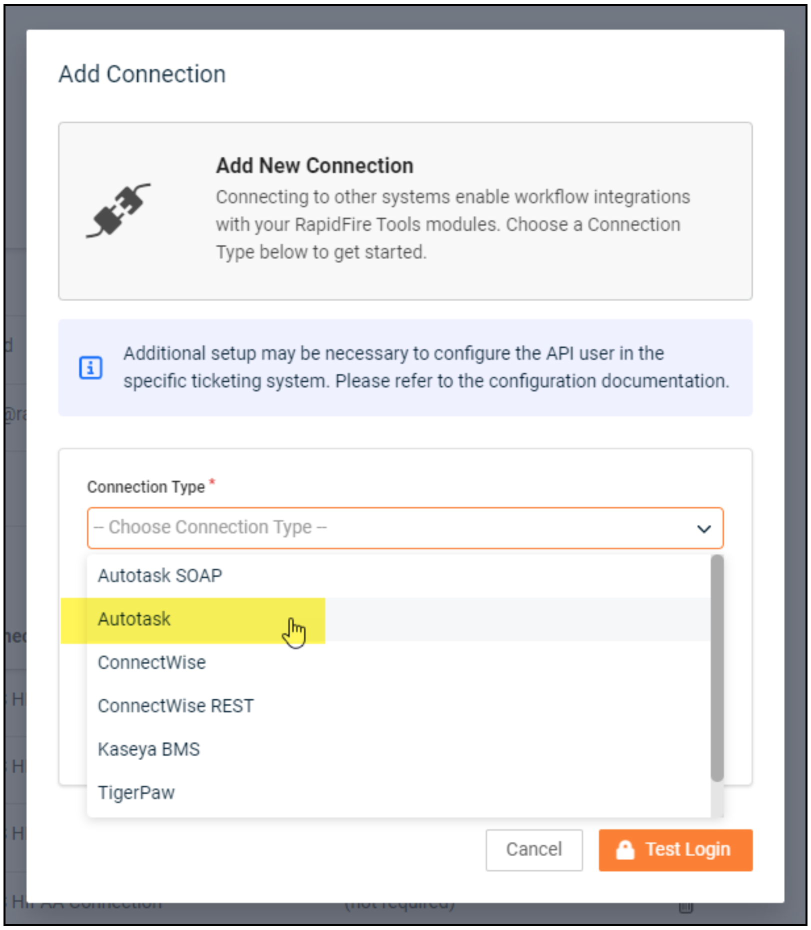
Your Portal account can now be used to create tickets for any Alerts or To Do items listed in the Portal for the RapidFire Tools Portal Site you selected.

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).



Add Connection

Add New Connection

Connecting to other systems enable workflow integrations with your RapidFire Tools modules. Choose a Connection Type below to get started.

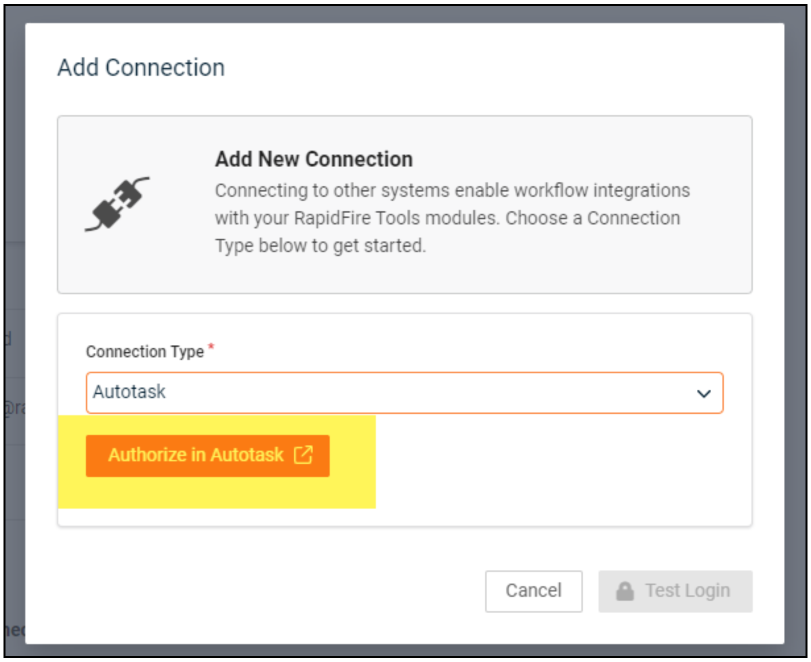
Additional setup may be necessary to configure the API user in the specific ticketing system. Please refer to the configuration documentation.

Connection Type *

-- Choose Connection Type --

© 2024 RapidFire Tools, Inc. All rights reserved.

4. Click **Authenticate in Autotask**.



Add Connection

Add New Connection

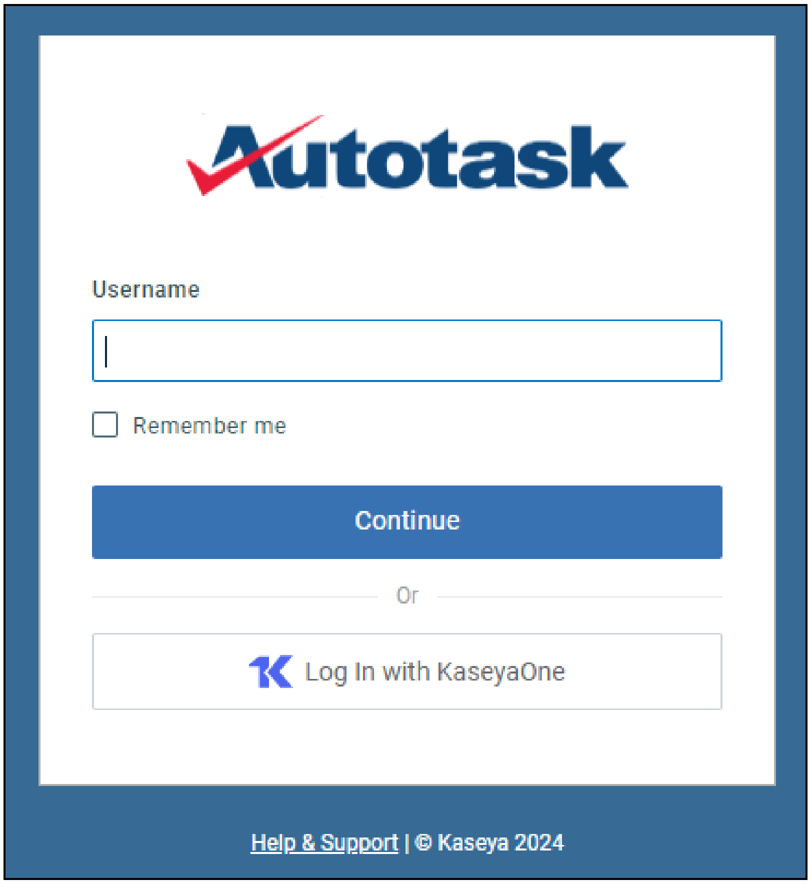
Connecting to other systems enable workflow integrations with your RapidFire Tools modules. Choose a Connection Type below to get started.

Connection Type *

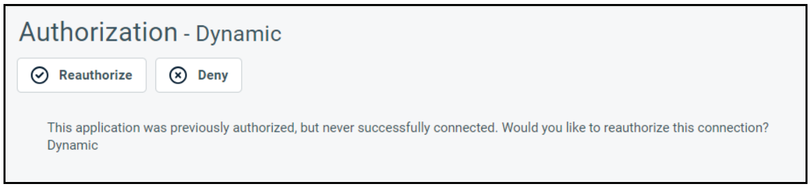
Autotask

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.

© 2024 RapidFire Tools, Inc. All rights reserved.



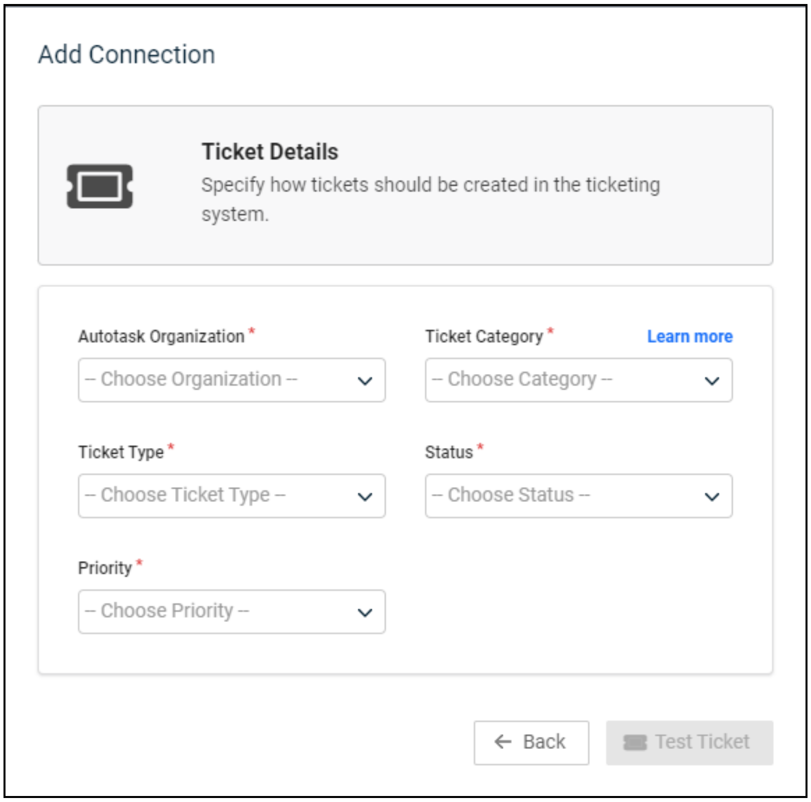
6. If promoted, click **Reauthorize** to create the connection.



This application was previously authorized, but never successfully connected. Would you like to reauthorize this connection?
Dynamic

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**.

© 2024 RapidFire Tools, Inc. All rights reserved.



Add Connection

Ticket Details

Specify how tickets should be created in the ticketing system.

Autotask Organization * -- Choose Organization --

Ticket Category * -- Choose Category --

Ticket Type * -- Choose Ticket Type --

Status * -- Choose Status --

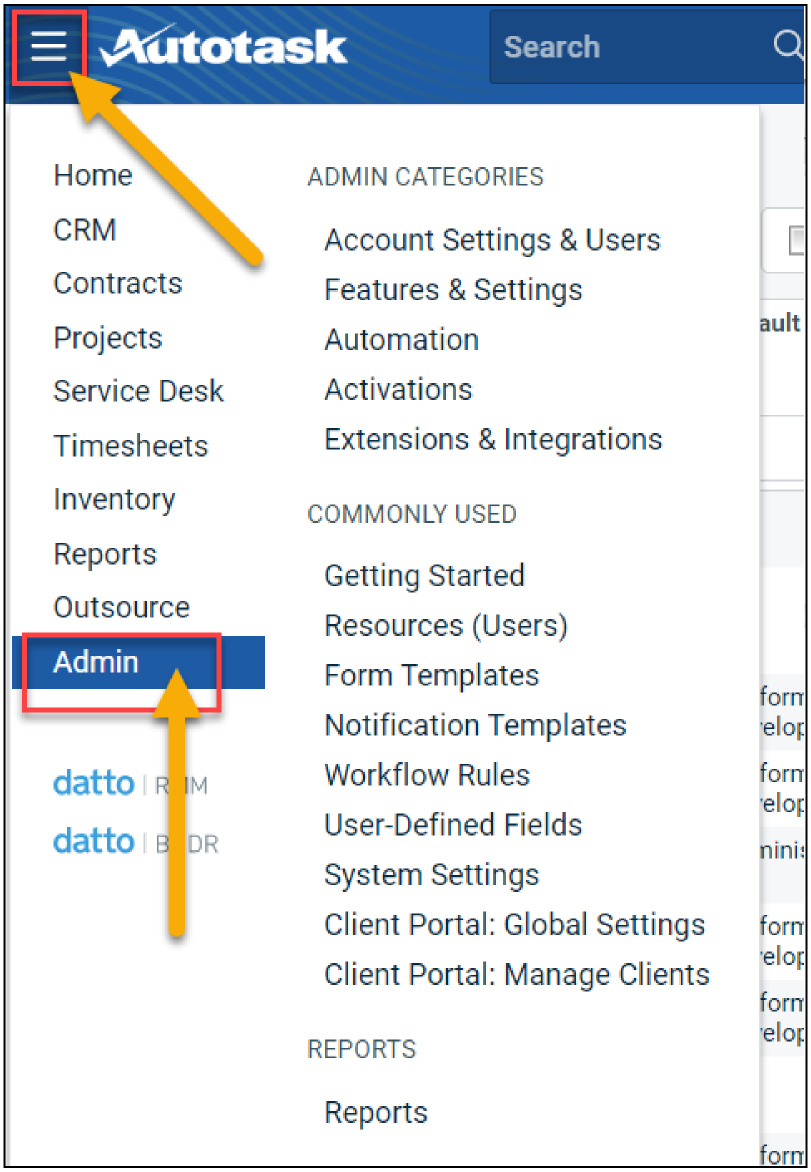
Priority * -- Choose Priority --

© 2024 RapidFire Tools, Inc. All rights reserved.

Set Up Autotask (SOAP) Integration

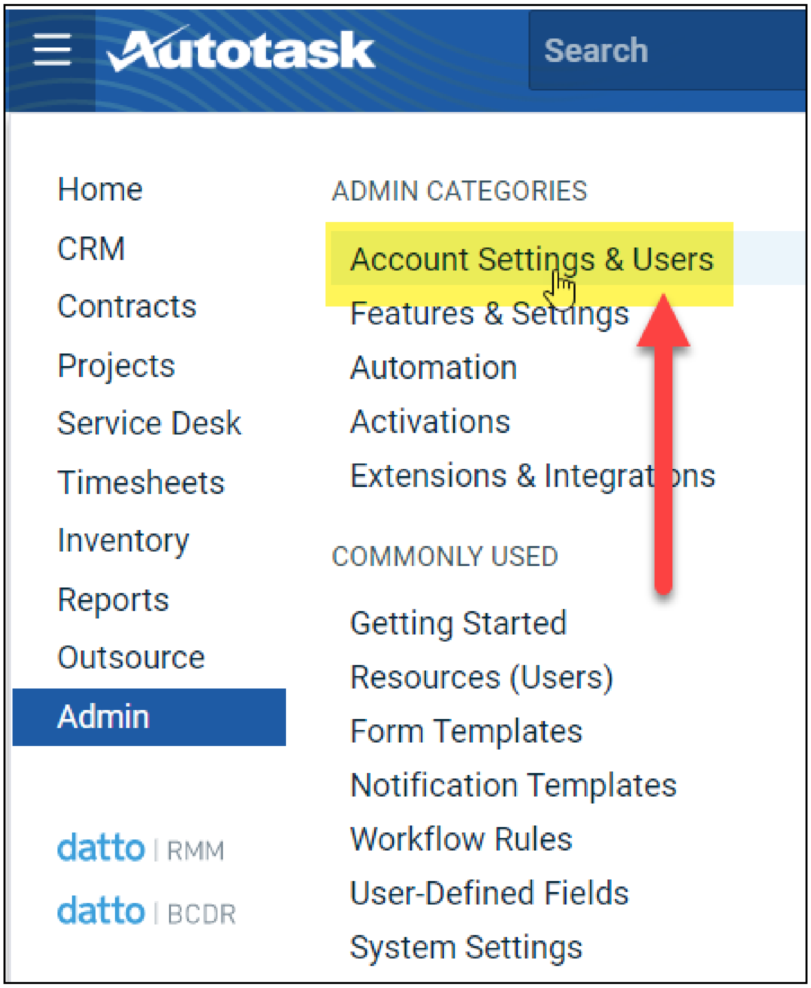
To set up a connection with the Autotask (SOAP) system, you will need to **create an API User in Autotask**. To do this:

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

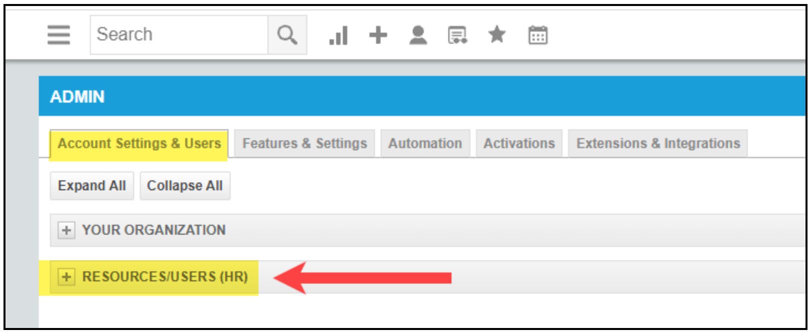


3. From the **Admin** menu, click **Account Settings & Users**.

© 2024 RapidFire Tools, Inc. All rights reserved.

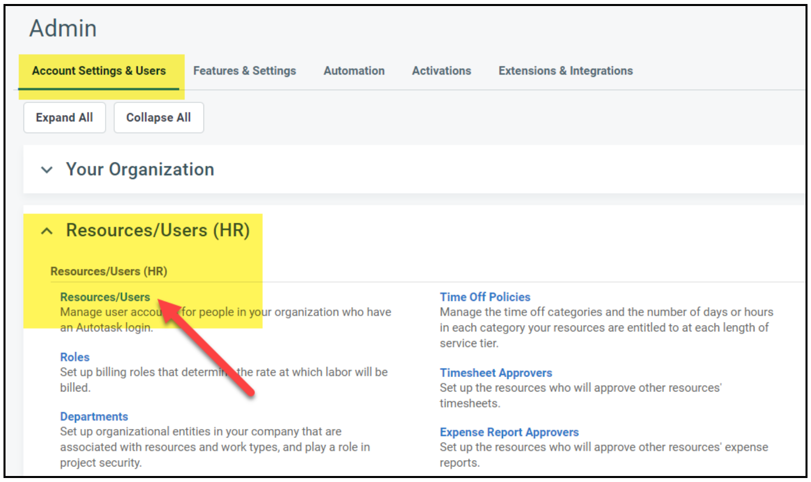


4. Next, click **Resources/Users (HR)** to expand the menu.



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

© 2024 RapidFire Tools, Inc. All rights reserved.



Admin

Your Organization

Resources/Users (HR)

Resources/Users (HR)

Resources/Users
Manage user accounts for people in your organization who have an Autotask login.

Roles
Set up billing roles that determine the rate at which labor will be billed.

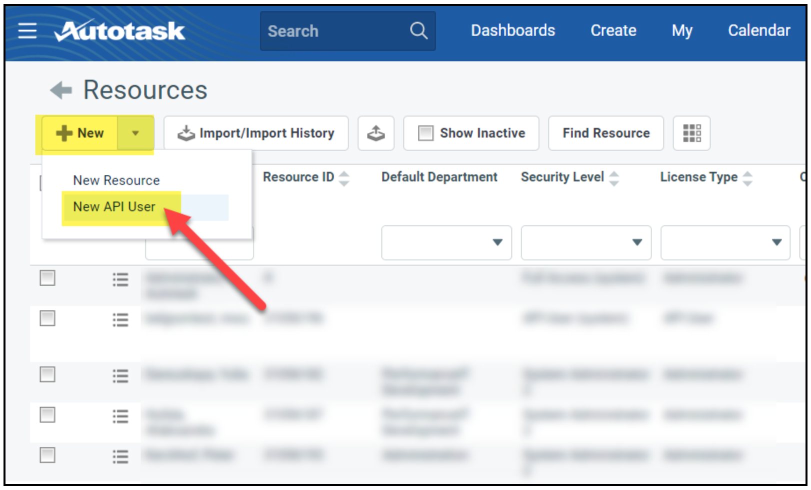
Departments
Set up organizational entities in your company that are associated with resources and work types, and play a role in project security.

Time Off Policies
Manage the time off categories and the number of days or hours in each category your resources are entitled to at each length of service tier.

Timesheet Approvers
Set up the resources who will approve other resources' timesheets.

Expense Report Approvers
Set up the resources who will approve other resources' expense reports.

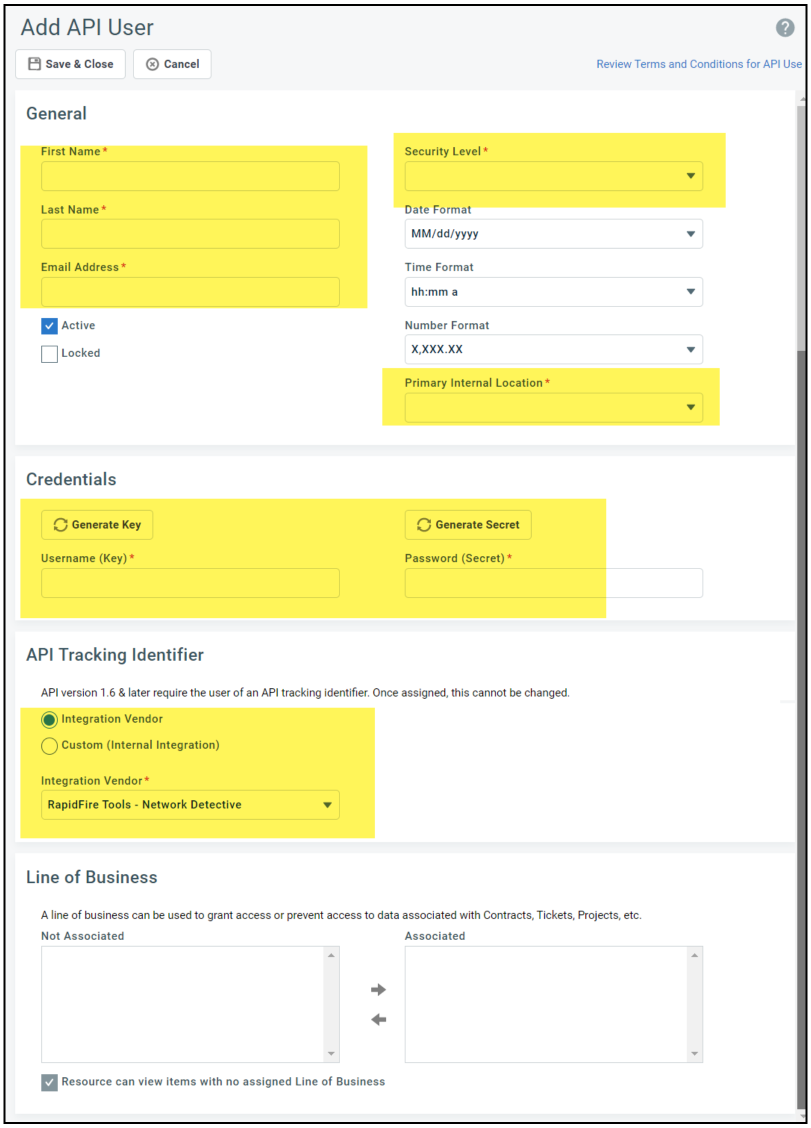
6. Hover your mouse over the drop-down menu to the right of the **New** button, then select **New API User**.



Resources

[redacted]

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



General

First Name*

Last Name*

Email Address*

☑ Active

□ Locked

Security Level*

Date Format: MM/dd/yyyy

Time Format: hh:mm a

Number Format: X,XXX.XX

Primary Internal Location*

Credentials

Username (Key)*

Password (Secret)*

API Tracking Identifier

API version 1.6 & later require the user of an API tracking identifier. Once assigned, this cannot be changed.

● Integration Vendor

○ Custom (Internal Integration)

Integration Vendor*: RapidFire Tools - Network Detective

Line of Business

A line of business can be used to grant access or prevent access to data associated with Contracts, Tickets, Projects, etc.

Not Associated

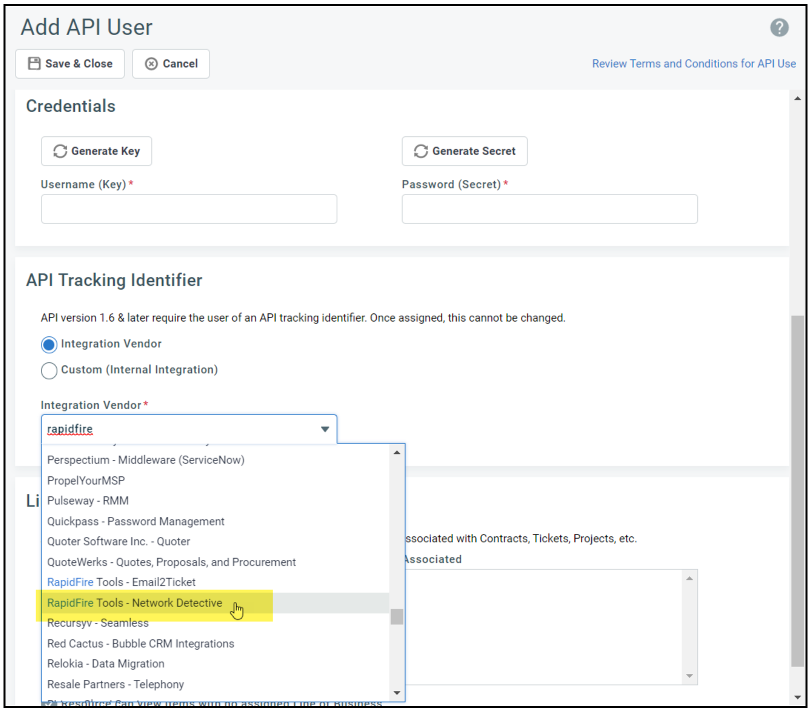
Associated

☑ Resource can view items with no assigned Line of Business

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

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

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



Credentials

Username (Key) *

Password (Secret) *

API Tracking Identifier

API version 1.6 & later require the user of an API tracking identifier. Once assigned, this cannot be changed.

● Integration Vendor

○ Custom (Internal Integration)

Integration Vendor *

rapidfire

Perspectium - Middleware (ServiceNow)
PropelYourMSP
Pulseway - RMM
Quickpass - Password Management
Quoter Software Inc. - Quoter
QuoteWerks - Quotes, Proposals, and Procurement
RapidFire Tools - Email2Ticket
RapidFire Tools - Network Detective
Recursyv - Seamless
Red Cactus - Bubble CRM Integrations
Relokia - Data Migration
Resale Partners - Telephony

Li

ssociated with Contracts, Tickets, Projects, etc.

Associated

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

© 2024 RapidFire Tools, Inc. All rights reserved.

Set Up ConnectWise REST Integration

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

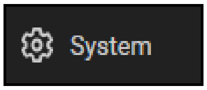
Step 1 — Download and Install the ConnectWise Manage Internet Client Application

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

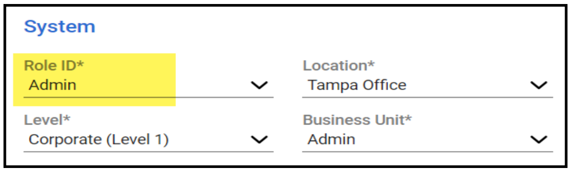
1. From the ConnectWise dashboard, click **System** from the side menu.



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**.



System

Role ID*: Admin

Location*: Tampa Office

Level*: Corporate (Level 1)

Business Unit*: Admin

© 2024 RapidFire Tools, Inc. All rights reserved.

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.

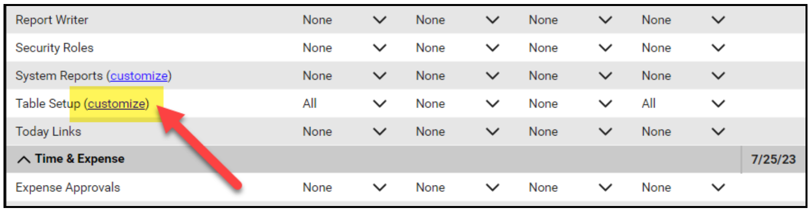
Module		Add Level	Edit Level	Delete Level	Inquire Level
Companies					
	Company Maintenance				All
	Configurations	All	All		All
	Contacts	All	All		All
Service Desk					
	Service Tickets	All	All		All
System					
	API Reports				All
	Table Setup* *Customized Table Setup: Allow Company / Company Status,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

© 2024 RapidFire Tools, Inc. All rights reserved.

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)				

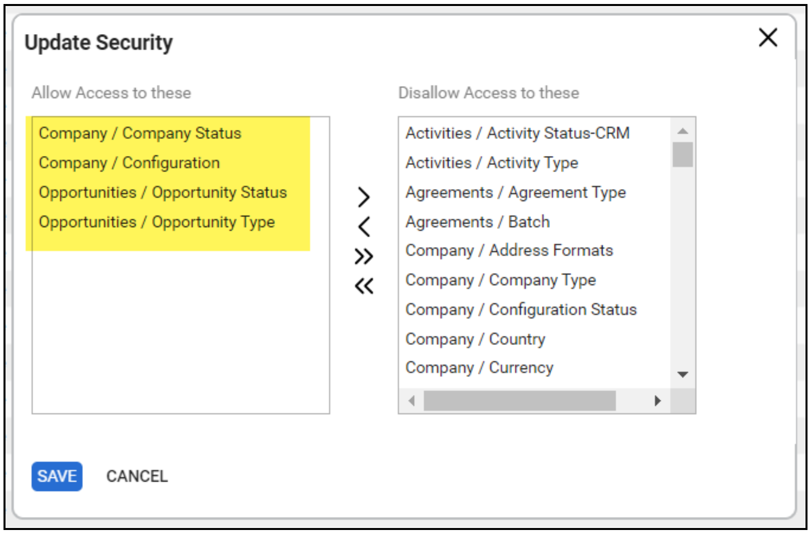
Table Setup Configuration

From Table Setup, click **customize**.



Report Writer	None	None	None	None
Security Roles	None	None	None	None
System Reports (customize)	None	None	None	None
Table Setup (customize)	All	None	None	All
Today Links	None	None	None	None
Time & Expense				7/25/23
Expense Approvals	None	None	None	None

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



Update Security

Allow Access to these

- Company / Company Status
- Company / Configuration
- Opportunities / Opportunity Status
- Opportunities / Opportunity Type

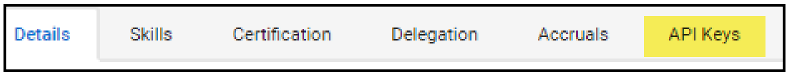
Disallow Access to these

- Activities / Activity Status-CRM
- Activities / Activity Type
- Agreements / Agreement Type
- Agreements / Batch
- Company / Address Formats
- Company / Company Type
- Company / Configuration Status
- Company / Country
- Company / Currency

© 2024 RapidFire Tools, Inc. All rights reserved.

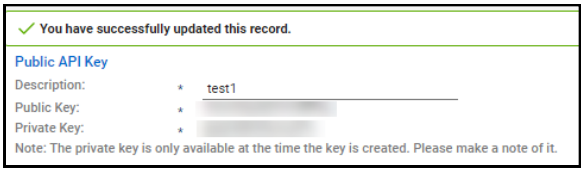
Step 3 — Create an API Key in the ConnectWise Ticketing System

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



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

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



✓ You have successfully updated this record.

Public API Key

Description: * test1

Public Key: * [redacted]

Private Key: * [redacted]

Note: The private key is only available at the time the key is created. Please make a note of it.

Step 4 — Configure Service Tables in ConnectWise

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

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

1. **Service Board**

© 2024 RapidFire Tools, Inc. All rights reserved.

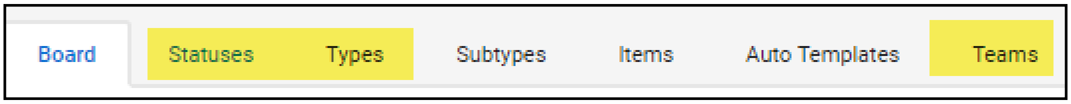
You must have a Service Board created within ConnectWise. In addition, within the Service Board, you must create values for the following fields. You can create values for these fields from the Service Board page:

a. **Statuses**

b. **Types**

c. **Teams**

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



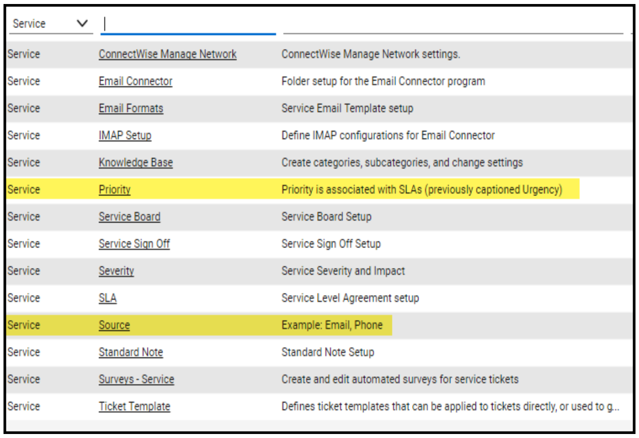
In addition, you must define values for two additional Service Tables:

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.

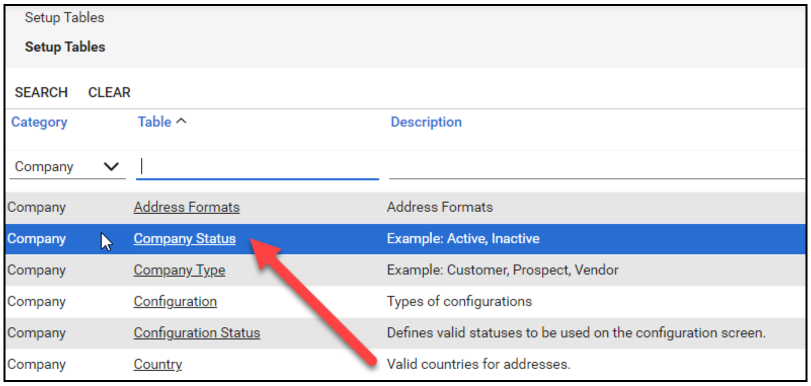
© 2024 RapidFire Tools, Inc. All rights reserved.

Step 5 — Remove "Disallow Saving" Flag from Company

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

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

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



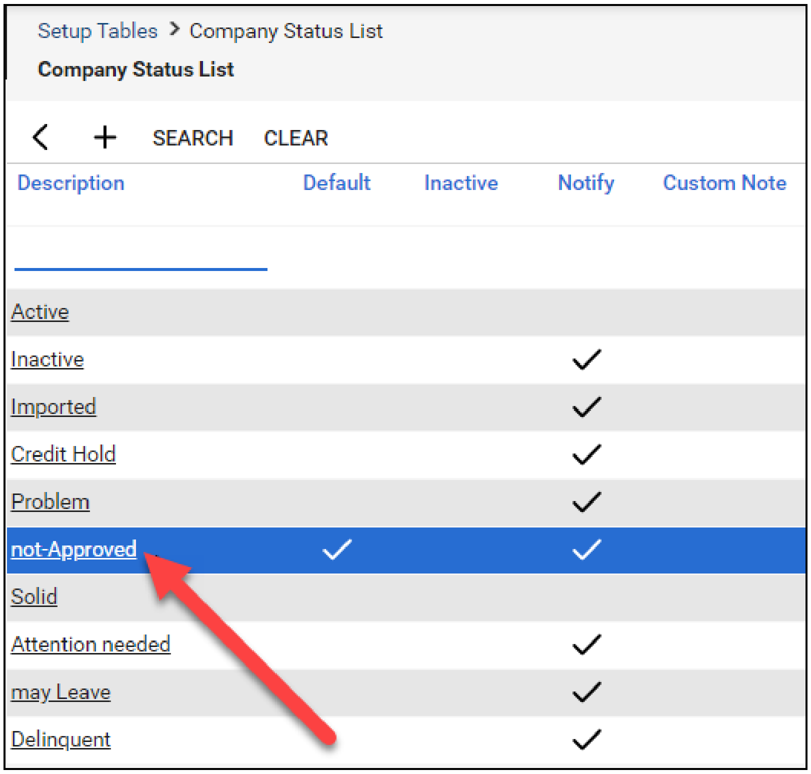
Setup Tables

Setup Tables

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

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

© 2024 RapidFire Tools, Inc. All rights reserved.

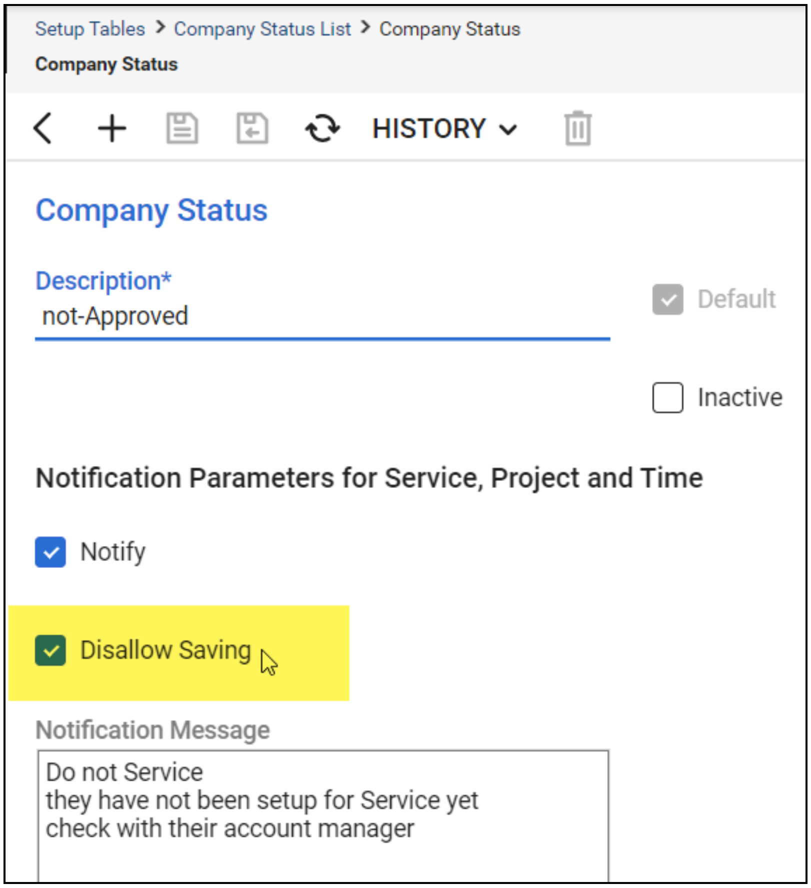


Setup Tables > Company Status List

Company Status List

Description	Default	Inactive	Notify	Custom Note
Active				
Inactive			✓	
Imported			✓	
Credit Hold			✓	
Problem			✓	
not-Approved	✓		✓	
Solid				
Attention needed			✓	
may Leave			✓	
Delinquent			✓	

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



Company Status

Description*: not-Approved

☑ Default

□ Inactive

Notification Parameters for Service, Project and Time

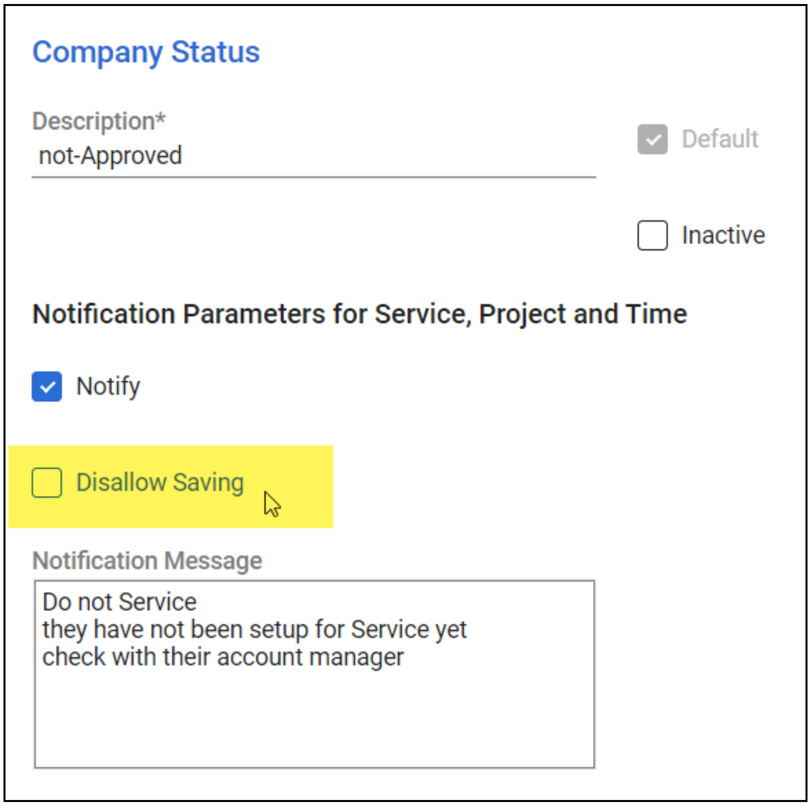
☑ Notify

☑ Disallow Saving

Notification Message

Do not Service
they have not been setup for Service yet
check with their account manager

© 2024 RapidFire Tools, Inc. All rights reserved.



Company Status

Description*
not-Approved

☑ Default

□ Inactive

Notification Parameters for Service, Project and Time

☑ Notify

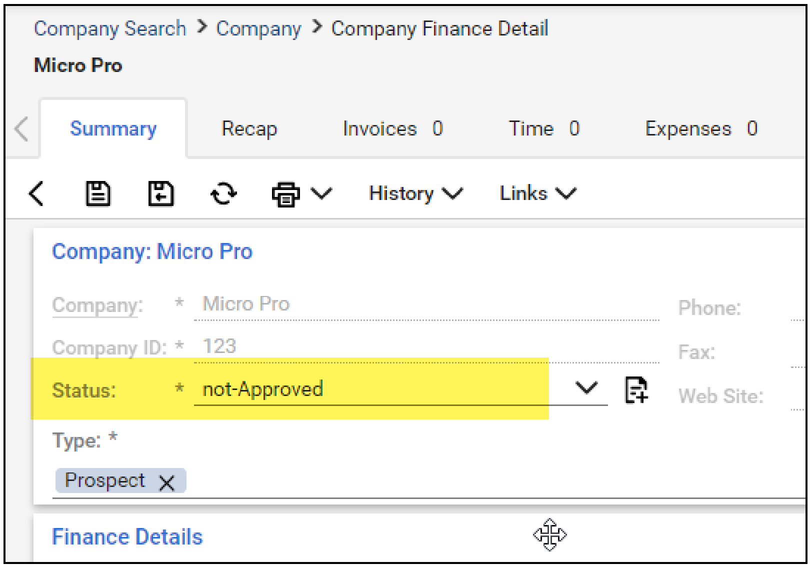
□ Disallow Saving

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.

© 2024 RapidFire Tools, Inc. All rights reserved.



Company Search > Company > Company Finance Detail

Micro Pro

Company: Micro Pro

Company: * Micro Pro

Company ID: * 123

Status: * not-Approved

Type: *

Prospect

Phone:

Fax:

Web Site:

Finance Details

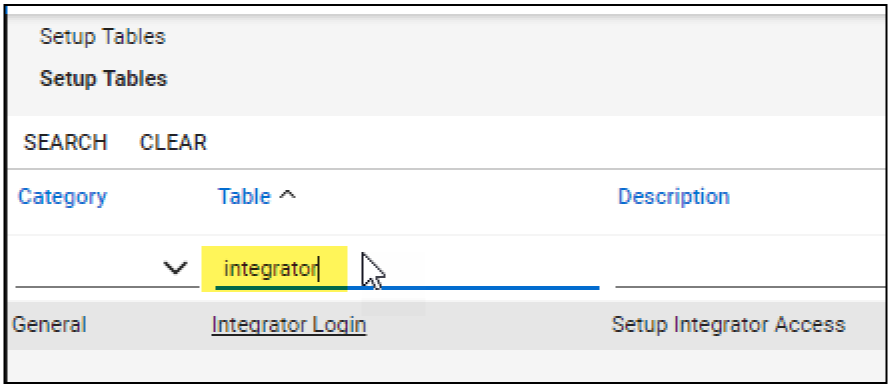
Set Up ConnectWise SOAP Integration

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.



Setup Tables

Setup Tables

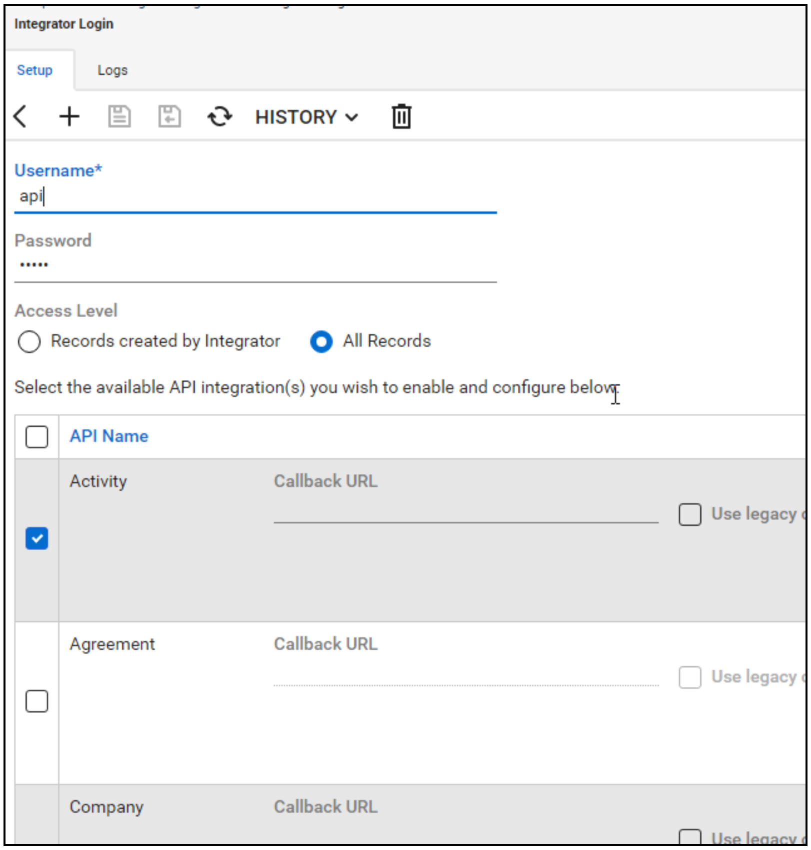
SEARCH CLEAR

Category	Table ^	Description
	integrator	
General	Integrator Login	Setup Integrator Access

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

© 2024 RapidFire Tools, Inc. All rights reserved.

- MemberApi
- ReportingApi
- SystemApi
- ConfigurationApi



Username*
api

Password
•••••

Access Level
○ Records created by Integrator ● All Records

Select the available API integration(s) you wish to enable and configure below

□	API Name		
☑	Activity	Callback URL	□ Use legacy
□	Agreement	Callback URL	□ Use legacy
	Company	Callback URL	□ Use legacy

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

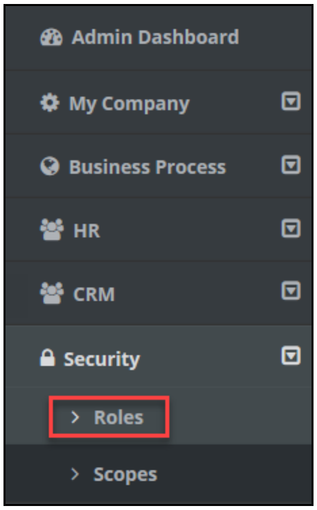
> **Note:** If you already have an Integrator Login configured, you may use it as long as the Company and Configuration APIs are enabled.)

© 2024 RapidFire Tools, Inc. All rights reserved.

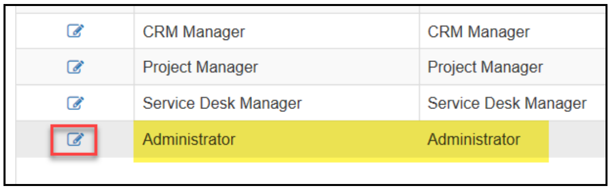
Set Up Kaseya BMS Integration

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**.

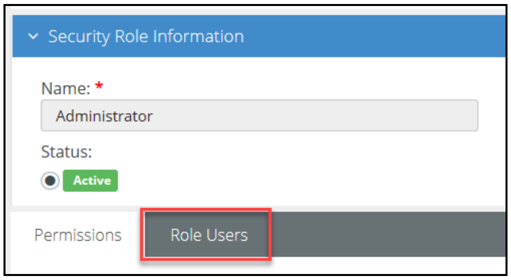


3. Click **Open/Edit** on the Administrator Role.



✎	CRM Manager	CRM Manager
✎	Project Manager	Project Manager
✎	Service Desk Manager	Service Desk Manager
✎	Administrator	Administrator

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



Name: *
Administrator

Status:
● Active

5. Click **Add**.

© 2024 RapidFire Tools, Inc. All rights reserved.

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.

© 2024 RapidFire Tools, Inc. All rights reserved.

Create Global Service Plans for Cyber Hawk

Service Plans contain a set of Security Policies that Cyber Hawk can detect and alert upon at a Site. You can also configure how Cyber Hawk will respond to each individual Security Policy (like emailing the Tech Group or creating a ticket) and save this as part of your plan.

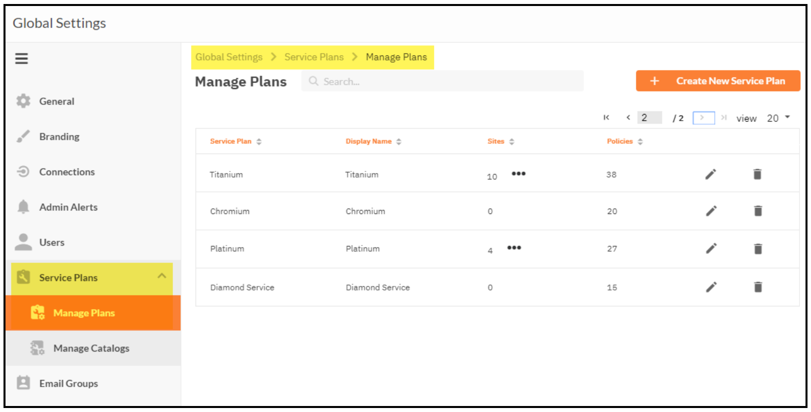
Note: You can think of Service Plans as the "tiers" of Security Services you can offer your clients depending on their needs (think Bronze, Silver, Gold, etc.). You can even create *Service Catalogs* to show clients your service offerings in an easy-to-read chart (see "Create Service Catalogs" on page 200).

From global **Settings (Admin)** ⚙ > **Service Plans** > **Manage Plans**, you can create a new Service Plan or modify one of the existing "out of the box" plans. You can then quickly apply this Service Plan to each of your Cyber Hawk Sites during the set up process.

Important: When you update a Service Plan at the global level, Policy changes will carry over to the Sites using the Service Plan. The only exception to this is if the Site is using a "Modified" or edited version of a Service Plan.

This topic covers how to create a new Service Plan from scratch:

1. First, in the RapidFire Tools Portal, go to global **Settings (Admin)** ⚙ > **Service Plans** > **Manage Plans**.

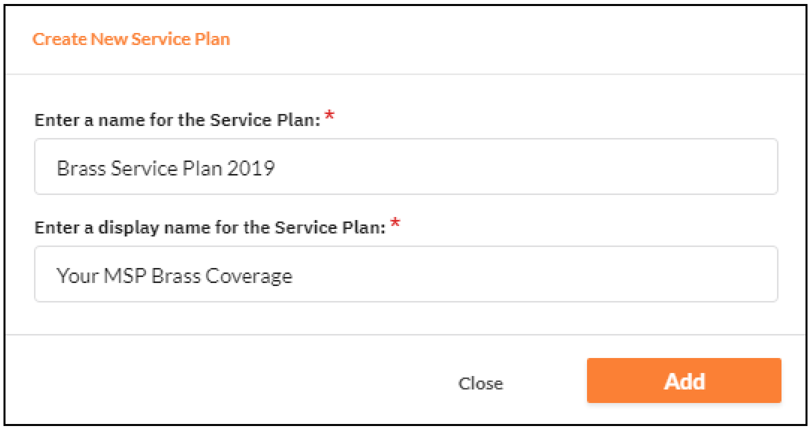


Service Plan	Display Name	Sites	Policies
Titanium	Titanium	10 •••	38
Chromium	Chromium	0	20
Platinum	Platinum	4 •••	27
Diamond Service	Diamond Service	0	15

2. Click **Create New Service Plan**.
3. Enter a name and display name for the Service Plan. Click **Add**.

© 2024 RapidFire Tools, Inc. All rights reserved.

Note: The *Display Name* is what appears when you apply the plan to a Site or include it in a Catalog for clients to view.



Create New Service Plan

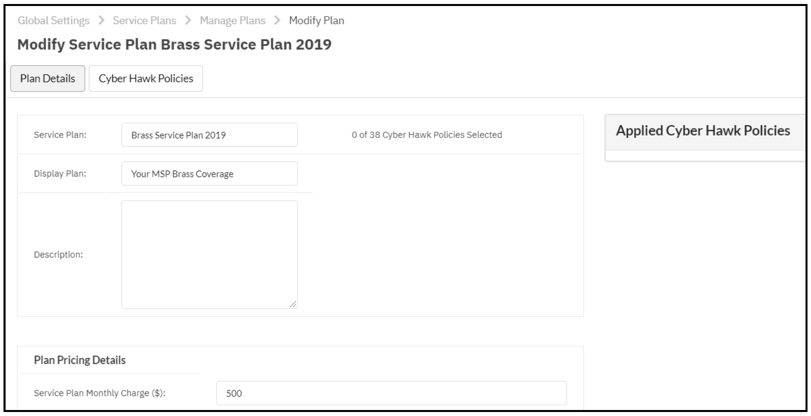
Enter a name for the Service Plan: *

Brass Service Plan 2019

Enter a display name for the Service Plan: *

Your MSP Brass Coverage

4. The Modify Service Plan window will appear. Enter basic information about the Service Plan, such as a short Description and Plan Pricing Details.



Global Settings > Service Plans > Manage Plans > Modify Plan

Modify Service Plan Brass Service Plan 2019

Plan Details
Cyber Hawk Policies

Service Plan: Brass Service Plan 2019

0 of 38 Cyber Hawk Policies Selected

Applied Cyber Hawk Policies

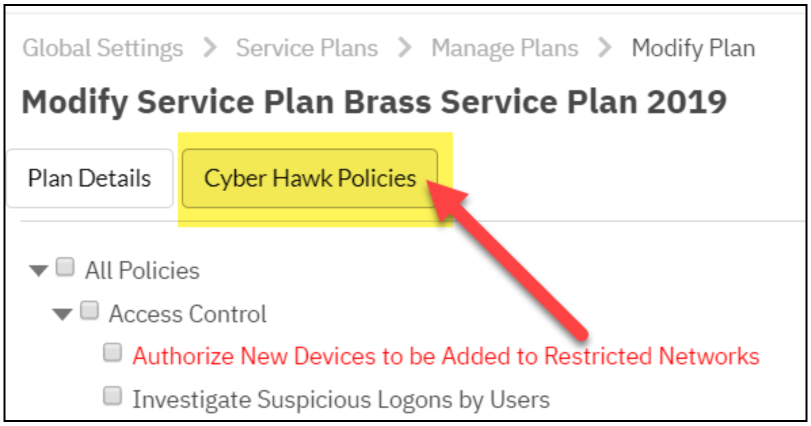
Display Plan: Your MSP Brass Coverage

Description:

Plan Pricing Details

Service Plan Monthly Charge ($): 500

5. Next, click on the Cyber Hawk Policies tab.



Global Settings > Service Plans > Manage Plans > Modify Plan

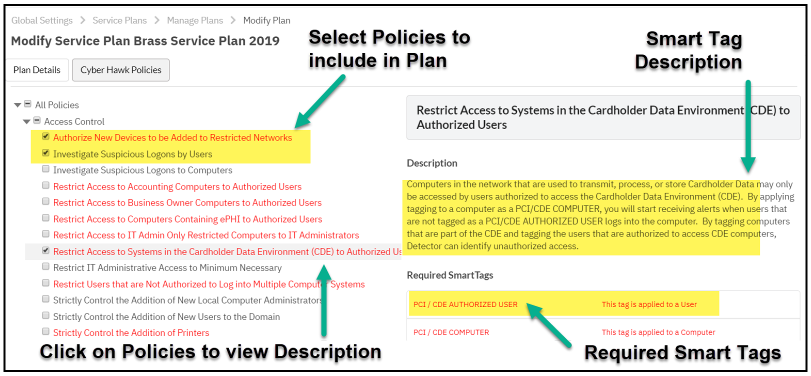
Modify Service Plan Brass Service Plan 2019

Plan Details
Cyber Hawk Policies

- ☐ All Policies
  - ☐ Access Control
    - ☐ Authorize New Devices to be Added to Restricted Networks
    - ☐ Investigate Suspicious Logons by Users

© 2024 RapidFire Tools, Inc. All rights reserved.

Here you can see all of the available Security Policies that Cyber Hawk can detect and alert upon within the Site's network.



Global Settings > Service Plans > Manage Plans > Modify Plan

Modify Service Plan Brass Service Plan 2019

Plan Details | Cyber Hawk Policies

- All Policies
  - Access Control
    - ☑ Authorize New Devices to be Added to Restricted Networks
    - ☑ Investigate Suspicious Logons by Users
    - □ Investigate Suspicious Logons to Computers
    - □ Restrict Access to Accounting Computers to Authorized Users
    - □ Restrict Access to Business Owner Computers to Authorized Users
    - □ Restrict Access to Computers Containing ePHI to Authorized Users
    - □ Restrict Access to IT Admin Only Restricted Computers to IT Administrators
    - ☑ Restrict Access to Systems in the Cardholder Data Environment (CDE) to Authorized Us
    - □ Restrict IT Administrative Access to Minimum Necessary
    - □ Restrict Users that are Not Authorized to Log into Multiple Computer Systems
    - □ Strictly Control the Addition of New Local Computer Administrators
    - □ Strictly Control the Addition of New Users to the Domain
    - □ Strictly Control the Addition of Printers

Restrict Access to Systems in the Cardholder Data Environment (CDE) to Authorized Users

Description

Computers in the network that are used to transmit, process, or store Cardholder Data may only be accessed by users authorized to access the Cardholder Data Environment (CDE). By applying tagging to a computer as a PCI/CDE COMPUTER, you will start receiving alerts when users that are not tagged as a PCI/CDE AUTHORIZED USER logs into the computer. By tagging computers that are part of the CDE and tagging the users that are authorized to access CDE computers, Detector can identify unauthorized access.

Required SmartTags

PCI / CDE AUTHORIZED USER	This tag is applied to a User
PCI / CDE COMPUTER	This tag is applied to a Computer

Select Policies to include in Plan

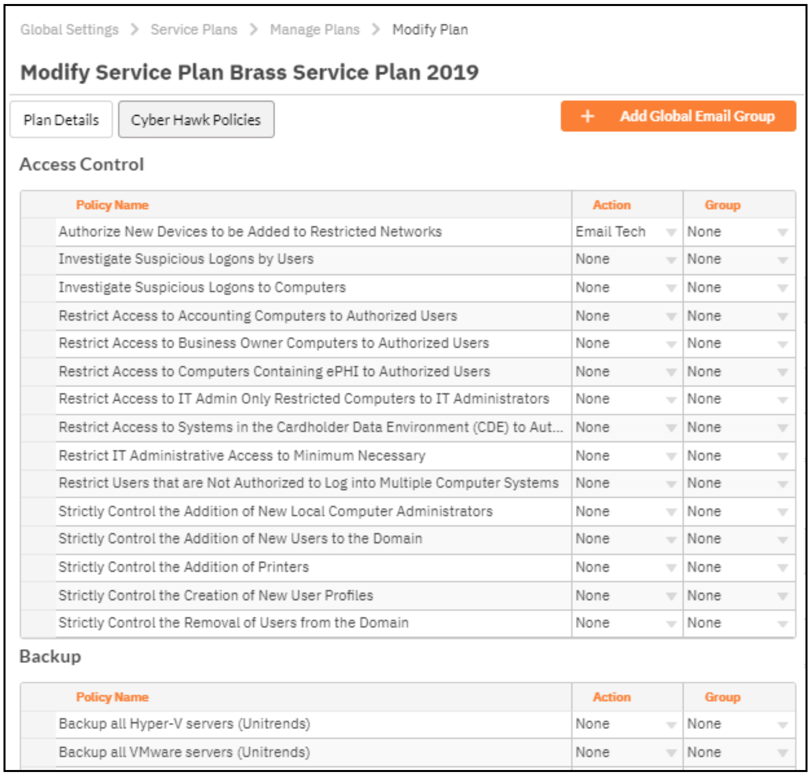
Smart Tag Description

Click on Policies to view Description

Required Smart Tags

6. Check the box next to each Security Policy to include in the plan. Click ▶ to expand the category of available options.
7. Click on a Policy to read a Description of that Policy, as well as to see any **Required Smart Tags**. You will need to deploy these Smart Tags on the appropriate network assets (such as Users or Computers) in order for Cyber Hawk to enforce these policies.
8. When you have selected the Security Policies you want to include in the Service Plan, click **Configure Notifications**.
9. Next, assign **Actions** and **Email Groups** for each Security Policy's Notification Rule. This is where you tell Cyber Hawk what to do when it discovers a potential security policy violation.

© 2024 RapidFire Tools, Inc. All rights reserved.


Global Settings > Service Plans > Manage Plans > Modify Plan
Plan Details
Cyber Hawk Policies
+ Add Global Email Group

Modify Service Plan Brass Service Plan 2019

Access Control

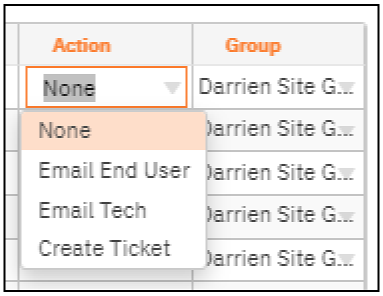
Policy Name	Action	Group
Authorize New Devices to be Added to Restricted Networks	Email Tech	None
Investigate Suspicious Logons by Users	None	None
Investigate Suspicious Logons to Computers	None	None
Restrict Access to Accounting Computers to Authorized Users	None	None
Restrict Access to Business Owner Computers to Authorized Users	None	None
Restrict Access to Computers Containing ePHI to Authorized Users	None	None
Restrict Access to IT Admin Only Restricted Computers to IT Administrators	None	None
Restrict Access to Systems in the Cardholder Data Environment (CDE) to Aut...	None	None
Restrict IT Administrative Access to Minimum Necessary	None	None
Restrict Users that are Not Authorized to Log into Multiple Computer Systems	None	None
Strictly Control the Addition of New Local Computer Administrators	None	None
Strictly Control the Addition of New Users to the Domain	None	None
Strictly Control the Addition of Printers	None	None
Strictly Control the Creation of New User Profiles	None	None
Strictly Control the Removal of Users from the Domain	None	None

Backup

Policy Name	Action	Group
Backup all Hyper-V servers (Unitrends)	None	None
Backup all VMware servers (Unitrends)	None	None

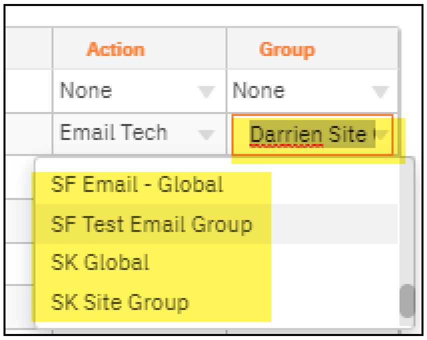
10. First, assign each Policy a Notification Rule/**Action**. Actions include:

    - **None**: Take no action.
    - **Email End User**: Send an email to an end user group. The end user will then make a decision about whether to request further investigation from the Tech Team.
    - **Email Tech**: Send an email to the Tech Team to investigate the issue.
    - **Create a Ticket**: Automatically Create a Ticket in your favorite PSA/ticketing system



11. Select the Email **Group Name** (the email group to whom to send either an End User or Tech email notification).

© 2024 RapidFire Tools, Inc. All rights reserved.



12. When you have assigned *Actions* and *Groups* to all Security Policies, click **Save**. You can then apply this Service Plan to your existing or new Cyber Hawk Sites.

Note: To Do items and Alerts generated by Cyber Hawk will remain in the RapidFire Tools Portal for two weeks before they are automatically removed.

© 2024 RapidFire Tools, Inc. All rights reserved.

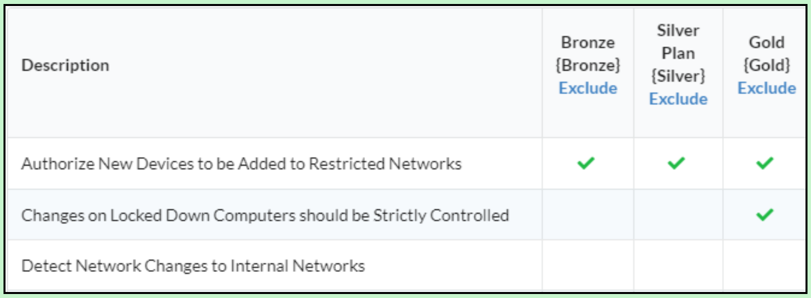
Create Service Catalogs

Note: This feature is intended for MSPs who are using Cyber Hawk to sell their security services; it is not intended for organizations who are using Cyber Hawk internally within their own network.

Cyber Hawk allows you to create **Service Catalogs** as a way to market your security services to potential customers.

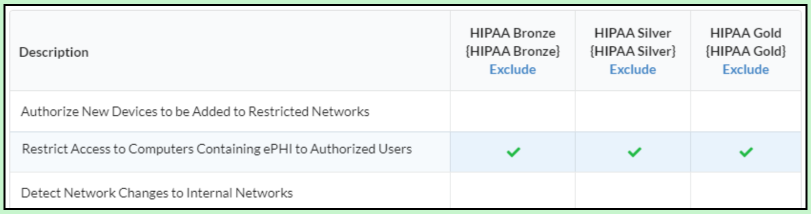
- A Service Catalog contains an easy-to-read matrix of each "tier" of security service you want to offer, such as "Bronze," "Silver," "Gold," or your own custom plans.
- You can generate catalogs as Word documents in order to market your services.
- Cyber Hawk also allows you to create multiple catalogs for different types of customers.

EXAMPLE: For example, you might want to have a generic *Bronze*, *Silver*, and *Gold* offering for a wide range of potential customers.



Description	Bronze {Bronze} Exclude	Silver Plan {Silver} Exclude	Gold {Gold} Exclude
Authorize New Devices to be Added to Restricted Networks	✓	✓	✓
Changes on Locked Down Computers should be Strictly Controlled			✓
Detect Network Changes to Internal Networks			

At the same time, you can also maintain service plans geared toward potential customers who require specialized HIPAA security services.



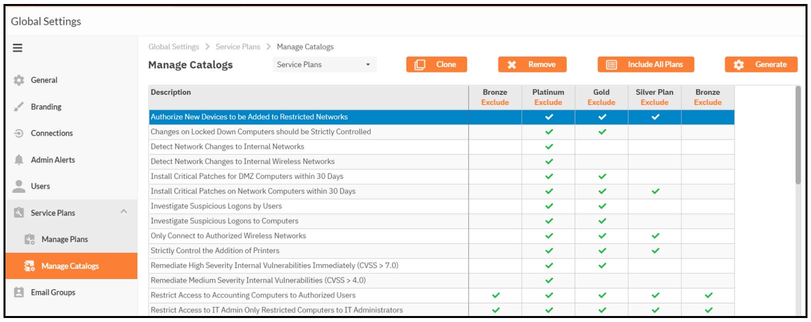
Description	HIPAA Bronze {HIPAA Bronze} Exclude	HIPAA Silver {HIPAA Silver} Exclude	HIPAA Gold {HIPAA Gold} Exclude
Authorize New Devices to be Added to Restricted Networks			
Restrict Access to Computers Containing ePHI to Authorized Users	✓	✓	✓
Detect Network Changes to Internal Networks			

To create and generate a Service Catalog:

© 2024 RapidFire Tools, Inc. All rights reserved.

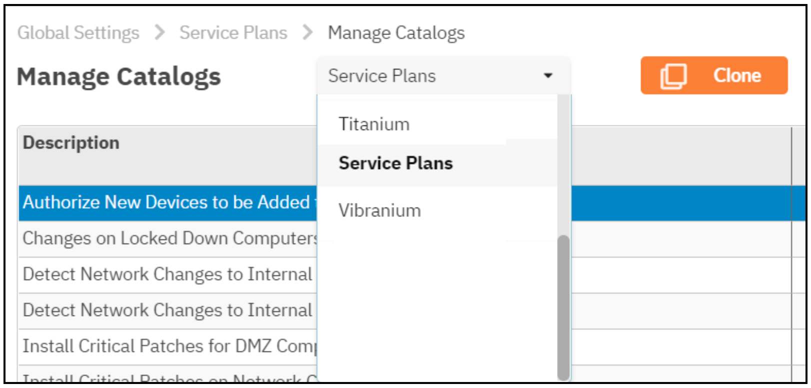
Important: Before you can create a catalog, be sure that you have already created each individual plan that you wish to include in the Catalog. See also "Create Global Service Plans for Cyber Hawk" on page 97.

1. Go to global **Settings (Admin)** ⚙ > **Service Plans** > **Manage Catalogs**. The Manage Catalogs screen will appear.

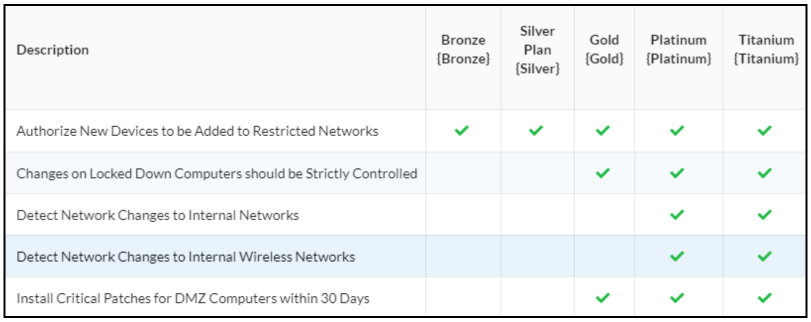


Description	Bronze Exclude	Platinum Exclude	Gold Exclude	Silver Plan Exclude	Bronze Exclude
Authorize New Devices to be Added to Restricted Networks		✓	✓	✓	
Changes on Locked Down Computers should be Strictly Controlled		✓	✓		
Detect Network Changes to Internal Networks		✓			
Detect Network Changes to Internal Wireless Networks		✓			
Install Critical Patches for DMZ Computers within 30 Days		✓	✓		
Install Critical Patches on Network Computers within 30 Days		✓	✓	✓	
Investigate Suspicious Logons by Users		✓	✓		
Investigate Suspicious Logons to Computers		✓	✓		
Only Connect to Authorized Wireless Networks		✓	✓	✓	
Strictly Control the Addition of Printers		✓	✓	✓	
Remediate High Severity Internal Vulnerabilities Immediately (CVSS > 7.0)		✓	✓		
Remediate Medium Severity Internal Vulnerabilities (CVSS > 4.0)		✓			
Restrict Access to Accounting Computers to Authorized Users	✓	✓	✓	✓	✓
Restrict Access to IT Admin Only Restricted Computers to IT Administrators	✓	✓	✓	✓	✓

2. From the drop-down menu, select **All Plans**.


Global Settings > Service Plans > Manage Catalogs
Manage Catalogs
Service Plans
Clone
Titanium
Service Plans
Vibranium
Description
Authorize New Devices to be Added t
Changes on Locked Down Computers
Detect Network Changes to Internal
Detect Network Changes to Internal
Install Critical Patches for DMZ Comp
Install Critical Patches on Network C

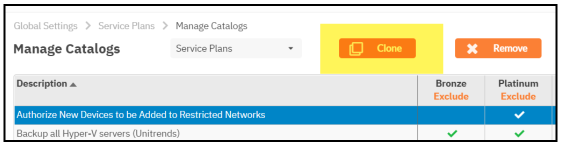
3. Here you can see a matrix displaying all of your Service Plans. A *green check mark* indicates that the Service Plan contains the Security Policy, as in the image below.



Description	Bronze {Bronze}	Silver Plan {Silver}	Gold {Gold}	Platinum {Platinum}	Titanium {Titanium}
Authorize New Devices to be Added to Restricted Networks	✓	✓	✓	✓	✓
Changes on Locked Down Computers should be Strictly Controlled			✓	✓	✓
Detect Network Changes to Internal Networks				✓	✓
Detect Network Changes to Internal Wireless Networks				✓	✓
Install Critical Patches for DMZ Computers within 30 Days			✓	✓	✓

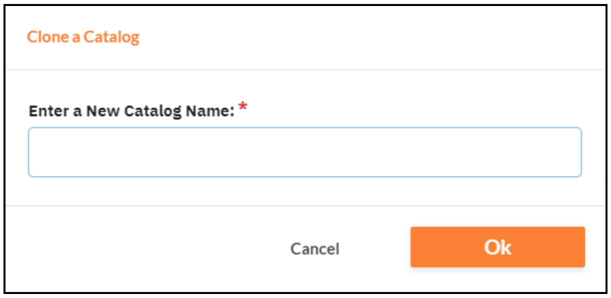
4. To make a new catalog, click **Clone**.

© 2024 RapidFire Tools, Inc. All rights reserved.

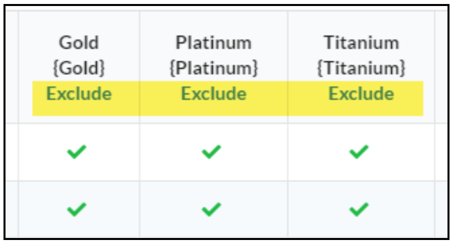


Description ▲	Bronze Exclude	Platinum Exclude
Authorize New Devices to be Added to Restricted Networks		✓
Backup all Hyper-V servers (Unitrends)	✓	✓

5. Enter a **name** for the new catalog. Click **OK**.

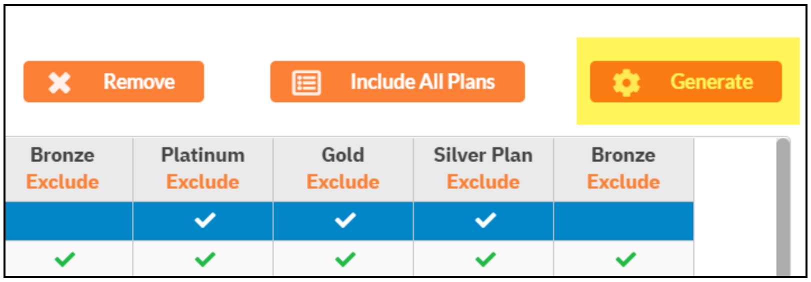


6. To create your custom catalog, click **Exclude** underneath each plan that you wish to REMOVE from the catalog. Continue removing plans until the catalog contains only the plans you want.



Gold {Gold} Exclude	Platinum {Platinum} Exclude	Titanium {Titanium} Exclude
✓	✓	✓
✓	✓	✓

7. When you are finished, click **Generate**. Your catalog will then appear as a Word document download.



Bronze Exclude	Platinum Exclude	Gold Exclude	Silver Plan Exclude	Bronze Exclude
	✓	✓	✓	
✓	✓	✓	✓	✓

Your Catalog will also be automatically saved and available from the drop-down menu.

© 2024 RapidFire Tools, Inc. All rights reserved.

Cyber Hawk Security Policy Violation Alerts

Whenever Cyber Hawk discovers a potential security policy violation on the network, it alerts your team and helps them respond to and mitigate the issue. This section covers everything you need to know about Cyber Hawk's security policy violation alerts.

Security Policy Violation Alert Notification Rule Actions

You assign Cyber Hawk an **Action** for each Security Policy being enforced on the network. Whenever Cyber Hawk discovers a potential violation of a Security Policy, it automatically performs the Action.

There are four available Actions. These are:

Action	Description and Features
1. Email Tech Group	1. Send your technicians an *Alert Notification* directing them to investigate the issue. 2. Create an Alert item in the Portal.
2. Email End User	1. Send an *End User Alert Notification* to End User(s) in your client's company. 2. The End User can then decide how your technicians respond to the Alert. End Users can direct your company’s technicians to: • *Investigate the Alert*. The Tech Group will then receive an Alert Notification, and an Alert item will be created in the Portal. • *Set up an Ignore Rule* to ignore the Alert in the future. The Tech Group will receive an Ignore Alert Notification and will be prompted to set up the Ignore Rule.
3. Create a Ticket	Generate a ticket based on the policy violation in your preferred PSA system. **Note:** See "Set Up and Assign a Ticketing/PSA System Integration to a Site" on page 65.
4. None	Take no action. An Alert item will still be created in the portal and can be managed there.

© 2024 RapidFire Tools, Inc. All rights reserved.

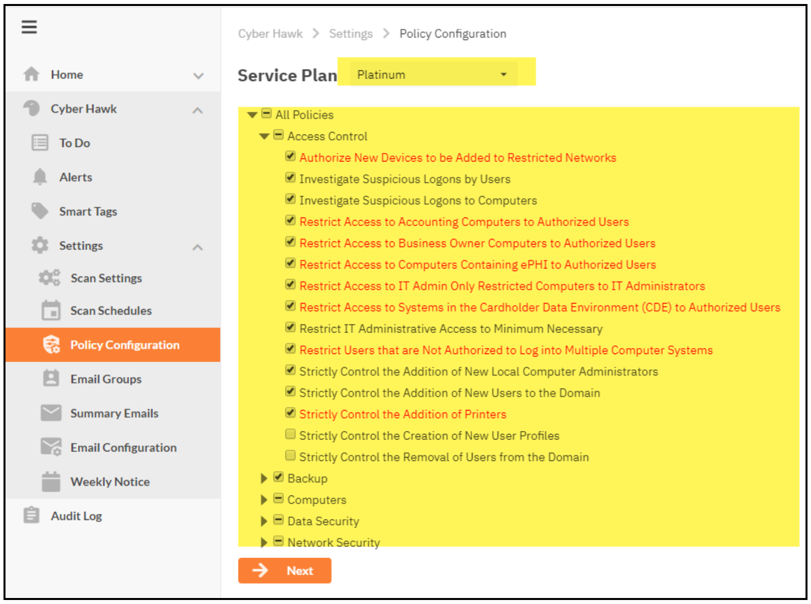
Set Up End User Alert Notifications

You can set up Cyber Hawk to send **End User Alert Notifications** whenever Cyber Hawk discovers a possible security policy violation on the network.

> **Tip:** End User Alerts allow the client to give your technicians some guidance in responding to a particular security alert.

To configure end user alerts:

1. From the Site, go to **Cyber Hawk** tab > **Settings** > **Policy Configuration**.
2. From the **Select Policies** page, ensure that you have the correct Service Plan and policies applied to the Site. Then click **Next**.



Cyber Hawk > Settings > Policy Configuration

Service Plan: Platinum

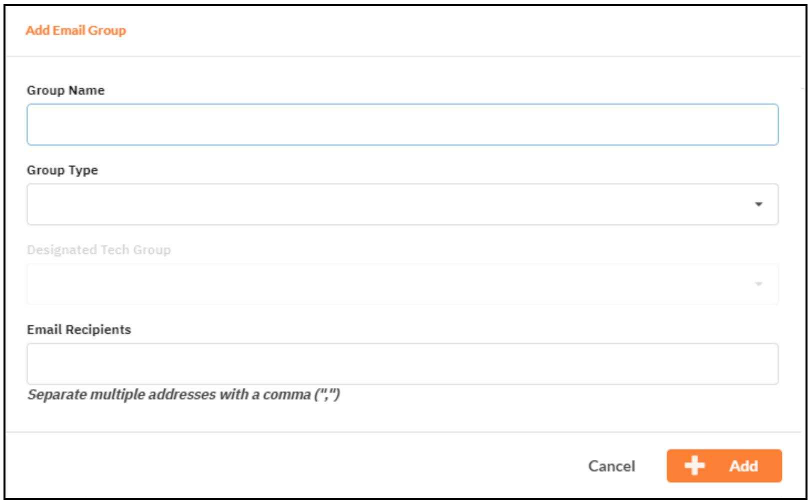
- All Policies
  - Access Control
    - ☑ Authorize New Devices to be Added to Restricted Networks
    - ☑ Investigate Suspicious Logons by Users
    - ☑ Investigate Suspicious Logons to Computers
    - ☑ Restrict Access to Accounting Computers to Authorized Users
    - ☑ Restrict Access to Business Owner Computers to Authorized Users
    - ☑ Restrict Access to Computers Containing ePHI to Authorized Users
    - ☑ Restrict Access to IT Admin Only Restricted Computers to IT Administrators
    - ☑ Restrict Access to Systems in the Cardholder Data Environment (CDE) to Authorized Users
    - ☑ Restrict IT Administrative Access to Minimum Necessary
    - ☑ Restrict Users that are Not Authorized to Log into Multiple Computer Systems
    - ☑ Strictly Control the Addition of New Local Computer Administrators
    - ☑ Strictly Control the Addition of New Users to the Domain
    - ☑ Strictly Control the Addition of Printers
    - □ Strictly Control the Creation of New User Profiles
    - □ Strictly Control the Removal of Users from the Domain
  - ☑ Backup
  - Computers
  - Data Security
  - Network Security

3. To send the notifications to a new email group, click **Add Site Email Group**.

4. Enter the new email group **Name**, select the **Group Type** (End User), then enter the **Designated Tech Group** who will respond to the End User *Investigate* and *Ignore* requests.

© 2024 RapidFire Tools, Inc. All rights reserved.

Enter the email addresses for the End User Group. Click **Add**.



Add Email Group

Group Name

Group Type

Designated Tech Group

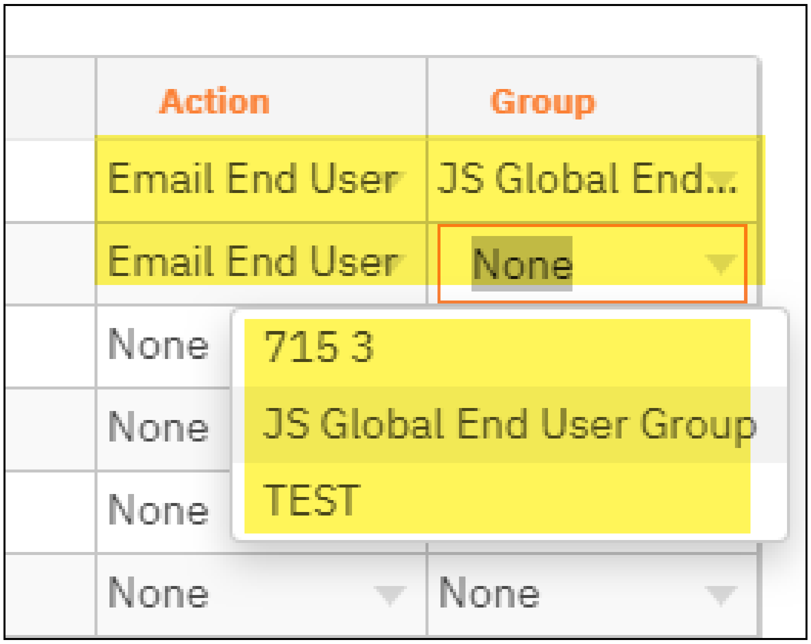
Email Recipients

Separate multiple addresses with a comma (",")

5. For each policy that you wish to send notifications, select **Email End User** from the **Action** drop-down menu in the list of policy names.

> **Note:** The list of policy names displays the list of security policies currently being enforced at the Site. To modify the policy configuration, see "Edit Security Policies Enforced at a Site" on page 118.

6. Select the **Email Group** name from the **Group Name** drop-down menu. Click **Save**.



Action	Group
Email End User	JS Global End...
Email End User	None
None	
None	
None	
None	None

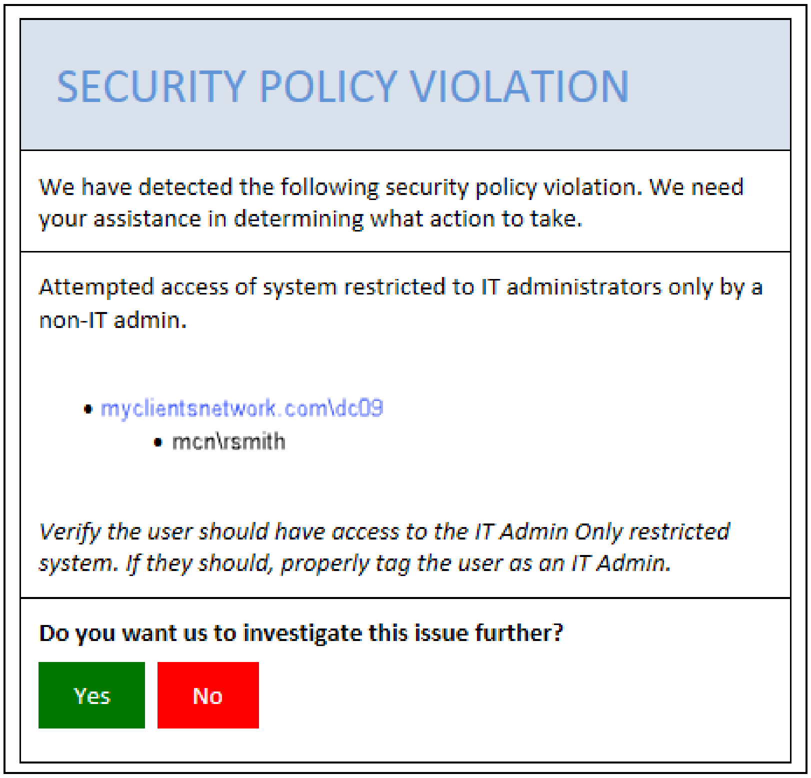
© 2024 RapidFire Tools, Inc. All rights reserved.

The chosen End User Email Group will now receive security policy violation alerts when Cyber Hawk discovers anomalies, changes, or threats on the network.

More about End User Security Policy Violation Alert Notifications

This purpose of the End User Notifications feature is to notify individuals within your client's company about Security Policy Violations via selected Cyber Hawk Alerts.

In cases where your technicians will require guidance from your client as to how your technicians should to respond to a particular Security Policy Violation Alert, you can configure Cyber Hawk to send End User Alert Notifications directly to email recipients in your client's company.



SECURITY POLICY VIOLATION

We have detected the following security policy violation. We need your assistance in determining what action to take.

Attempted access of system restricted to IT administrators only by a non-IT admin.

- myclientsnetwork.com\dc09
  - mcn\rsmith

Verify the user should have access to the IT Admin Only restricted system. If they should, properly tag the user as an IT Admin.

Do you want us to investigate this issue further?

Upon your client's receipt of an Alert, your client can assign To Do items to your technicians. The To Do items may request that your technicians:

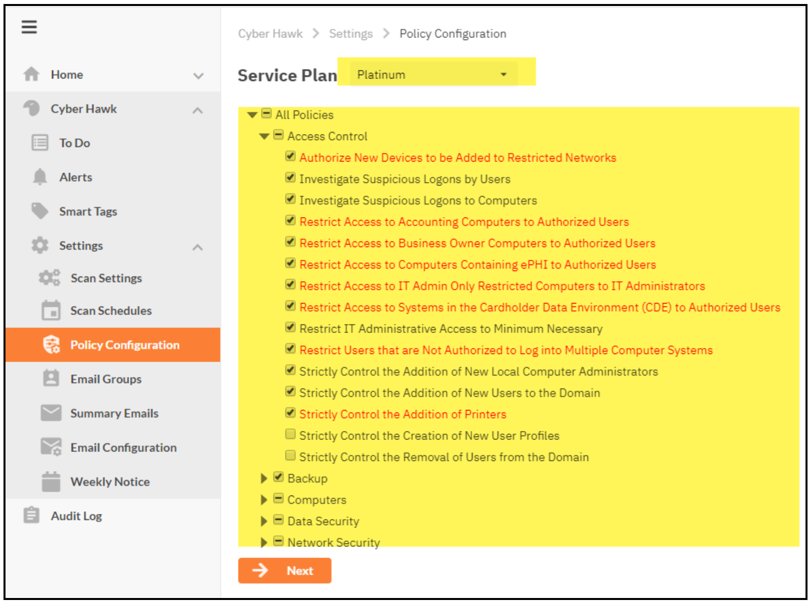
- Investigate the Alert
- Assign an Ignore Rule to a specific Alert to address False Positives

End User Alerts are configured and controlled by a Notification Rule assigned to a specific Security Policy. Notification Rules are configured either through the use of the Notification Rules setup or the Policy Configuration features located within the Cyber Hawk Settings window.

Set Up Tech Group Alert Notifications

You can set up Cyber Hawk to send **Tech Group Alert Notifications** whenever Cyber Hawk discovers a possible security policy violation on the network. To do this:

1. From the Site, go to **Cyber Hawk** tab > **Settings** > **Policy Configuration**.
2. From the **Select Policies** page, click **Next**.



Cyber Hawk > Settings > Policy Configuration

Service Plan: Platinum

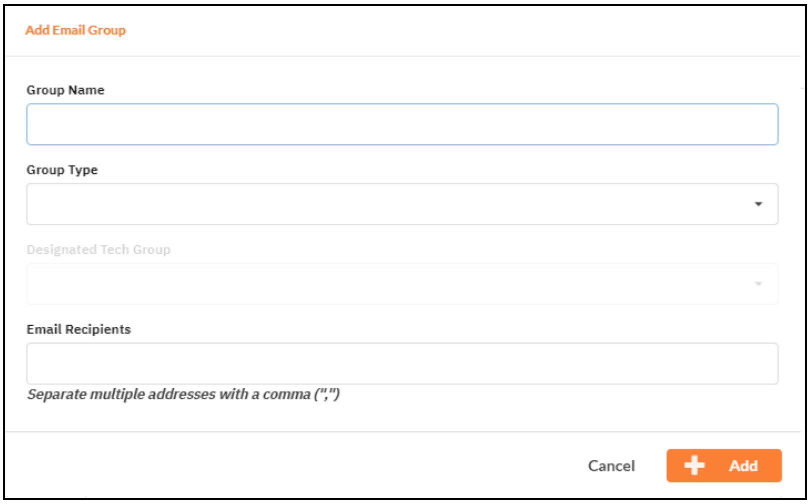
- ⊟ All Policies
  - ⊟ Access Control
    - ☑ Authorize New Devices to be Added to Restricted Networks
    - ☑ Investigate Suspicious Logons by Users
    - ☑ Investigate Suspicious Logons to Computers
    - ☑ Restrict Access to Accounting Computers to Authorized Users
    - ☑ Restrict Access to Business Owner Computers to Authorized Users
    - ☑ Restrict Access to Computers Containing ePHI to Authorized Users
    - ☑ Restrict Access to IT Admin Only Restricted Computers to IT Administrators
    - ☑ Restrict Access to Systems in the Cardholder Data Environment (CDE) to Authorized Users
    - ☑ Restrict IT Administrative Access to Minimum Necessary
    - ☑ Restrict Users that are Not Authorized to Log into Multiple Computer Systems
    - ☑ Strictly Control the Addition of New Local Computer Administrators
    - ☑ Strictly Control the Addition of New Users to the Domain
    - ☑ Strictly Control the Addition of Printers
    - ☐ Strictly Control the Creation of New User Profiles
    - ☐ Strictly Control the Removal of Users from the Domain
  - ☑ Backup
  - ⊟ Computers
  - ⊟ Data Security
  - ⊟ Network Security

3. To send the notifications to a new email group, click **Add Email Group**.

4. Enter the new email group **Name** and select the **Group Type** (Tech).

   Enter the email addresses for the Tech User Group. Click **Next**.

© 2024 RapidFire Tools, Inc. All rights reserved.



Add Email Group

Group Name

Group Type

Designated Tech Group

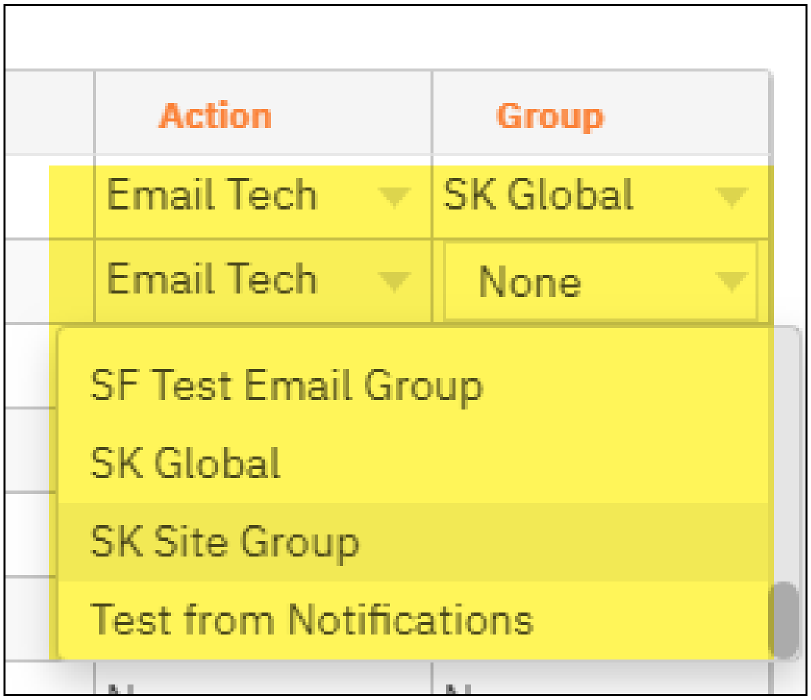
Email Recipients

Separate multiple addresses with a comma (",")

5. For each policy that you wish to send notifications, select **Email Tech** from the **Action** drop-down menu in the list of policy names.

> **Note:** The list of policy names displays the list of security policies currently being enforced at the Site. To modify the policy configuration, see "Edit Security Policies Enforced at a Site" on page 118.

6. Select the **Email Group** name from the **Group Name** drop-down menu. Click **Save**



Action	Group
Email Tech	SK Global
Email Tech	None

© 2024 RapidFire Tools, Inc. All rights reserved.

The chosen Tech Email Group will now receive security policy violation alerts when Cyber Hawk discovers anomalies, changes, or threats on the network.

© 2024 RapidFire Tools, Inc. All rights reserved.

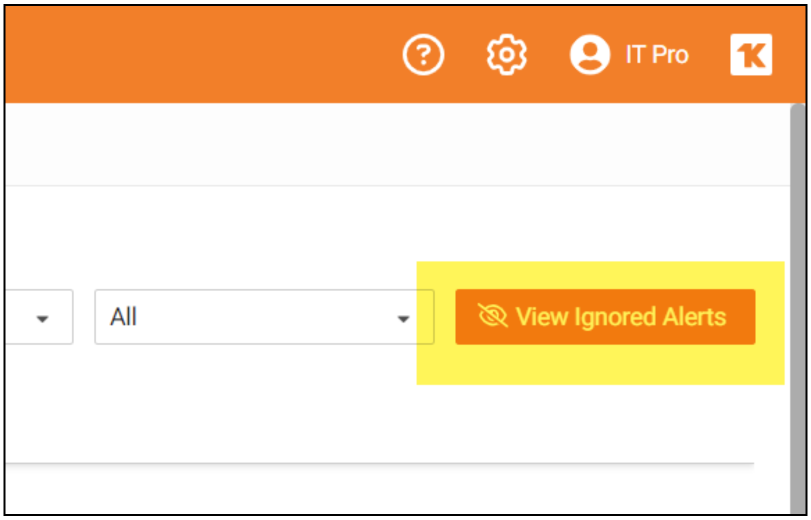
Managing and Deleting “Ignore” Alert Rules

With Cyber Hawk, you have the ability to select Alerts that you can “Ignore” through the use of the RapidFire Tools Portal’s Ignore Alert process as a method to minimize Cyber Hawk alerting on ACT false positives.

In order to view and delete Ignore Alert Rules assigned to a particular alert for a Site associated with your Cyber Hawk Appliance, you can use the **View Ignored Alerts** feature.

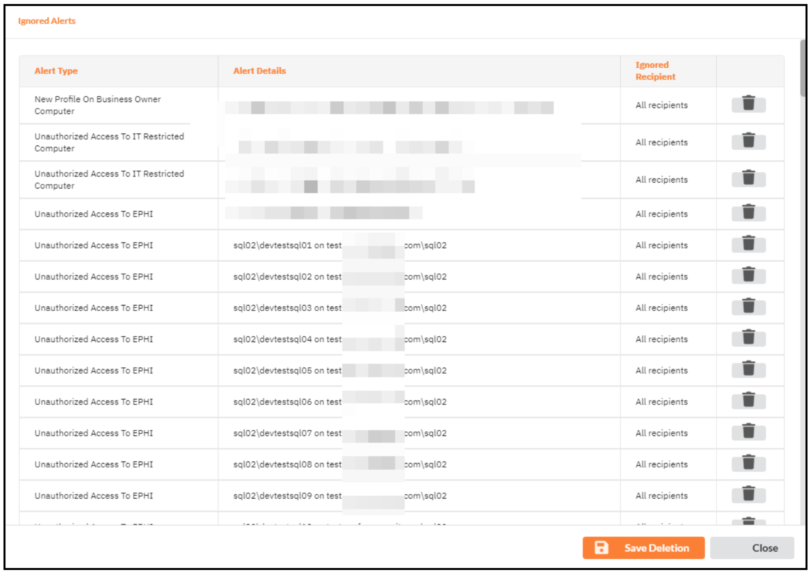
Follow these steps to view and delete Cyber Hawk Alert ignore rules:

1. Open your Cyber Hawk Site and go to **Cyber Hawk tab** > **Alerts**.
2. Click **View Ignored Alerts**.



3. The Ignored Alerts window will be displayed. Select the 🗑 icon next to the Ignore Alert rule that you would like to delete.

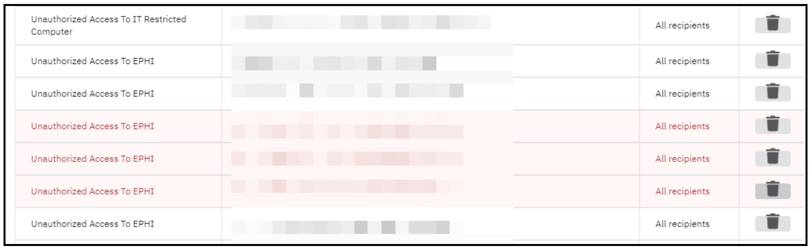
© 2024 RapidFire Tools, Inc. All rights reserved.



Ignored Alerts

Alert Type	Alert Details	Ignored Recipient	
New Profile On Business Owner Computer	[redacted]	All recipients	🗑
Unauthorized Access To IT Restricted Computer	[redacted]	All recipients	🗑
Unauthorized Access To IT Restricted Computer	[redacted]	All recipients	🗑
Unauthorized Access To EPHI	[redacted]	All recipients	🗑
Unauthorized Access To EPHI	sql02\devtestsql01 on test[redacted]com\sql02	All recipients	🗑
Unauthorized Access To EPHI	sql02\devtestsql02 on test[redacted]com\sql02	All recipients	🗑
Unauthorized Access To EPHI	sql02\devtestsql03 on test[redacted]com\sql02	All recipients	🗑
Unauthorized Access To EPHI	sql02\devtestsql04 on test[redacted]com\sql02	All recipients	🗑
Unauthorized Access To EPHI	sql02\devtestsql05 on test[redacted]com\sql02	All recipients	🗑
Unauthorized Access To EPHI	sql02\devtestsql06 on test[redacted]com\sql02	All recipients	🗑
Unauthorized Access To EPHI	sql02\devtestsql07 on test[redacted]com\sql02	All recipients	🗑
Unauthorized Access To EPHI	sql02\devtestsql08 on test[redacted]com\sql02	All recipients	🗑
Unauthorized Access To EPHI	sql02\devtestsql09 on test[redacted]com\sql02	All recipients	🗑

Selected Ignore Alert rules will be shaded out indicating that these rules will be deleted after the Alert Rule settings are saved.



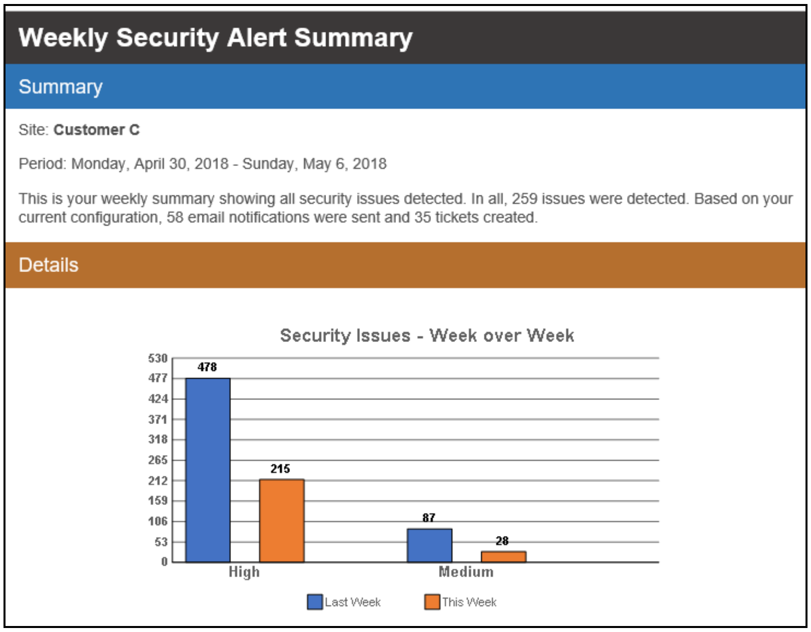
Unauthorized Access To IT Restricted Computer	[redacted]	All recipients	🗑
Unauthorized Access To EPHI	[redacted]	All recipients	🗑
Unauthorized Access To EPHI	[redacted]	All recipients	🗑
Unauthorized Access To EPHI	[redacted]	All recipients	🗑
Unauthorized Access To EPHI	[redacted]	All recipients	🗑
Unauthorized Access To EPHI	[redacted]	All recipients	🗑
Unauthorized Access To EPHI	[redacted]	All recipients	🗑

4. After selecting the Ignore Alert rules that you want to delete, click **Save Deletions** button in the Ignored Alerts window.

© 2024 RapidFire Tools, Inc. All rights reserved.

Cyber Hawk Security Alert Email Summaries

Cyber Hawk can generate Weekly and Monthly Security Alert Email Summaries. These summaries provide an overview of all issues detected on the network. Use the Security Alert summaries to communicate the value of your security service to your clients.



Weekly Security Alert Summary

Summary

Site: **Customer C**

Period: Monday, April 30, 2018 - Sunday, May 6, 2018

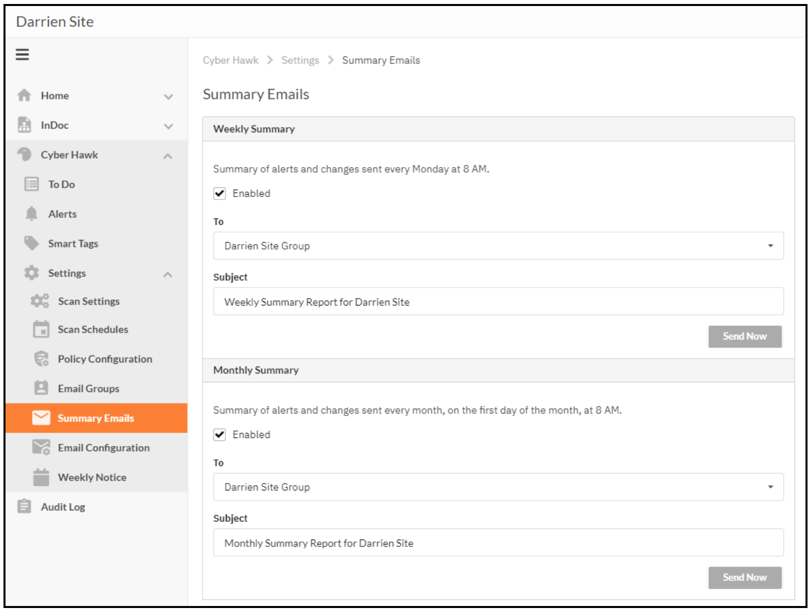
This is your weekly summary showing all security issues detected. In all, 259 issues were detected. Based on your current configuration, 58 email notifications were sent and 35 tickets created.

Details

To configure Weekly and Monthly Security Alert Summaries:

1. Open your Cyber Hawk Site, and then go to **Cyber Hawk** tab > **Settings** > **Summary Emails**.

© 2024 RapidFire Tools, Inc. All rights reserved.



Summary Emails

Weekly Summary

Summary of alerts and changes sent every Monday at 8 AM.

☑ Enabled

To: Darrien Site Group

Subject: Weekly Summary Report for Darrien Site

Monthly Summary

Summary of alerts and changes sent every month, on the first day of the month, at 8 AM.

☑ Enabled

To: Darrien Site Group

Subject: Monthly Summary Report for Darrien Site

2. Choose whether to enable **Weekly** and **Monthly** Summaries. Select the Recipient Email Group from the **To:** drop down menu.
3. Enter a **Subject** line for the email. You can optionally choose to **Send Now**.
4. When you are finished, click **Save**.

You can also click **Send Now** to immediately send the email. Otherwise, it will be sent at the time noted in the interface.

What's in the Cyber Hawk Alert Summaries?
A comparison of high and medium level issues week over week or month over month
Security issues by day of the week
A table containing high risk security issues, including number of occurrences and issue type
A table containing medium risk security issues, including number of occurrences and issue type
Number of tickets created
High risk security issues detected, but not alerted (you can change your security policies in order to act on these issues and generate alerts)
Assets with the most alerts (such as PCs or printers)
Users with the most security issues
User and permission changes on the network (users added, removed, or promoted to administrator)

© 2024 RapidFire Tools, Inc. All rights reserved.

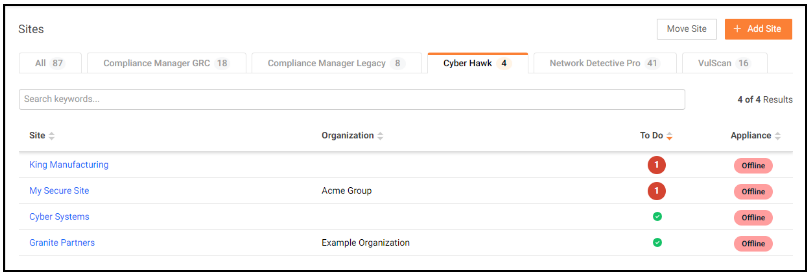
What's in the Cyber Hawk Alert Summaries?
Group security policy changes
Network changes (such as the addition of new devices)

© 2024 RapidFire Tools, Inc. All rights reserved.

Edit Security Policies Enforced at a Site

You can edit or modify the security policies that Cyber Hawk enforces at a Site. To do this:

1. Open the Site that needs a change to its security policies.

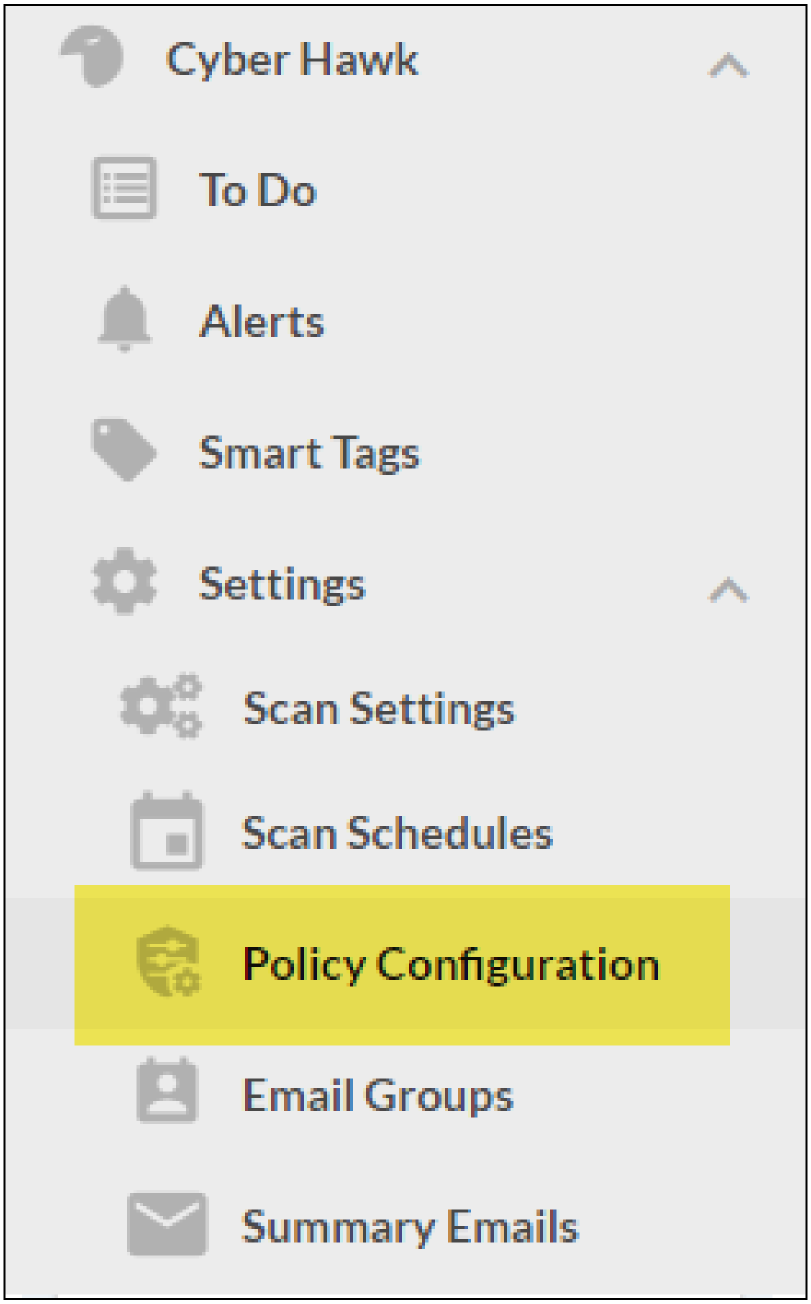


4 of 4 Results

Site	Organization	To Do	Appliance
King Manufacturing		1	Offline
My Secure Site	Acme Group	1	Offline
Cyber Systems		✓	Offline
Granite Partners	Example Organization	✓	Offline

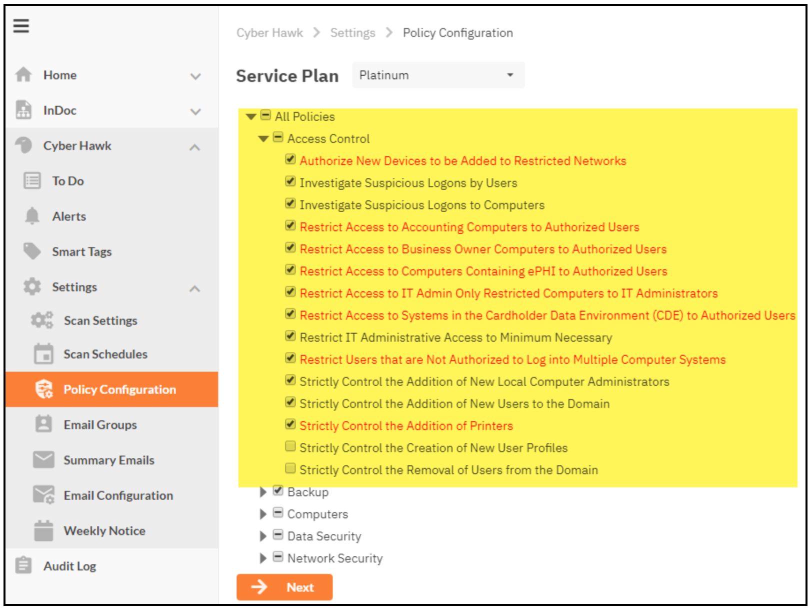
2. Go to the **Cyber Hawk tab** > **Settings** > **Policy Configuration**.

© 2024 RapidFire Tools, Inc. All rights reserved.



3. Select or un-select the policies you wish to modify. Click **Next**.

© 2024 RapidFire Tools, Inc. All rights reserved.

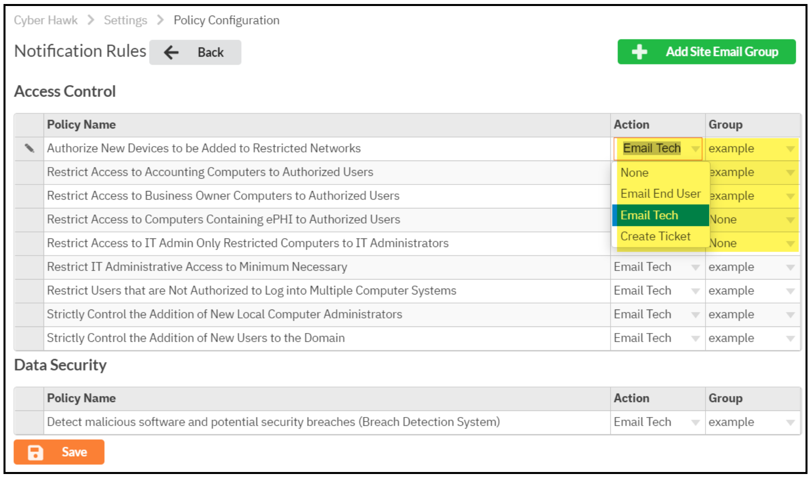


Cyber Hawk > Settings > Policy Configuration

Service Plan Platinum

- ⊟ All Policies
  - ⊟ Access Control
    - ☑ Authorize New Devices to be Added to Restricted Networks
    - ☑ Investigate Suspicious Logons by Users
    - ☑ Investigate Suspicious Logons to Computers
    - ☑ Restrict Access to Accounting Computers to Authorized Users
    - ☑ Restrict Access to Business Owner Computers to Authorized Users
    - ☑ Restrict Access to Computers Containing ePHI to Authorized Users
    - ☑ Restrict Access to IT Admin Only Restricted Computers to IT Administrators
    - ☑ Restrict Access to Systems in the Cardholder Data Environment (CDE) to Authorized Users
    - ☑ Restrict IT Administrative Access to Minimum Necessary
    - ☑ Restrict Users that are Not Authorized to Log into Multiple Computer Systems
    - ☑ Strictly Control the Addition of New Local Computer Administrators
    - ☑ Strictly Control the Addition of New Users to the Domain
    - ☑ Strictly Control the Addition of Printers
    - □ Strictly Control the Creation of New User Profiles
    - □ Strictly Control the Removal of Users from the Domain
  - ☑ Backup
  - ⊟ Computers
  - ⊟ Data Security
  - ⊟ Network Security

4. Make any changes to the **Notification Rules** for the policies.



Cyber Hawk > Settings > Policy Configuration

Notification Rules

Access Control

Policy Name	Action	Group
Authorize New Devices to be Added to Restricted Networks	Email Tech	example
Restrict Access to Accounting Computers to Authorized Users	None	example
Restrict Access to Business Owner Computers to Authorized Users	Email End User	example
Restrict Access to Computers Containing ePHI to Authorized Users	Email Tech	None
Restrict Access to IT Admin Only Restricted Computers to IT Administrators	Create Ticket	None
Restrict IT Administrative Access to Minimum Necessary	Email Tech	example
Restrict Users that are Not Authorized to Log into Multiple Computer Systems	Email Tech	example
Strictly Control the Addition of New Local Computer Administrators	Email Tech	example
Strictly Control the Addition of New Users to the Domain	Email Tech	example

Data Security

Policy Name	Action	Group
Detect malicious software and potential security breaches (Breach Detection System)	Email Tech	example

5. Click **Save**. The policy changes will take effect when Cyber Hawk next performs a scan and sends out alerts.

© 2024 RapidFire Tools, Inc. All rights reserved.

Security Policy Details

The table below documents each Security Policy, including the "Smart Tags" on page 178 that must be used in combination with the policy.

Policy (policies with red background require Smart Tag configuration)	Description of policy	Required Tag(s)	Smart Tag Category
Authorize New Devices to be Added to Restricted Networks	Notify when new devices are connected to specified IP Range(s)	Restricted Network	IP Ranges
Investigate Suspicious Logons by Users	Notify if user logs in outside of normal time frames based on algorithmic analaysis of individual users login behavior	n/a	n/a
Investigate Suspicious Logons to Computers	Notify if user logs into computer that they have not logged into previously	n/a	n/a
Restrict Access to Accounting Computers to Authorized Users	Designate assets that only specified users should log into. Notify if non authorized users perform interactive logon. (Requires both tags to function)	Accounting Computer; Accounting User	Computers; Users
Restrict Access to Business Owner Computers to Authorized Users	Designate assets that only specified users should log into. Notify if non authorized users perform interactive logon. (Requires both tags to function)	Business Owner PC; Business Owner	Computers; Users
Restrict Access to Computers Containing ePHI to Authorized Users	Designate assets that only specified users should log into. Notify if non authorized users perform interactive logon. (Requires both tags to function) If EPHI is discovered on EPHI authorized devices during file scan it will be ignored	HIPAA/EPHI Authorized Computer; HIPAA/EPHI Authorized User	Computers; Users
Restrict Access to IT Admin Only Restricted Computers to IT Administrators	Designate assets that only specified users should log into. Notify if non authorized users perform interactive logon. (Requires both tags to function)	Restricted IT; Admin Only IT Admin	Computers; Users
Restrict Access to Systems in	Designate assets that only specified users should log into. Notify if non	PCI/CDE Authorized	Computers;

© 2024 RapidFire Tools, Inc. All rights reserved.

Policy (policies with red background require Smart Tag configuration)	Description of policy	Required Tag(s)	Smart Tag Category
the Cardholder Data Environment (CDE) to Authorized Users	authorized users perform interactive logon. If Cardholder Data I is discovered on CDE authorized devices during file scan it will be ignored	Computer; PCI/CDE Authorized User	Users
Restrict IT Administrative Access to Minimum Necessary	Notify if users account is promoted to Administrator access rights	n/a	n/a
Restrict Users that are Not Authorized to Log into Multiple Computer Systems	Notify if a user logs into more than one computer	Single Desktop User	Users
Strictly Control the Addition of New Local Computer Administrators	Notify if new local administrator account is created or local user is promoted to local administrator	n/a	n/a
Strictly Control the Addition of New Users to the Domain	Notify if new user accounts are added to the domain	n/a	n/a
Strictly Control the Addition of Printers	Notify if printers/printer drivers are detected that are not tagged as authorized	Authorized Printer	Printers
Strictly Control the Creation of New User Profiles	Notify if new user profile is detected (when user accesses system for first time)	n/a	n/a
Strictly Control the Removal of Users from the Domain	Notify if user account is removed from domain	n/a	n/a
Backup all Windows servers (Unitrends)	Notify if Windows servers are not properly backed up (requires Unitrends credentials in scan configuration)	n/a	n/a
Backup all Hyper-V servers (Unitrends)	Notify if Hyper V Servers are not properly backed up (requires Unitrends credentials in scan configuration)	n/a	n/a

© 2024 RapidFire Tools, Inc. All rights reserved.

Policy (policies with red background require Smart Tag configuration)	Description of policy	Required Tag(s)	Smart Tag Category
Backup all VMware servers (Unitrends)	Notify if VMware servers are not properly (requires Unitrends credentials in scan configuration)	n/a	n/a
Investigate all backup failures (Unitrends)	Notify if Unitrends server backup fails (requires Unitrends credentials in scan configuration)	n/a	n/a
Changes on Locked Down Computers should be Strictly Controlled	Notify when specified devices have software added/removed, drive changes (removable drive)	Locked Down	Computers
Enable automatic screen lock for users with access to sensitive information	Notify if user logs into device that does not have automatic screen lock enabled	Sensitive User	Users
Enable automatic screen lock on computers with sensitive information	Notify if devices do not have automatic screen lock enabled PII discovered on devices tagged as Sensitive Computer will be ignored	Sensitive Computer	Computers
Install Critical Patches for DMZ Computers within 30 Days	DMZ is designated by tagging to closely monitor critical patch application	DMZ computer	Computers
Install Critical Patches on Network Computers within 30 Days	Notify if devices are missing critical patches	n/a	n/a
Restrict Internet Access for Computers that are Not Authorized to Access the Internet Directly	Notify if specified devices connect to the internet	No Direct Internet Access	Computers
Strictly Control the Clearing of System and Audit Logs	Notify if event logs are cleared	n/a	n/a

© 2024 RapidFire Tools, Inc. All rights reserved.

Policy (policies with red background require Smart Tag configuration)	Description of policy	Required Tag(s)	Smart Tag Category
Detect malicious software and potential security breaches (Breach Detection System)	Notify if ransomware, malware or footholds are detected on network devices (scan runs once per week)	n/a	n/a
Only store cardholder data on designated systems	Cardholder Data discovered on devices tagged as PCI/CDE Authorized Computer will be ignored	PCI/CDE Authorized Computer	Computers
Only store ePHI on designated systems	EPHI discovered on devices taged as HIPAA/EPHI Authorized Computer will be ignored	HIPAA/EPHI Authorized Computer	Computers
Only store Personally Identifiable Information (PII) on systems marked as sensitive	PII discovered on devices tagged as Sensitive Computer will be ignored	Sensitive Computer	Computers
Detect Network Changes to Internal Networks	Notify when devices are (dis)connected to/from LAN. Guest networks can be ignored via tagging	Guest Network	IP Ranges
Detect Network Changes to Internal Wireless Networks	Notify when devices are (dis)connected to/from wireless networks. Guest networks can be ignored via tagging	Guest Wireless Network	IP Ranges
Only Connect to Authorized Wireless Networks	Notify if devices on network have connected to SSID not tagged as authorized	Authorized SSID	SSIDs
Remediate High Severity Internal Vulnerabilities Immediately (CVSS > 7.0)	Notify if Level 2 (weekly) scan detects Internal Vulnerablity with CVSS score greater than 7.0	n/a	n/a
Remediate Medium Severity Internal Vulnerabilities (CVSS > 4.0)	Notify if Level 2 (weekly) scan detects Internal Vulnerablity with CVSS score greater than 4.0	n/a	n/a
Strictly control changes to Group Policy	Notify if changes to GPO are detected	n/a	n/a

© 2024 RapidFire Tools, Inc. All rights reserved.

Policy (policies with red background require Smart Tag configuration)	Description of policy	Required Tag(s)	Smart Tag Category
Strictly control changes to the Default Domain Policy	Notify if changes are made to Default Domain policy	n/a	n/a
Strictly control DNS on Locked Down Networks	Notify of DNS changes to specified IP ranges	Locked Down DNS	IP Ranges

© 2024 RapidFire Tools, Inc. All rights reserved.

Cyber Hawk Alert Response Workflows

Whenever Cyber Hawk discovers a potential security issue on the network, it generates an Alert Notification according to rules that you define. (See also "Security Policy Violation Alert Notification Rule Actions" on page 105.)

Cyber Hawk gives you flexibility when responding to potential security issues. Users can respond to these Alert Notifications in several ways, including:

- Cyber Hawk can automatically **create a Ticket in a Ticketing System/PSA** that you specify in the Portal Settings. See "Set Up and Assign a Ticketing/PSA System Integration to a Site" on page 65.
- Cyber Hawk can automatically **send Tech Group Members an Alert Notification**. Technicians can then investigate the issue by responding to the email notification and To Do item in the Portal.
- Cyber Hawk can **send End Users an Alert Notification**. The End User can assess the issue and then choose to send an Investigate Alert Request to the Tech Group. The Tech Group then investigates the issue.
- Alternatively, End Users can **submit an Ignore Alert Request to the Tech Group**. Tech Group Members then process the Ignore Alert Request.

The section below details each of these workflows.

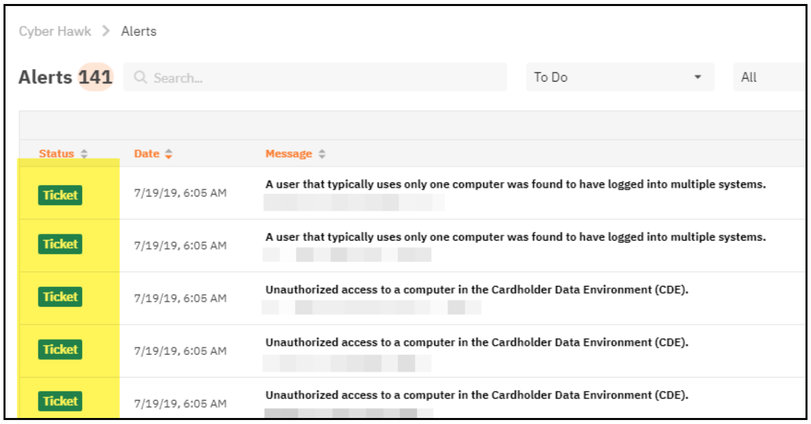
© 2024 RapidFire Tools, Inc. All rights reserved.

Create a Ticket from an Alert

In this use case, Cyber Hawk Alerts that are generated will automatically create Tickets in the Ticketing/PSA System that is configured to operate with the Site that is used to manage your Cyber Hawk Appliance.

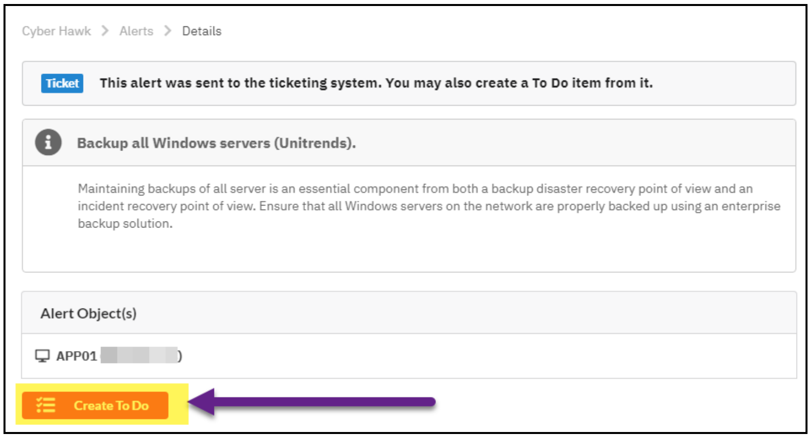
> **Note:** To learn more, see "Set Up and Assign a Ticketing/PSA System Integration to a Site" on page 65.

After a Daily Alert triggers a Ticket to be automatically generated, the Alert will be placed into the RapidFire Tools Alert Queue. This Alert will be assigned the Status of **Ticket** indicating that a ticket was created on your company's Ticketing/PSA system when the Alert was generated by the Cyber Hawk Appliance.



Status	Date	Message
Ticket	7/19/19, 6:05 AM	A user that typically uses only one computer was found to have logged into multiple systems. [redacted]
Ticket	7/19/19, 6:05 AM	A user that typically uses only one computer was found to have logged into multiple systems. [redacted]
Ticket	7/19/19, 6:05 AM	Unauthorized access to a computer in the Cardholder Data Environment (CDE). [redacted]
Ticket	7/19/19, 6:05 AM	Unauthorized access to a computer in the Cardholder Data Environment (CDE). [redacted]
Ticket	7/19/19, 6:05 AM	Unauthorized access to a computer in the Cardholder Data Environment (CDE). [redacted]

You can click on the item to open the item details page, where you can also **Create a To Do** item for the Tech group to investigate.



Ticket This alert was sent to the ticketing system. You may also create a To Do item from it.

Backup all Windows servers (Unitrends).

Maintaining backups of all server is an essential component from both a backup disaster recovery point of view and an incident recovery point of view. Ensure that all Windows servers on the network are properly backed up using an enterprise backup solution.

Alert Object(s)

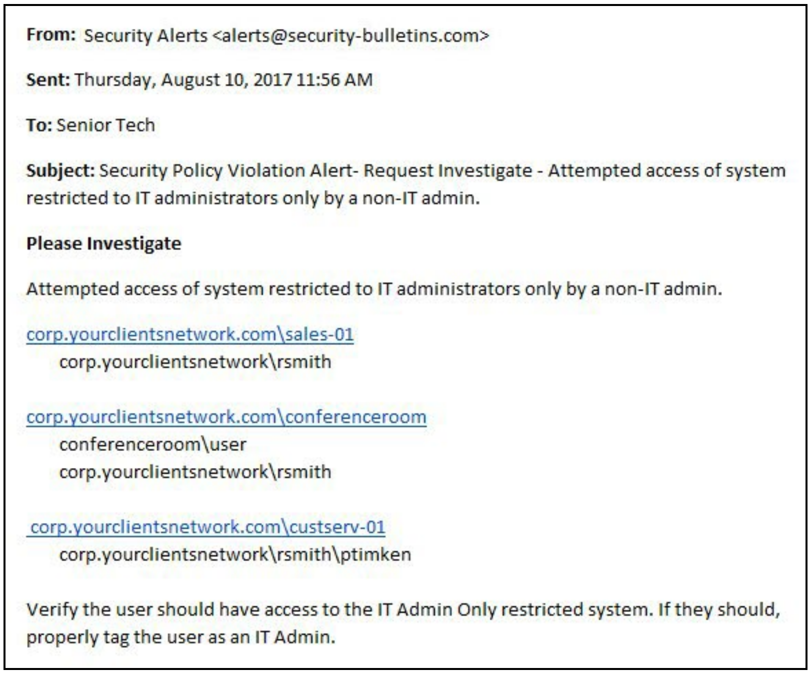
APP01 [redacted])

© 2024 RapidFire Tools, Inc. All rights reserved.

Respond to an Alert Investigation Request (Tech Group)

When Cyber Hawk discovers a potential security issue on the network, it will send you an Alert Notification Email and create a To Do item in the Portal. To respond to the Alert Investigation request:

1. Review the Alert Notification Email and click the link next to the Alert Item.



From: Security Alerts <alerts@security-bulletins.com>

Sent: Thursday, August 10, 2017 11:56 AM

To: Senior Tech

Subject: Security Policy Violation Alert- Request Investigate - Attempted access of system restricted to IT administrators only by a non-IT admin.

Please Investigate

Attempted access of system restricted to IT administrators only by a non-IT admin.

corp.yourclientsnetwork.com\sales-01
corp.yourclientsnetwork\rsmith

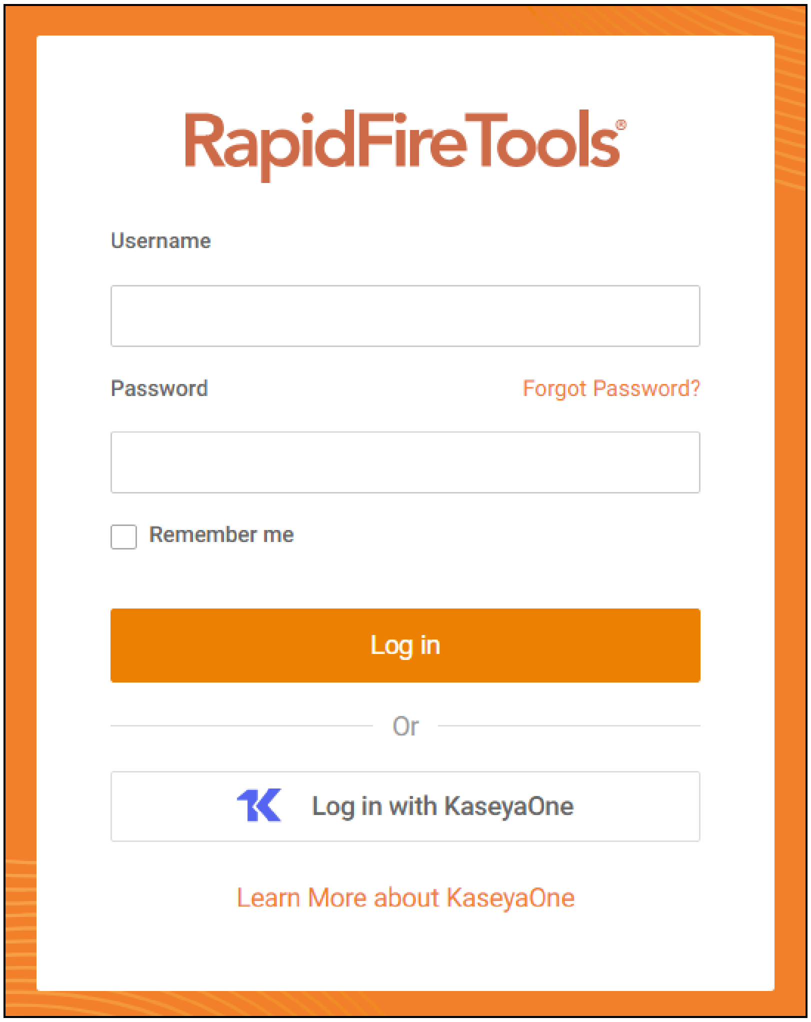
corp.yourclientsnetwork.com\conferenceroom
conferenceroom\user
corp.yourclientsnetwork\rsmith

corp.yourclientsnetwork.com\custserv-01
corp.yourclientsnetwork\rsmith\ptimken

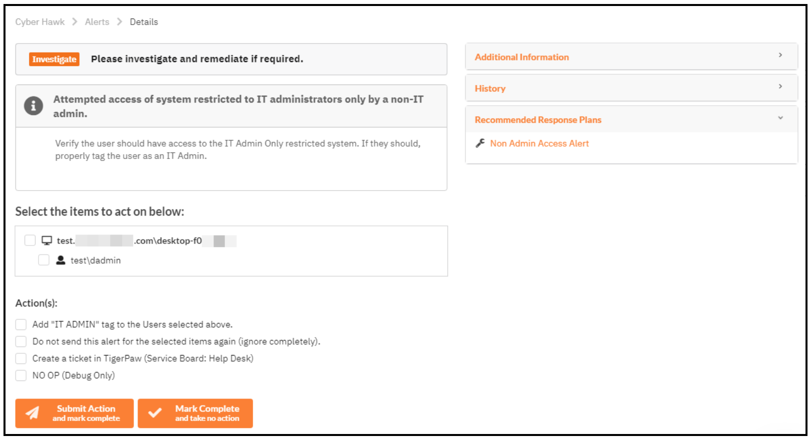
Verify the user should have access to the IT Admin Only restricted system. If they should, properly tag the user as an IT Admin.

2. The RapidFire Tools Login Page will be displayed. Log in to the Portal using your credentials.

© 2024 RapidFire Tools, Inc. All rights reserved.



After you log in, the Alert Item will appear.



Please investigate and remediate if required.

Attempted access of system restricted to IT administrators only by a non-IT admin.

Verify the user should have access to the IT Admin Only restricted system. If they should, properly tag the user as an IT Admin.

Select the items to act on below:

□ test.[redacted].com\desktop-f0[redacted]

□ test\dadmin

Action(s):

□ Add "IT ADMIN" tag to the Users selected above.

□ Do not send this alert for the selected items again (ignore completely).

□ Create a ticket in TigerPaw (Service Board: Help Desk)

□ NO OP (Debug Only)

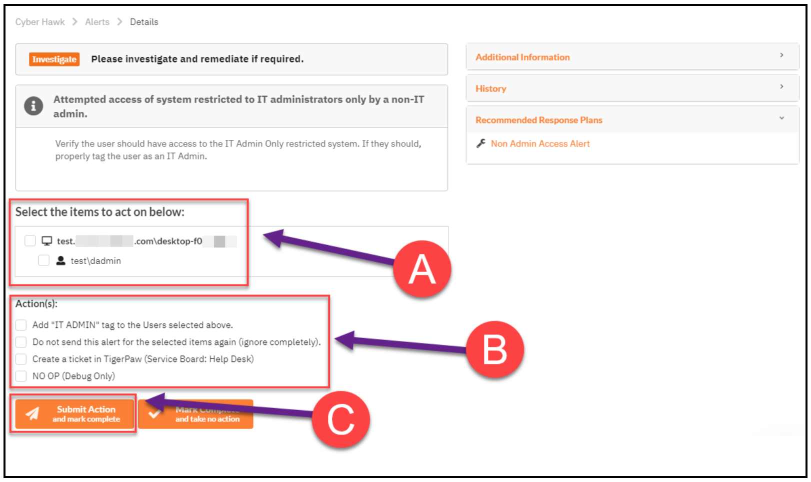
Submit Action and mark complete
Mark Complete and take no action

© 2024 RapidFire Tools, Inc. All rights reserved.

Note: Click ▶ to the right of the Alert for Additional Information, History, Recommended Response Plans, and Related To Do items.

3. Respond to the Alert incident and Investigate Request using these steps:

   a. Select the **computers, users, or other "items"** referenced within the Investigate Request.



Cyber Hawk > Alerts > Details

Investigate Please investigate and remediate if required.

Attempted access of system restricted to IT administrators only by a non-IT admin.

Verify the user should have access to the IT Admin Only restricted system. If they should, properly tag the user as an IT Admin.

Additional Information ›

History ›

Recommended Response Plans ˅

Non Admin Access Alert

Select the items to act on below:

□ test.[redacted].com\desktop-f0[redacted]

□ test\dadmin

Action(s):

□ Add "IT ADMIN" tag to the Users selected above.

□ Do not send this alert for the selected items again (ignore completely).

□ Create a ticket in TigerPaw (Service Board: Help Desk)

□ NO OP (Debug Only)

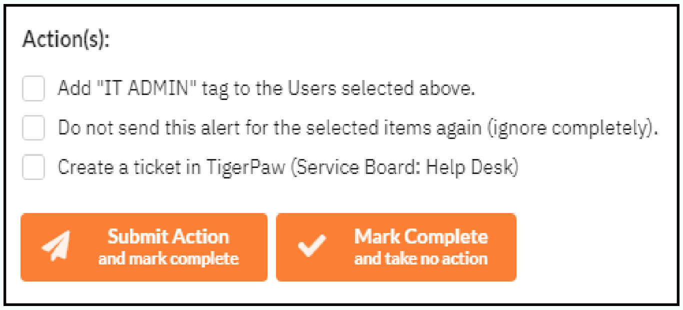
Submit Action and mark complete
Mark Complete and take no action
A
B
C

   b. Select the **Action(s)** that will be assigned to the request. In this case, the Actions available for assignment may include:

- **Remove or add Cyber Hawk Smart-Tags** to computers, users, or other items
- **Create a Ticket** in the Ticketing System you have Mapped to the Site.
- **Assign an Ignore Rule** to the Alert by selecting the "Do not send this alert for the selected items again (ignore completely)".
- Cancel the entire request.

© 2024 RapidFire Tools, Inc. All rights reserved.

Note: You can submit multiple actions for a To Do item.



Action(s):

□ Add "IT ADMIN" tag to the Users selected above.

□ Do not send this alert for the selected items again (ignore completely).

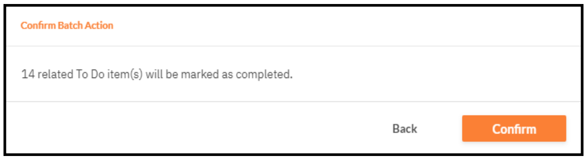
□ Create a ticket in TigerPaw (Service Board: Help Desk)

Submit Action and mark complete
Mark Complete and take no action

4. Click **Submit** to complete your response to the Alert.

   i. In cases where the Alert has multiple Related Alerts, confirm that you wish to apply the actions to these Alerts, as well.

   Note: Related Alerts are Alerts that have been duplicated over time as a result of a recurring Security Policy violation.

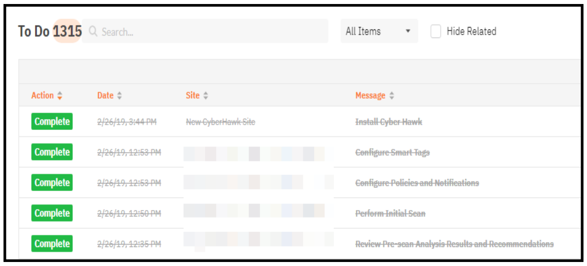


Confirm Batch Action

14 related To Do item(s) will be marked as completed.

A confirmation message will appear.

The completed To Do item's Alert will be moved into the Alerts Queue and marked as **Complete**.



Action	Date	Site	Message
Complete	~~2/26/19, 3:44 PM~~	~~New CyberHawk Site~~	~~Install Cyber Hawk~~
Complete	~~2/26/19, 12:53 PM~~	[redacted]	~~Configure Smart Tags~~
Complete	~~2/26/19, 12:53 PM~~	[redacted]	~~Configure Policies and Notifications~~
Complete	~~2/26/19, 12:50 PM~~	[redacted]	~~Perform Initial Scan~~
Complete	~~2/26/19, 12:35 PM~~	[redacted]	~~Review Pre-scan Analysis Results and Recommendations~~

© 2024 RapidFire Tools, Inc. All rights reserved.

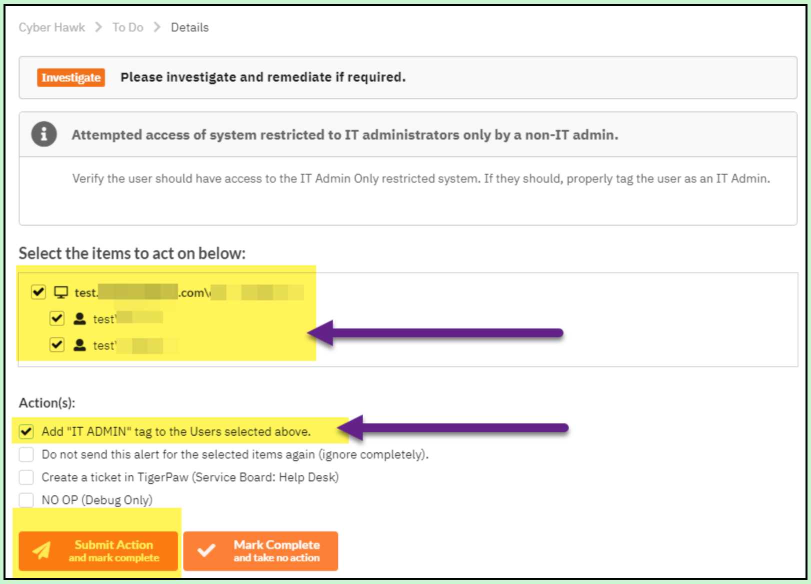
EXAMPLE:

Three Alert Response Scenarios using Cyber Hawk

Let's walk through three scenarios where a Technician responds to security alerts sent out by Cyber Hawk:

#1: "Attempted access of system restricted to IT administrators only by a non-IT admin"

A user is attempting to access a system that should only be accessed by an IT Admin. Cyber Hawk sends you a security alert. You investigate the issue and determine the user is actually an IT Admin and *should* have access to the system. You can use a **Smart Tag** to prevent Cyber Hawk from reporting this "false positive" again. To do this:



Cyber Hawk > To Do > Details

Investigate **Please investigate and remediate if required.**

Attempted access of system restricted to IT administrators only by a non-IT admin.

Verify the user should have access to the IT Admin Only restricted system. If they should, properly tag the user as an IT Admin.

Select the items to act on below:

- ☑ test.[redacted].com\[redacted]
  - ☑ test\[redacted]
  - ☑ test\[redacted]

Action(s):

☑ Add "IT ADMIN" tag to the Users selected above.
☐ Do not send this alert for the selected items again (ignore completely).
☐ Create a ticket in TigerPaw (Service Board: Help Desk)
☐ NO OP (Debug Only)

1. Check the **users** who should have access to the system.
2. Check the **Add "IT Admin" tag to the Users Selected above** option.
3. Click **Submit**.

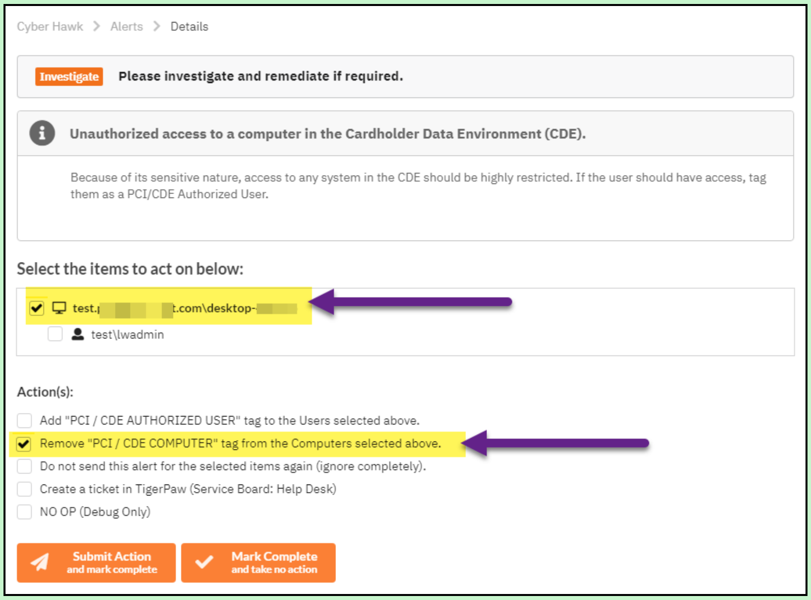
This will add the **IT Admin Smart Tag** to the selected users. Cyber Hawk will now understand that the selected user should have access to the system.

© 2024 RapidFire Tools, Inc. All rights reserved.

Note: This will also change the Smart Tag configuration in the Cyber Hawk settings for this Site.

#2: "Unauthorized access to a computer in the Cardholder Data Environment (CDE)"

Here's another example. You receive an alert that there is unauthorized access to a computer in the Cardholder Data Environment (CDE). You investigate the issue and determine the computer is actually *not* part of the CDE. To prevent this issue from occurring again, you can remove the **"PCI/CDE Computer" Smart Tag** from the selected systems. To do this:



Please investigate and remediate if required.

Unauthorized access to a computer in the Cardholder Data Environment (CDE).

Because of its sensitive nature, access to any system in the CDE should be highly restricted. If the user should have access, tag them as a PCI/CDE Authorized User.

Select the items to act on below:

☑ test.[redacted]t.com\desktop-[redacted]
☐ test\lwadmin

Action(s):

☐ Add "PCI / CDE AUTHORIZED USER" tag to the Users selected above.
☑ Remove "PCI / CDE COMPUTER" tag from the Computers selected above.
☐ Do not send this alert for the selected items again (ignore completely).
☐ Create a ticket in TigerPaw (Service Board: Help Desk)
☐ NO OP (Debug Only)

1. Check the **systems** to remove from the CDE
2. Check **Remove "PCI / CDE Computer" tag from the selected computers**.
3. Click **Submit**.

Cyber Hawk will now understand that the computer is NOT part of the CDE.

Note: This will also change the Smart Tag configuration in the Cyber Hawk settings for this Site.

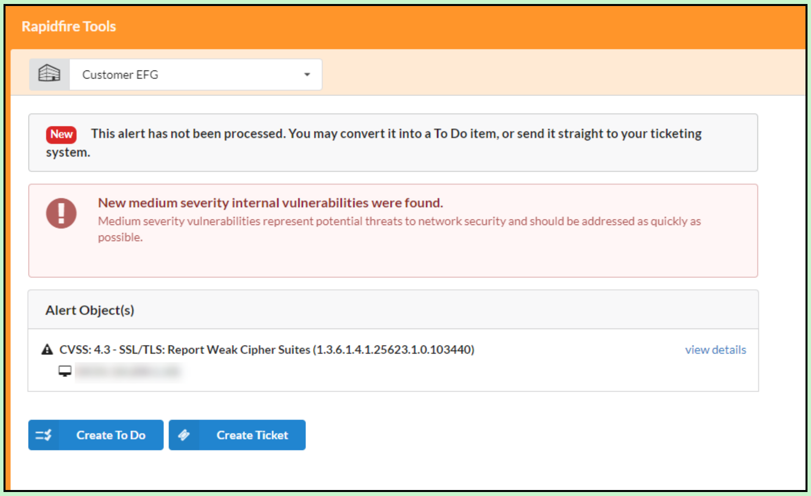
© 2024 RapidFire Tools, Inc. All rights reserved.

#3: "New medium severity internal vulnerabilities were found"

As a result of the internal vulnerability scan performed by Cyber Hawk, a medium severity internal vulnerability is discovered on the network.

In this example, this alert does not have a defined **Action** in the Cyber Hawk Security Policy Notification Rules. Cyber Hawk reports the issue as an alert item viewable in the RapidFire Tools Portal under the **Alerts Queue**.

You open the Alert in the Alerts Queue. You can then **Create a To Do item** for the technician group, or you can **Create a Ticket** in your chosen PSA/ticketing system. You choose to **Create a To Do item**.



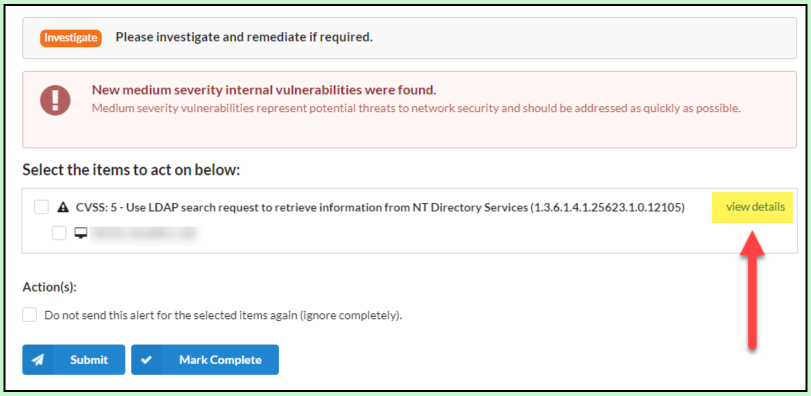
New This alert has not been processed. You may convert it into a To Do item, or send it straight to your ticketing system.

New medium severity internal vulnerabilities were found.
Medium severity vulnerabilities represent potential threats to network security and should be addressed as quickly as possible.

Alert Object(s)

CVSS: 4.3 - SSL/TLS: Report Weak Cipher Suites (1.3.6.1.4.1.25623.1.0.103440) view details
[redacted]

In this case, there are no smart tags associated with this alert. Click **View Details** to review the diagnostic forensic information.


Investigate Please investigate and remediate if required.

New medium severity internal vulnerabilities were found.
Medium severity vulnerabilities represent potential threats to network security and should be addressed as quickly as possible.

Select the items to act on below:

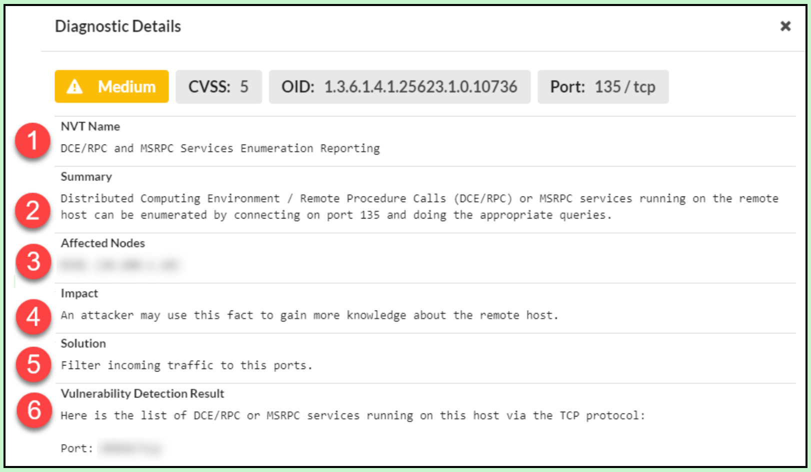
□ CVSS: 5 - Use LDAP search request to retrieve information from NT Directory Services (1.3.6.1.4.1.25623.1.0.12105) view details
□ [redacted]

Action(s):

□ Do not send this alert for the selected items again (ignore completely).

Diagnostic details will appear as a result of the Cyber Hawk scan. This includes:

© 2024 RapidFire Tools, Inc. All rights reserved.



Diagnostic Details

Medium | CVSS: 5 | OID: 1.3.6.1.4.1.25623.1.0.10736 | Port: 135 / tcp

NVT Name
DCE/RPC and MSRPC Services Enumeration Reporting

Summary
Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.

Affected Nodes
[redacted]

Impact
An attacker may use this fact to gain more knowledge about the remote host.

Solution
Filter incoming traffic to this ports.

Vulnerability Detection Result
Here is the list of DCE/RPC or MSRPC services running on this host via the TCP protocol:

Port: [redacted]

1. Name of issue
2. Issue summary
3. Affected Nodes
4. Impact
5. Proposed Solution
6. Vulnerability Detection Results

Use this information to remediate the issue. Then click **Mark Complete**.

© 2024 RapidFire Tools, Inc. All rights reserved.

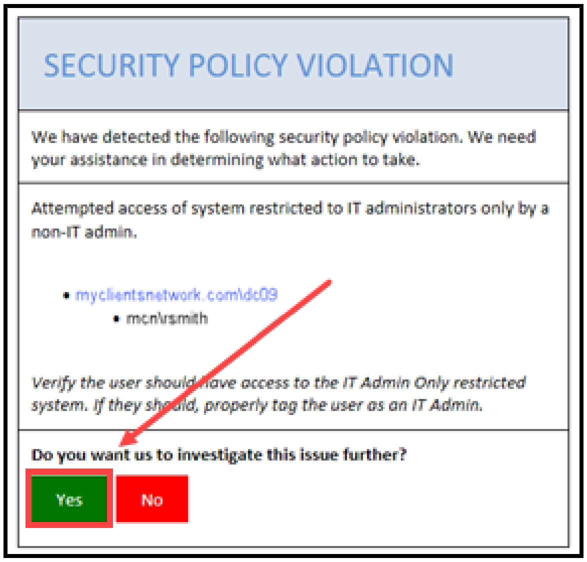
Send the Tech Group an Alert Investigation Request (End User)

You can configure Cyber Hawk to send End Users an Alert Notification whenever a scan reveals a possible security policy violation on the network.

When Cyber Hawk discovers a potential issue, the end user will receive a Security Policy Violation email. This email describes the Alert and allows you to decide whether the Tech Group should investigate the issue further.

In order to request that the Tech Group investigate an issue, follow these steps:

1. Click **Yes** to initiate the investigation request.



SECURITY POLICY VIOLATION

We have detected the following security policy violation. We need your assistance in determining what action to take.

Attempted access of system restricted to IT administrators only by a non-IT admin.

- myclientsnetwork.com\dc09
    - mcn\rsmith

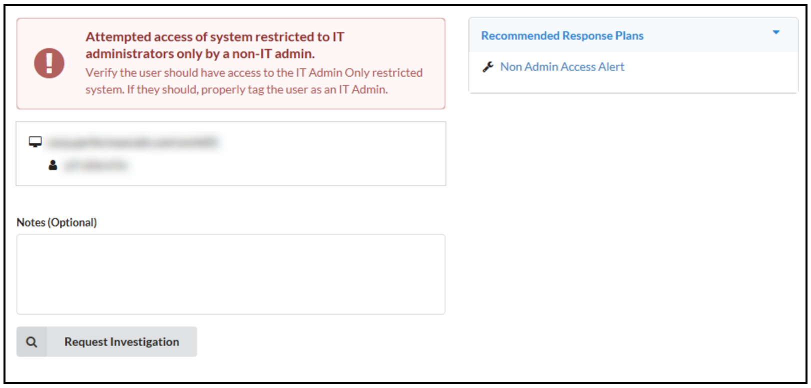
Verify the user should have access to the IT Admin Only restricted system. If they should, properly tag the user as an IT Admin.

Do you want us to investigate this issue further?

A web browser will open and display a page for you to create an Investigate Request.

2. Enter an optional note and click **Request Investigation**.

© 2024 RapidFire Tools, Inc. All rights reserved.



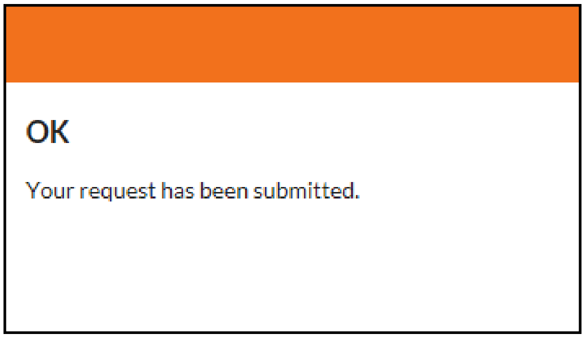
Attempted access of system restricted to IT administrators only by a non-IT admin.
Verify the user should have access to the IT Admin Only restricted system. If they should, properly tag the user as an IT Admin.

[redacted]
[redacted]

Notes (Optional)

> **Note:** End Users only see the screen above. They do not see the **To Do** or **Alerts** tabs.

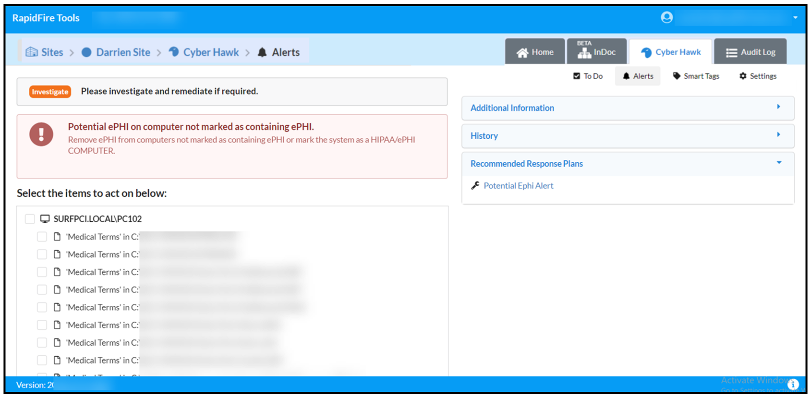
A confirmation will appear indicating that your request has been sent to the Tech Group and added to the RapidFire Tools Portal To Do List.



OK

Your request has been submitted.

An Investigate To Do item will be created for the technicians assigned to service the End User's network.



Investigate Please investigate and remediate if required.

Potential ePHI on computer not marked as containing ePHI.
Remove ePHI from computers not marked as containing ePHI or mark the system as a HIPAA/ePHI COMPUTER.

Select the items to act on below:

- □ SURFPCI.LOCAL\PC102
  - □ 'Medical Terms' in C:[redacted]
  - □ 'Medical Terms' in C:[redacted]
  - □ 'Medical Terms' in C:[redacted]
  - □ 'Medical Terms' in C:[redacted]
  - □ 'Medical Terms' in C:[redacted]
  - □ 'Medical Terms' in C:[redacted]
  - □ 'Medical Terms' in C:[redacted]
  - □ 'Medical Terms' in C:[redacted]

Version: 2[redacted]

© 2024 RapidFire Tools, Inc. All rights reserved.

For details on how the Tech Group responds to End User Alert Investigation Requests, look here.

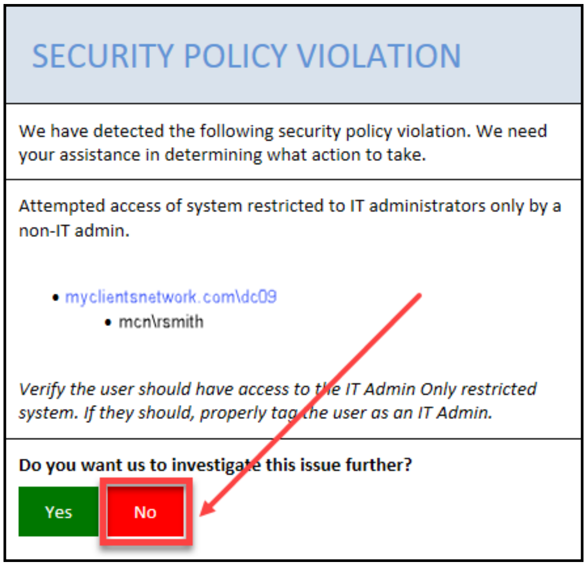
© 2024 RapidFire Tools, Inc. All rights reserved.

Request that the Tech Group Ignore an Alert (End User)

When an End User receives a Security Policy Violation notification, the user can opt to ignore the alert. This is helpful when the user knows that the alert is a "false positive," i.e. an accident or error.

The End User can pass this information along to the Tech Group to inform them to ignore the alert. To do this:

1. Click **No** in the Security Policy Violation email to initiate the Ignore Alert Request.



SECURITY POLICY VIOLATION

We have detected the following security policy violation. We need your assistance in determining what action to take.

Attempted access of system restricted to IT administrators only by a non-IT admin.

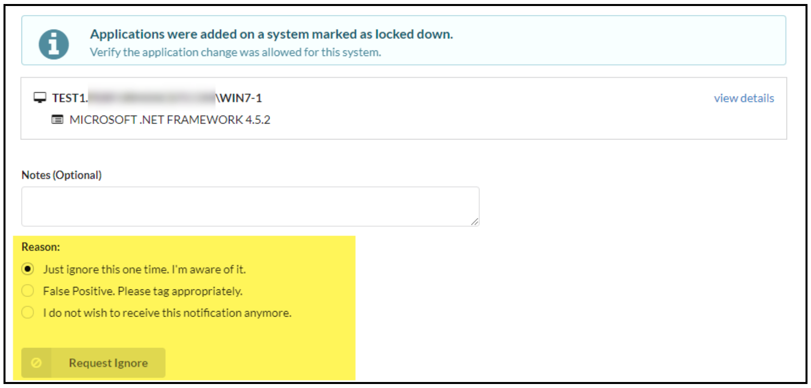
- myclientsnetwork.com\dc09
  - mcn\rsmith

Verify the user should have access to the IT Admin Only restricted system. If they should, properly tag the user as an IT Admin.

Do you want us to investigate this issue further?

A web browser will open and display a page for you to create a request to ignore the alert.

2. Complete the Request Ignore page by adding an optional note and selecting a **Reason** for the issue to be ignored. Then click **Request Ignore**.



Applications were added on a system marked as locked down.
Verify the application change was allowed for this system.

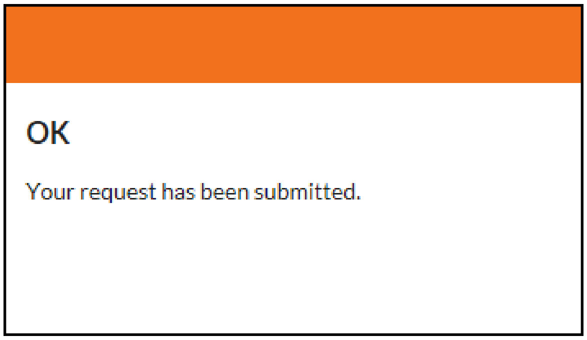
TEST1.[redacted]\WIN7-1
MICROSOFT .NET FRAMEWORK 4.5.2

Notes (Optional)

Reason:
● Just ignore this one time. I'm aware of it.
○ False Positive. Please tag appropriately.
○ I do not wish to receive this notification anymore.

© 2024 RapidFire Tools, Inc. All rights reserved.

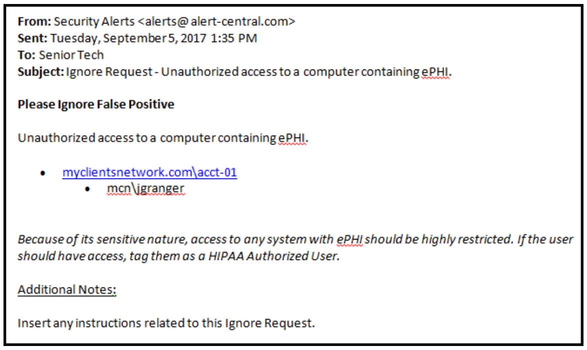
A confirmation will appear indicating that your ignore request has been sent to the Tech Group and added to the RapidFire Tools Portal To Do List.



OK

Your request has been submitted.

An Ignore Request is then sent to the technicians assigned to service the End User's network.



From: Security Alerts <alerts@ alert-central.com>
Sent: Tuesday, September 5, 2017 1:35 PM
To: Senior Tech
Subject: Ignore Request - Unauthorized access to a computer containing ePHI.

Please Ignore False Positive

Unauthorized access to a computer containing ePHI.

- myclientsnetwork.com\acct-01
  - mcn\jgranger

Because of its sensitive nature, access to any system with ePHI should be highly restricted. If the user should have access, tag them as a HIPAA Authorized User.

Additional Notes:

Insert any instructions related to this Ignore Request.

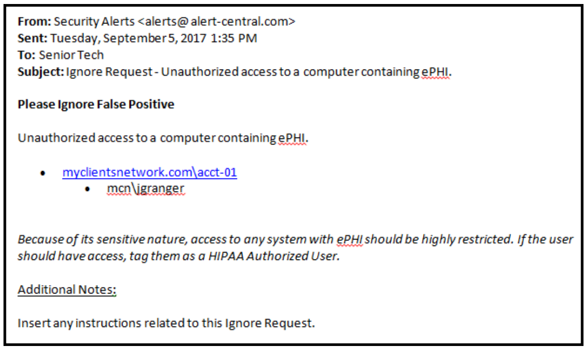
© 2024 RapidFire Tools, Inc. All rights reserved.

Process an Ignore Alert Request (Tech Group)

When an End User requests that an issue be ignored, the Tech Group will receive an Ignore Request notification. Ignore Requests direct technicians to apply an Ignore Rule to an Alert. This helps eliminate false positives.

To process an Ignore Alert Request as a member of the Tech Group:

1. Click the link in the Ignore Request email.



From: Security Alerts <alerts@ alert-central.com>
Sent: Tuesday, September 5, 2017 1:35 PM
To: Senior Tech
Subject: Ignore Request - Unauthorized access to a computer containing ePHI.

Please Ignore False Positive

Unauthorized access to a computer containing ePHI.

- myclientsnetwork.com\acct-01
  - mcn\jgranger

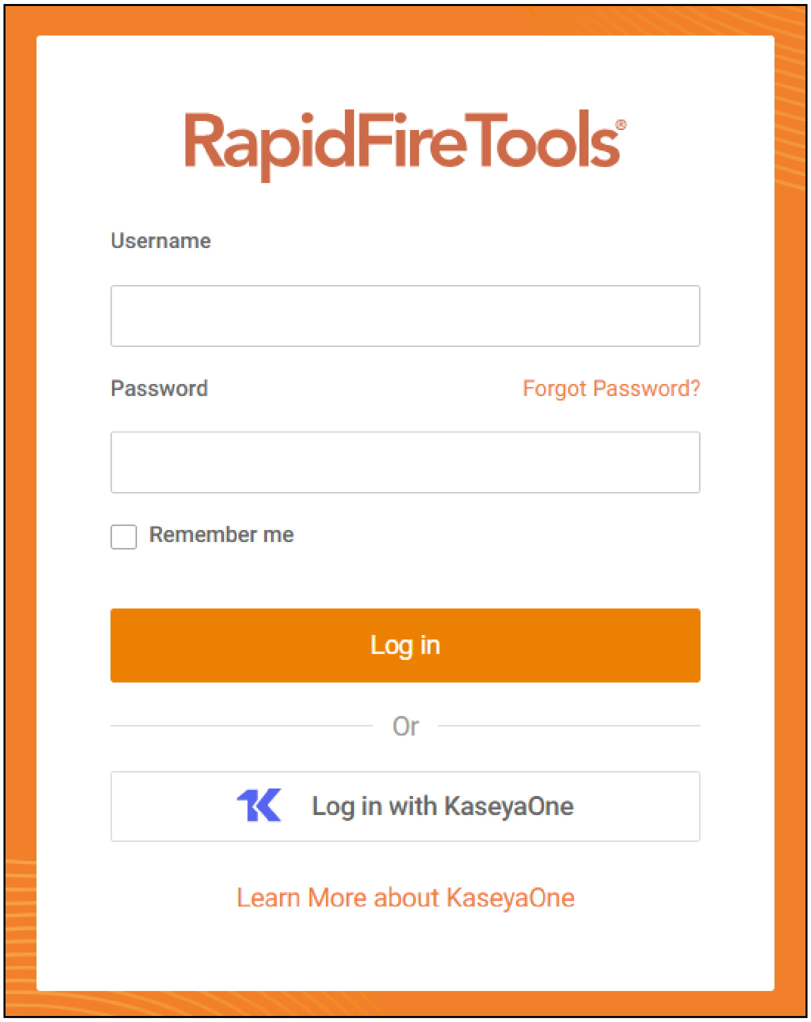
Because of its sensitive nature, access to any system with ePHI should be highly restricted. If the user should have access, tag them as a HIPAA Authorized User.

Additional Notes:

Insert any instructions related to this Ignore Request.

2. The RapidFire Tools Login Page will be displayed. Log in to the Portal using your Detective credentials.

© 2024 RapidFire Tools, Inc. All rights reserved.



RapidFireTools®

Username

Password Forgot Password?

□ Remember me

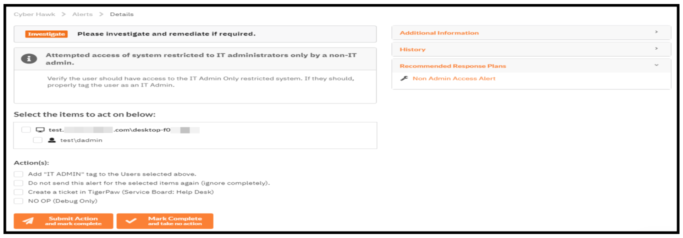
Log in

Or

Log in with KaseyaOne

Learn More about KaseyaOne

3. After you log in, the Alert Item will appear.



Cyber Hawk > Alerts > Details

Investigate Please investigate and remediate if required.

Attempted access of system restricted to IT administrators only by a non-IT admin.

Verify the user should have access to the IT Admin Only restricted system. If they should, properly tag the user as an IT Admin.

Select the items to act on below:

□ test.[redacted].com\desktop-f0[redacted]

□ test\dadmin

Action(s):

□ Add "IT ADMIN" tag to the Users selected above.

□ Do not send this alert for the selected items again (ignore completely).

□ Create a ticket in TigerPaw (Service Board: Help Desk)

□ NO OP (Debug Only)

Submit Action and mark complete
Mark Complete and take no action
Additional Information
History
Recommended Response Plans
Non Admin Access Alert

> **Note:** Click ▸ to the right of the Alert for Additional Information, History, Recommended Response Plans, and Related To Do items.

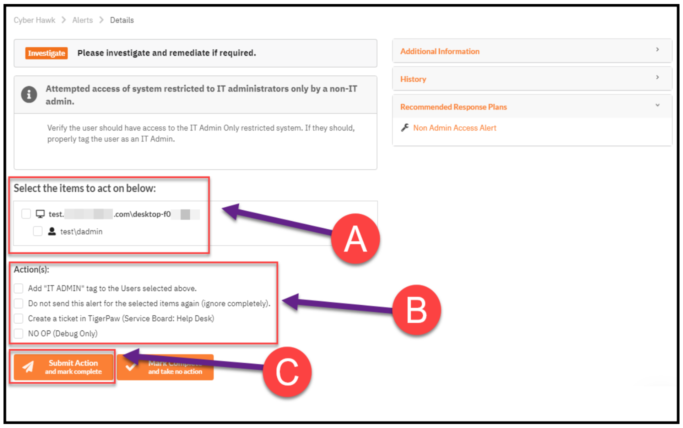
4. Additional Information and History section headings to review any additional details concerning the Alert.

5. Respond to the Alert incident and Ignore Request using these steps:

© 2024 RapidFire Tools, Inc. All rights reserved.

a. Select the **computers, users, or other "items"** referenced within the Ignore Request.

b. Select the **Action(s)** that will be assigned to the request. In this case, the Ignore Actions available for assignment may include:



Cyber Hawk > Alerts > Details

Investigate Please investigate and remediate if required.

Attempted access of system restricted to IT administrators only by a non-IT admin.

Verify the user should have access to the IT Admin Only restricted system. If they should, properly tag the user as an IT Admin.

Additional Information

History

Recommended Response Plans

Non Admin Access Alert

Select the items to act on below:

□ test.[redacted].com\desktop-f0[redacted]

□ test\dadmin

Action(s):

□ Add "IT ADMIN" tag to the Users selected above.

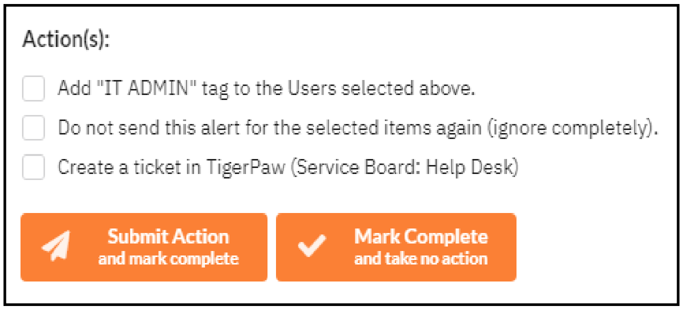
□ Do not send this alert for the selected items again (ignore completely).

□ Create a ticket in TigerPaw (Service Board: Help Desk)

□ NO OP (Debug Only)

Submit Action and mark complete
Mark Complete and take no action
A
B
C

- **Remove or add Cyber Hawk Smart-Tags** to computers, users, or other items.
- **Assign an Ignore Rule** to the Alert by selecting the "Do not send this alert for the selected items again (ignore completely)".
- **Create a Ticket** in the Ticketing System you have Mapped to the Site.
- Cancel the entire request by selecting no Actions and selecting the Mark Complete button.



Action(s):

□ Add "IT ADMIN" tag to the Users selected above.

□ Do not send this alert for the selected items again (ignore completely).

□ Create a ticket in TigerPaw (Service Board: Help Desk)

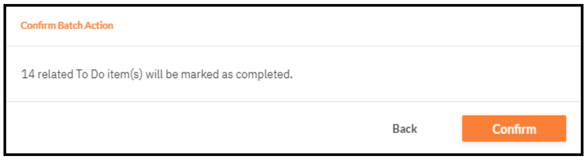
Submit Action and mark complete
Mark Complete and take no action

> **Note:** The user can perform both the remove/add Smart-Tag Action along with creating an Ignore Rule or any other Action simultaneously when processing the Alert's To Do item.

c. Select the **Submit** button to complete the processing of the Ignore Request To Do item.

© 2024 RapidFire Tools, Inc. All rights reserved.

6. This window is displayed in cases where you are processing an Alert that has one or more “Related Alerts”.

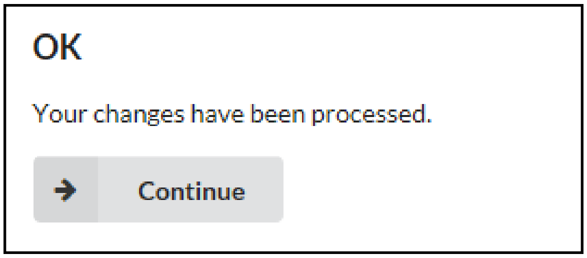


Confirm Batch Action

14 related To Do item(s) will be marked as completed.

7. Related Alerts are essentially alerts that have been duplicated on a day by day basis as a result of a recurring Security Policy violation. Select the Confirm button to complete the To Do item and close any Related Alerts.

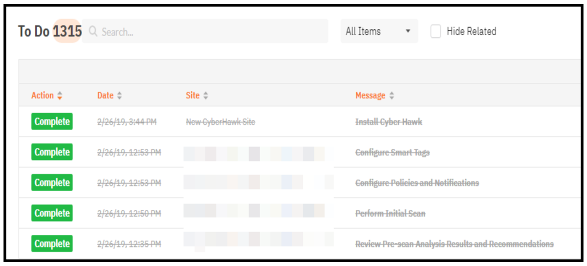
   A Confirmation of your submission will be displayed



OK

Your changes have been processed.

The completed To Do item’s Alert will be moved into the Alerts Queue contained within the RapidFire Tools Portal with a Status assigned as Complete



Action	Date	Site	Message
Complete	~~2/26/19, 3:44 PM~~	~~New CyberHawk Site~~	~~Install Cyber Hawk~~
Complete	~~2/26/19, 12:53 PM~~	[redacted]	~~Configure Smart Tags~~
Complete	~~2/26/19, 12:53 PM~~	[redacted]	~~Configure Policies and Notifications~~
Complete	~~2/26/19, 12:50 PM~~	[redacted]	~~Perform Initial Scan~~
Complete	~~2/26/19, 12:35 PM~~	[redacted]	~~Review Pre-scan Analysis Results and Recommendations~~

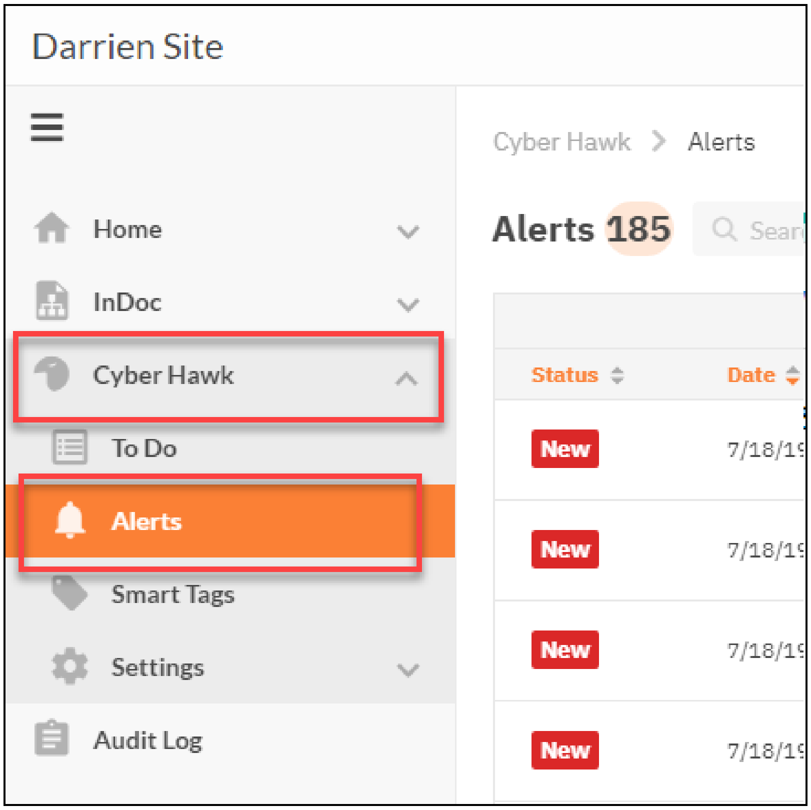
Using the RapidFire Tools Portal

This section covers using the RapidFire Tools Portal for Cyber Hawk. The RapidFire Tools Portal gives your tech group and end users at the client's site more capabilities in responding to Cyber Hawk security policy violation alerts.

© 2024 RapidFire Tools, Inc. All rights reserved.

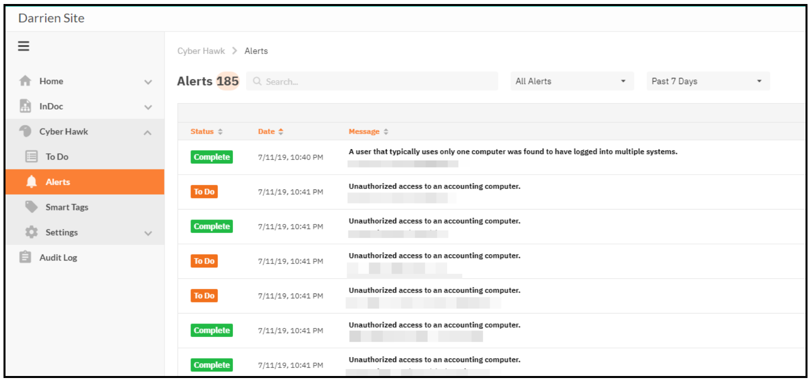
Alerts

When Cyber Hawk discovers a potential security policy violation, it creates an item in the **Alerts** sub-tab.



Status	Date
New	7/18/1
New	7/18/1
New	7/18/1
New	7/18/1

The Alerts tab provides a "bird's eye view" of all suspicious activity on the target network. Every issue identified by Cyber Hawk appears in the **Alerts** tab.



Status	Date	Message
Complete	7/11/19, 10:40 PM	A user that typically uses only one computer was found to have logged into multiple systems. [redacted]
To Do	7/11/19, 10:41 PM	Unauthorized access to an accounting computer. [redacted]
Complete	7/11/19, 10:41 PM	Unauthorized access to an accounting computer. [redacted]
To Do	7/11/19, 10:41 PM	Unauthorized access to an accounting computer. [redacted]
To Do	7/11/19, 10:41 PM	Unauthorized access to an accounting computer. [redacted]
Complete	7/11/19, 10:41 PM	Unauthorized access to an accounting computer. [redacted]
Complete	7/11/19, 10:41 PM	Unauthorized access to an accounting computer. [redacted]

© 2024 RapidFire Tools, Inc. All rights reserved.

Each Alert’s entry in the Queue presents the Alert’s Status, the Date the Alert was generated, which Site it is associated with and the Message that was generated as part of the Alert’s creation.

How Long Do Alerts Last in the Portal?

Cyber Hawk Alert Items are retained in the Alert Queue for a period of 2 weeks before being removed from the RapidFIre Tools Portal.

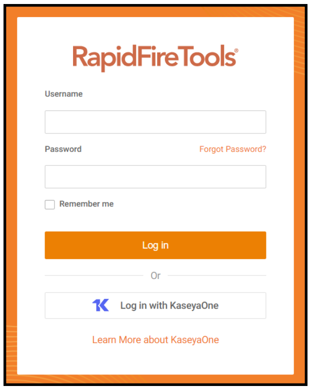
See also:

- "View and Process Alerts" below
- "Alert Item Statuses" on the facing page
- "Filter Alert Queue by Status" on page 150
- "Create To Do Items from Alerts " on page 157
- "Revert Completed Alerts Back to the To Do Items" on page 151

View and Process Alerts

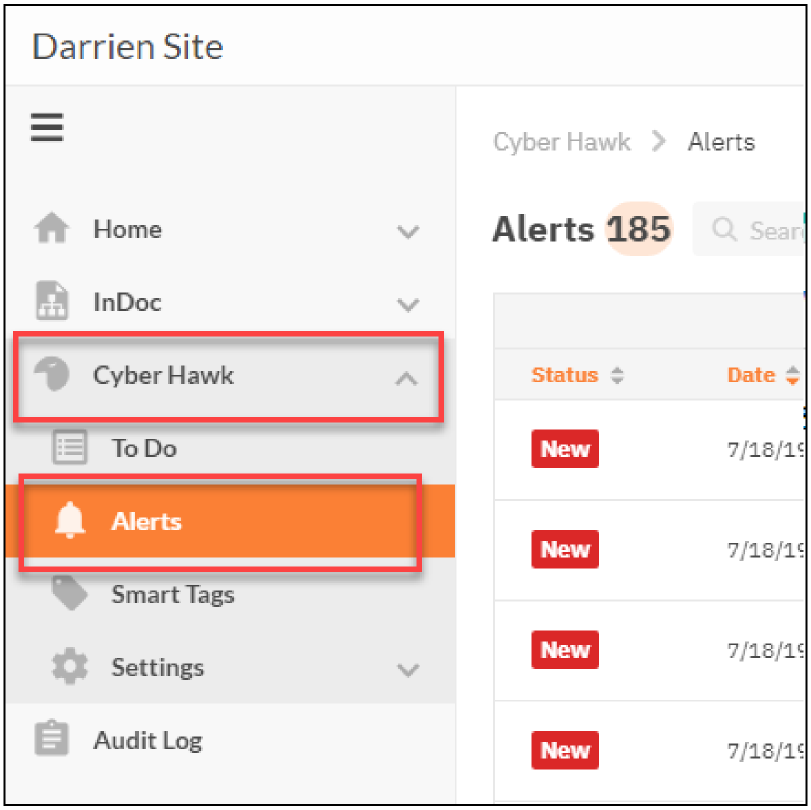
To view and process Alert items:

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



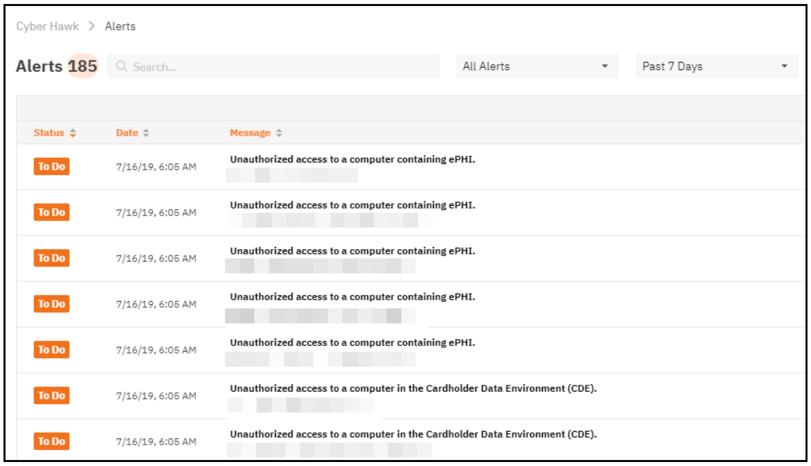
2. Open your Site and go to the **Cyber Hawk tab** > **Alerts**.

© 2024 RapidFire Tools, Inc. All rights reserved.



Status	Date
New	7/18/1
New	7/18/1
New	7/18/1
New	7/18/1

3. **Click on an Alert item** to investigate the issue and access additional features.



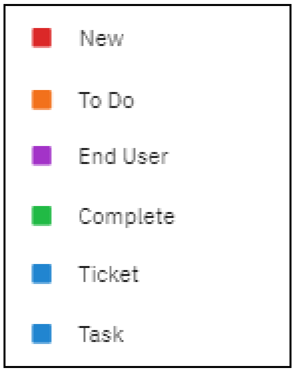
Status	Date	Message
To Do	7/16/19, 6:05 AM	Unauthorized access to a computer containing ePHI. [redacted]
To Do	7/16/19, 6:05 AM	Unauthorized access to a computer containing ePHI. [redacted]
To Do	7/16/19, 6:05 AM	Unauthorized access to a computer containing ePHI. [redacted]
To Do	7/16/19, 6:05 AM	Unauthorized access to a computer containing ePHI. [redacted]
To Do	7/16/19, 6:05 AM	Unauthorized access to a computer containing ePHI. [redacted]
To Do	7/16/19, 6:05 AM	Unauthorized access to a computer in the Cardholder Data Environment (CDE). [redacted]
To Do	7/16/19, 6:05 AM	Unauthorized access to a computer in the Cardholder Data Environment (CDE). [redacted]

Alert Item Statuses

For each Alert in the Alert Queue, a Status is assigned.

These statuses are:

© 2024 RapidFire Tools, Inc. All rights reserved.



🟥 New
🟧 To Do
🟪 End User
🟩 Complete
🟦 Ticket
🟦 Task

New – Cyber Hawk has discovered a security policy violation, but you have not assigned an **Action** to this policy. Click on the item to create a new To Item for your Tech Group to investigate, or a create a ticket in your PSA.

To Do – this status indicates that the Alert is associated with an open To Do item. The Tech Group has been assigned to investigate this issue. You can view the list of issues assigned to the Tech Group from the To Do tab.

End User – this status indicates that the Alert has been sent to an end user at the client site. The End User will review the alert and request that your Tech Group investigate or ignore the issue.

Complete – this status indicates that an Alert associated with a To Do item has been processed and closed. You can click on the item to revert/reopen it.

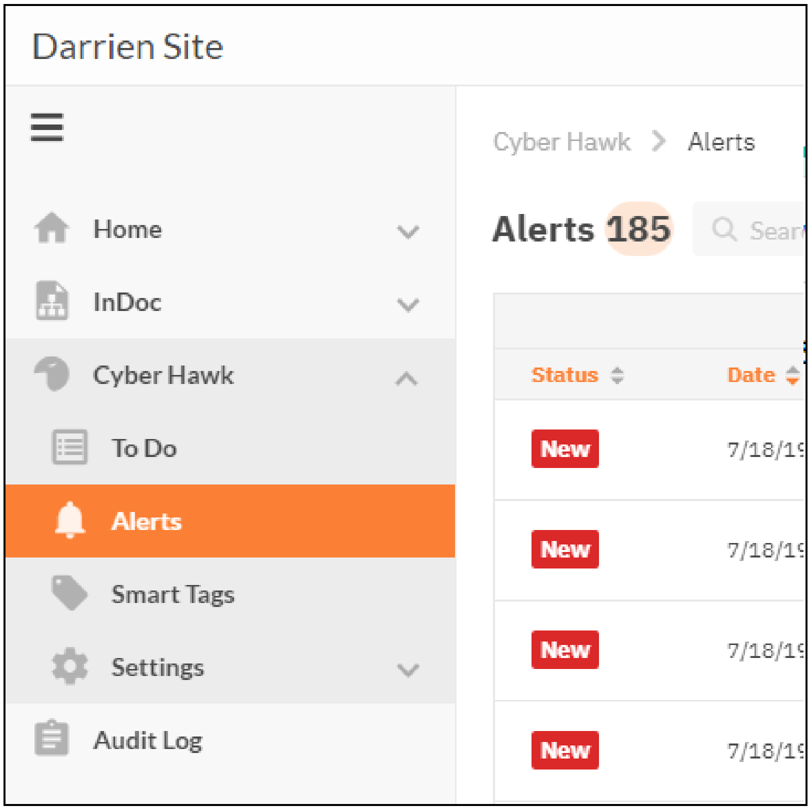
Ticket – this status indicates that an Alert's notification rule was set to automatically generate a Ticket in the Ticketing/PSA system configured to operate with the Cyber Hawk system and a specific Site used to manage a Cyber Hawk.

Task – this status is for tasks that must be completed to advance a compliance assessment using Audit Guru.

© 2024 RapidFire Tools, Inc. All rights reserved.

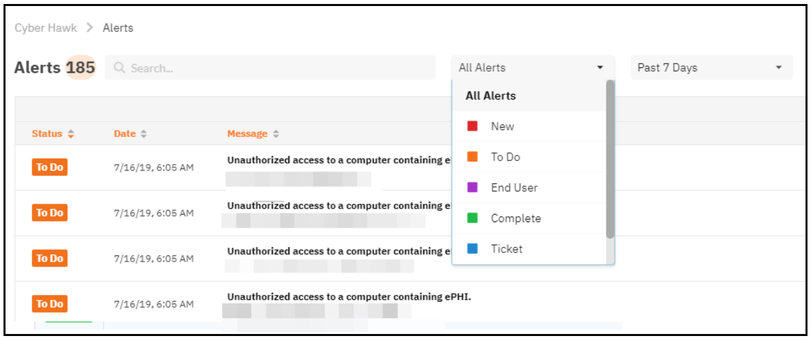
Filter Alert Queue by Status

1. Select the Alerts view.



Status	Date
New	7/18/19
New	7/18/19
New	7/18/19
New	7/18/19

2. Select the Status for the types of Alerts that you want to be displayed in the Alerts Queue.

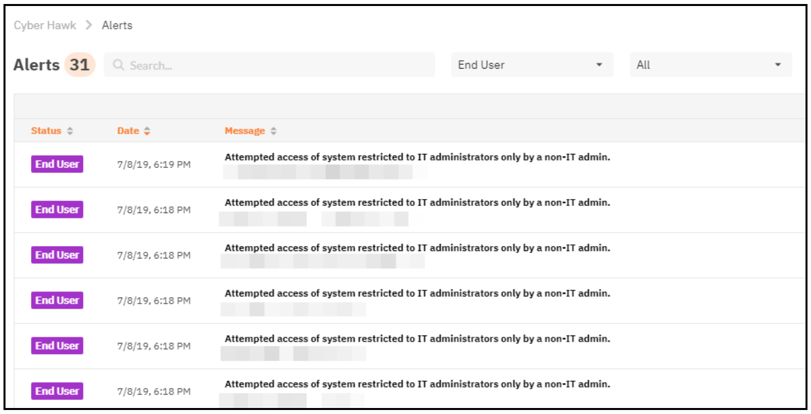


Status	Date	Message
To Do	7/16/19, 6:05 AM	Unauthorized access to a computer containing e
To Do	7/16/19, 6:05 AM	Unauthorized access to a computer containing e
To Do	7/16/19, 6:05 AM	Unauthorized access to a computer containing e
To Do	7/16/19, 6:05 AM	Unauthorized access to a computer containing ePHI.

3. The Alert Queue list will be updated to display Alert items that are assigned the

© 2024 RapidFire Tools, Inc. All rights reserved.

Status you selected.



Status	Date	Message
End User	7/8/19, 6:19 PM	Attempted access of system restricted to IT administrators only by a non-IT admin. [redacted]
End User	7/8/19, 6:18 PM	Attempted access of system restricted to IT administrators only by a non-IT admin. [redacted]
End User	7/8/19, 6:18 PM	Attempted access of system restricted to IT administrators only by a non-IT admin. [redacted]
End User	7/8/19, 6:18 PM	Attempted access of system restricted to IT administrators only by a non-IT admin. [redacted]
End User	7/8/19, 6:18 PM	Attempted access of system restricted to IT administrators only by a non-IT admin. [redacted]
End User	7/8/19, 6:18 PM	Attempted access of system restricted to IT administrators only by a non-IT admin. [redacted]

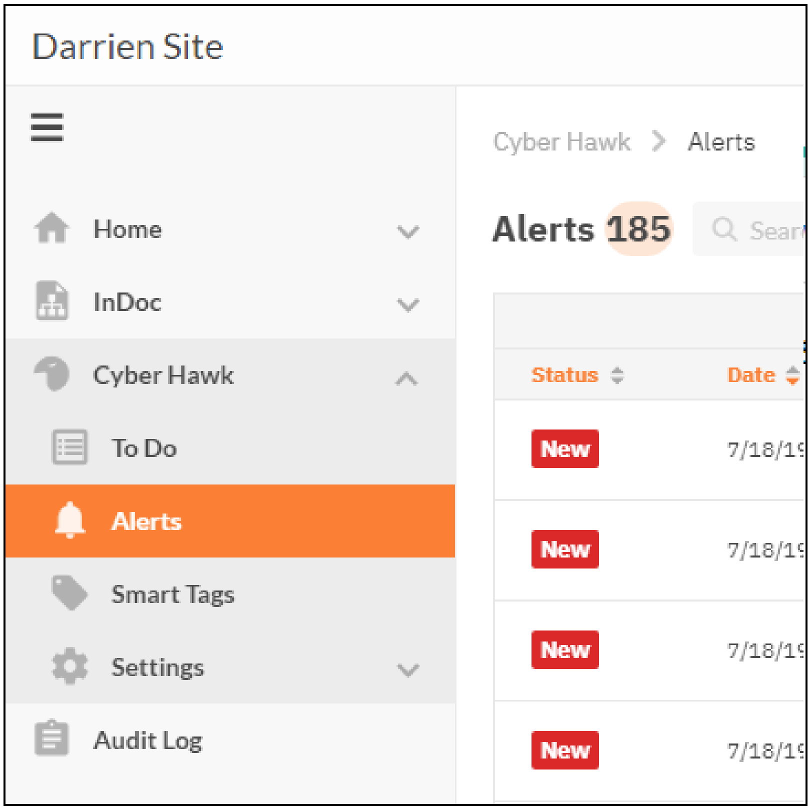
Revert Completed Alerts Back to the To Do Items

To move a Completed Alert back to the To Do list for further reinvestigation and Alert Response Action processing you may “Revert” the Completed Alert.

Follow these steps to Revert a Completed Alert item back to the To Do list:

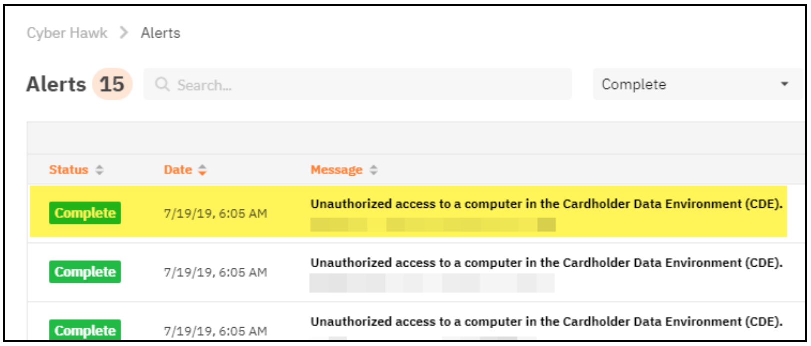
© 2024 RapidFire Tools, Inc. All rights reserved.

1. Select the **Alerts** view.



Status	Date
New	7/18/1
New	7/18/1
New	7/18/1
New	7/18/1

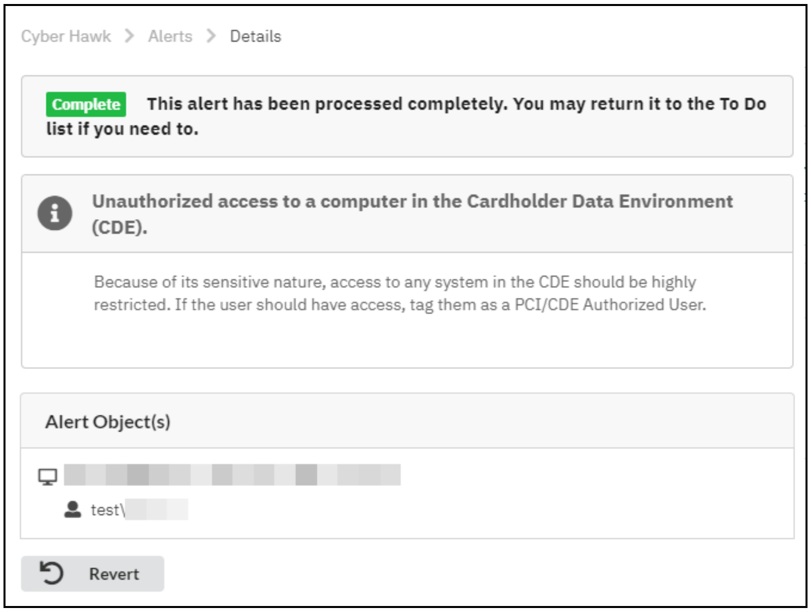
2. To view an Alert's details, click on a Completed Alert item to open the Alert details page.



Status	Date	Message
Complete	7/19/19, 6:05 AM	Unauthorized access to a computer in the Cardholder Data Environment (CDE). [redacted]
Complete	7/19/19, 6:05 AM	Unauthorized access to a computer in the Cardholder Data Environment (CDE). [redacted]
Complete	7/19/19, 6:05 AM	Unauthorized access to a computer in the Cardholder Data Environment (CDE).

3. The Alert's details page is displayed

© 2024 RapidFire Tools, Inc. All rights reserved.



Complete This alert has been processed completely. You may return it to the To Do list if you need to.

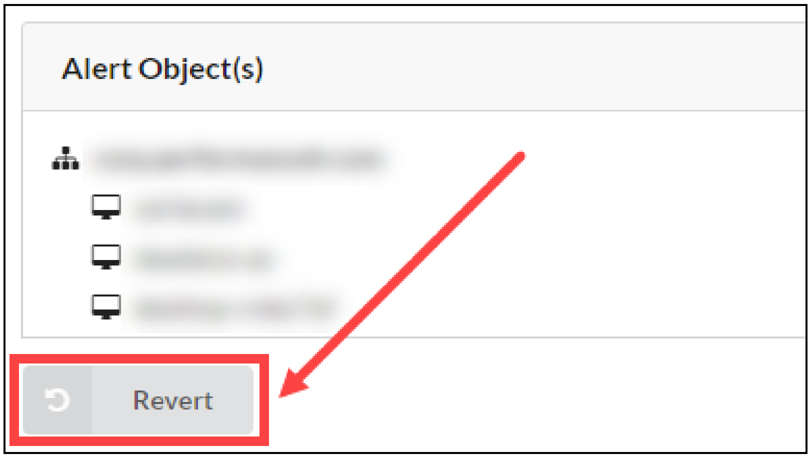
Unauthorized access to a computer in the Cardholder Data Environment (CDE).

Because of its sensitive nature, access to any system in the CDE should be highly restricted. If the user should have access, tag them as a PCI/CDE Authorized User.

Alert Object(s)

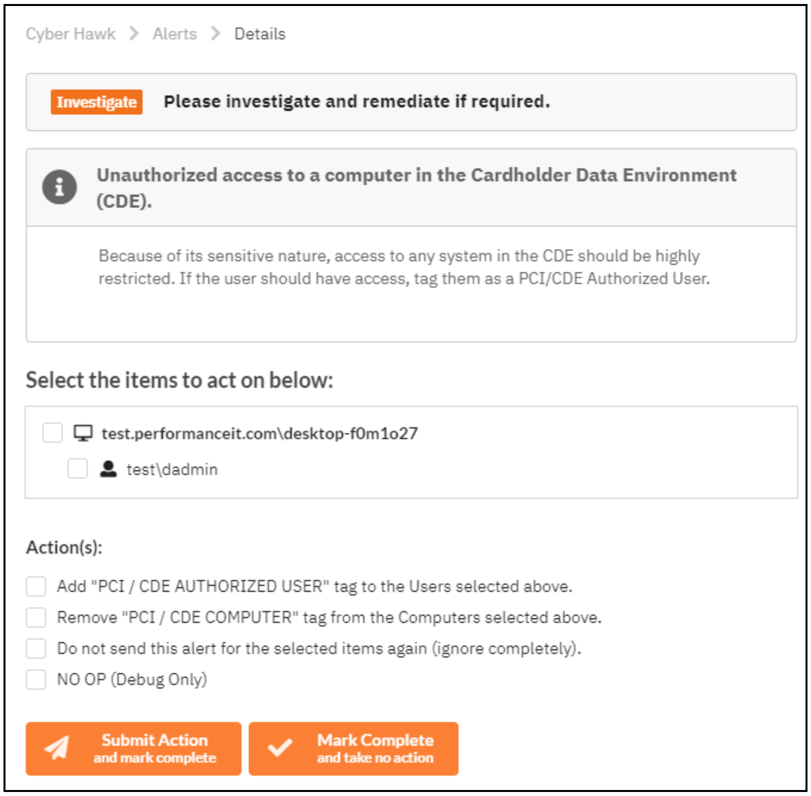
test\

4. Select the Revert button to create a To Do item for the selected Alert.



5. The To Do item will be added to the To Do list, and the Alert's To Do item page will be automatically displayed.

© 2024 RapidFire Tools, Inc. All rights reserved.



Cyber Hawk > Alerts > Details

Investigate Please investigate and remediate if required.

Unauthorized access to a computer in the Cardholder Data Environment (CDE).

Because of its sensitive nature, access to any system in the CDE should be highly restricted. If the user should have access, tag them as a PCI/CDE Authorized User.

Select the items to act on below:

□ test.performanceit.com\desktop-f0m1o27
  □ test\dadmin

Action(s):

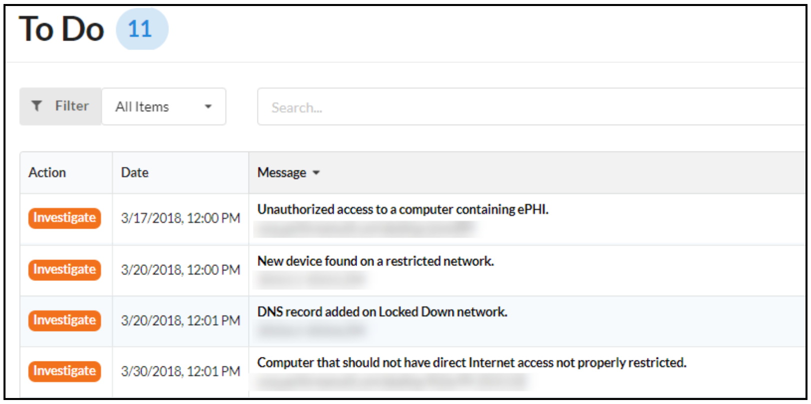
□ Add "PCI / CDE AUTHORIZED USER" tag to the Users selected above.
□ Remove "PCI / CDE COMPUTER" tag from the Computers selected above.
□ Do not send this alert for the selected items again (ignore completely).
□ NO OP (Debug Only)

6. Process the Alert’s To Do item as by select the Actions to apply to the Alert and Submit to Complete the item.

© 2024 RapidFire Tools, Inc. All rights reserved.

To Dos

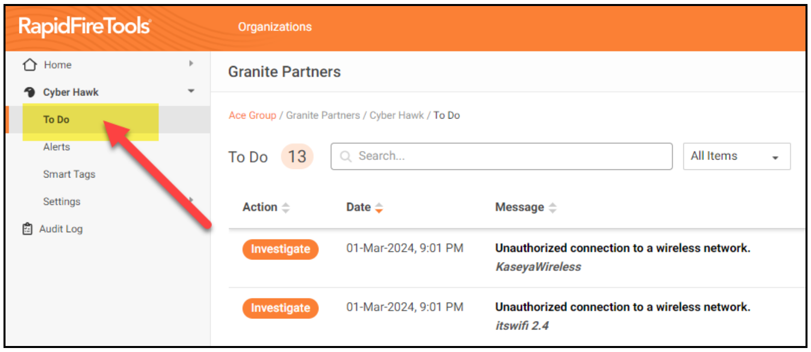
To Dos for Cyber Hawk are Alerts that have been assigned to your Tech Group for investigation.



To Do 11

Action	Date	Message
Investigate	3/17/2018, 12:00 PM	Unauthorized access to a computer containing ePHI. [redacted]
Investigate	3/20/2018, 12:00 PM	New device found on a restricted network. [redacted]
Investigate	3/20/2018, 12:01 PM	DNS record added on Locked Down network. [redacted]
Investigate	3/30/2018, 12:01 PM	Computer that should not have direct Internet access not properly restricted. [redacted]

Tip: You can think of **To Dos** as a *sub-status* of Alerts. All To Dos can be viewed in the Alerts tab, where they will have the status of "To Do." To Do items themselves do not have a status; they are just one possible phase in processing alerts using Cyber Hawk. To Do items and the To Do tab help organize alerts that have been assigned to your technicians.



Granite Partners

Ace Group / Granite Partners / Cyber Hawk / To Do

To Do 13

Action	Date	Message
Investigate	01-Mar-2024, 9:01 PM	**Unauthorized connection to a wireless network.** *KaseyaWireless*
Investigate	01-Mar-2024, 9:01 PM	**Unauthorized connection to a wireless network.** *itswifi 2.4*

When you set up Cyber Hawk at a Site, you can choose to:

A. Configure a Notification Action to assign To Dos to the Tech Group automatically (see "Set Up Tech Group Alert Notifications" on page 110)

B. Configure a Notification Action to request that an End User evaluate the alert, and then request your Tech Group to *investigate* or *ignore* the issue (see "Set Up End User Alert Notifications" on page 106)

Note: End Users do not receive To Dos.

© 2024 RapidFire Tools, Inc. All rights reserved.

C. Browse the Alerts queue and choose whether to *manually assign alerts to the Tech group* or *create tickets in your favorite PSA/Ticketing system*

> **Note:** You must perform one of the above actions for your Tech Group to receive To Dos.

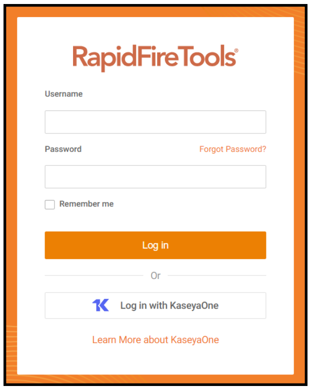
How Long Do To Do Items Last in the Portal?

Cyber Hawk To Do Items are retained in the To Do Queue for a period of 2 weeks before being removed from the RapidFIre Tools Portal.

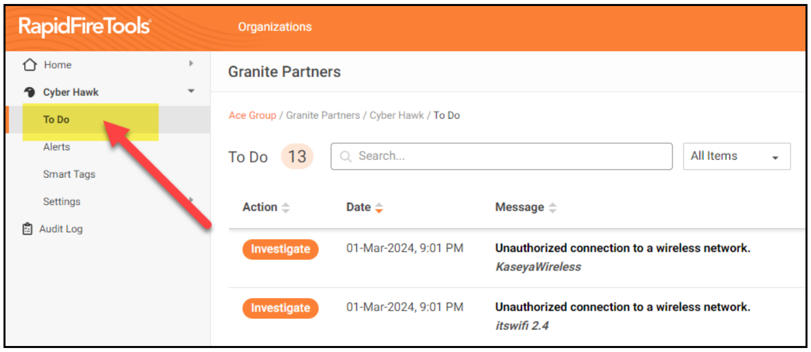
View and Process To Dos

To view and process To Do items:

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



2. From your Cyber Hawk site, click the **To Do** tab.



Action	Date	Message
Investigate	01-Mar-2024, 9:01 PM	**Unauthorized connection to a wireless network.** *KaseyaWireless*
Investigate	01-Mar-2024, 9:01 PM	**Unauthorized connection to a wireless network.** *itswifi 2.4*

3. **Click on a To Do item** to investigate the issue and access additional features.

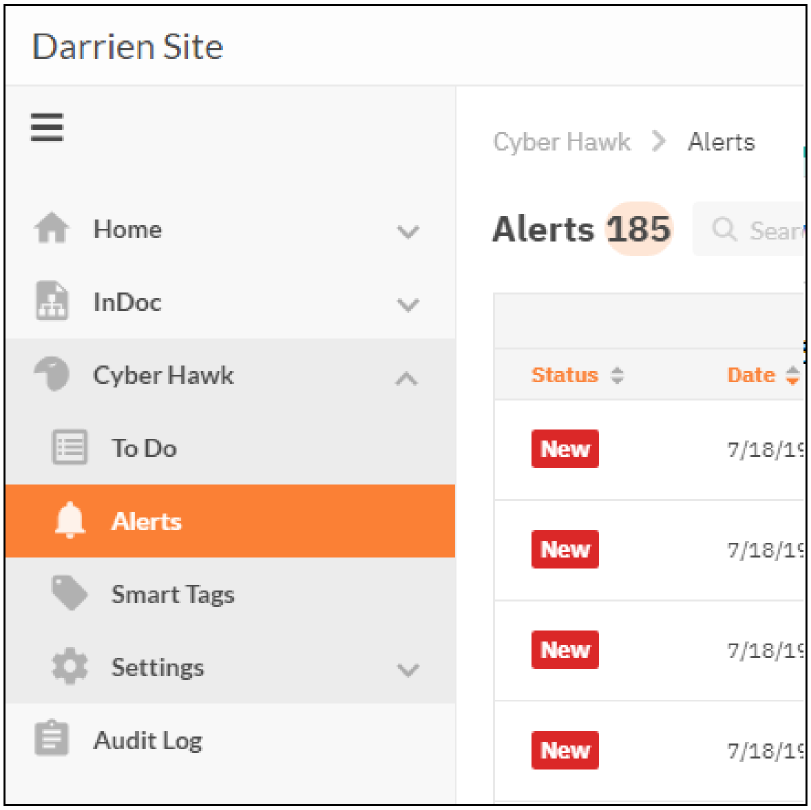
© 2024 RapidFire Tools, Inc. All rights reserved.

Create To Do Items from Alerts

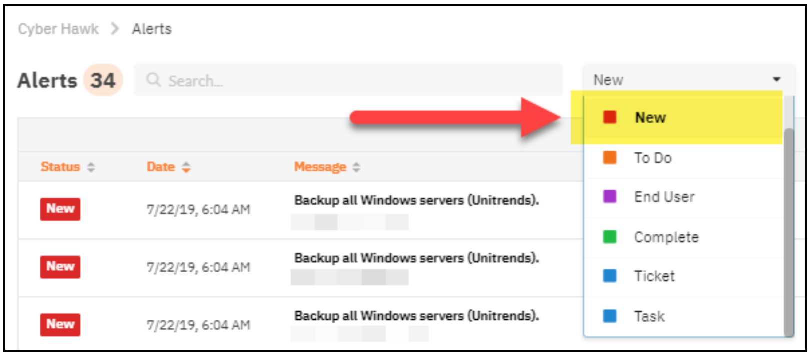
To Do items can be created for Alerts that have been assigned a Status of either “New” or “Ticket” to the Alert when the Alert is viewed in the Alert Queue.

Follow the steps below to create a To Do item from an Alert located in the Alert Queue:

1. Select the **Alerts** view to access the Alert Queue.



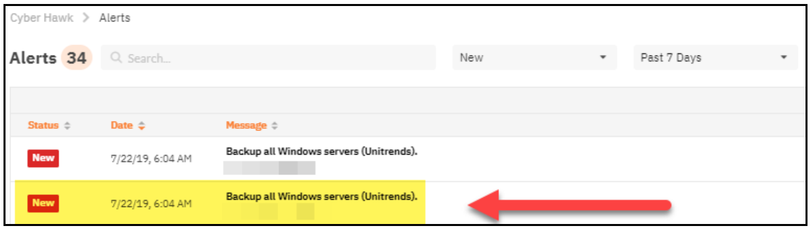
2. Filter the Alerts to view Alert items that have been assigned a Status of either “New” or “Ticket”.



Status	Date	Message
New	7/22/19, 6:04 AM	Backup all Windows servers (Unitrends).
New	7/22/19, 6:04 AM	Backup all Windows servers (Unitrends).
New	7/22/19, 6:04 AM	Backup all Windows servers (Unitrends).

© 2024 RapidFire Tools, Inc. All rights reserved.

3. Select a specific Alert to view the Alert's details.

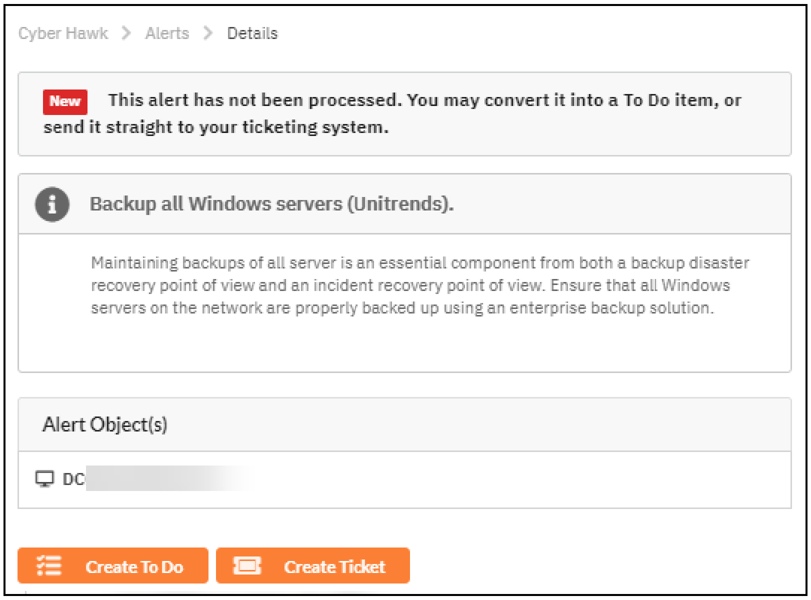


Cyber Hawk > Alerts

Alerts 34 Search... New Past 7 Days

Status	Date	Message
New	7/22/19, 6:04 AM	Backup all Windows servers (Unitrends). [redacted]
New	7/22/19, 6:04 AM	Backup all Windows servers (Unitrends). [redacted]

4. The Alert's Details window will be displayed.



Cyber Hawk > Alerts > Details

New This alert has not been processed. You may convert it into a To Do item, or send it straight to your ticketing system.

Backup all Windows servers (Unitrends).

Maintaining backups of all server is an essential component from both a backup disaster recovery point of view and an incident recovery point of view. Ensure that all Windows servers on the network are properly backed up using an enterprise backup solution.

Alert Object(s)

DC[redacted]

5. To transform the Alert into a To Do item or generate a Ticket from the Alert, select either the Create To Do or the Create Ticket option.

   Or, you can select the Alerts view to return to the Alerts Queue.

   If you select the Create To Do option, the To Do item will be added to the To Do list, and the Alert's To Do item page will be automatically displayed.

   If you select the Create Ticket option, then a Ticket will be created in the Ticketing/PSA system that is Mapped to the Cyber Hawk Site as defined in the RapidFire Tools Portal Settings.

© 2024 RapidFire Tools, Inc. All rights reserved.

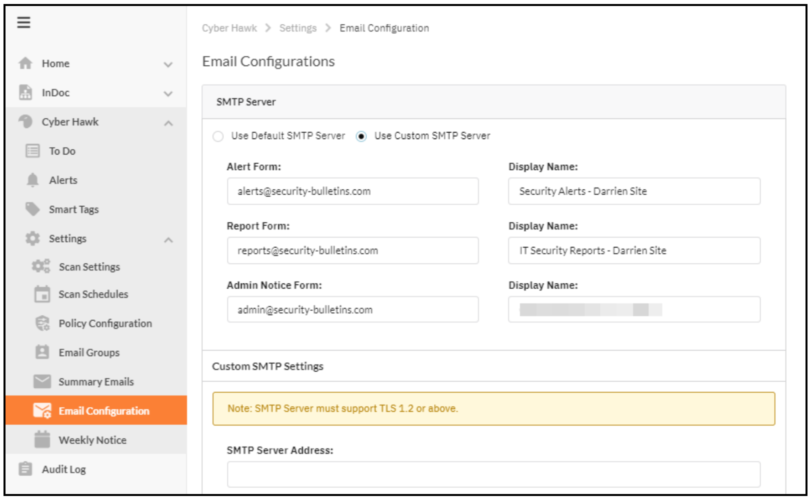
Set Up Custom SMTP Server Support

Follow these steps to set up the use of your own SMTP server to send Alerts and Notices from Cyber Hawk.

1. From your Cyber Hawk Site, go to **Cyber Hawk tab** > **Settings** > **Email Configuration**.

   The Email Configuration window will be displayed.

2. Select **Use Custom SMTP Server** tab within the Email Configuration window to access the Custom SMTP Server settings.



Cyber Hawk > Settings > Email Configuration

Email Configurations

SMTP Server

○ Use Default SMTP Server ● Use Custom SMTP Server

Alert Form: alerts@security-bulletins.com

Display Name: Security Alerts - Darrien Site

Report Form: reports@security-bulletins.com

Display Name: IT Security Reports - Darrien Site

Admin Notice Form: admin@security-bulletins.com

Display Name: [redacted]

Custom SMTP Settings

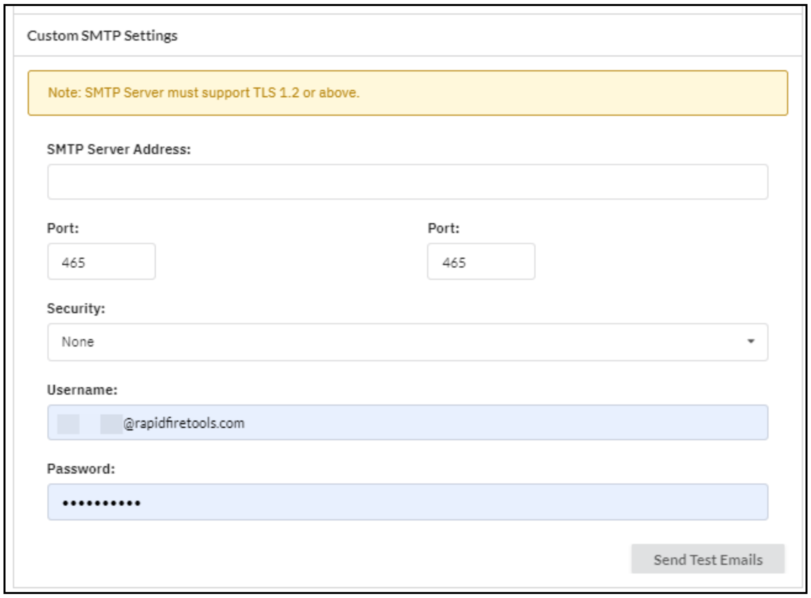
Note: SMTP Server must support TLS 1.2 or above.

SMTP Server Address:

3. Configure the following to set up your Customer SMTP Server to send Cyber Hawk Alerts and Notices:

   - Alert From email address and display name
   - Report From email address and display name
   - SMTP Server Address
   - Port Number
   - Security Method
   - SMTP Server Username and Password

© 2024 RapidFire Tools, Inc. All rights reserved.


Custom SMTP Settings

Note: SMTP Server must support TLS 1.2 or above.

SMTP Server Address:

Port: 465

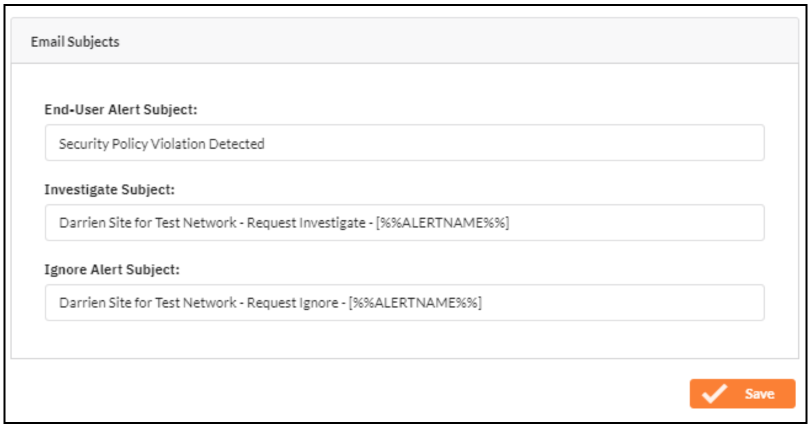
Port: 465

Security: None

Username: [redacted] [redacted]@rapidfiretools.com

Password: ••••••••••

You can likewise enter custom **Email Subject Lines** for various types of Alerts:


Email Subjects

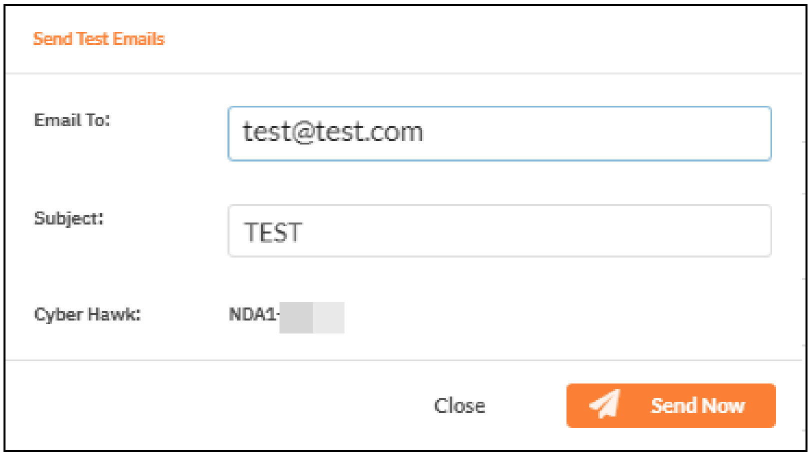
End-User Alert Subject: Security Policy Violation Detected

Investigate Subject: Darrien Site for Test Network - Request Investigate - [%%ALERTNAME%%]

Ignore Alert Subject: Darrien Site for Test Network - Request Ignore - [%%ALERTNAME%%]

4. Click **Send Test Email** to test the SMTP email Server configuration and email addresses.
5. Click the **Send Now** button in the Send Test Emails window. The status of the email test is displayed in the Send Test Emails window.

© 2024 RapidFire Tools, Inc. All rights reserved.



Send Test Emails

Email To: test@test.com

Subject: TEST

Cyber Hawk: NDA1-[redacted]

After a successful test has been completed, click **OK** to close the Send Test Emails window.

6. When you are finished, click **Save**.

© 2024 RapidFire Tools, Inc. All rights reserved.

Allow Clients to Access Portal and Manage Tickets

You can create **Site Restricted** user accounts in the RapidFire Tools Portal for Cyber Hawk clients. This can allow clients to access and manage their Cyber Hawk **Alerts** and **To Dos**. Your clients will only see what's relevant to them – and nothing else!

Here's how you do it:

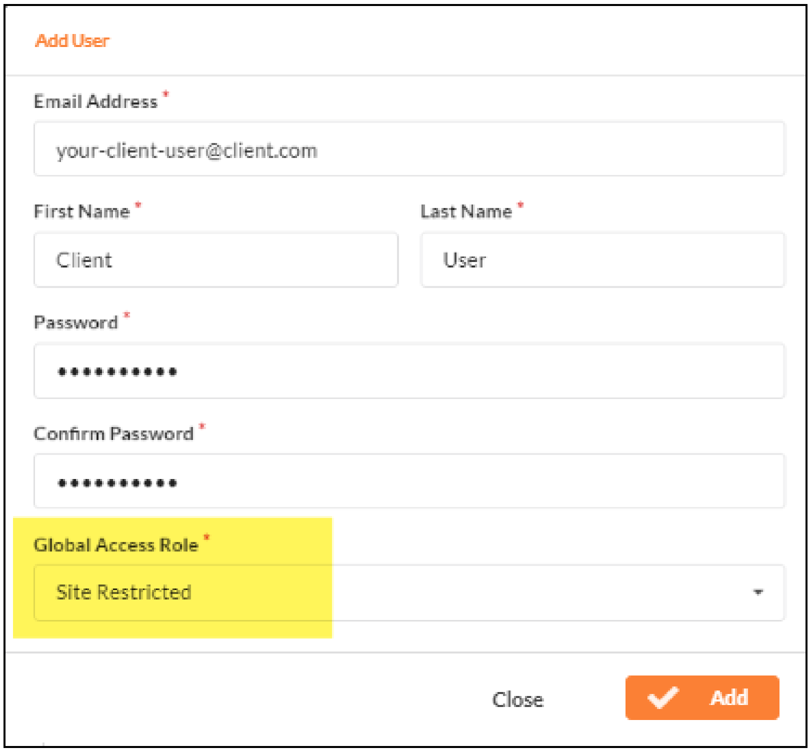
Step 1 — Create Site Restricted User in Portal

1. Log into the RapidFire Tools Portal as a Master or Admin user.
2. Go to global **Settings (Admin)** ⚙ > **Users**.
3. Click **Add User**.
4. Enter the client user's information, including a password. Repeat this for each client user you wish to add.

   Important: You will later need to send the user(s) their login credentials, so take note of them.

5. Choose the **Site Restricted** *Global Access Role* for the user(s). This will restrict the client user(s) to only those Sites to which you grant them access. They will likewise be restricted from accessing any Portal Admin Settings.

© 2024 RapidFire Tools, Inc. All rights reserved.



Add User

Email Address *: your-client-user@client.com

First Name *: Client

Last Name *: User

Password *: ••••••••••

Confirm Password *: ••••••••••

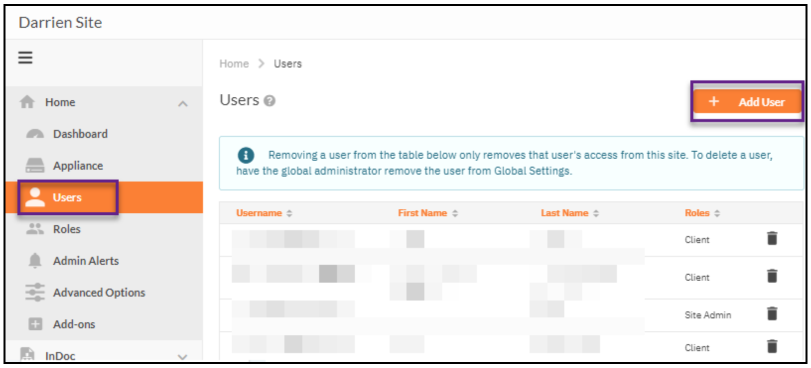
Global Access Role *: Site Restricted

6. Click **Add**.

> **Note:** Look here for a complete breakdown of "Users and Global Access Roles" on page 166.

Step 2 — Assign User to Site

1. Open the Site to which you wish to add clients. Go to **Home** > **Users**.



Removing a user from the table below only removes that user's access from this site. To delete a user, have the global administrator remove the user from Global Settings.

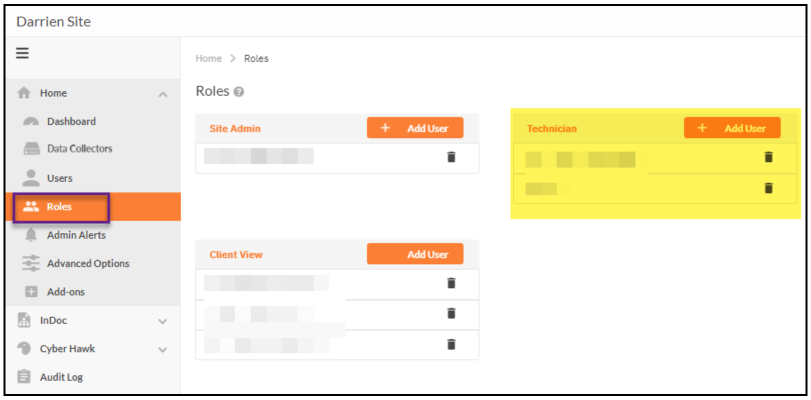
Username	First Name	Last Name	Roles
[redacted]	[redacted]	[redacted]	Client
[redacted]	[redacted]	[redacted]	Client
[redacted]	[redacted]	[redacted]	Site Admin
[redacted]	[redacted]	[redacted]	Client

2. Click **Add User**. Select the client user(s) you created earlier.

3. Click **Add**. The user(s) will be associated with this Site. The last step is to assign the user to the proper Site **Role**.

Step 3 — Assign User to Technician Role

1. Next go to **Site Settings** > **Roles**.
2. Choose the **Technician** Role and click **Add User**.



Note: Look here for more details on "RapidFire Tools Portal Site Roles" on page 172.

3. Select the client users and click **Add**.
4. (Optional) If you would like the client users to receive Cyber Hawk email notifications, you will need to add them to the Email Group in the Cyber Hawk Settings applied to the Security Policy.

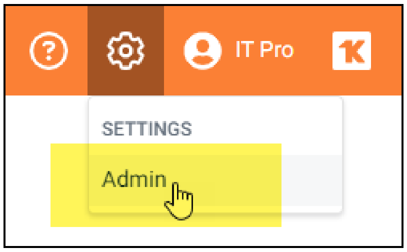
Note: Be sure that you send the client(s) the login credentials you created for them, as well as the URL for the Portal (https://www.youritportal.com).

The client can then log into the RapidFire Tools Portal and process **Alerts** and **To Do** items.

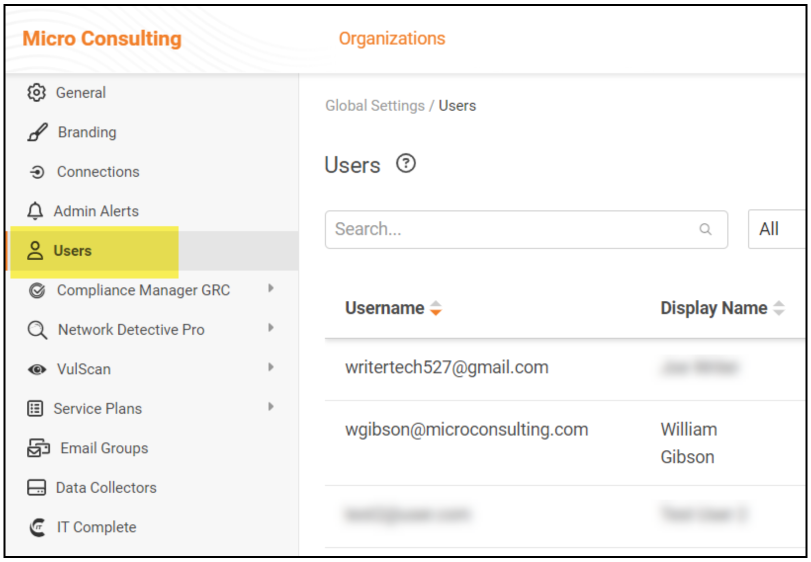
© 2024 RapidFire Tools, Inc. All rights reserved.

Manage Users (Global Level)

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

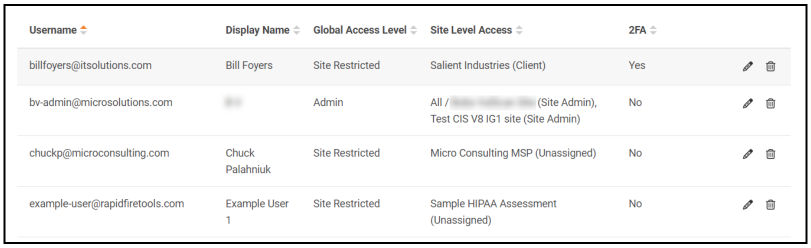


From the **Users** page, you can see a list of users associated with your account.



Username	Display Name
writertech527@gmail.com	[redacted]
wgibson@microconsulting.com	William Gibson
[redacted]	[redacted]

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	[redacted]	Admin	All / [redacted] (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

© 2024 RapidFire Tools, Inc. All rights reserved.

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 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

© 2024 RapidFire Tools, Inc. All rights reserved.

Global Access Role	Description
	- 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" below
- "Edit User at Global Level" on page 170

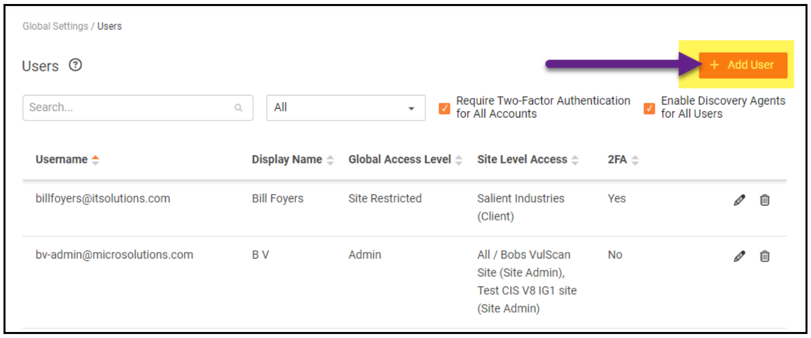
Add User at Global Level

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.

© 2024 RapidFire Tools, Inc. All rights reserved.

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**.



Global Settings / Users

Users ⓘ

+ Add User

Search...

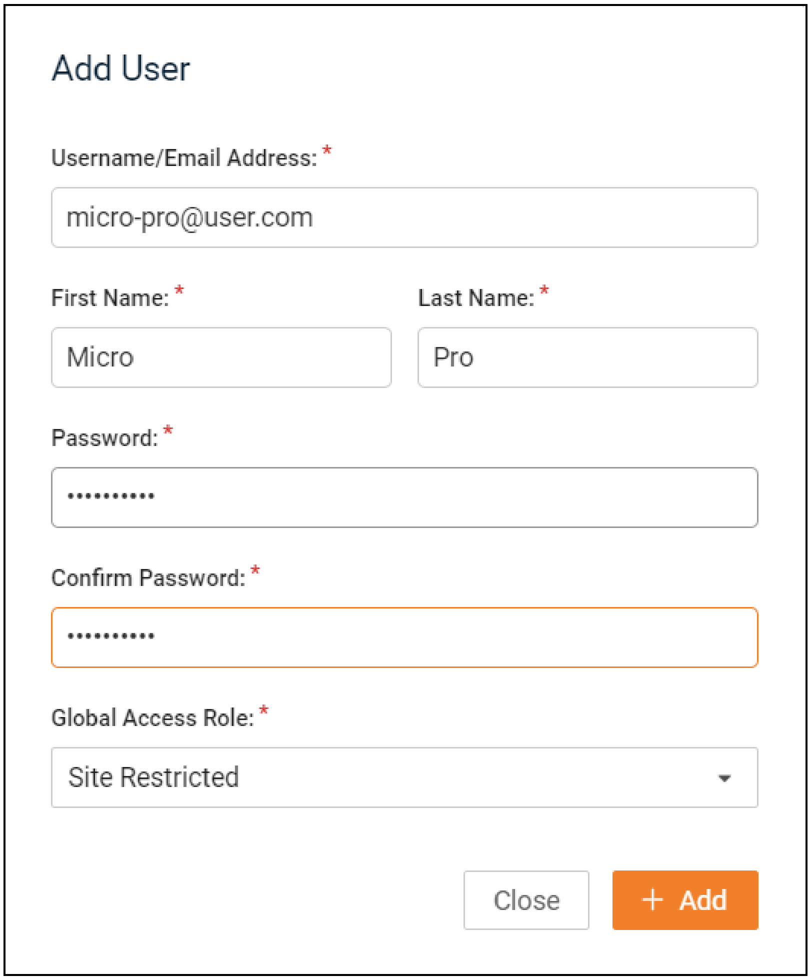
All

☑ Require Two-Factor Authentication for All Accounts

☑ Enable Discovery Agents for All Users

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	B V	Admin	All / Bobs VulScan Site (Site Admin), Test CIS V8 IG1 site (Site Admin)	No

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



Add User

Username/Email Address: *
micro-pro@user.com

First Name: *
Micro

Last Name: *
Pro

Password: *
••••••••••

Confirm Password: *
••••••••••

Global Access Role: *
Site Restricted

© 2024 RapidFire Tools, Inc. All rights reserved.

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. **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 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

© 2024 RapidFire Tools, Inc. All rights reserved.

Global Access Role	Description
	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

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

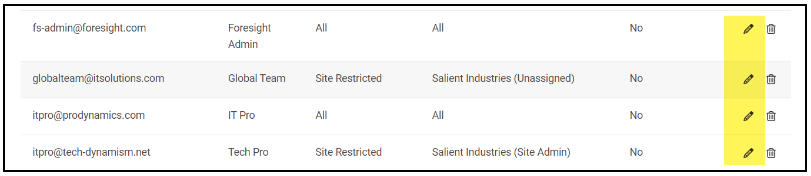
Edit User at Global Level

> **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 165 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.

© 2024 RapidFire Tools, Inc. All rights reserved.



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**.

RapidFire Tools Portal Site Roles

Site **Roles** are assigned to Portal users on a site-by-site basis. Assign Roles to grant users certain levels of access at a particular site in the Portal.

Tip: You can use Roles to collaborate with other users outside of your organization, while ensuring they can only access what they need to perform a given task.

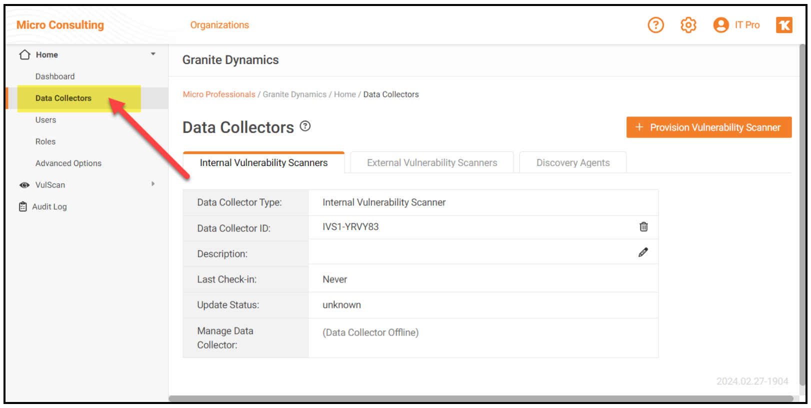
Refer to the table below for a breakdown of site Roles by product.

Role (Site Level)	RapidFire Tools Product		
	COMPLIANCE MANAGER	CYBER HAWK	INDOC (REPORTER)
Site Administrator	• Global Master or Admin who creates site is default Site Admin • Perform all Assessment Tasks • Access all Site Settings • Assign Users and Roles	• Access all Site Settings • Assign Users and Roles	• Access all Site Settings • Assign Users and Roles • Access all InDoc features
Technician	• Installs and configures appliance and scan settings • Troubleshoots automated scans • SME for target network	• Manage Alerts and To Dos • Configure Cyber Hawk Policies and Notification Rules • Configure Scan Settings • Configure Smart Tag • Configure Schedules	• Access most InDoc features, except Client View
Internal Auditor	• Completes To Do list tasks to perform the assessment • Completes worksheets and surveys • Invites Subject Matter Experts to contribute to forms	N/A	N/A
Subject Matter Expert	• Receives email invitations to contribute to worksheets and surveys • Can only see and edit forms; cannot access any other portal features	N/A	N/A

Role (Site Level)	RapidFire Tools Product		
	• Does not receive To Do tasks		
Client View	N/A	N/A	• Can only view and download published reports

Manage Site Data Collectors

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



Data Collector Type:	Internal Vulnerability Scanner
Data Collector ID:	IVS1-YRVY83
Description:	
Last Check-in:	Never
Update Status:	unknown
Manage Data Collector:	(Data Collector Offline)

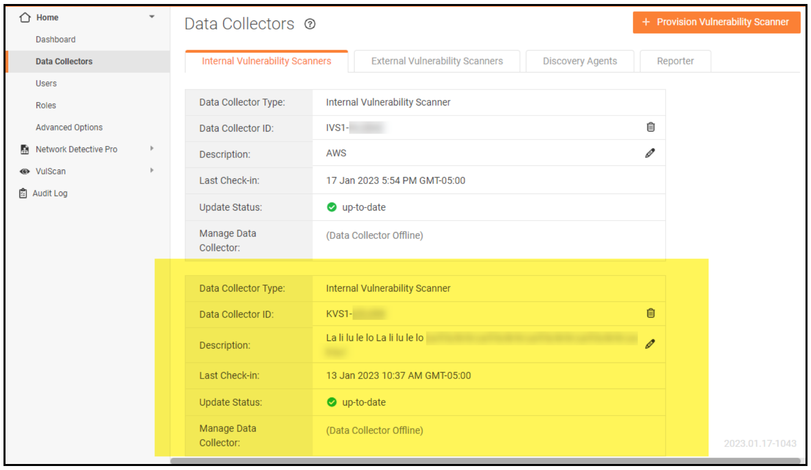
The **Data Collectors** page presents each "data collector" – also known as an *appliance* or *server* - deployed on the Site network. This includes data collectors for the various managed services: Cyber Hawk, Audit Guru, Reporter, and other product types.

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.

© 2024 RapidFire Tools, Inc. All rights reserved.



Data Collector Type:	Internal Vulnerability Scanner
Data Collector ID:	IVS1-[redacted]
Description:	AWS
Last Check-in:	17 Jan 2023 5:54 PM GMT-05:00
Update Status:	✓ up-to-date
Manage Data Collector:	(Data Collector Offline)

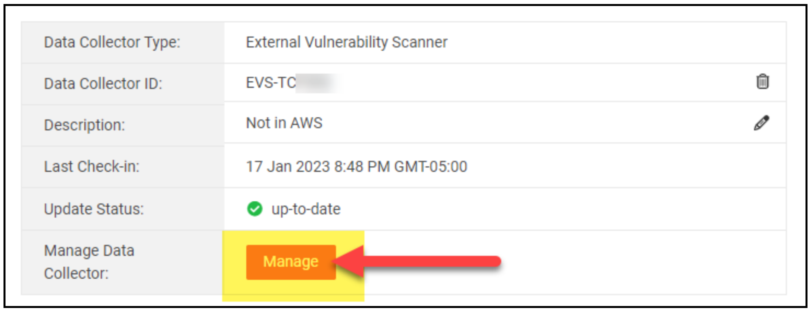
Data Collector Type:	Internal Vulnerability Scanner
Data Collector ID:	KVS1-[redacted]
Description:	La li lu le lo La li lu le lo [redacted]
Last Check-in:	13 Jan 2023 10:37 AM GMT-05:00
Update Status:	✓ up-to-date
Manage Data Collector:	(Data Collector Offline)

For each data collector, you can quickly see:

Data Collector Type	For example: Audit Guru, 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.

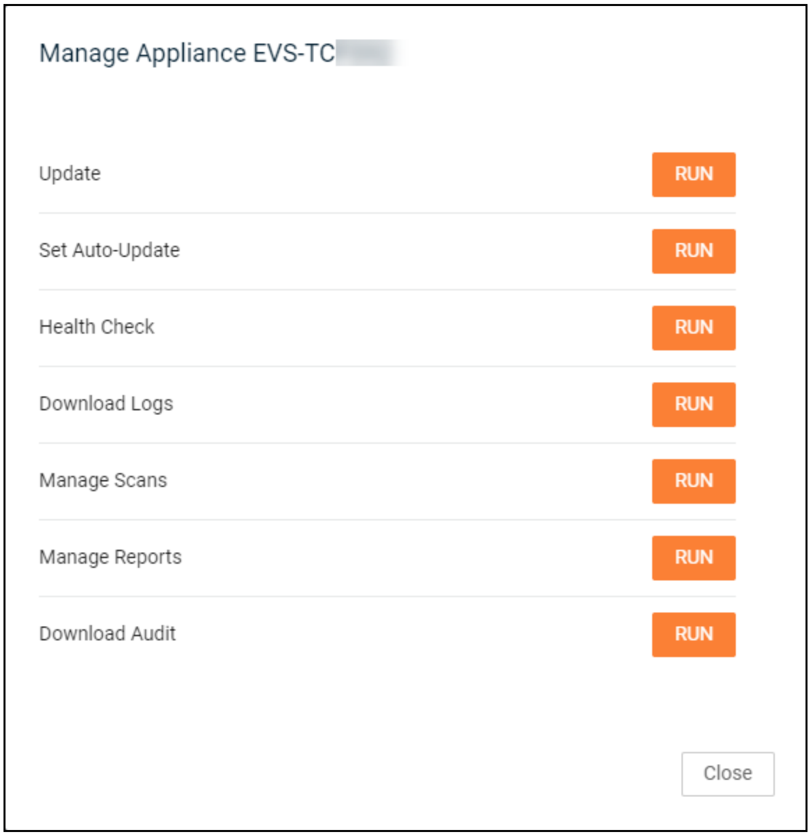
Data Collector Commands

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.

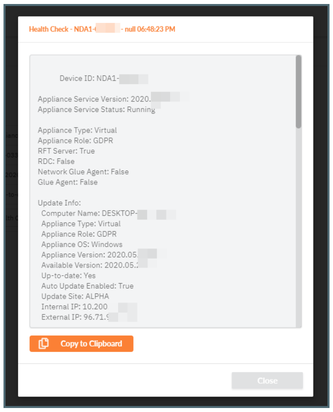


Data Collector Type:	External Vulnerability Scanner
Data Collector ID:	EVS-TC[redacted]
Description:	Not in AWS
Last Check-in:	17 Jan 2023 8:48 PM GMT-05:00
Update Status:	✓ up-to-date
Manage Data Collector:	Manage

© 2024 RapidFire Tools, Inc. All rights reserved.

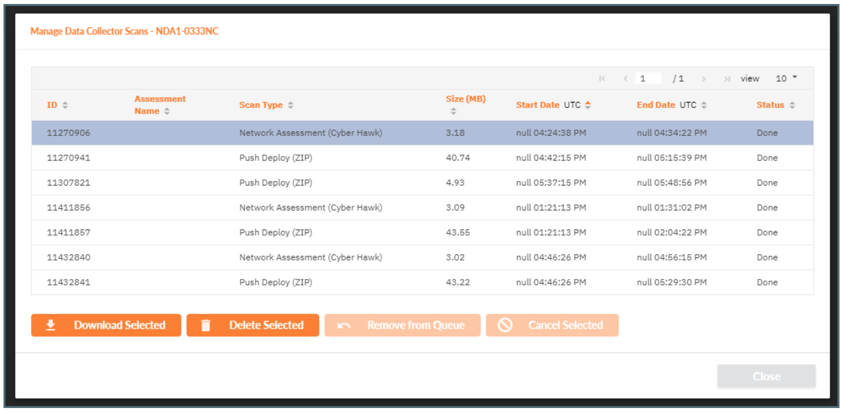


Manage Appliance EVS-TC[redacted]

Update	Update the data collector to the latest version. Note that this will cancel all current scans.
Set Auto-Update	Order the data collector to automatically update itself when a new version becomes available.
Health Check	Access technical information about the data collector's current status. Can be copied as a text file for troubleshooting.  Health Check - NDA1-[redacted] - null 06:48:23 PM Device ID: NDA1-[redacted] Appliance Service Version: 2020.[redacted] Appliance Service Status: Running Appliance Type: Virtual Appliance Role: GDPR RFT Server: True RDC: False Network Glue Agent: False Glue Agent: False Update Info: Computer Name: DESKTOP-[redacted] Appliance Type: Virtual Appliance Role: GDPR Appliance OS: Windows Appliance Version: 2020.05.[redacted] Available Version: 2020.05.[redacted] Up-to-date: Yes Auto Update Enabled: True Update Site: ALPHA Internal IP: 10.200[redacted] External IP: 96.71.[redacted]
Download Logs	Download log files for troubleshooting purposes.

© 2024 RapidFire Tools, Inc. All rights reserved.

<table>
<tr>
<td>Manage Scans</td>
<td>
View and manage all scans assigned to the appliance.

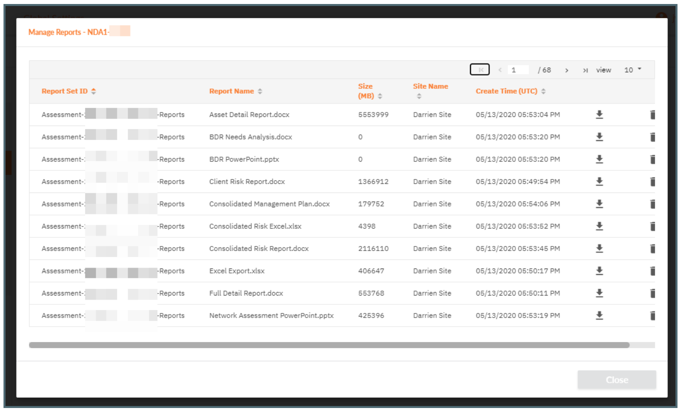


Manage Data Collector Scans - NDA1-0333NC

<table>
<tr><th>ID</th><th>Assessment Name</th><th>Scan Type</th><th>Size (MB)</th><th>Start Date UTC</th><th>End Date UTC</th><th>Status</th></tr>
<tr><td>11270906</td><td></td><td>Network Assessment (Cyber Hawk)</td><td>3.18</td><td>null 04:24:38 PM</td><td>null 04:34:22 PM</td><td>Done</td></tr>
<tr><td>11270941</td><td></td><td>Push Deploy (ZIP)</td><td>40.74</td><td>null 04:42:15 PM</td><td>null 05:15:39 PM</td><td>Done</td></tr>
<tr><td>11307821</td><td></td><td>Push Deploy (ZIP)</td><td>4.93</td><td>null 05:37:15 PM</td><td>null 05:48:56 PM</td><td>Done</td></tr>
<tr><td>11411856</td><td></td><td>Network Assessment (Cyber Hawk)</td><td>3.09</td><td>null 01:21:13 PM</td><td>null 01:31:02 PM</td><td>Done</td></tr>
<tr><td>11411857</td><td></td><td>Push Deploy (ZIP)</td><td>43.55</td><td>null 01:21:13 PM</td><td>null 02:04:22 PM</td><td>Done</td></tr>
<tr><td>11432840</td><td></td><td>Network Assessment (Cyber Hawk)</td><td>3.02</td><td>null 04:46:26 PM</td><td>null 04:56:15 PM</td><td>Done</td></tr>
<tr><td>11432841</td><td></td><td>Push Deploy (ZIP)</td><td>43.22</td><td>null 04:46:26 PM</td><td>null 05:29:30 PM</td><td>Done</td></tr>
</table>

Here you can:

- Download scan files
- Delete completed scans and their associated files
- Remove queued scans
- Cancel scans in progress
</td>
</tr>
<tr>
<td>Manage Reports (Reporter only)</td>
<td>
Access and manage reports stored on the Reporter appliance.



Manage Reports - NDA1-[redacted]

<table>
<tr><th>Report Set ID</th><th>Report Name</th><th>Size (MB)</th><th>Site Name</th><th>Create Time (UTC)</th><th></th><th></th></tr>
<tr><td>Assessment-[redacted]-Reports</td><td>Asset Detail Report.docx</td><td>5553999</td><td>Darrien Site</td><td>05/13/2020 05:53:04 PM</td><td>⬇</td><td>🗑</td></tr>
<tr><td>Assessment-[redacted]-Reports</td><td>BDR Needs Analysis.docx</td><td>0</td><td>Darrien Site</td><td>05/13/2020 05:53:20 PM</td><td>⬇</td><td>🗑</td></tr>
<tr><td>Assessment-[redacted]-Reports</td><td>BDR PowerPoint.pptx</td><td>0</td><td>Darrien Site</td><td>05/13/2020 05:53:20 PM</td><td>⬇</td><td>🗑</td></tr>
<tr><td>Assessment-[redacted]-Reports</td><td>Client Risk Report.docx</td><td>1366912</td><td>Darrien Site</td><td>05/13/2020 05:49:54 PM</td><td>⬇</td><td>🗑</td></tr>
<tr><td>Assessment-[redacted]-Reports</td><td>Consolidated Management Plan.docx</td><td>179752</td><td>Darrien Site</td><td>05/13/2020 05:54:06 PM</td><td>⬇</td><td>🗑</td></tr>
<tr><td>Assessment-[redacted]-Reports</td><td>Consolidated Risk Excel.xlsx</td><td>4398</td><td>Darrien Site</td><td>05/13/2020 05:53:52 PM</td><td>⬇</td><td>🗑</td></tr>
<tr><td>Assessment-[redacted]-Reports</td><td>Consolidated Risk Report.docx</td><td>2116110</td><td>Darrien Site</td><td>05/13/2020 05:53:45 PM</td><td>⬇</td><td>🗑</td></tr>
<tr><td>Assessment-[redacted]-Reports</td><td>Excel Export.xlsx</td><td>406647</td><td>Darrien Site</td><td>05/13/2020 05:50:17 PM</td><td>⬇</td><td>🗑</td></tr>
<tr><td>Assessment-[redacted]-Reports</td><td>Full Detail Report.docx</td><td>553768</td><td>Darrien Site</td><td>05/13/2020 05:50:11 PM</td><td>⬇</td><td>🗑</td></tr>
<tr><td>Assessment-[redacted]-Reports</td><td>Network Assessment PowerPoint.pptx</td><td>425396</td><td>Darrien Site</td><td>05/13/2020 05:53:19 PM</td><td>⬇</td><td>🗑</td></tr>
</table>

</td>
</tr>
<tr>
<td>Download Audit</td>
<td>Download the audit log for the appliance.</td>
</tr>
</table>

© 2024 RapidFire Tools, Inc. All rights reserved.

Smart Tags

This section covers everything you need to know about Cyber Hawk Smart Tags.

Defining Smart Tags

Cyber Hawk incorporates a proprietary feature named “Smart Tags”. The Smart Tags feature allows you to fine-tune the Cyber Hawk to adapt to each client’s unique IT environment to detect network Anomalies, Changes, and Threats (ACT).

Smart Tags allow you to enrich the detection system by adding information about specific users, assets, and settings that helps Cyber Hawk get “smarter” about what it is finding. That means more potential threats identified with fewer “false positives.”

Here are some of the Smart Tags available for use:

Tag	Applied To	For What?	Why?
ACCOUNTING COMPUTER	Computer	Computers that can either access or are running accounting systems	Identifies when non-accounting users attempt to access these computers
ACCOUNTING USER	User	These users should have access to accounting systems	Identifies who should have access to accounting systems
AUTHORIZED PRINTER	Printer	Printers that are allowed on the network	Helps identify which computers are allowed to be published on the network
AUTHORIZED SSID	SSID	Indicates which wireless networks that computers on the network may connect to for network access	Allows identification of wireless networks that are safe to connect to
BUSINESS OWNER	User	Business owners typically have more sensitive information on their systems	Helps associated business owners with their computers

© 2024 RapidFire Tools, Inc. All rights reserved.

Tag	Applied To	For What?	Why?
BUSINESS OWNER PC	Computer	Computers used by business owners	Raises the computer's security significance
DMZ COMPUTER	Computer	Computers in the DMZ typically bridge the public Internet and private internal network	Because these computers are exposed to the outside network, their security becomes more significant
GUEST NETWORK	IP Range	IP ranges that are reserved for guest networks.	Network changes from this range typically do not indicate a security concern.
GUEST WIRELESS NETWORK	IP Range	IP ranges that are reserved for guest networks.	Network changes from this range typically do not indicate a security concern.
HIPAA/ePHI AUTHORIZED USER	User	These users are allowed to access computers containing ePHI.	Indicates which users can access computers with ePHI.
HIPAA/ePHI COMPUTER	Computer	Computers that contain ePHI.	Allows identification of unauthorized access to a system with ePHI.
IT ADMIN	User	IT Administrators typically have more access to network resources than the typical user	Identifies who should have this elevated level of access
LOCKED DOWN	Computer	Locked down computers are highly controlled systems where changes are limited	Changes to locked down computers are more significant than other computers
LOCKED DOWN DNS	Network	Tag a network to detect DNS changes on	Any changes in DNS for the specified subnet will

© 2024 RapidFire Tools, Inc. All rights reserved.

Tag	Applied To	For What?	Why?
			trigger this alert. It is used in environments where you are certain there should be no DNS changes.
NO DIRECT INTERNET ACCESS	Computer	Computers that should have no direct Internet access (web or otherwise)	Allows identification of changes that might inadvertently grant Internet access
PCI/CDE AUTHORIZED USER	User	These users are allowed to access computers in the Cardholder Data Environment (CDE)	Indicates which users can access the CDE
PCI/CDE COMPUTER	Computer	Computers that are a part of the Cardholder Data Environment (CDE)	Allows identification of unauthorized access to the CDE
RESTRICTED IT ADMIN ONLY	Computer	Some computers (typically servers) should only be access directly by IT Administrators	Allows alerting when access occurs by non-IT Admin users
RESTRICTED NETWORK	IP Range	Restricted networks are defined as networks where the appearance of new devices is very rare	Tagging an IP range as a restricted network indicates changes are more significant
SENSITIVE COMPUTER	Computer	Tag a computer that contains sensitive information	This represents a computer that has sensitive information on it
SENSITIVE USER	User	Tag a user that works on sensitive information	This represents a user that works on sensitive information
SINGLE DESKTOP USER	User	Users that have dedicated	Enhances detection of

© 2024 RapidFire Tools, Inc. All rights reserved.

Tag	Applied To	For What?	Why?
		desktop and should never log into other systems directly	anomalies by identifying which users have been assigned a computer
VIRTUAL MACHINE	Computer	Computers that are not physical devices	Distinguishing between physical and virtual computers help determine what changes are considered abnormal
AUTHORIZED PRINTER	Printer	Printers that are allowed on the network	Helps identify which printers are allowed to be published on the network
TRANSIENT PRINTER	Printer	Transient printers are routinely put on and taken off the network	Allows for the removal of false positives related to inactivity and theft

© 2024 RapidFire Tools, Inc. All rights reserved.

Using Smart Tags

You can select, configure, or modify, your Smart Tags at any time. That allows you to see what kind of alerts Cyber Hawk is sending you and create the tags you want to use to “tweak” the Cyber Hawk system.

The use of Smart Tags improves the detection of Anomalies, Changes, and Threats (ACT) by providing additional “knowledge” of the network environment to the Cyber Hawk. Once the Cyber Hawk has scanned your network for the first time, you can explore the data and assign Smart Tags to entries like computers and users.

The use of the Smart Tags feature presumes that the Level 1 (Daily) Scan and/or Level 2 (Weekly) Scan types available on the Cyber Hawk Appliance have been configured and performed.

EXAMPLE:

Here are some examples of how you might use the Smart Tags to fine-tune Cyber Hawk’s alerts for a particular client:

- **Restricted Computer Access Detection**

Within Cyber Hawk, you can tag a particular computer as being “RESTRICTED IT ADMIN ONLY”. Then, when any user logs into the computer that has not been tagged “IT ADMIN”, Cyber Hawk will send an alert.

- **Changes to Locked Down Computer Detection**

Within Cyber Hawk, you can tag a particular computer as “Locked Down” (meaning, do not allow changes to this computer). If someone manages to install an application on this machine, then Cyber Hawk will detect that the application was installed and send an Alert. In this way, tagging can remove false positives and increases the relevance of alerts.

- **Wireless Network Availability Detection**

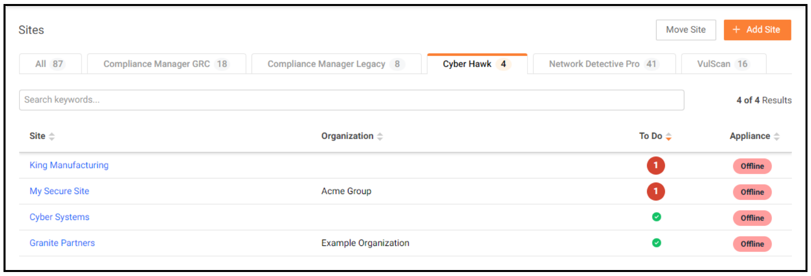
Within Cyber Hawk, you can tag a specific wireless network as a “GUEST WIRELESS NETWORK” telling Cyber Hawk it does not need to worry about new devices appearing on it. But if a new device shows up on any non-guest network, then the appearance is significant and Cyber Hawk will send you an alert so you can determine if it is worth looking into.

Add and Configure Smart Tags

To add and configure Smart Tags to enable Cyber Hawk to recognize any Anomalies, Changes and Threats (ACT) that trigger Daily Alerts or Weekly Notice alerts, perform the following steps.

Step 1 — Select the Site

Open your Cyber Hawk Site in the RapidFire Tools Portal.

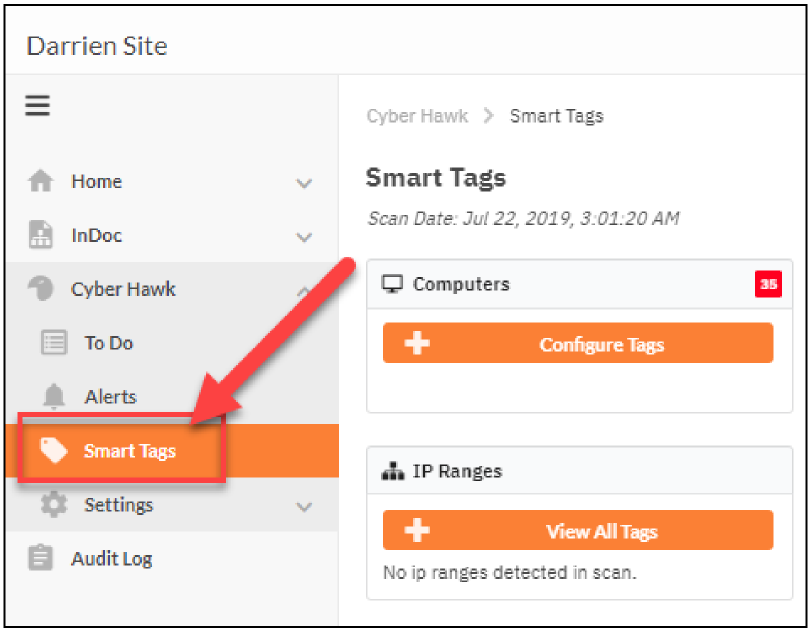


4 of 4 Results

Site	Organization	To Do	Appliance
King Manufacturing		1	Offline
My Secure Site	Acme Group	1	Offline
Cyber Systems		✓	Offline
Granite Partners	Example Organization	✓	Offline

Step 2 — Open Smart Tags

After you open the Site, go to the **Cyber Hawk** tab > **Smart Tags**.

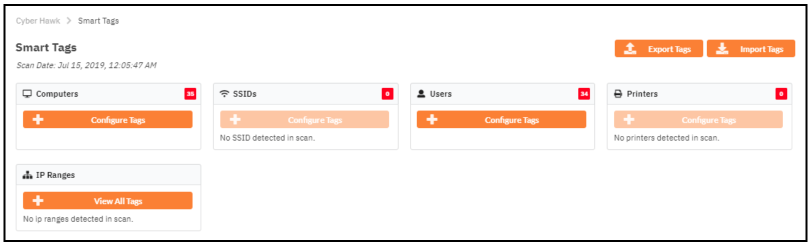


Scan Date: Jul 22, 2019, 3:01:20 AM

No ip ranges detected in scan.

© 2024 RapidFire Tools, Inc. All rights reserved.

You can then view each Smart Tag available for you to apply to the network. If there are no assets detected for a particular Smart Tag category, those Smart Tags will be unavailable.



Smart Tags

Scan Date: Jul 15, 2019, 12:05:47 AM

No SSID detected in scan.

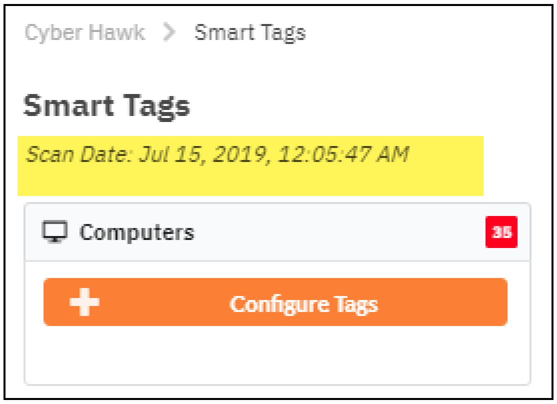
No printers detected in scan.

No ip ranges detected in scan.

Step 3 — Verify Scan Data

Before you can apply Smart Tags, you must have scan data for the site. Cyber Hawk will perform scans as part of the set up process, but it's good to double check that your appliance is configured to perform scans regularly and that you have the latest data.

You can see the date of your latest scan at the top of the Smart Tags page.



Smart Tags

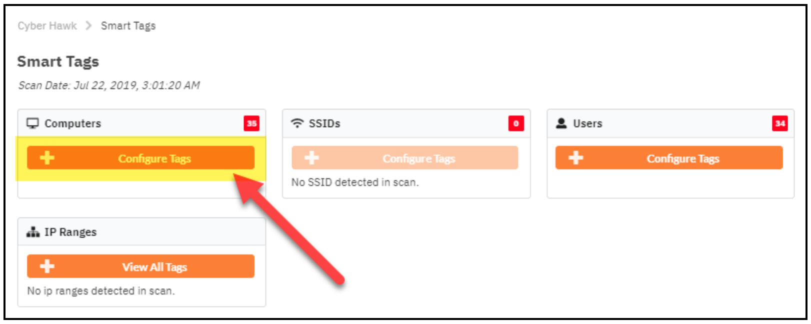
Scan Date: Jul 15, 2019, 12:05:47 AM

If you have no scan data, be sure you have set up and configured scans for your Cyber Hawk appliance. See "Setting Up Cyber Hawk" on page 12.

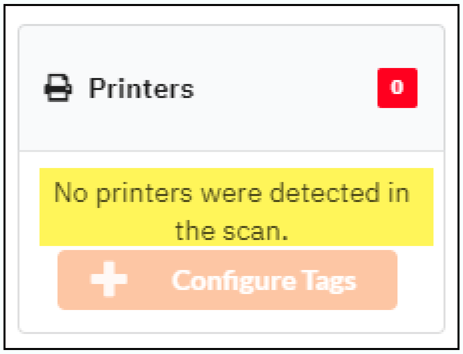
Step 4 — Apply Smart Tags

1. Choose the type of network assets to which to assign Smart Tags (for example, *Computers* or *Users*). Click **Configure Tags**.

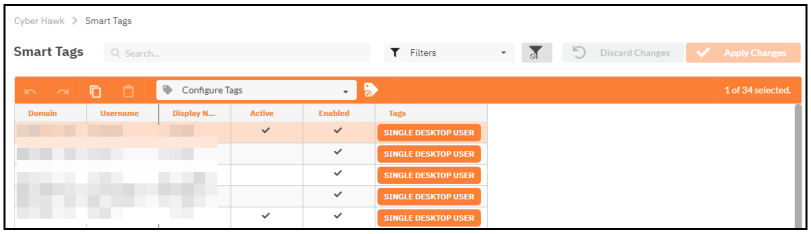
© 2024 RapidFire Tools, Inc. All rights reserved.



Note: If the network scan does not uncover assets, the **Configure Tags** button will not be available.



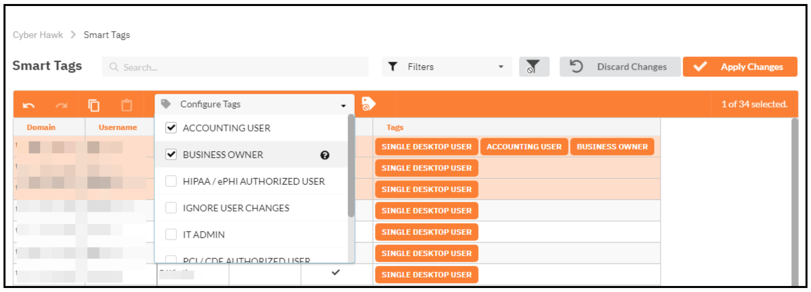
2. A list of assets or users will appear based on the results of the network scan. From the list, select one or more assets or users to receive smart tags. You can **SHIFT + click** to select multiple assets/users at once.



Domain	Username	Display N...	Active	Enabled	Tags
[redacted]	[redacted]	[redacted]	✓	✓	SINGLE DESKTOP USER
[redacted]	[redacted]	[redacted]		✓	SINGLE DESKTOP USER
[redacted]	[redacted]	[redacted]		✓	SINGLE DESKTOP USER
[redacted]	[redacted]	[redacted]		✓	SINGLE DESKTOP USER
[redacted]	[redacted]	[redacted]	✓	✓	SINGLE DESKTOP USER

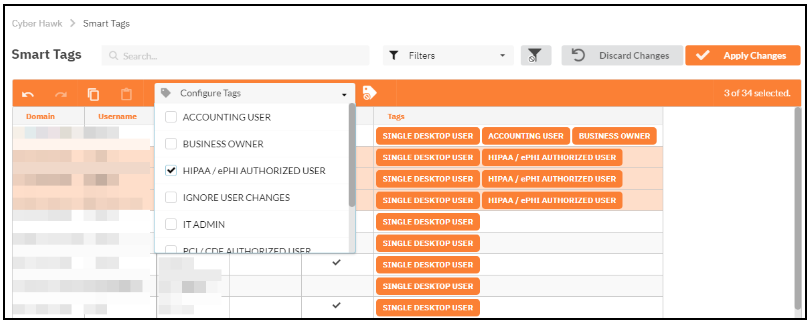
3. With the chosen assets still selected, click on one or more **Smart Tags** at the bottom of the screen.

© 2024 RapidFire Tools, Inc. All rights reserved.



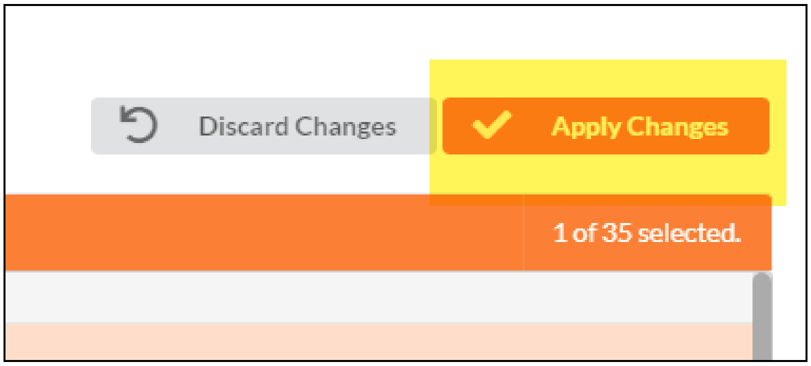
☑ ACCOUNTING USER
☑ BUSINESS OWNER
□ HIPAA / ePHI AUTHORIZED USER
□ IGNORE USER CHANGES
□ IT ADMIN
□ PCI / CDE AUTHORIZED USER

This will associate the Smart Tag(s) with the selected assets.



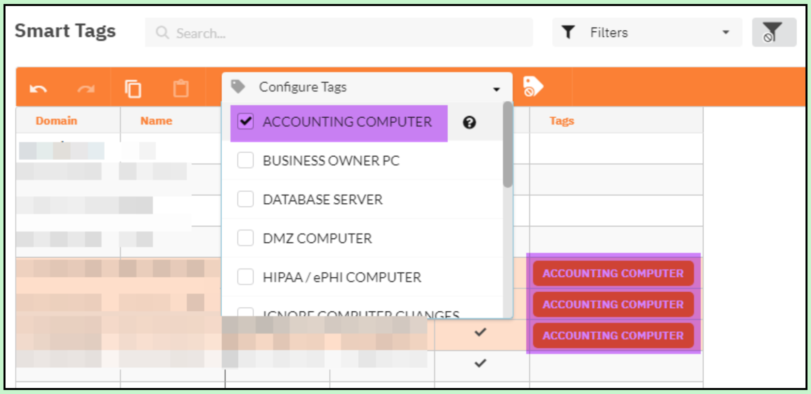
□ ACCOUNTING USER
□ BUSINESS OWNER
☑ HIPAA / ePHI AUTHORIZED USER
□ IGNORE USER CHANGES
□ IT ADMIN
□ PCI / CDE AUTHORIZED USER

4. Click **Apply Changes** to save your **Smart Tag** configuration.

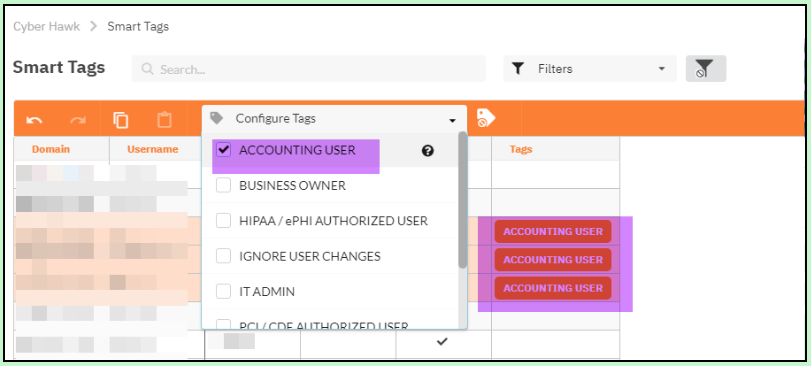


5. Return to **[Your Site]** > **Cyber Hawk** > **Smart Tags**. Continue tagging network assets (*Computers*, *Users*, *Printers*, etc.) until you have assigned all Smart Tags necessary to enforce your chosen Security Policies.

EXAMPLE: If a PC on the target network is an Accounting Computer, you can assign that PC the **Accounting Computer** Smart Tag.



Likewise, you can then assign authorized users the **Accounting User** Smart Tag.



This lets Cyber Hawk know that the designated accounting computers should only be accessed by authorized accounting users. If a non-accounting user attempts to access the PC, Cyber Hawk will generate an alert.

When you have assigned all recommended smart tags to network assets and users, return to the To Do item and click **Mark Complete**.

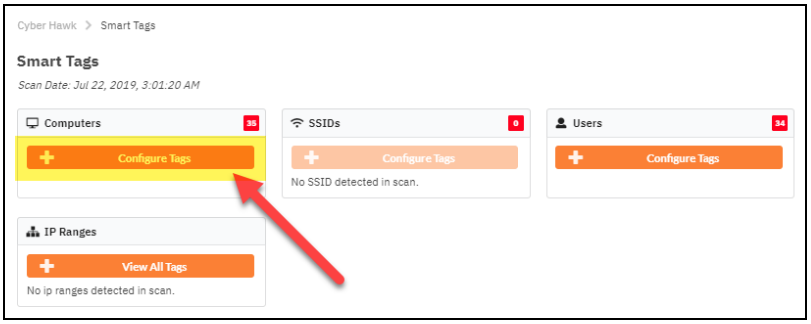
© 2024 RapidFire Tools, Inc. All rights reserved.

Edit Smart-Tags

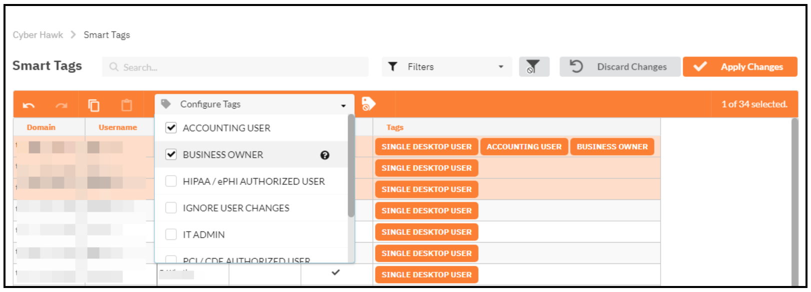
You can edit Smart Tags at any time. Note that changes to alerts will not occur until 1) your next scheduled Cyber Hawk scan and 2) your next scheduled set of alert notifications following the scan.

To edit Smart tags for a Site:

1. Go to **Cyber Hawk** tab > **Smart Tags**.
2. Next to an asset category, click **Configure Tags**.



3. Click on a particular asset from the list.
4. To add or remove a smart tag, select the tags from the **Configure Tags** drop-down menu.



5. When you are finished, click **Apply Changes**.

Export and Import Smart Tags

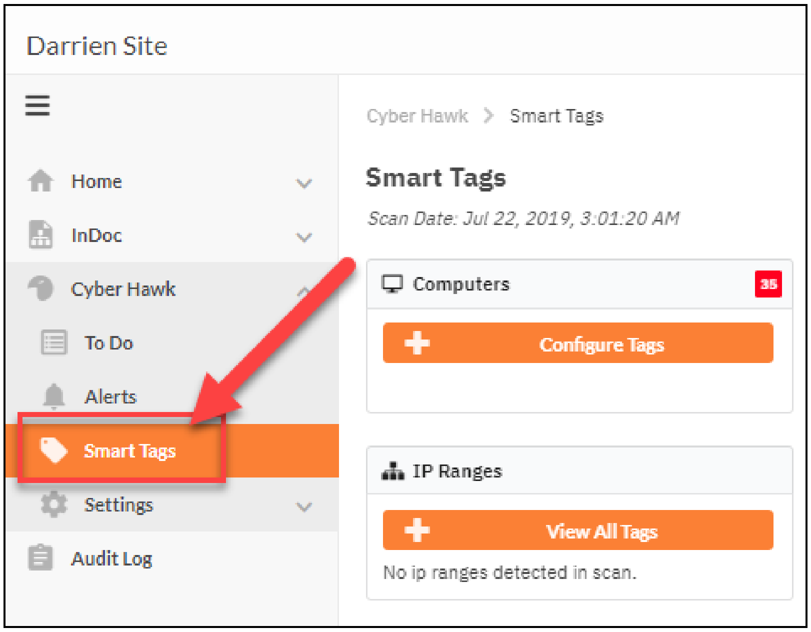
You can export and import Smart Tags using Cyber Hawk. This allows you to copy and paste your Smart Tag configuration. This is useful if you need to delete and create a new Site, for example.

Note that importing Smart Tags to a Site will overwrite any current Smart Tag configuration for that Site.

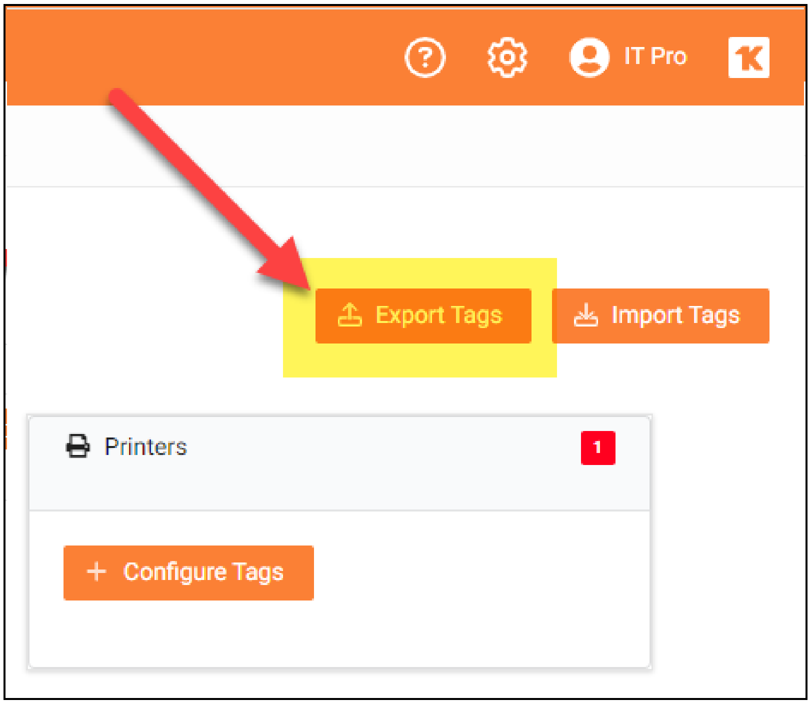
Also note that you can only export Smart Tags to a Site if 1) that Site has the same network assets (users, computers, etc.) as the original Site, 2) you have performed a successful scan for the new Site to detect these assets.

Export Smart Tags

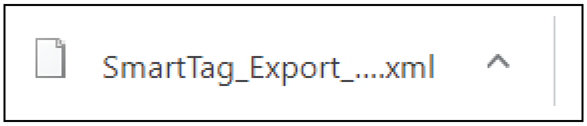
1. Open your Cyber Hawk Site and go to the **Cyber Hawk** tab > **Smart Tags**.



2. Click the **Export Tags** button.



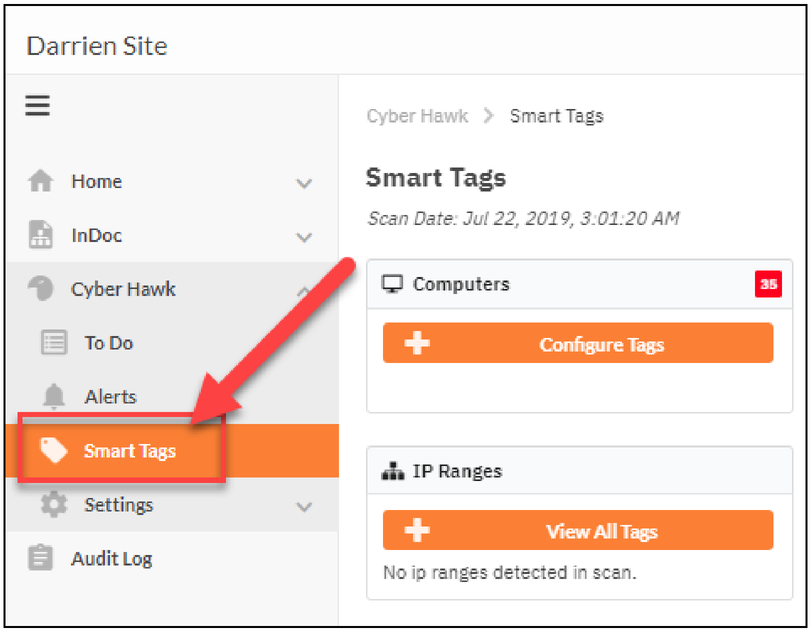
3. The download will initiate containing an **.xml file** with all Smart Tags for the Site. Open this file and note the location of the file.



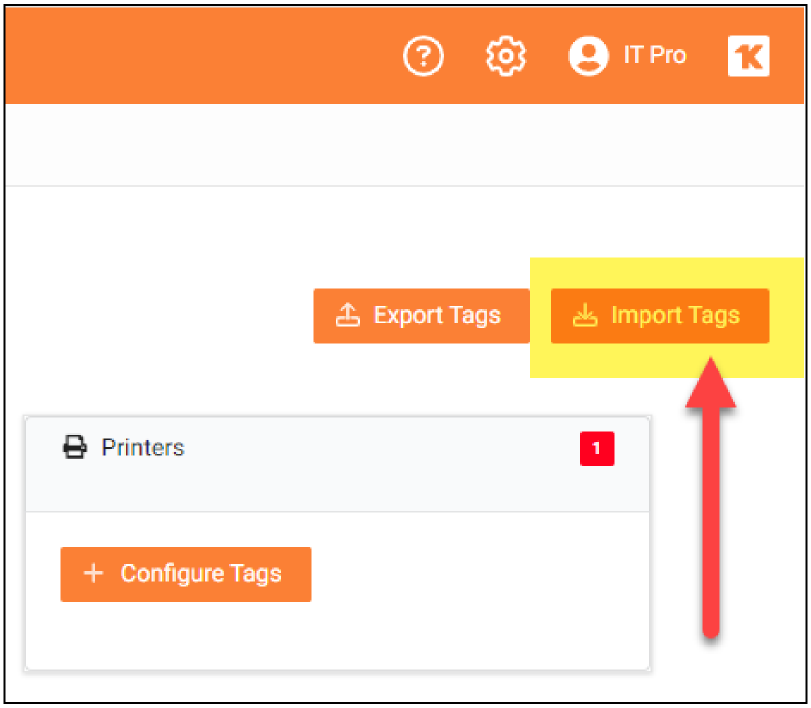
© 2024 RapidFire Tools, Inc. All rights reserved.

Import Smart Tags

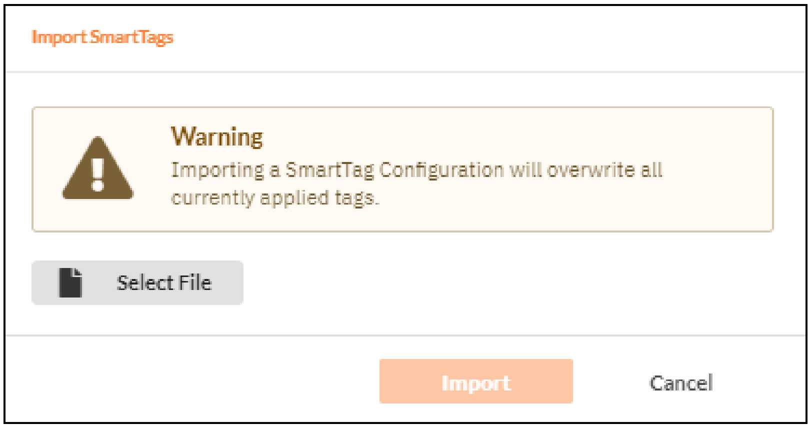
1. Open your Cyber Hawk Site and go to the **Cyber Hawk** tab > **Smart Tags**.



2. Click the **Import Tags** button.



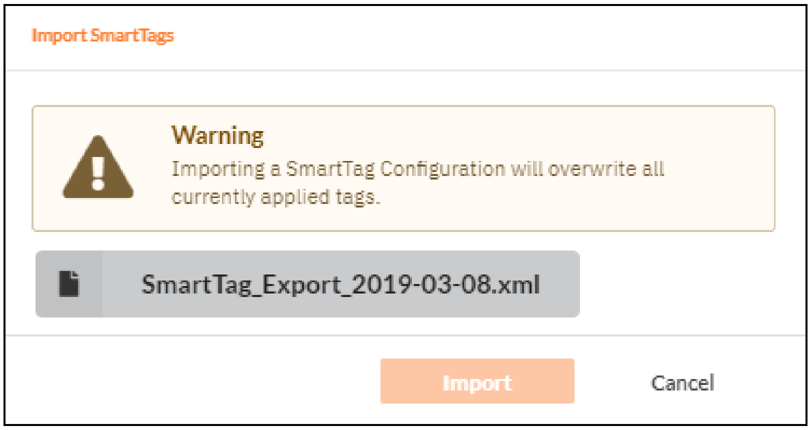
3. Click **Select File** and choose the .xml file containing the Smart Tags.



Import SmartTags

Warning
Importing a SmartTag Configuration will overwrite all currently applied tags.

4. Click **Import**. Your Smart Tags will then be applied to the Site.



Import SmartTags

Warning
Importing a SmartTag Configuration will overwrite all currently applied tags.

SmartTag_Export_2019-03-08.xml

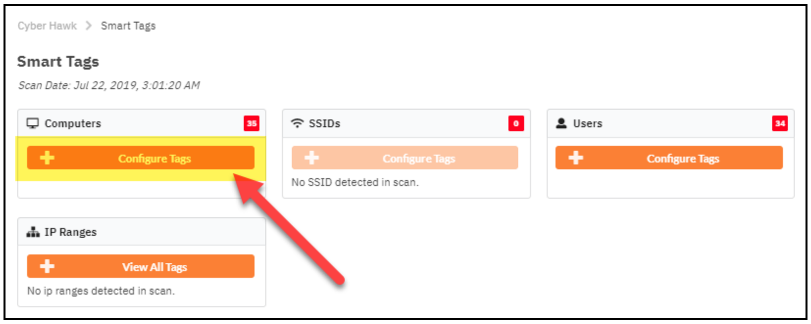
© 2024 RapidFire Tools, Inc. All rights reserved.

Delete Smart Tags

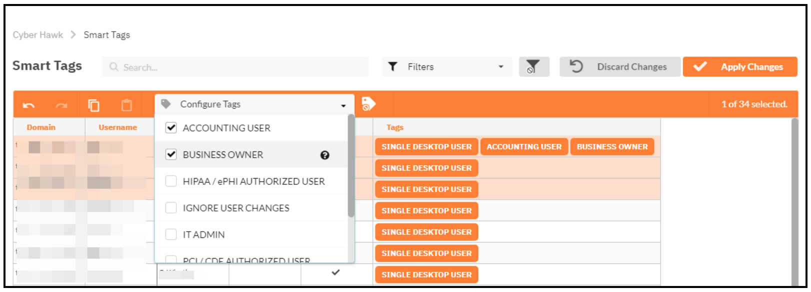
Use the following steps to delete a Smart Tag:

To edit Smart tags for a Site:

1. From the Site, go to **Cyber Hawk** tab > **Smart Tags**.
2. Choose the category of assets that has the tag you want to remove, then click **Configure Tags**.



3. Click on the asset that has the tag you wish to delete.
4. To remove a smart tag, unselect the tag from the **Configure Tags** list.



5. When you are finished, click **Apply Changes**.

© 2024 RapidFire Tools, Inc. All rights reserved.

Service Plans and Catalogs

This section covers everything you need to know about Cyber Hawk Service Plans and Catalogs.

Using the Service Plan Creator

There are four use cases for the Service Plan Creator:

- Create Service Plans that are used to offer and deliver one-time Assessment Services
- Create Service Plans that leverage Cyber Hawk to deliver an on-going Security Policy-based Service Offering to your customers using the Cyber Hawk Appliance
- Create Service Catalogs used to produce a Service Catalog document in Word format. The purpose of the Service Catalog document is to enable you to produce marketing literature, sales proposals, and service agreements. The Service Catalog document presents:
    - a Service Plan Matrix of the plans you are proposing to a prospective client or customer
    - descriptions of the Security Policies and Procedures associated with each Service Plan
    - a list of reports deliverables for each of the proposed plans
- Generate a stand-alone Service Plan Matrix document in Word format summarizing the Service Plans you created

The next section outlines the steps necessary to create Service Plans and Catalogs.

Create Service Plans

Service Plans contain a set of **Security Policies** that Cyber Hawk can detect and alert upon at a Site. You can also configure how Cyber Hawk will respond to each individual Security Policy (like emailing the **Tech Group** or creating a ticket) and save this as part of your plan.

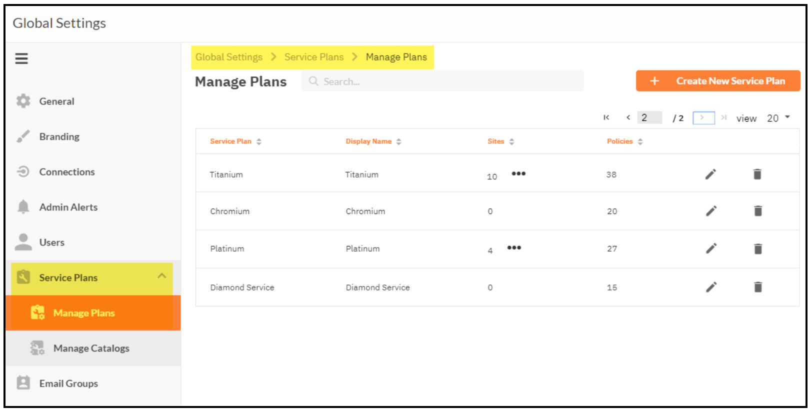
> **Note:** You can think of **Service Plans** as the "tiers" of **Security Services** you can offer your clients depending on their needs (think *Bronze*, *Silver*, *Gold*, etc.). You can even create Service Catalogs to show clients your service offerings in an easy-to-read chart (see "Create Service Catalogs" on page 200).

From global **Settings (Admin)** ⚙ > **Service Plans** > **Manage Plans**, you can create a new Service Plan or modify one of the existing "out of the box" plans. You can then quickly apply this Service Plan to each of your Cyber Hawk Sites during the set up process for each of your Sites.

To create a new Service Plan, follow these steps:

Step 1 — Create a New Service Plan

1. First, in the RapidFire Tools Portal, go to global **Settings (Admin)** ⚙ > **Service Plans** > **Manage Plans**.

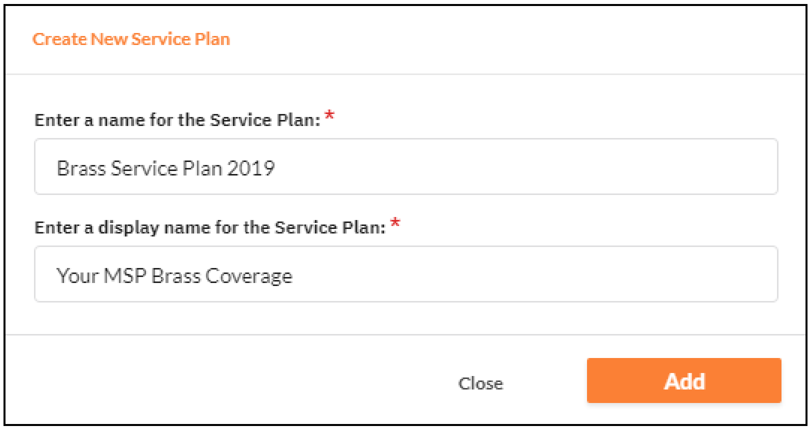


Service Plan	Display Name	Sites	Policies
Titanium	Titanium	10	38
Chromium	Chromium	0	20
Platinum	Platinum	4	27
Diamond Service	Diamond Service	0	15

2. Click **Create New Service Plan**.
3. Enter a **Name** and **Display name** for the Service Plan. Click **Add**.

© 2024 RapidFire Tools, Inc. All rights reserved.

Note: The *Display Name* is what appears when you apply the plan to a Site or include it in a **Catalog** for clients to view.



Create New Service Plan

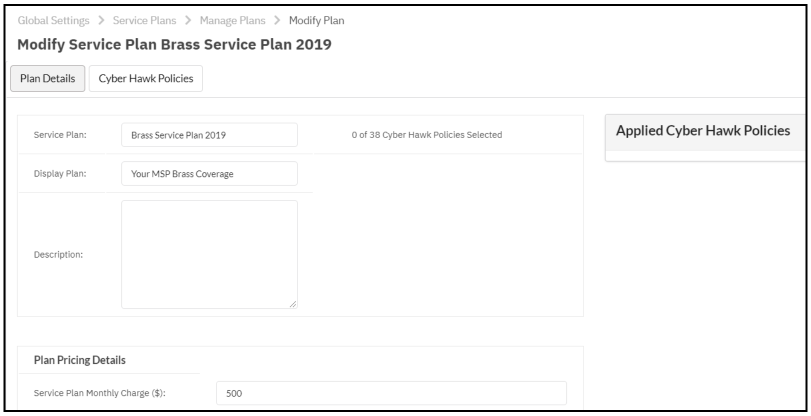
Enter a name for the Service Plan: *

Brass Service Plan 2019

Enter a display name for the Service Plan: *

Your MSP Brass Coverage

4. The **Modify Service Plan** window will appear. Enter basic information about the Service Plan, such as a short **Description** and **Plan Pricing Details**.



Global Settings > Service Plans > Manage Plans > Modify Plan

Modify Service Plan Brass Service Plan 2019

Service Plan: Brass Service Plan 2019

0 of 38 Cyber Hawk Policies Selected

Display Plan: Your MSP Brass Coverage

Description:

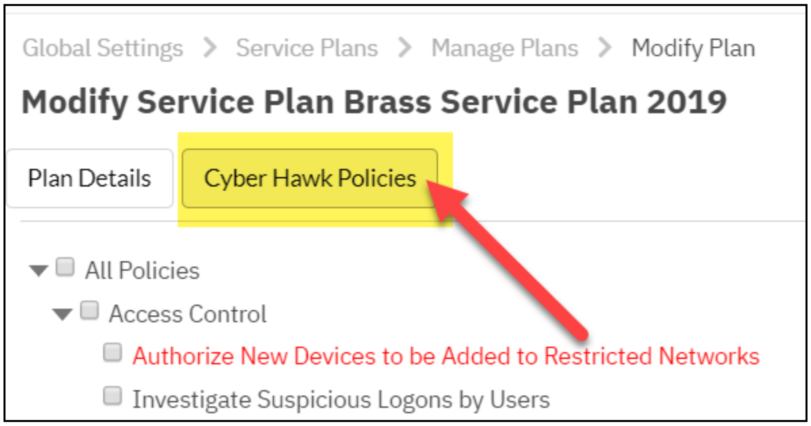
Plan Pricing Details

Service Plan Monthly Charge ($): 500

Step 2 — Assign Security Policies to Your Service Plan

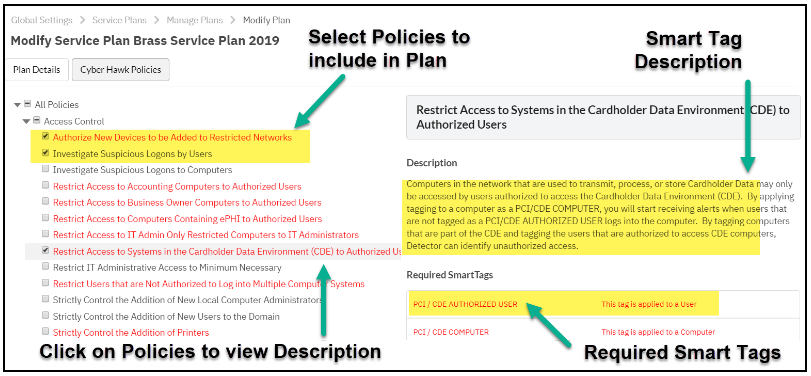
© 2024 RapidFire Tools, Inc. All rights reserved.

1. Next, click on the **Cyber Hawk Policies** tab.


Global Settings > Service Plans > Manage Plans > Modify Plan
Modify Service Plan Brass Service Plan 2019
Plan Details
Cyber Hawk Policies

- □ All Policies
  - □ Access Control
    - □ Authorize New Devices to be Added to Restricted Networks
    - □ Investigate Suspicious Logons by Users

Here you can see all of the available Security Policies that Cyber Hawk can detect and alert upon within the Site's network.


Global Settings > Service Plans > Manage Plans > Modify Plan
Modify Service Plan Brass Service Plan 2019
Plan Details
Cyber Hawk Policies
Select Policies to include in Plan
Smart Tag Description
Click on Policies to view Description
Required Smart Tags

- ⊟ All Policies
  - ⊟ Access Control
    - ☑ Authorize New Devices to be Added to Restricted Networks
    - ☑ Investigate Suspicious Logons by Users
    - □ Investigate Suspicious Logons to Computers
    - □ Restrict Access to Accounting Computers to Authorized Users
    - □ Restrict Access to Business Owner Computers to Authorized Users
    - □ Restrict Access to Computers Containing ePHI to Authorized Users
    - □ Restrict Access to IT Admin Only Restricted Computers to IT Administrators
    - ☑ Restrict Access to Systems in the Cardholder Data Environment (CDE) to Authorized Us
    - □ Restrict IT Administrative Access to Minimum Necessary
    - □ Restrict Users that are Not Authorized to Log into Multiple Computer Systems
    - □ Strictly Control the Addition of New Local Computer Administrators
    - □ Strictly Control the Addition of New Users to the Domain
    - □ Strictly Control the Addition of Printers

Restrict Access to Systems in the Cardholder Data Environment (CDE) to Authorized Users

Description

Computers in the network that are used to transmit, process, or store Cardholder Data may only be accessed by users authorized to access the Cardholder Data Environment (CDE). By applying tagging to a computer as a PCI/CDE COMPUTER, you will start receiving alerts when users that are not tagged as a PCI/CDE AUTHORIZED USER logs into the computer. By tagging computers that are part of the CDE and tagging the users that are authorized to access CDE computers, Detector can identify unauthorized access.

Required SmartTags

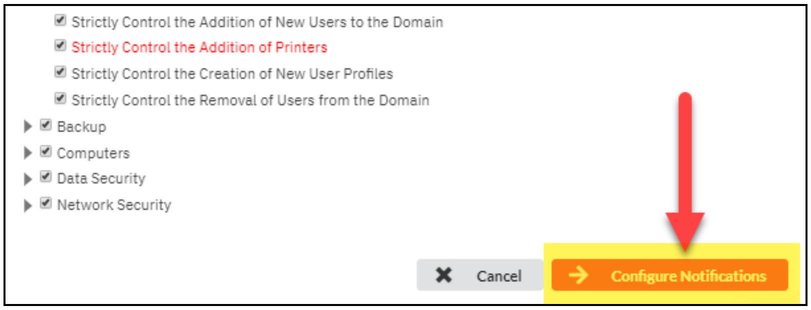
PCI / CDE AUTHORIZED USER	This tag is applied to a User
PCI / CDE COMPUTER	This tag is applied to a Computer

2. Check the box next to each Security Policy to include in the plan. Click ▶ to expand each available Policy category.
3. Click on a Policy to read a **Description** of that Policy, as well as to see any **Required Smart Tags**. You will need to deploy these Smart Tags on the appropriate network assets (such as Users or Computers) in order for Cyber Hawk to enforce these policies.

Step 3 — Configure Notifications for Security Policies

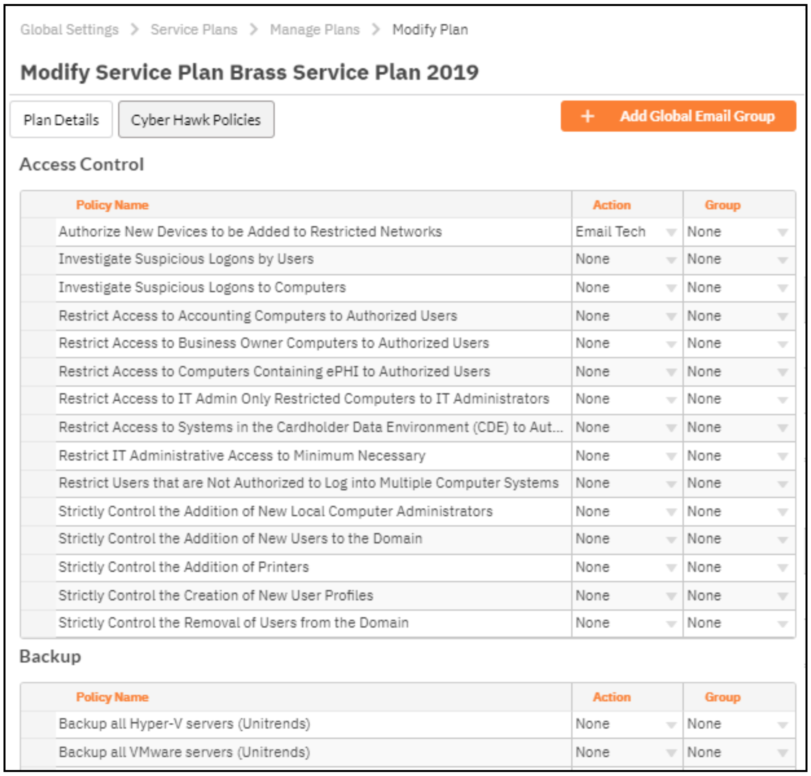
1. When you have selected the Security Policies you want to include in the Service Plan, click **Configure Notifications**.

© 2024 RapidFire Tools, Inc. All rights reserved.



☑ Strictly Control the Addition of New Users to the Domain
☑ Strictly Control the Addition of Printers
☑ Strictly Control the Creation of New User Profiles
☑ Strictly Control the Removal of Users from the Domain
▸ ☑ Backup
▸ ☑ Computers
▸ ☑ Data Security
▸ ☑ Network Security

2. Next, assign **Actions** and **Email Groups** for each Security Policy's Notification Rule. This is where you tell Cyber Hawk what to do when it discovers a potential security policy violation.



Global Settings > Service Plans > Manage Plans > Modify Plan

Modify Service Plan Brass Service Plan 2019

Plan Details
Cyber Hawk Policies
+ Add Global Email Group

Access Control

Policy Name	Action	Group
Authorize New Devices to be Added to Restricted Networks	Email Tech	None
Investigate Suspicious Logons by Users	None	None
Investigate Suspicious Logons to Computers	None	None
Restrict Access to Accounting Computers to Authorized Users	None	None
Restrict Access to Business Owner Computers to Authorized Users	None	None
Restrict Access to Computers Containing ePHI to Authorized Users	None	None
Restrict Access to IT Admin Only Restricted Computers to IT Administrators	None	None
Restrict Access to Systems in the Cardholder Data Environment (CDE) to Aut...	None	None
Restrict IT Administrative Access to Minimum Necessary	None	None
Restrict Users that are Not Authorized to Log into Multiple Computer Systems	None	None
Strictly Control the Addition of New Local Computer Administrators	None	None
Strictly Control the Addition of New Users to the Domain	None	None
Strictly Control the Addition of Printers	None	None
Strictly Control the Creation of New User Profiles	None	None
Strictly Control the Removal of Users from the Domain	None	None

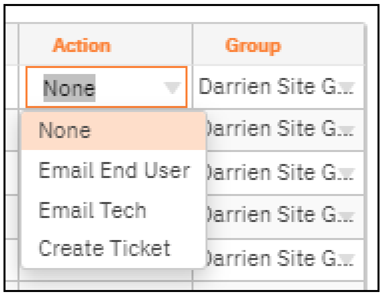
Backup

Policy Name	Action	Group
Backup all Hyper-V servers (Unitrends)	None	None
Backup all VMware servers (Unitrends)	None	None

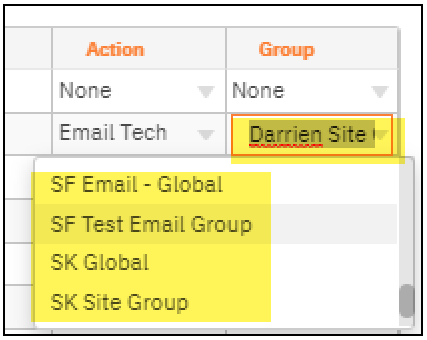
3. First, assign each Policy a Notification Rule/**Action**. Actions include:
    - **None**: Take no action.
    - **Email End User**: Send an email to an end user group. The end user will then make a decision about whether to request further investigation from the Tech Team.

© 2024 RapidFire Tools, Inc. All rights reserved.

- **Email Tech**: Send an email to the Tech Team to investigate the issue.
- **Create a Ticket**: Automatically Create a Ticket in your favorite PSA/ticketing system



4. Select the Email **Group Name** (the email group to whom to send either an End User or Tech email notification).



5. When you have assigned *Actions* and *Groups* to all Security Policies, click **Save**. You can then apply this Service Plan to your existing or new Cyber Hawk Sites.

> **Note:** To Do items and Alerts generated by Cyber Hawk will remain in the RapidFire Tools Portal for two weeks before they are automatically removed.

© 2024 RapidFire Tools, Inc. All rights reserved.

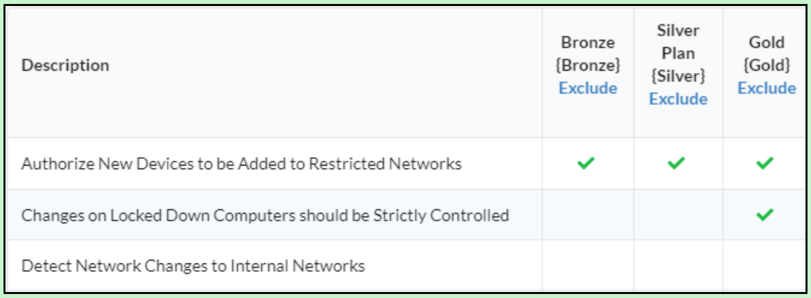
Create Service Catalogs

Note: This feature is intended for MSPs who are using Cyber Hawk to sell their security services; it is not intended for organizations who are using Cyber Hawk internally within their own network.

Cyber Hawk allows you to create **Service Catalogs** as a way to market your security services to potential customers.

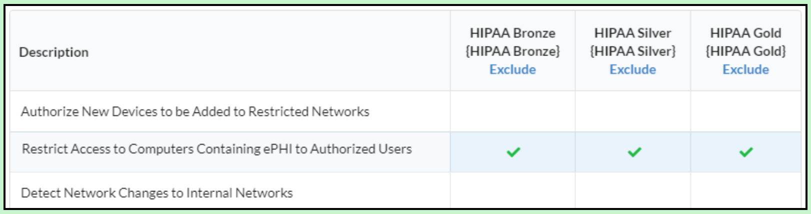
- A Service Catalog contains an easy-to-read matrix of each "tier" of security service you want to offer, such as "Bronze," "Silver," "Gold," or your own custom plans.
- You can generate catalogs as Word documents in order to market your services.
- Cyber Hawk also allows you to create multiple catalogs for different types of customers.

EXAMPLE: For example, you might want to have a generic *Bronze*, *Silver*, and *Gold* offering for a wide range of potential customers.



Description	Bronze {Bronze} Exclude	Silver Plan {Silver} Exclude	Gold {Gold} Exclude
Authorize New Devices to be Added to Restricted Networks	✓	✓	✓
Changes on Locked Down Computers should be Strictly Controlled			✓
Detect Network Changes to Internal Networks			

At the same time, you can also maintain service plans geared toward potential customers who require specialized HIPAA security services.



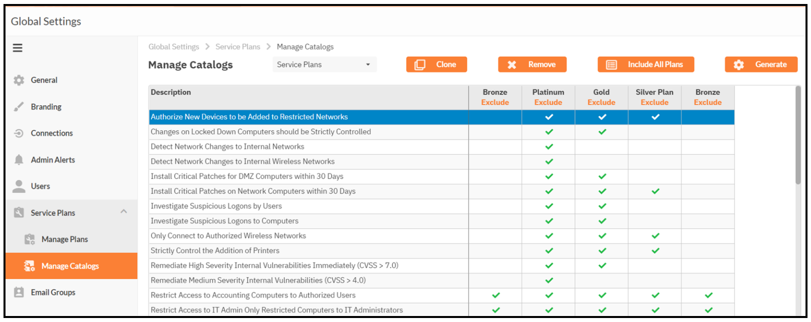
Description	HIPAA Bronze {HIPAA Bronze} Exclude	HIPAA Silver {HIPAA Silver} Exclude	HIPAA Gold {HIPAA Gold} Exclude
Authorize New Devices to be Added to Restricted Networks			
Restrict Access to Computers Containing ePHI to Authorized Users	✓	✓	✓
Detect Network Changes to Internal Networks			

To create and generate a Service Catalog:

© 2024 RapidFire Tools, Inc. All rights reserved.

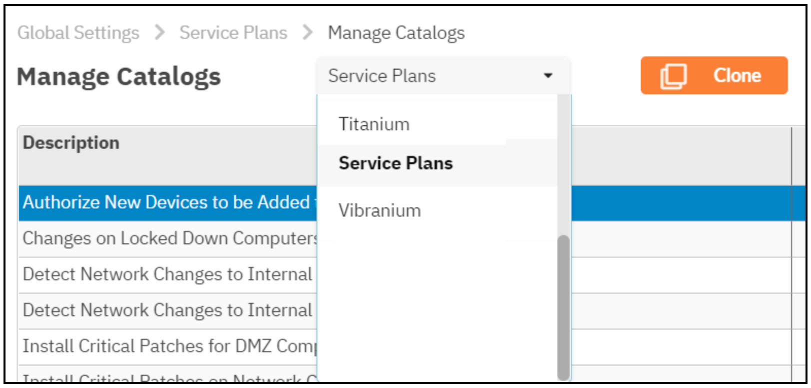
Important: Before you can create a catalog, be sure that you have already created each individual plan that you wish to include in the Catalog. See also "Create Global Service Plans for Cyber Hawk" on page 97.

1. Go to global **Settings (Admin)** ⚙ > **Service Plans** > **Manage Catalogs**. The Manage Catalogs screen will appear.



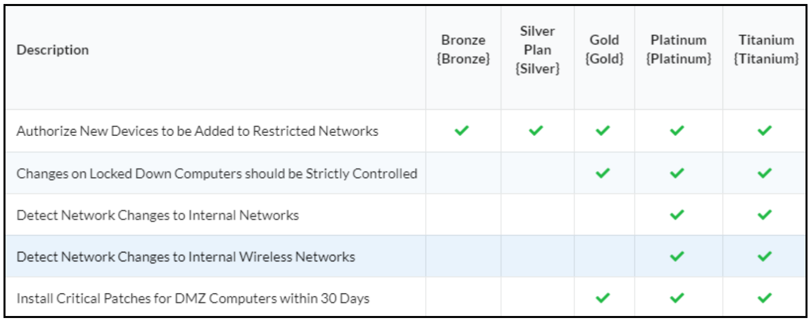
Description	Bronze Exclude	Platinum Exclude	Gold Exclude	Silver Plan Exclude	Bronze Exclude
Authorize New Devices to be Added to Restricted Networks		✓	✓	✓	
Changes on Locked Down Computers should be Strictly Controlled		✓	✓		
Detect Network Changes to Internal Networks		✓			
Detect Network Changes to Internal Wireless Networks		✓			
Install Critical Patches for DMZ Computers within 30 Days		✓	✓		
Install Critical Patches on Network Computers within 30 Days		✓	✓	✓	
Investigate Suspicious Logons by Users		✓	✓		
Investigate Suspicious Logons to Computers		✓	✓		
Only Connect to Authorized Wireless Networks		✓	✓	✓	
Strictly Control the Addition of Printers		✓	✓	✓	
Remediate High Severity Internal Vulnerabilities Immediately (CVSS > 7.0)		✓	✓		
Remediate Medium Severity Internal Vulnerabilities (CVSS > 4.0)		✓			
Restrict Access to Accounting Computers to Authorized Users	✓	✓	✓	✓	✓
Restrict Access to IT Admin Only Restricted Computers to IT Administrators	✓	✓	✓	✓	✓

2. From the drop-down menu, select **All Plans**.



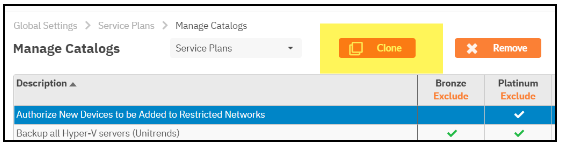
Description
Authorize New Devices to be Added t
Changes on Locked Down Computers
Detect Network Changes to Internal
Detect Network Changes to Internal
Install Critical Patches for DMZ Com
Install Critical Patches on Network C

3. Here you can see a matrix displaying all of your Service Plans. A *green check mark* indicates that the Service Plan contains the Security Policy, as in the image below.



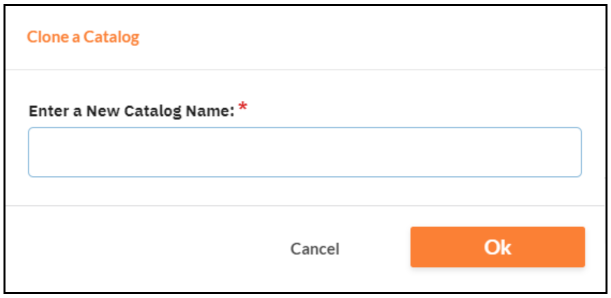
Description	Bronze {Bronze}	Silver Plan {Silver}	Gold {Gold}	Platinum {Platinum}	Titanium {Titanium}
Authorize New Devices to be Added to Restricted Networks	✓	✓	✓	✓	✓
Changes on Locked Down Computers should be Strictly Controlled			✓	✓	✓
Detect Network Changes to Internal Networks				✓	✓
Detect Network Changes to Internal Wireless Networks				✓	✓
Install Critical Patches for DMZ Computers within 30 Days			✓	✓	✓

4. To make a new catalog, click **Clone**.



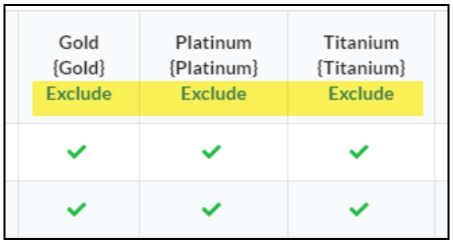
Description ▲	Bronze Exclude	Platinum Exclude
Authorize New Devices to be Added to Restricted Networks		✓
Backup all Hyper-V servers (Unitrends)	✓	✓

5. Enter a **name** for the new catalog. Click **OK**.



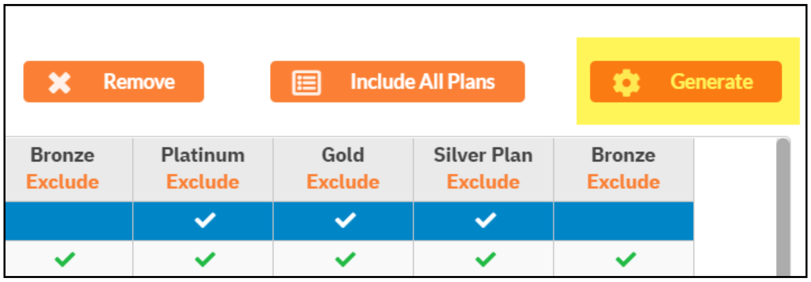
Enter a New Catalog Name: *

6. To create your custom catalog, click **Exclude** underneath each plan that you wish to REMOVE from the catalog. Continue removing plans until the catalog contains only the plans you want.



Gold {Gold} Exclude	Platinum {Platinum} Exclude	Titanium {Titanium} Exclude
✓	✓	✓
✓	✓	✓

7. When you are finished, click **Generate**. Your catalog will then appear as a Word document download.



Bronze Exclude	Platinum Exclude	Gold Exclude	Silver Plan Exclude	Bronze Exclude
	✓	✓	✓	
✓	✓	✓	✓	✓

Your Catalog will also be automatically saved and available from the drop-down menu.

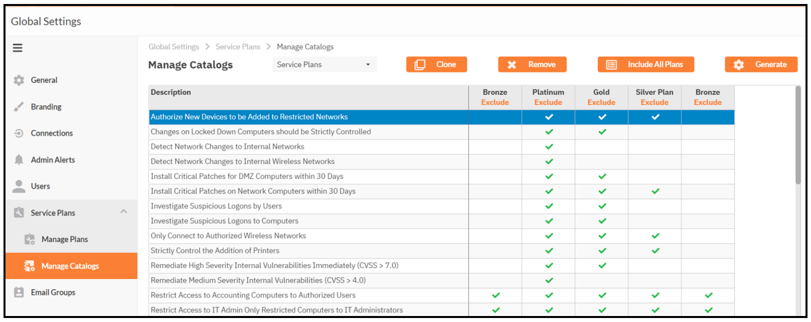
Generate a Service Catalog Document

After you have created a Service Catalog, you can **generate a Service Catalog document in Microsoft Word format**.

The Service Catalog document will contain a list of the Security Plans you have assigned to your Service Catalog(s) along with an overview of the Service Plan Security Policies.

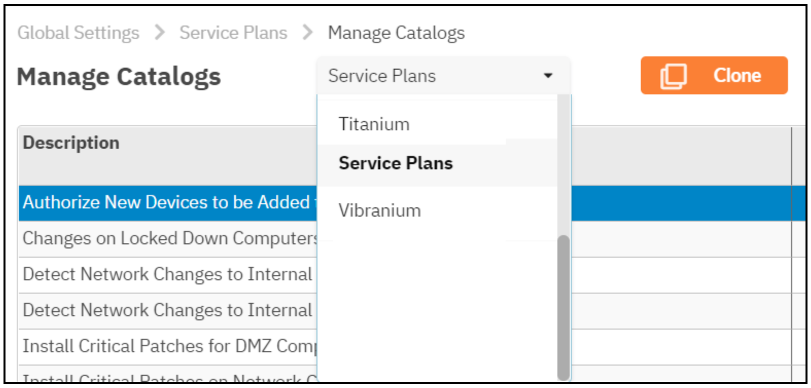
To generate the Service Catalog document, follow these steps:

1. From the RapidFire Tools Portal, go to global **Settings (Admin)** ⚙ > **Service Plans** > **Manage Catalogs**.



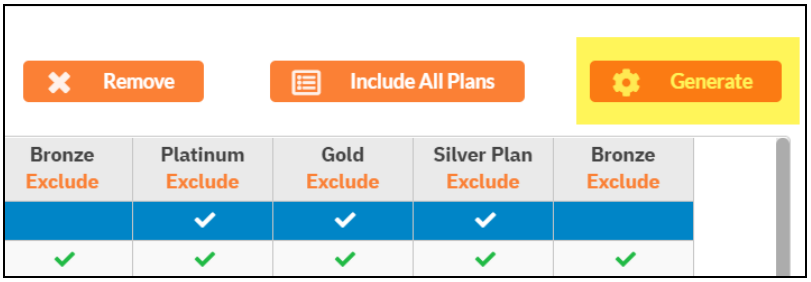
Description	Bronze Exclude	Platinum Exclude	Gold Exclude	Silver Plan Exclude	Bronze Exclude
Authorize New Devices to be Added to Restricted Networks		✓	✓	✓	
Changes on Locked Down Computers should be Strictly Controlled		✓	✓		
Detect Network Changes to Internal Networks		✓			
Detect Network Changes to Internal Wireless Networks		✓			
Install Critical Patches for DMZ Computers within 30 Days		✓	✓		
Install Critical Patches on Network Computers within 30 Days		✓	✓	✓	
Investigate Suspicious Logons by Users		✓	✓		
Investigate Suspicious Logons to Computers		✓	✓		
Only Connect to Authorized Wireless Networks		✓	✓	✓	
Strictly Control the Addition of Printers		✓	✓	✓	
Remediate High Severity Internal Vulnerabilities Immediately (CVSS > 7.0)		✓	✓		
Remediate Medium Severity Internal Vulnerabilities (CVSS > 4.0)		✓			
Restrict Access to Accounting Computers to Authorized Users	✓	✓	✓	✓	✓
Restrict Access to IT Admin Only Restricted Computers to IT Administrators	✓	✓	✓	✓	✓

2. Select the catalog you want to generate from **Manage Catalogs drop-down** menu.


Global Settings > Service Plans > Manage Catalogs
Manage Catalogs
Service Plans
Clone
Description
Titanium
Service Plans
Vibranium
Authorize New Devices to be Added t
Changes on Locked Down Computers
Detect Network Changes to Internal
Detect Network Changes to Internal
Install Critical Patches for DMZ Comp

3. Click **Generate**.

© 2024 RapidFire Tools, Inc. All rights reserved.



Bronze Exclude	Platinum Exclude	Gold Exclude	Silver Plan Exclude	Bronze Exclude
	✓	✓	✓	
✓	✓	✓	✓	✓

4. Select **Service Plan Catalog**.
5. Click **OK**.

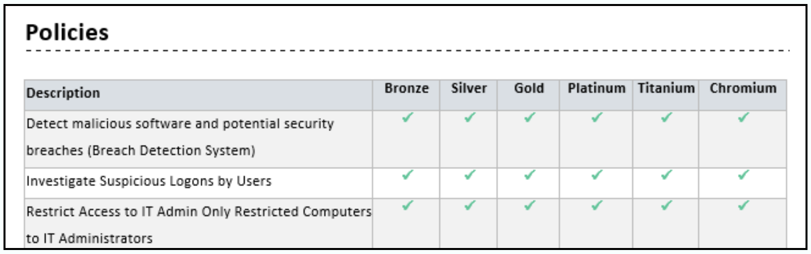
   You can then download and open the document in Microsoft Word, where you can edit or print the document.

© 2024 RapidFire Tools, Inc. All rights reserved.

Generate a Service Plan Matrix Document

After you have created a Service Plan, you can **generate a Service Plan Matrix document in Microsoft Word format**.

> **Note:** The Service Plan Matrix provides a visual overview of the Security Policies in each of the Service Plans that you have included in one of your Catalogs.

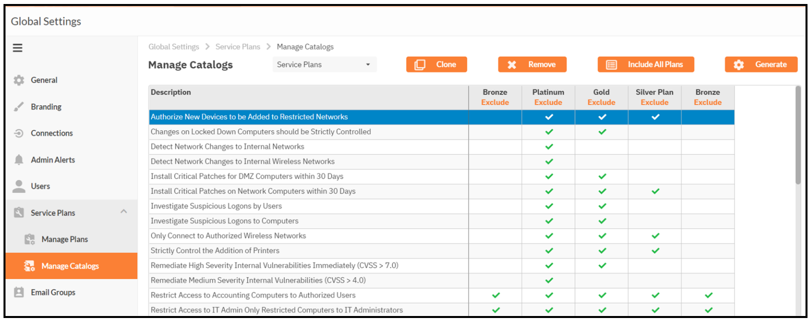


Policies

Description	Bronze	Silver	Gold	Platinum	Titanium	Chromium
Detect malicious software and potential security breaches (Breach Detection System)	✓	✓	✓	✓	✓	✓
Investigate Suspicious Logons by Users	✓	✓	✓	✓	✓	✓
Restrict Access to IT Admin Only Restricted Computers to IT Administrators	✓	✓	✓	✓	✓	✓

To generate the Service Plan Matrix document for one of your Catalogs, follow these steps:

1. From the RapidFire Tools Portal, go to global **Settings (Admin)** ⚙ > **Service Plans** > **Manage Catalogs**.

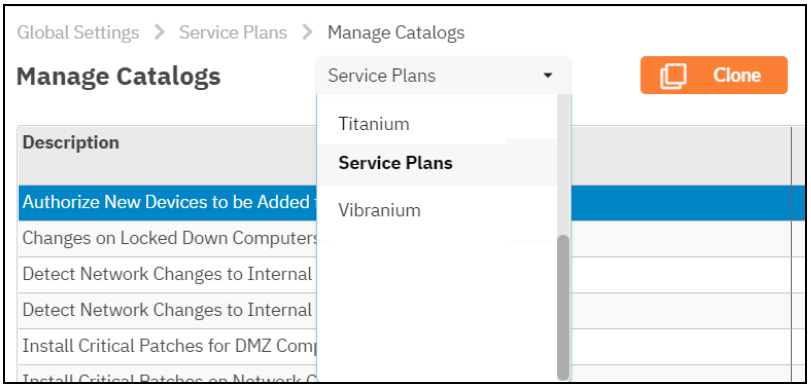


Description	Bronze Exclude	Platinum Exclude	Gold Exclude	Silver Plan Exclude	Bronze Exclude
Authorize New Devices to be Added to Restricted Networks		✓	✓	✓	
Changes on Locked Down Computers should be Strictly Controlled		✓	✓		
Detect Network Changes to Internal Networks		✓			
Detect Network Changes to Internal Wireless Networks		✓			
Install Critical Patches for DMZ Computers within 30 Days		✓	✓		
Install Critical Patches on Network Computers within 30 Days		✓	✓	✓	
Investigate Suspicious Logons by Users		✓	✓		
Investigate Suspicious Logons to Computers		✓	✓		
Only Connect to Authorized Wireless Networks		✓	✓	✓	
Strictly Control the Addition of Printers		✓	✓	✓	
Remediate High Severity Internal Vulnerabilities Immediately (CVSS > 7.0)		✓	✓		
Remediate Medium Severity Internal Vulnerabilities (CVSS > 4.0)		✓			
Restrict Access to Accounting Computers to Authorized Users	✓	✓	✓	✓	✓
Restrict Access to IT Admin Only Restricted Computers to IT Administrators	✓	✓	✓	✓	✓

2. Select the catalog you want to generate from **Manage Catalogs drop-down** menu.

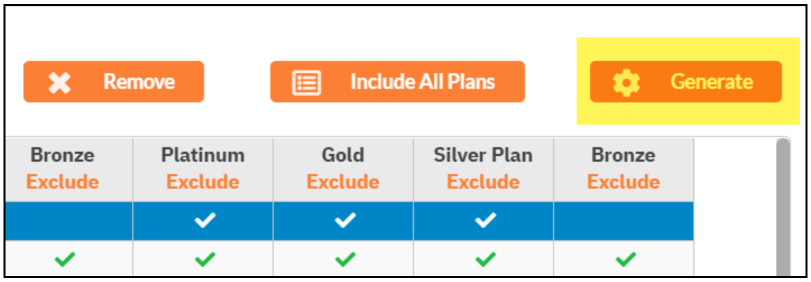
RapidFireTools®

© 2024 RapidFire Tools, Inc. All rights reserved.



Description
Authorize New Devices to be Added
Changes on Locked Down Computers
Detect Network Changes to Internal
Detect Network Changes to Internal
Install Critical Patches for DMZ Comp
Install Critical Patches on Network C

3. Click **Generate**.



Bronze Exclude	Platinum Exclude	Gold Exclude	Silver Plan Exclude	Bronze Exclude
	✓	✓	✓	
✓	✓	✓	✓	✓

4. Select **Service Plan Matrix**.
5. Click **OK**.

   You can then download and open the document in Microsoft Word, where you can edit or print the document.

© 2024 RapidFire Tools, Inc. All rights reserved.

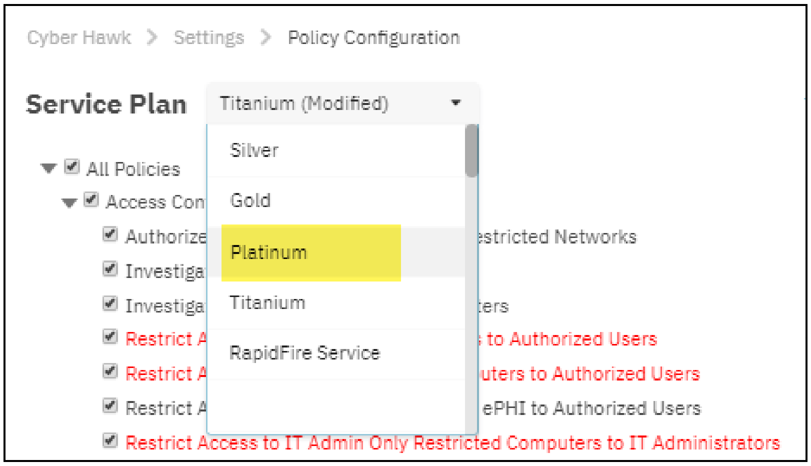
Generate a Sample Master Services Agreement for a Service Plan

After you have created a Service Plan, you can generate a sample Master Services Agreement (MSA) document in Microsoft Word format.

Note: The sample MSA document will include an example of terms and conditions for an MSA and reference an Exhibit that will present a list of the Security Policies and Procedures that reflect the Service Plan that will be selected when setting up the Cyber Hawk for your customer.

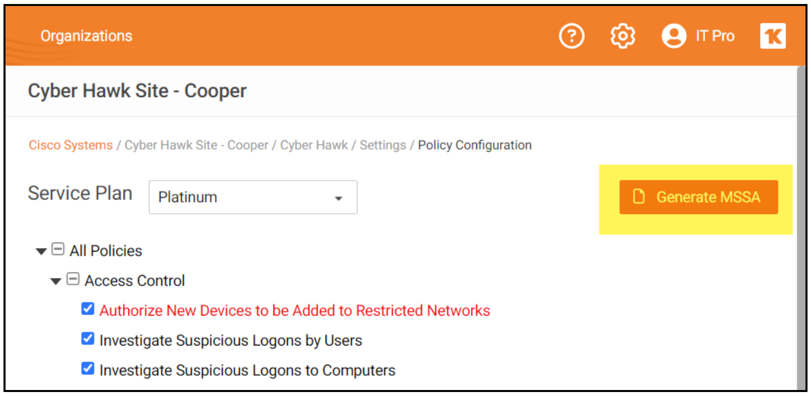
To generate the Sample MSA document, follow these steps:

1. Open the Site for which to generate the MSA.
2. Go to **Cyber Hawk** > **Settings** > **Security** > **Policy Configuration**.
3. Ensure the correct Service Plan has been applied to the Site. This is the plan that will be included in the MSA.



4. Click **Generate MSSA**.

© 2024 RapidFire Tools, Inc. All rights reserved.



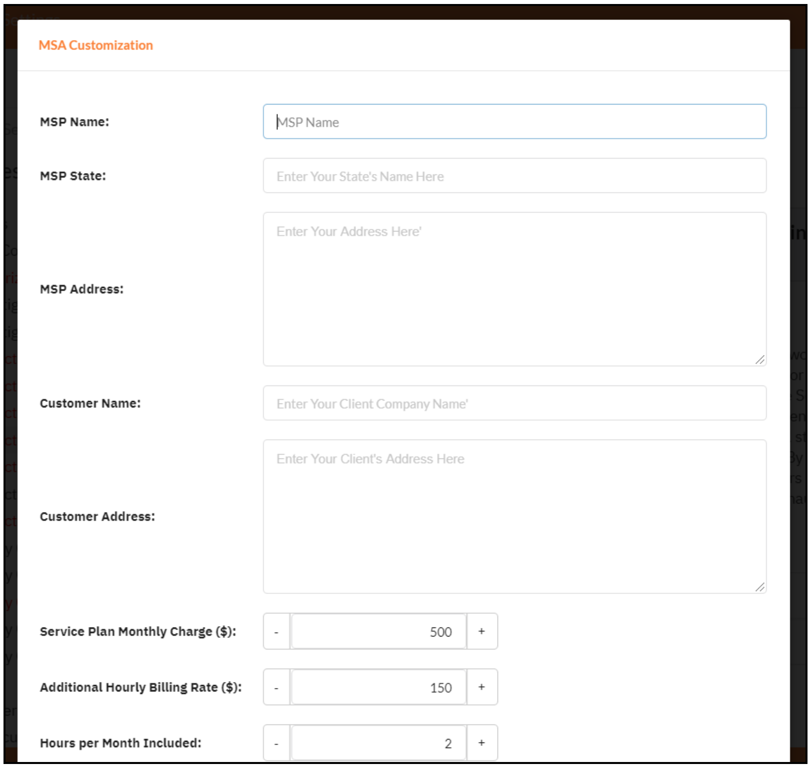
Cyber Hawk Site - Cooper

Cisco Systems / Cyber Hawk Site - Cooper / Cyber Hawk / Settings / Policy Configuration

Service Plan: Platinum

- ⊟ All Policies
  - ⊟ Access Control
    - ☑ Authorize New Devices to be Added to Restricted Networks
    - ☑ Investigate Suspicious Logons by Users
    - ☑ Investigate Suspicious Logons to Computers

5. Enter your custom information for the MSSA.

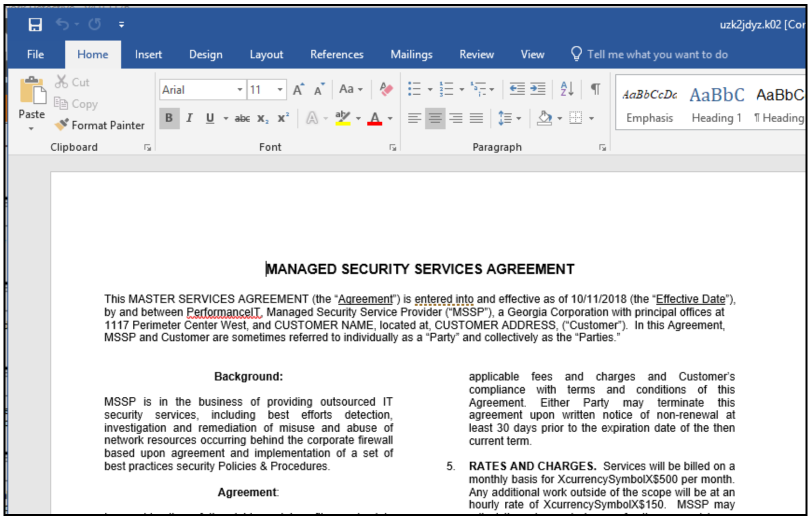


MSA Customization

MSP Name:	MSP Name
MSP State:	Enter Your State's Name Here
MSP Address:	Enter Your Address Here'
Customer Name:	Enter Your Client Company Name'
Customer Address:	Enter Your Client's Address Here
Service Plan Monthly Charge ($):	500
Additional Hourly Billing Rate ($):	150
Hours per Month Included:	2

6. A Word doc version of the MSSA will open. You can provide this to the client when and how you see fit.

© 2024 RapidFire Tools, Inc. All rights reserved.



MANAGED SECURITY SERVICES AGREEMENT

This MASTER SERVICES AGREEMENT (the "Agreement") is entered into and effective as of 10/11/2018 (the "Effective Date"), by and between PerformanceIT, Managed Security Service Provider ("MSSP"), a Georgia Corporation with principal offices at 1117 Perimeter Center West, and CUSTOMER NAME, located at, CUSTOMER ADDRESS, ("Customer"). In this Agreement, MSSP and Customer are sometimes referred to individually as a "Party" and collectively as the "Parties."

Background:

MSSP is in the business of providing outsourced IT security services, including best efforts detection, investigation and remediation of misuse and abuse of network resources occurring behind the corporate firewall based upon agreement and implementation of a set of best practices security Policies & Procedures.

Agreement:

applicable fees and charges and Customer's compliance with terms and conditions of this Agreement. Either Party may terminate this agreement upon written notice of non-renewal at least 30 days prior to the expiration date of the then current term.

5. **RATES AND CHARGES.** Services will be billed on a monthly basis for XcurrencySymbolX$500 per month. Any additional work outside of the scope will be at an hourly rate of XcurrencySymbolX$150. MSSP may

7. You can come back and modify the security policy at any time, as well as generate a new MSSA.

© 2024 RapidFire Tools, Inc. All rights reserved.

Managing Service Plans

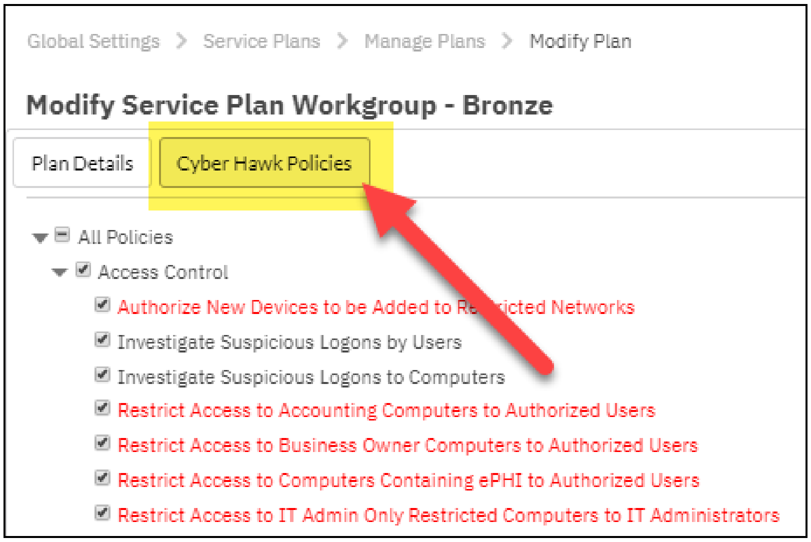
The instructions below detail the processes used to Modify and Delete Service Plans.

Edit a Service a Plan (Global Settings)

Important: When you update a Service Plan from Global Settings, each Site currently using that plan will be updated, as well.

To edit a Service Plan, follow these steps:

1. From within the RapidFire Tools Portal, go to global **Settings (Admin)** ⚙ > **Service Plans** > **Manage Plans**.
2. Select the **Edit** ✎ icon on the Service Plan that you would like to edit.
3. The Modify Service Plan window will be displayed. Click **Cyber Hawk Policies**.



Global Settings > Service Plans > Manage Plans > Modify Plan

Modify Service Plan Workgroup - Bronze

- ▾ ⊟ All Policies
  - ▾ ☑ Access Control
    - ☑ Authorize New Devices to be Added to Restricted Networks
    - ☑ Investigate Suspicious Logons by Users
    - ☑ Investigate Suspicious Logons to Computers
    - ☑ Restrict Access to Accounting Computers to Authorized Users
    - ☑ Restrict Access to Business Owner Computers to Authorized Users
    - ☑ Restrict Access to Computers Containing ePHI to Authorized Users
    - ☑ Restrict Access to IT Admin Only Restricted Computers to IT Administrators

4. Change the Cyber Hawk Security Policies, then click **Configure Notifications**.
5. Change the Actions and Groups associated with your Security Policies, then click **Save**.

Delete a Service Plan

Important: When you delete a Service Plan, you will need to manually apply a new Service Plan to any deployed Cyber Hawks that were using the deleted plan.

© 2024 RapidFire Tools, Inc. All rights reserved.

To Delete a Service Plan, follow these steps:

1. From within the RapidFire Tools Portal, go to global **Settings (Admin)** ⚙ > **Service Plans** > **Manage Plans**.
2. Select the delete icon 🗑 on the Service Plan that you would like to remove.
3. Confirm that you wish to delete the Service Plan.

© 2024 RapidFire Tools, Inc. All rights reserved.

Managing Service Catalogs

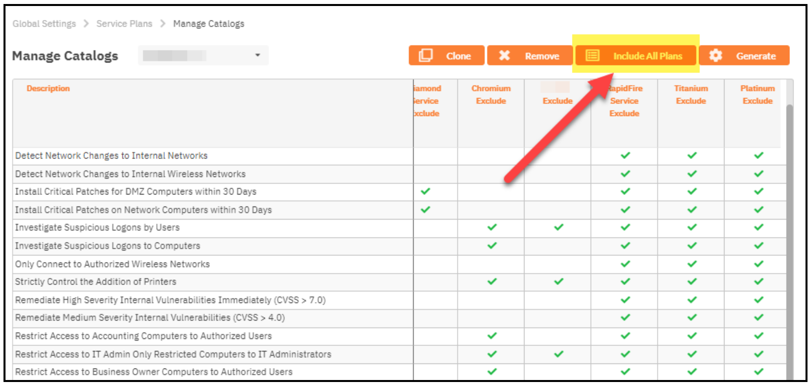
The instructions below detail the processes used to Modify and Remove (i.e. delete) Service Catalogs.

Add Service Plans to a Catalog

To Add a Service Plan to a Service Catalog, follow these steps:

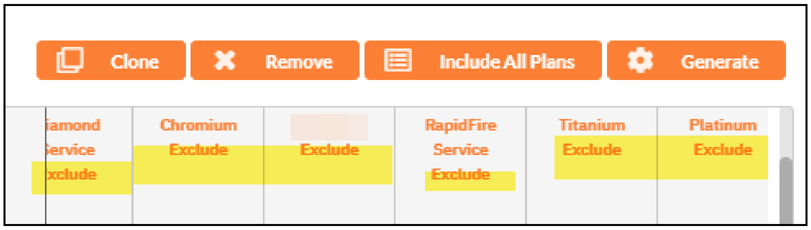
1. Go to global **Settings (Admin)** ⚙ > **Manage Catalogs**.
2. From the drop-down menu, select Service Catalog Name for the Catalog that you would like to edit.

   The selected Service Catalog will be displayed in the Manage Catalogs window. This Catalog will include the Service Plans previously added to the Catalog.
3. Click the **Include All Plans** button.



Description	iamond ervice xclude	Chromium Exclude	Exclude	apidFire Service Exclude	Titanium Exclude	Platinum Exclude
Detect Network Changes to Internal Networks				✓	✓	✓
Detect Network Changes to Internal Wireless Networks				✓	✓	✓
Install Critical Patches for DMZ Computers within 30 Days	✓			✓	✓	✓
Install Critical Patches on Network Computers within 30 Days	✓			✓	✓	✓
Investigate Suspicious Logons by Users		✓	✓	✓	✓	✓
Investigate Suspicious Logons to Computers		✓		✓	✓	✓
Only Connect to Authorized Wireless Networks				✓	✓	✓
Strictly Control the Addition of Printers		✓	✓	✓	✓	✓
Remediate High Severity Internal Vulnerabilities Immediately (CVSS > 7.0)				✓	✓	✓
Remediate Medium Severity Internal Vulnerabilities (CVSS > 4.0)				✓	✓	✓
Restrict Access to Accounting Computers to Authorized Users		✓		✓	✓	✓
Restrict Access to IT Admin Only Restricted Computers to IT Administrators		✓	✓	✓	✓	✓
Restrict Access to Business Owner Computers to Authorized Users		✓		✓	✓	✓

4. This action will add all of the other Service Plans that are currently not listed within the Catalog's Service Plan list.
5. Just below the name of each Service Plan is a link labeled Exclude. The selection of the Exclude Link removes the Service Plan from the Catalog.



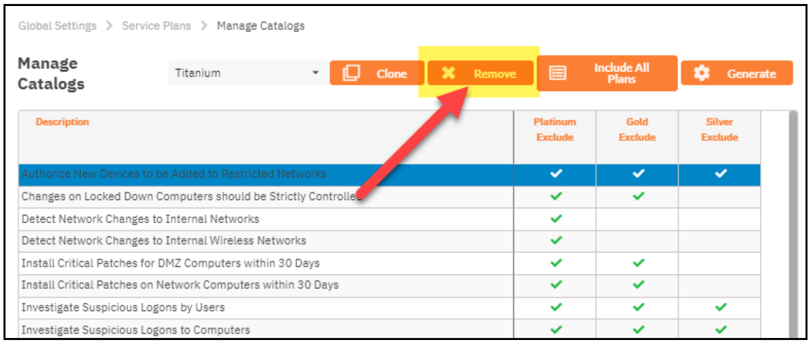
6. After you have Excluded the Services Plans that are not required, exit the Service Plan Creator.

© 2024 RapidFire Tools, Inc. All rights reserved.

Remove (Delete) a Service Catalog from the List of Catalogs

To Remove (delete) an entire Service Catalog, follow these steps:

1. From within the RapidFire Tools Portal, go to global **Settings (Admin)** > **Service Plans** > **Manage Catalogs**.
2. Select the catalog from the drop-down menu that you want to edit.
3. Click **Remove**.

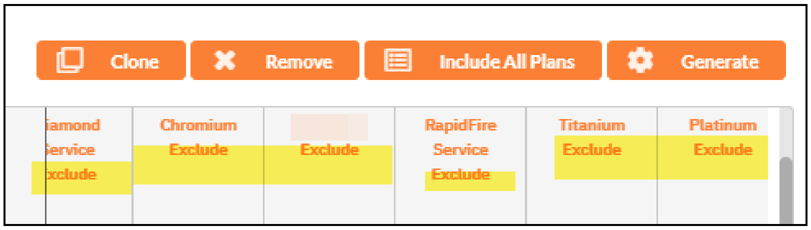


Description	Platinum Exclude	Gold Exclude	Silver Exclude
Authorize New Devices to be Added to Restricted Networks	✓	✓	✓
Changes on Locked Down Computers should be Strictly Controlled	✓	✓	
Detect Network Changes to Internal Networks	✓		
Detect Network Changes to Internal Wireless Networks	✓		
Install Critical Patches for DMZ Computers within 30 Days	✓	✓	
Install Critical Patches on Network Computers within 30 Days	✓	✓	
Investigate Suspicious Logons by Users	✓	✓	✓
Investigate Suspicious Logons to Computers	✓	✓	✓

Delete (Exclude) Service Plans from a Catalog

To delete a Service Plan from a Service Catalog, follow these steps:

1. From within the RapidFire Tools Portal, go to global **Settings (Admin)** > **Service Plans** > **Manage Catalogs**.
2. Select the catalog from the drop-down menu that you want to edit.
3. Click **Exclude** underneath the plan(s) that you want to remove from the catalog. Your changes will be automatically saved.



© 2024 RapidFire Tools, Inc. All rights reserved.

Default Cyber Hawk Service Plans

The default Cyber Hawk Service Plans available for selection after initial installation are the Bronze, Silver, Gold, and Platinum plans. Below is an overview of the default Security Policies associated with each Service Plan.

Security Policy Description	Bronze	Silver	Gold	Platinum
Authorize New Devices to be Added to Restricted Networks	✓	✓	✓	✓
Restrict Access to Accounting Computers to Authorized Users	✓	✓	✓	✓
Restrict Access to Business Owner Computers to Authorized Users	✓	✓	✓	✓
Restrict IT Administrative Access to Minimum Necessary	✓	✓	✓	✓
Restrict Users that are Not Authorized to Log into Multiple Computer Systems	✓	✓	✓	✓
Strictly Control the Addition of New Local Computer Administrators	✓	✓	✓	✓
Strictly Control the Addition of New Users to the Domain	✓	✓	✓	✓
Install Critical Patches on Network Computers within 30 Days		✓	✓	✓
Only Connect to Authorized Wireless Networks		✓	✓	✓
Strictly Control the Addition of Printers		✓	✓	✓
Restrict Access to IT Admin Only Restricted Computers to IT Administrators		✓	✓	✓

Security Policy Description	Bronze	Silver	Gold	Platinum
Users Should Only Access Authorized Systems		✓	✓	✓
Changes on Locked Down Computers should be Strictly Controlled			✓	✓
Install Critical Patches for DMZ Computers within 30 Days			✓	✓
Investigate Suspicious Logons by Users			✓	✓
Investigate Suspicious Logons to Computers			✓	✓
Remediate High Severity Internal Vulnerabilities Immediately (CVSS > 7.0)			✓	✓
Restrict Internet Access for Computers that are Not Authorized to Access the Internet Directly			✓	✓
Detect Network Changes to Internal Networks				✓
Detect Network Changes to Internal Wireless Networks				✓
Remediate Medium Severity Internal Vulnerabilities (CVSS > 4.0)				✓
Restrict Access to Computers Containing ePHI to Authorized Users				✓
Restrict Access to Systems in the Cardholder Data Environment (CDE) to Authorized Users				✓
Strictly Control the Clearing of System and Audit Logs				
Strictly Control the Removal of Users from the Domain				

© 2024 RapidFire Tools, Inc. All rights reserved.

Security Policy Description	Bronze	Silver	Gold	Platinum
Enable automatic screen lock on computers with sensitive information				
Enable automatic screen lock for users with access to sensitive information				
Strictly control DNS on Locked Down Networks				
Strictly control changes to Group Policy				
Strictly control changes to the Default Domain Policy				
Only store Personally Identifiable Information (PII) on systems marked as sensitive				
Strictly Control the Creation of New User Profiles				
Only store ePHI on designated systems				
Only store cardholder data on designated systems				
Backup all HyperV servers (Unitrends)				
Backup all VMware servers (Unitrends)				
Backup all Windows servers (Unitrends)				
Investigate all backup failures (Unitrends)				
Investigate all backup restore failures (Unitrends)				
Detect malicious software and potential security breaches (Breach Detection System)				

Appendices

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

© 2024 RapidFire Tools, Inc. All rights reserved.

Pre-Scan Network Configuration Checklist

RapidFire Tools products can gather a great deal of information from the target network with little advance preparation – and with very little footprint! However, if you are having trouble with scans, or you have the ability to configure the target network in advance, we recommend the settings below.

These checklists detail the recommended network configurations for both Windows **Domain** and **Workgroup** environments.

> **Note:** You must have the .NET 4.6.2 framework installed on machines in order to use all data collector and server/appliance tools.

Checklist for Domain Environments

Share this checklist with your IT Administrator and ask them to configure your network's Domain Controller as follows:

Complete	Domain Configuration
	GPO Configuration for Windows Firewall (Inbound Rules)
□	Allow *Windows Management Instrumentation (WMI)* service to operate through Windows Firewall This includes the following rules: • Windows Management Instrumentation (ASync-In) • Windows Management Instrumentation (WMI-In) • Windows Management Instrumentation (DCOM-In)
□	Allow *File and printer sharing* to operate through Windows Firewall This includes the following rules: • File and Printer Sharing (NB-Name-In) • File and Printer Sharing (SMB-In) • File and Printer Sharing (NB-Session-In)
□	Enable *Remote Registry* “read only” access on computers targeted for scanning.

Complete	Domain Configuration
	Note: Remote Registry access should be restricted for use by the user access account credentials to be used during network and local computer scan.
□	Enable the *Internet Control Message Protocol (ICMP)* to allow authorized ICMP echo request messages and ICMP echo reply messages to be sent and received by Windows computers and network devices. Windows firewall rules on Windows computers may need to be created/enabled to allow a computer: • operating a Kaseya-RapidFire Tools product network data collector to issue ICMP echo request messages to be sent to Windows computers and network devices • to send ICMP echo reply messages in response to an ICMP echo request **Note:** ICMP requests are used to detect active Windows computers and network devices to scan.
	GPO Configuration for Windows Services
□	*Windows Management Instrumentation (WMI)* • Startup Type: Automatic
□	*Windows Update Service* • Startup Type: Automatic
□	*Remote Registry* • Startup Type: Automatic
□	*Remote Procedure Call* • Startup Type: Automatic
	Network Shares
□	• *Admin$* must be present and accessible using supplied credentials (usually a local admin or user in the local Computer's Administrative Security group)

Complete	Domain Configuration
	3rd Party Firewalls
□	• Ensure that 3rd party Firewalls are configured similarly to Windows Firewall rules described within this checklist. **Note:** This is a requirment for both Active Directory and Workgroup Networks.

Checklist for Workgroup Environments

Before you perform a workgroup assessment, run the following PowerShell commands on the target network and the machine that will perform the scan. These three configurations should help you avoid most issues in a workgroup environment. Each command is followed by an explanation and link to Microsoft documentation.

1.
   ```
   reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system /v LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f
   ```

   By default, UAC only allows remote administration tasks to be performed by the Built-in Administrator account. To work around this, this command sets the LocalAccountTokenFilterPolicy registry key to 1. This allows any local admin to perform remote administrative tasks (i.e. access to system shares C$, Admin$, etc.).

   https://support.microsoft.com/en-us/help/951016/description-of-user-account-control-and-remote-restrictions-in-windows

2.
   ```
   netsh advfirewall firewall set rule group="windows management instrumentation (wmi)" new enable=yes
   ```

   This command creates an Inbound firewall rule to allow access to the WMI service and namespaces.

   https://docs.microsoft.com/en-us/windows/win32/wmisdk/connecting-to-wmi-remotely-starting-with-vista

3.
   ```
   netsh advfirewall firewall set rule group="File and Printer Sharing" new enable=Yes
   ```

This command creates an Inbound firewall rule which enables File and Printer Sharing on the machine. File and printer sharing is required in order to access the Admin$ share on remote machines.

https://answers.microsoft.com/en-us/windows/forum/all/turning-on-file-and-printer-sharing-windows-10/bb3066eb-f589-4021-8f71-617e70854354

You can also share this checklist with your IT Administrator and ask them to configure each computer in your workgroup as follows:

Complete?	Workgroup Configuration
	Network Settings
□	• *Admin$* must be present on the computers you wish to scan, and be accessible with the login credentials you provide for the scan
□	• *File and printer sharing* must be enabled on the computers you wish to scan
□	• *Ensure the Windows Services below are running and allowed to communicate through Windows Firewall*: • Windows Management Instrumentation (WMI) • Windows Update Service • Remote Registry • Remote Desktop • Remote Procedure Call
□	• Workgroup computer administrator user account credentials. **Note:** Before configuring scan settings for workgroups, prepare a list of the workgroup computer(s) adminstrator user account credentials for entry into the scan settings wizard.
□	Enable the *Internet Control Message Protocol (ICMP)* to allow authorized ICMP echo request messages and ICMP echo reply messages to be sent and received by Windows computers and network devices. Windows firewall rules on Windows computers may need to be created/enabled to allow a computer:

Complete?	Workgroup Configuration
	• operating a Kaseya-RapidFire Tools product network data collector to issue ICMP echo request messages to be sent to Windows computers and network devices • to send ICMP echo reply messages in response to an ICMP echo request **Note:** ICMP requests are used to detect active Windows computers and network devices to scan.

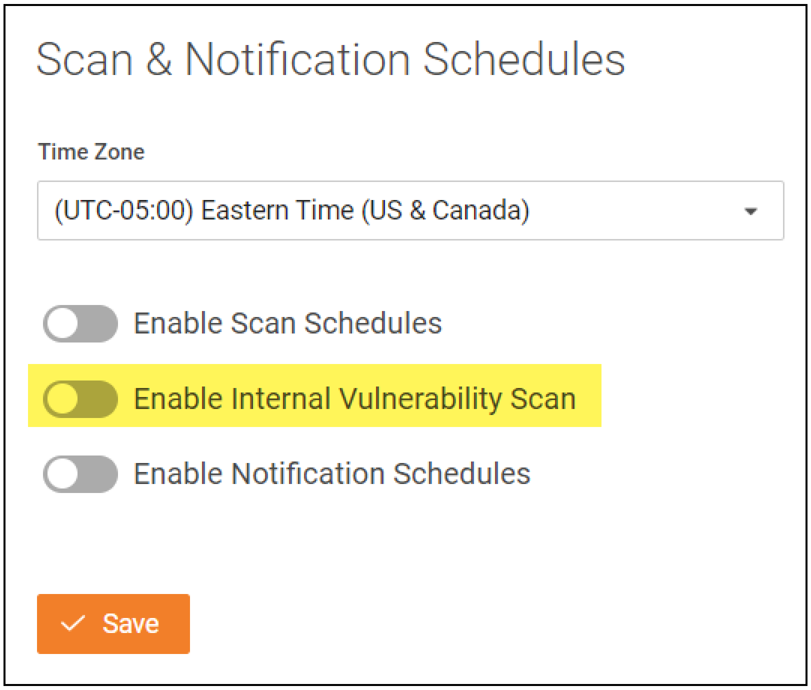
Migrate Cyber Hawk Virtual Appliance to Scan Server

The Cyber Hawk Virtual Appliance has been deprecated. The topic below details how to migrate the existing Cyber Hawk Virtual Appliance to the Scan Server. This involves decommissioning the Virtual Appliance and installing the new Scan Server.

Step 1 — Disable Internal Vulnerability Scan from Cyber Hawk Site

Important: Be sure to perform this step first. Failure to do so will prevent you from configuring the Internal Vulnerability scan after the scan server installation.

1. Navigate to **[Your Site]** > **Cyber Hawk** > **Settings** > **Scan & Notification Schedules**.
2. From **Enable Internal Vulnerability Scan**, **DISABLE** the slider.



Scan & Notification Schedules

Time Zone: (UTC-05:00) Eastern Time (US & Canada)

Enable Scan Schedules
Enable Internal Vulnerability Scan
Enable Notification Schedules
Save

3. Click **Save**.

Step 2 — Uninstall the Cyber Hawk Hyper-V/VMware Virtual Appliance

Uninstall the Cyber Hawk Virtual Appliance using Hyper-V or VMWare.

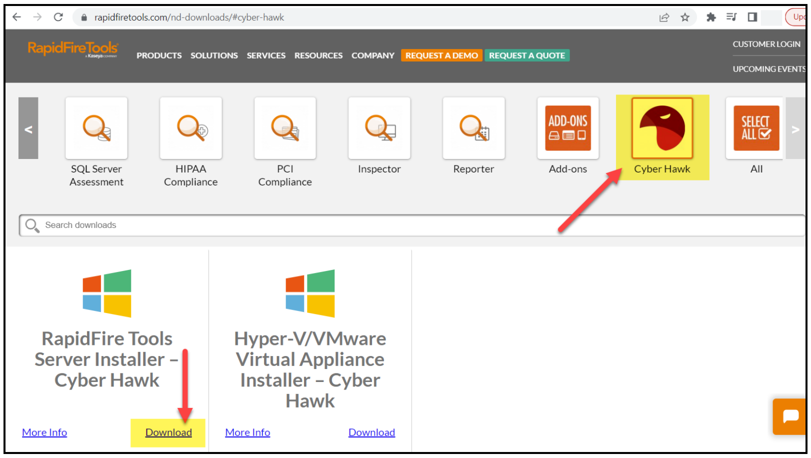
© 2024 RapidFire Tools, Inc. All rights reserved.

Step 3 — Contact Kaseya-RFT Support to Reclaim Appliance ID

Email support@rapidfiretools.com and request that the Appliance ID associated with your Cyber Hawk site be reclaimed. This will allow you to install a new appliance using the previous ID.

Step 4 — Install the Cyber Hawk RapidFire Tools Server

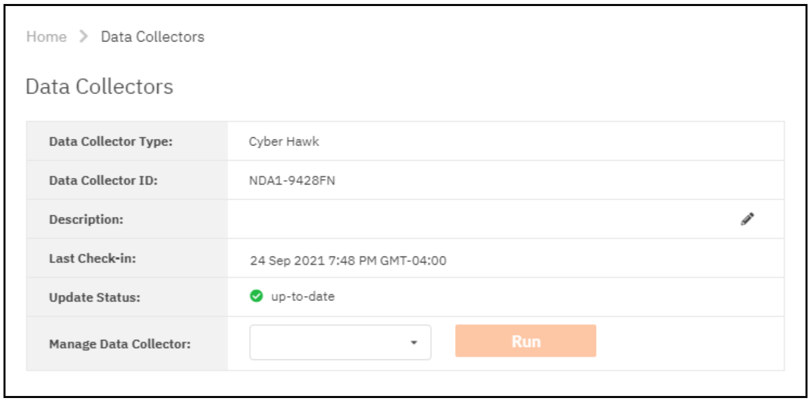
1. Visit www.rapidfiretools.com/nd and navigate to the Cyber Hawk tab.
2. Find and download the RapidFire Tools Server Installer for Cyber Hawk.



3. Run and install the RapidFire Tools Server. When prompted, select the Appliance ID that you reclaimed earlier. Look here for a complete walkthrough.

Step 5 — Configure Cyber Hawk Scan Settings

Open your Cyber Hawk Site and access **Home** > **Data Collectors**. Here you can verify that the RapidFire Tools Server is installed and online.



Home > Data Collectors

Data Collectors

Data Collector Type:	Cyber Hawk
Data Collector ID:	NDA1-9428FN
Description:	
Last Check-in:	24 Sep 2021 7:48 PM GMT-04:00
Update Status:	✓ up-to-date
Manage Data Collector:	Run

© 2024 RapidFire Tools, Inc. All rights reserved.

Once this is done:

1. Set up and configure Cyber Hawk Scan settings as detailed in the Cyber Hawk Web Console Quick Start Guide.
2. Use the VulScan integration to set up and perform internal vulnerability scans. This is detailed in the Cyber Hawk Quick Start Guide. You can also learn more about VulScan separately here.

© 2024 RapidFire Tools, Inc. All rights reserved.

Configure Cyber Hawk Scan Settings (Virtual Appliance)

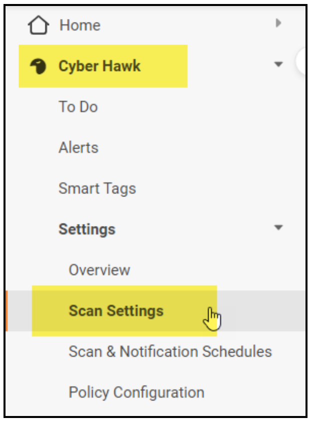
The topic below details how to configure the Scan Settings for the Virtual Appliance for Cyber Hawk.

Important: The Virtual Appliance for Cyber Hawk has been deprecated. See "Setting Up Cyber Hawk" on page 12 for the latest procedures for employing the RapidFire Tools Server and VulScan integration for internal vulnerability scanning.

- "Configure Scan Settings for Active Directory Domain" below
- "Configure Scan Settings for Workgroups" on page 237

Configure Scan Settings for Active Directory Domain

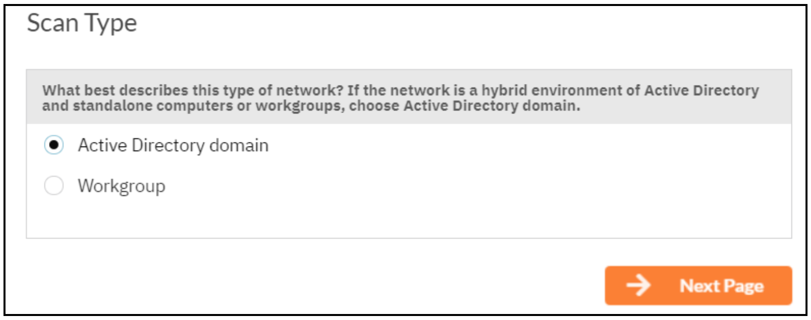
Set the **Scan Settings** from the **[Your Site]** > **Cyber Hawk** > **Settings** > **Scan Settings** page. Complete all required prompts.



Important: For best results, the target network must be configured to allow for successful scans on all network endpoints. See "Pre-Scan Network Configuration Checklist" on page 219 for configuration guidance.

Follow the steps below to configure the Scan Settings for the Cyber Hawk Appliance:

1. Select the Scan Type: **Active Directory Domain**. Click **Next Page**.



Scan Type

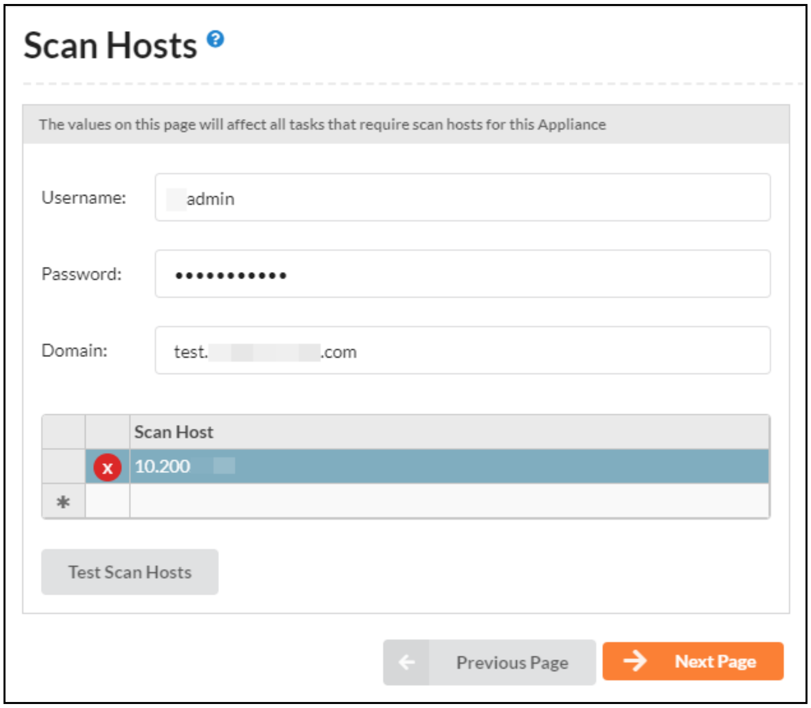
What best describes this type of network? If the network is a hybrid environment of Active Directory and standalone computers or workgroups, choose Active Directory domain.

● Active Directory domain

○ Workgroup

2. The **Scan Hosts** window will appear. Next assign scan hosts:

> **Note:** The Cyber Hawk Appliance requires access to at least one separate, additional PC on the client's network. This computer is called the "Scan Host." The **Scan Host** is used to initiate scans. For more information on Scan Host requirements, see "Additional Scan Host Details" on page 266.



Scan Hosts

The values on this page will affect all tasks that require scan hosts for this Appliance

Username: admin

Password: ●●●●●●●●●●●

Domain: test.[redacted].com

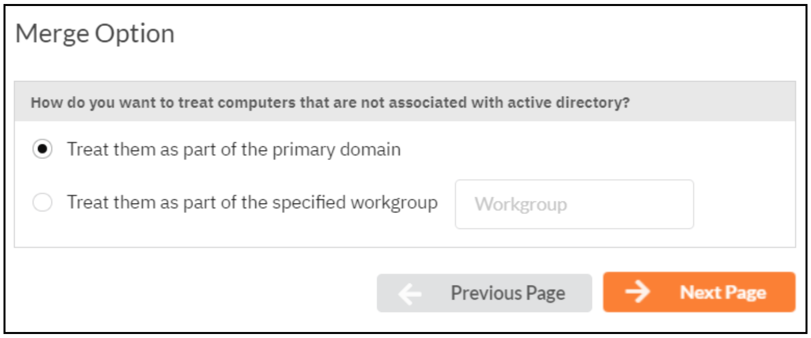
		Scan Host
	x	10.200 [redacted]
*		

- Enter one set of login credentials to access the PCs that you wish to designate as scan hosts.
- Enter the name of the domain (NOT the name of the domain controller).
- Enter the IPs or computer names of the computers that will initiate the scans.

© 2024 RapidFire Tools, Inc. All rights reserved.

> **Note:** Enter IPs for two or more scan hosts to avoid failed scans if one host becomes unavailable.

3. Once you have entered scan hosts, click **Test Scan Hosts** to be sure you can connect. If you are unable to connect, verify that the A) scan hosts meet the requirements listed here, B) that you have entered the values correctly.
4. The **Merge Options** page will appear. Configure how you wish to treat computers that are not associated with Active Directory. You can choose to:



Merge Option

How do you want to treat computers that are not associated with active directory?

● Treat them as part of the primary domain

○ Treat them as part of the specified workgroup Workgroup

   a. Treat them as part of the primary domain
   b. Treat them as part of a specific workgroup by entering a workgroup name
   c. Don't treat them as part of a domain (non-domain assets will appear separately in alerts and reports)

> **Tip:** Use this feature to tell Cyber Hawk how to handle computers that are not connected to the domain. This affects how they appear in alerts and reports.

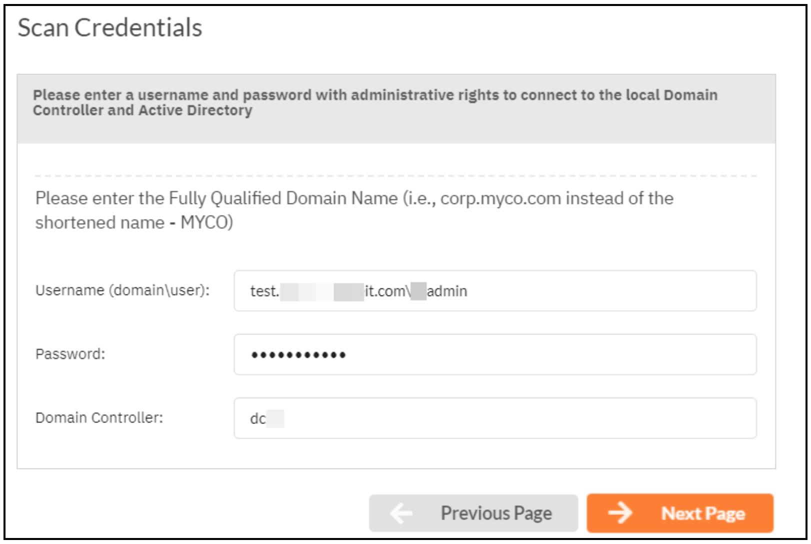
Select a merge option and click **Next Page**.

5. Enter a username and password with administrative rights to connect to the local **Domain Controller** and **Active Directory**.

> **Note:** Be sure to enter the **Fully Qualified Domain Name (FQDN)** name before the username. Example: **corp.myco.com\username**.

6. Also enter the **name or IP address of the Domain Controller**. Click **Next Page** to test a connection to the local Domain Controller and Active Directory to verify your credentials.

© 2024 RapidFire Tools, Inc. All rights reserved.



Scan Credentials

Please enter a username and password with administrative rights to connect to the local Domain Controller and Active Directory

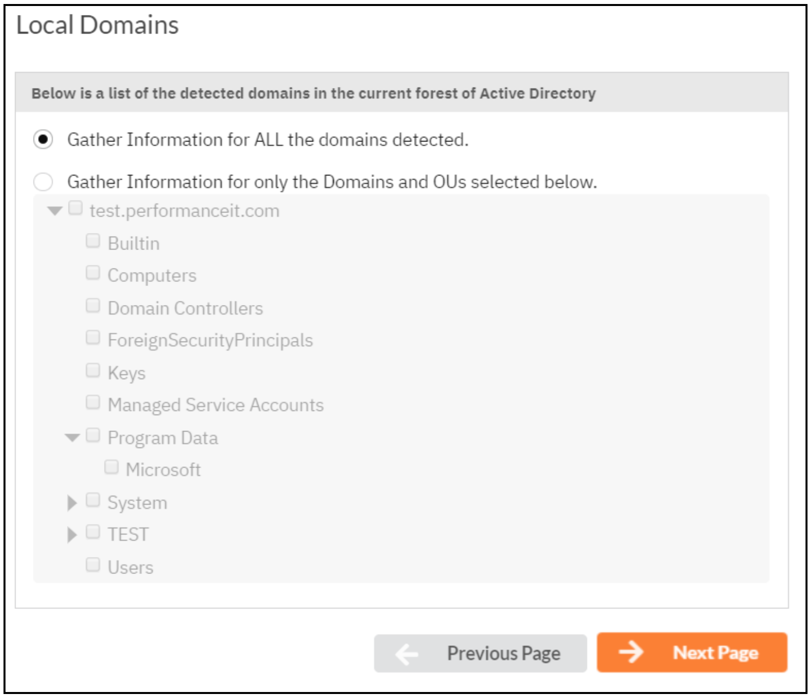
Please enter the Fully Qualified Domain Name (i.e., corp.myco.com instead of the shortened name - MYCO)

Username (domain\user): test.[redacted]it.com\[redacted]admin

Password: ••••••••••••

Domain Controller: dc[redacted]

7. The **Local Domains** window will appear. If you wish to scan only specific domains or OUs, select those here. Click **Next Page**.



Local Domains

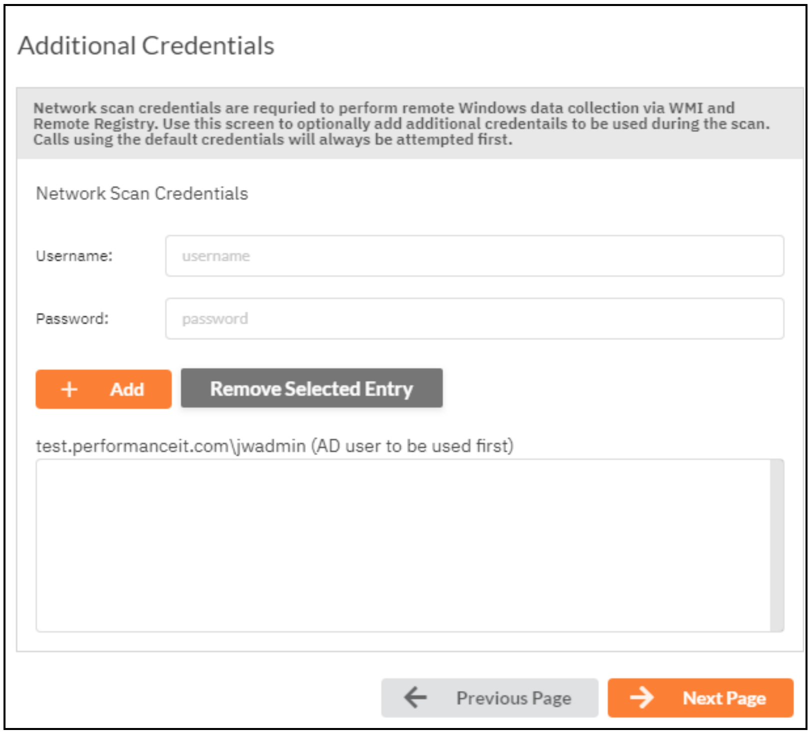
Below is a list of the detected domains in the current forest of Active Directory

● Gather Information for ALL the domains detected.

○ Gather Information for only the Domains and OUs selected below.

- □ test.performanceit.com
  - □ Builtin
  - □ Computers
  - □ Domain Controllers
  - □ ForeignSecurityPrincipals
  - □ Keys
  - □ Managed Service Accounts
  - □ Program Data
    - □ Microsoft
  - □ System
  - □ TEST
  - □ Users

8. The **Additional Credentials** screen will appear. Enter any additional credentials to be used during the scan. Click **Next**.



Additional Credentials

Network scan credentials are requried to perform remote Windows data collection via WMI and Remote Registry. Use this screen to optionally add additional credentails to be used during the scan. Calls using the default credentials will always be attempted first.

Network Scan Credentials

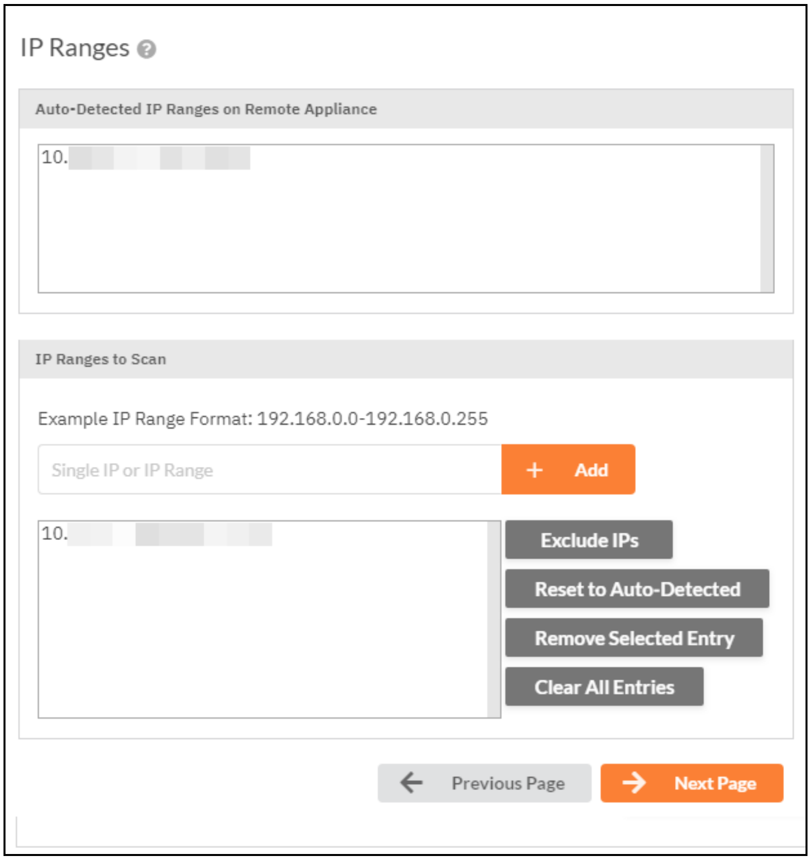
Username: username

Password: password

test.performanceit.com\jwadmin (AD user to be used first)

9. The **IP Ranges** screen will then appear. The Cyber Hawk 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**.

© 2024 RapidFire Tools, Inc. All rights reserved.



10.[redacted]

Example IP Range Format: 192.168.0.0-192.168.0.255

10.[redacted]

From this screen you can also:

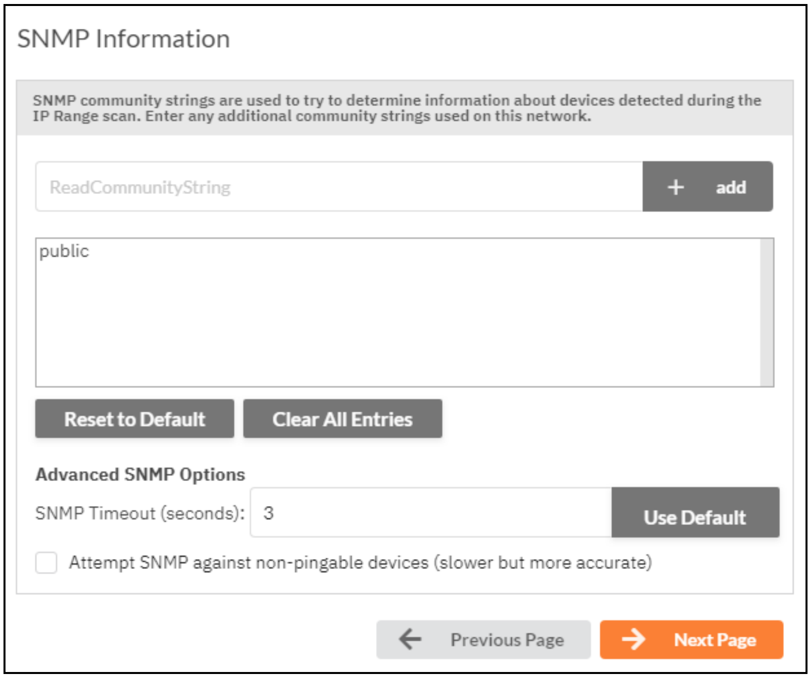
- Click **Reset to Default** to reset to the automatically suggested IP Range.
- **Exclude IPs** or IP ranges from the scan.

> **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.

Click **Next Page** once you have configured the IP ranges for the scan.

10. The **SNMP Information** window will appear. Enter any additional SNMP community strings used on the network. Click **Next Page**.

© 2024 RapidFire Tools, Inc. All rights reserved.



SNMP Information

SNMP community strings are used to try to determine information about devices detected during the IP Range scan. Enter any additional community strings used on this network.

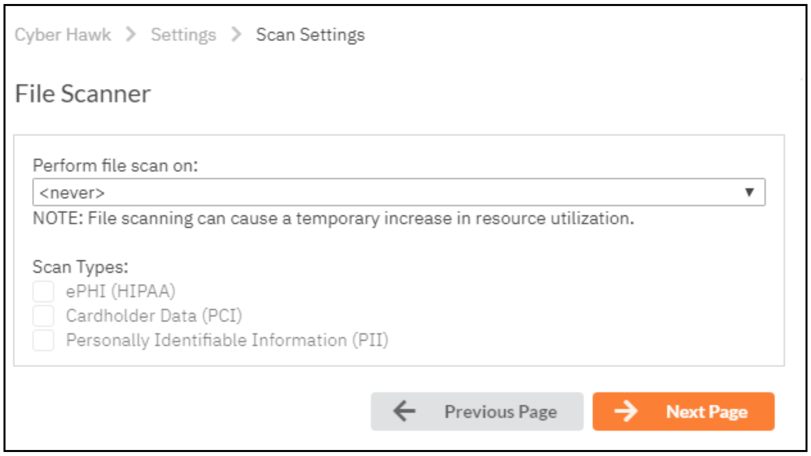
public

Advanced SNMP Options

SNMP Timeout (seconds): 3

□ Attempt SNMP against non-pingable devices (slower but more accurate)

11. The **File Scanner** window will appear. Choose what day of the week to perform the file scan. Select a day of the week from the drop-down menu. Next, select the Scan Types that will be performed:
    - **ePHI** (HIPAA) will scan for Electronic Protected Health Information
    - **Cardholder Data** (PCI) will scan for payment card numbers and other related information
    - **Personally Identifiable Information** (PII) will scan for information such as a person’s name or social security number



File Scanner

Perform file scan on: <never>

NOTE: File scanning can cause a temporary increase in resource utilization.

Scan Types:

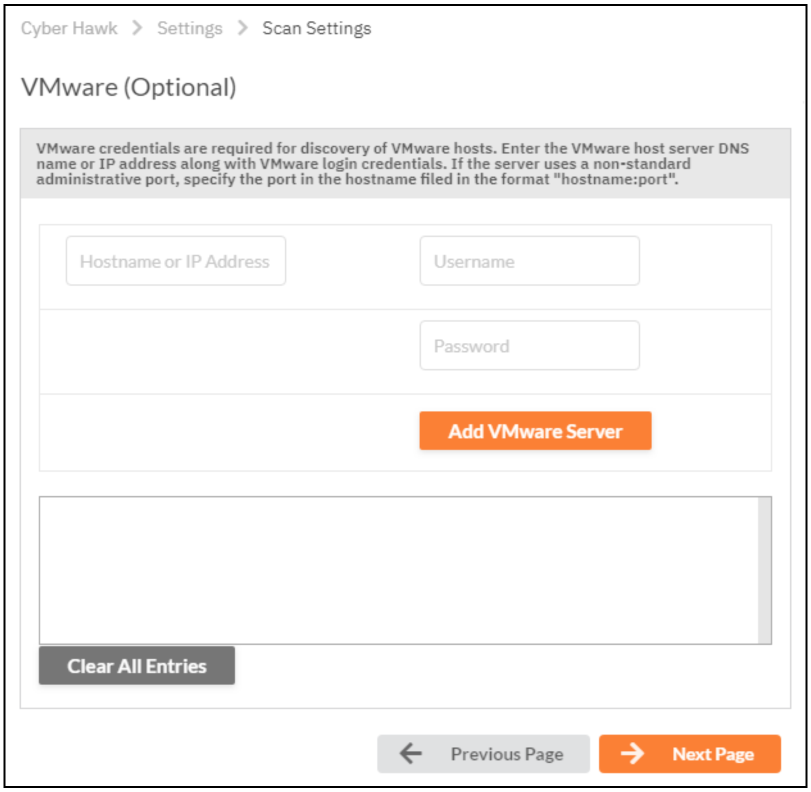
□ ePHI (HIPAA)

□ Cardholder Data (PCI)

□ Personally Identifiable Information (PII)

© 2024 RapidFire Tools, Inc. All rights reserved.

12. The optional **VMware** credentials window will appear. Enter the hostnames or IP Addresses of any VMware hosts that you wish to include in the scan. Likewise enter credentials needed to access the VMware hosts. Click **Next Page**.



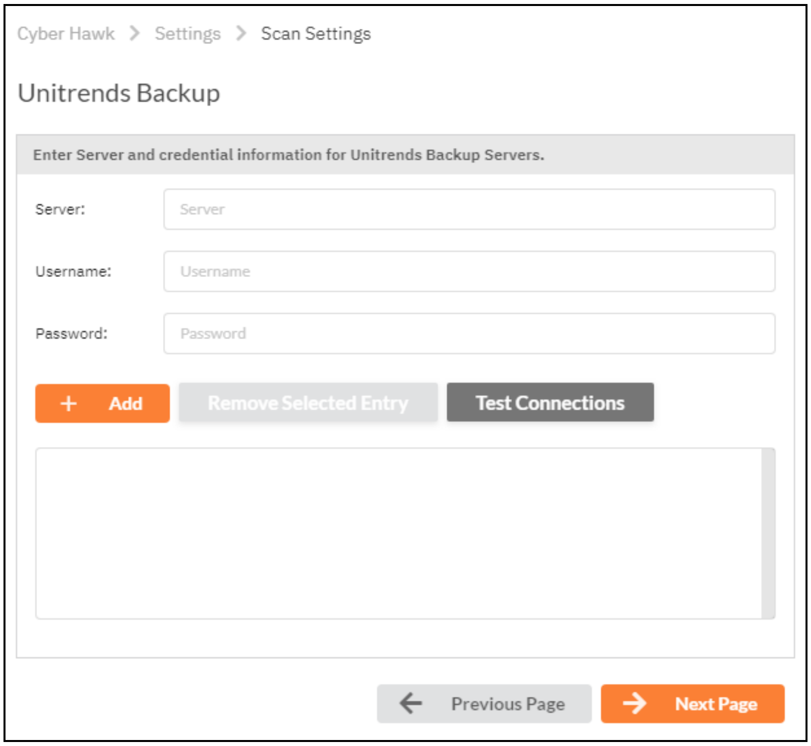
Cyber Hawk > Settings > Scan Settings

VMware (Optional)

VMware credentials are required for discovery of VMware hosts. Enter the VMware host server DNS name or IP address along with VMware login credentials. If the server uses a non-standard administrative port, specify the port in the hostname filed in the format "hostname:port".

13. The **Unitrends Backup** screen will appear. Enter the Unitrends Backup server name and login credentials.

© 2024 RapidFire Tools, Inc. All rights reserved.



Unitrends Backup

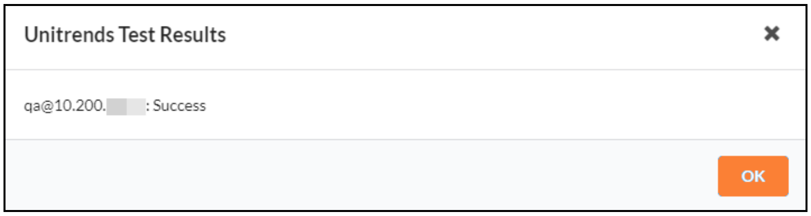
Enter Server and credential information for Unitrends Backup Servers.

Server:

Username:

Password:

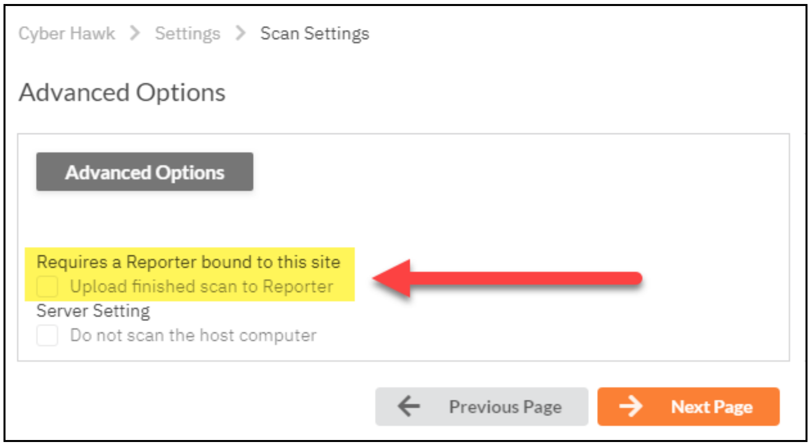
14. Click **Test Connection** to verify your Unitrends scan configuration.



Unitrends Test Results

qa@10.200.[redacted]: Success

15. If you are using a **Reporter** appliance, you can also choose whether to upload the finished scans to the Reporter. Click **Next Page**.



Advanced Options

Requires a Reporter bound to this site

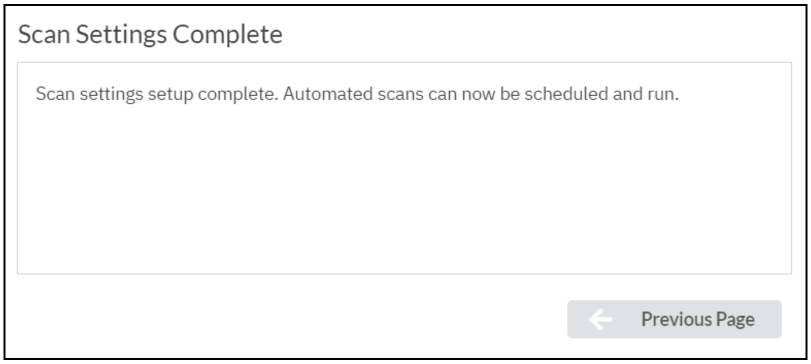
□ Upload finished scan to Reporter

Server Setting

□ Do not scan the host computer

© 2024 RapidFire Tools, Inc. All rights reserved.

16. Your scan settings will then be complete.



Scan Settings Complete

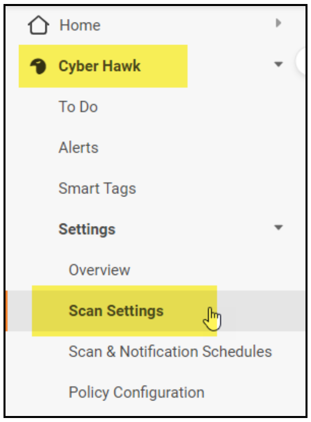
Scan settings setup complete. Automated scans can now be scheduled and run.

When you have finished entering the scan settings, return to the To Do list and click **Mark Complete** for the **Configure Scan Settings** To Do task.

© 2024 RapidFire Tools, Inc. All rights reserved.

Configure Scan Settings for Workgroups

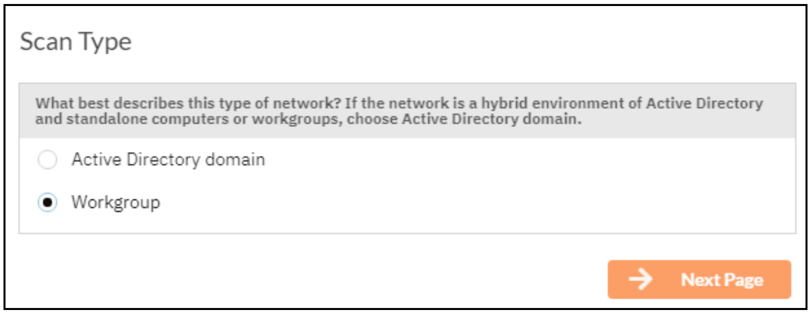
Set the **Scan Settings** from the **[Your Site]** > **Cyber Hawk** > **Settings** > **Scan Settings** page. Complete all required prompts.



Important: For best results, the target network must be configured to allow for successful scans on all network endpoints. See "Pre-Scan Network Configuration Checklist" on page 219 for configuration guidance for both Windows Active Directory and Workgroup environments.

Follow the steps below to configure the Scan Settings for the Cyber Hawk Appliance:

1. From the Scan Settings screen, select the Scan Type: **Workgroup**. Click **Next Page**.



Scan Type

What best describes this type of network? If the network is a hybrid environment of Active Directory and standalone computers or workgroups, choose Active Directory domain.

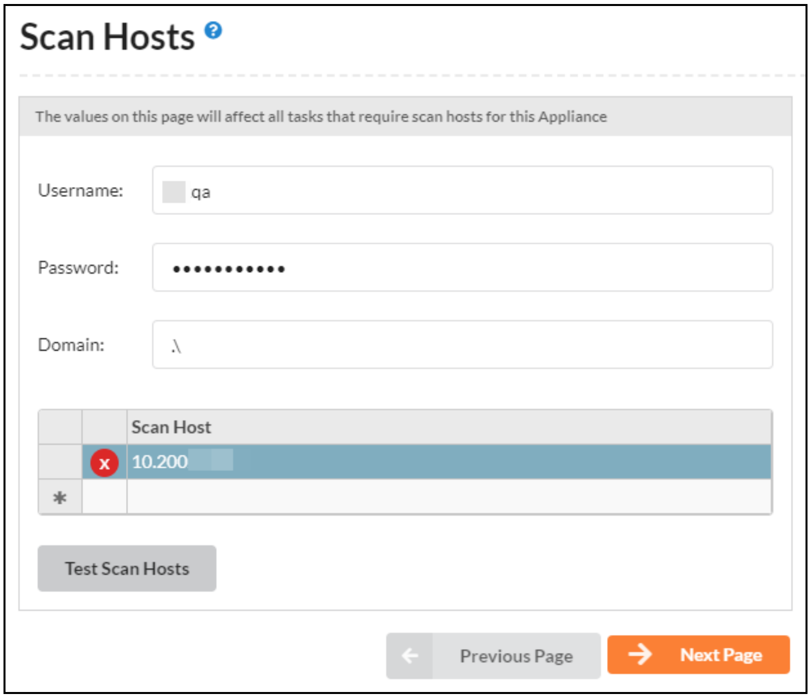
○ Active Directory domain

● Workgroup

Select a merge option and click **Next Page**.

2. The **Scan Hosts** window will appear. Next assign scan hosts:

> **Note:** The Cyber Hawk Appliance requires access to at least one separate, additional PC on the client's network. This computer is called the "Scan Host." The **Scan Host** is used to initiate scans. For more information on Scan Host requirements, see "Additional Scan Host Details" on page 266.



Scan Hosts

The values on this page will affect all tasks that require scan hosts for this Appliance

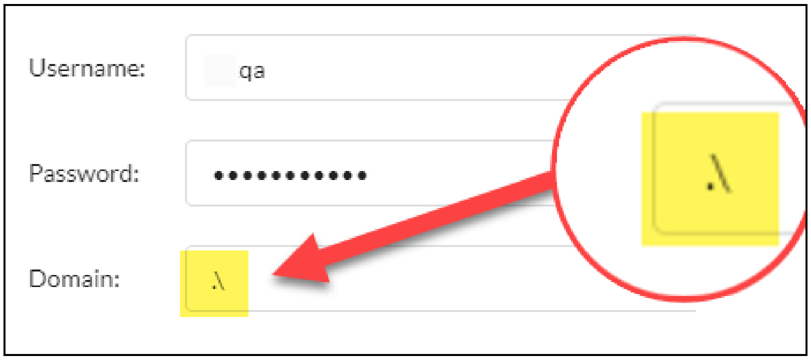
Username: qa

Password: •••••••••••

Domain: .\

		Scan Host
	☒	10.200
*		

- Enter one set of login credentials to access the PCs that you wish to designate as scan hosts.
- For Workgroups, enter the characters ".\" (without quotation marks) in the Domain field, as in the image below.



Username: qa

Password: •••••••••••

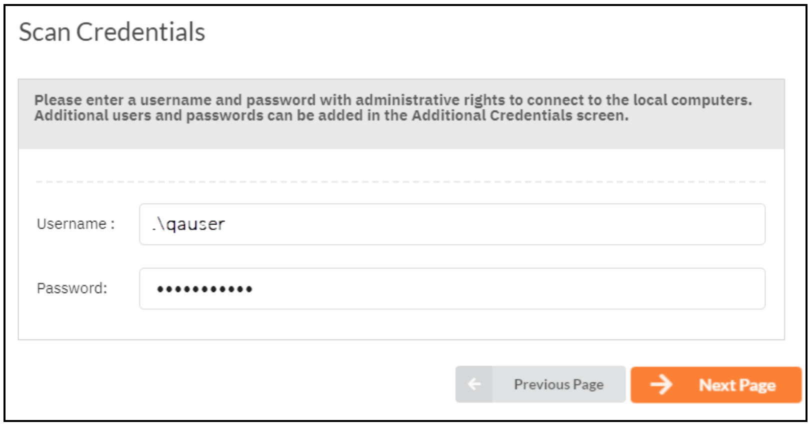
Domain: .\

- Enter the IPs or computer names of the computers that will initiate the scans.

© 2024 RapidFire Tools, Inc. All rights reserved.

> **Note:** Enter IPs for two or more scan hosts to avoid failed scans if one host becomes unavailable.

3. Once you have entered scan hosts, click **Test Scan Hosts** to be sure you can connect. If you are unable to connect, verify that the A) scan hosts meet the requirements listed here, B) that you have entered the values correctly.
4. Next enter **Scan Credentials** with administrative rights to connect to the local computers in the workgroup.

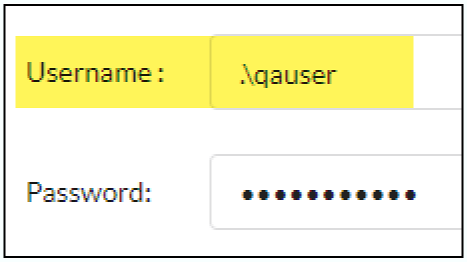


Scan Credentials

Please enter a username and password with administrative rights to connect to the local computers. Additional users and passwords can be added in the Additional Credentials screen.

Username : .\qauser

Password: •••••••••••

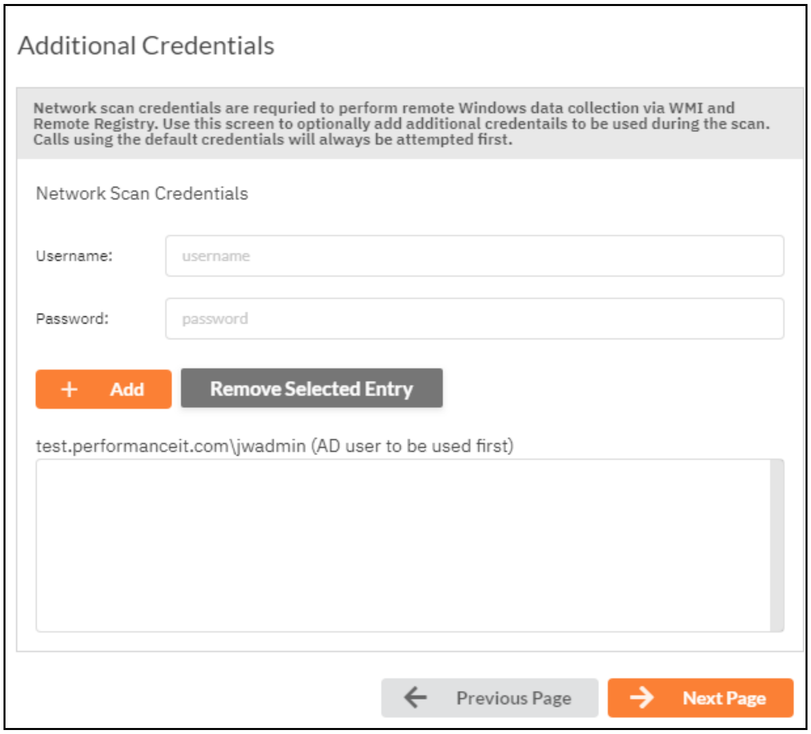
> **Note:** For Workgroups, enter the characters ".\" (without quotation marks) immediately before the username, as in the image below.
>
> 
>
> Username : .\qauser
>
> Password: •••••••••••

Click **Next Page** to test the connection and verify your credentials.

5. The **Additional Credentials** screen will appear. Enter any additional credentials to be used during the scan. Click **Next**.

> **Important:** If each workgroup PC has its own unique Admin username and password credentials, you will need to enter each set of credentials here in order to scan these PCs.

© 2024 RapidFire Tools, Inc. All rights reserved.



Additional Credentials

Network scan credentials are requried to perform remote Windows data collection via WMI and Remote Registry. Use this screen to optionally add additional credentails to be used during the scan. Calls using the default credentials will always be attempted first.

Network Scan Credentials

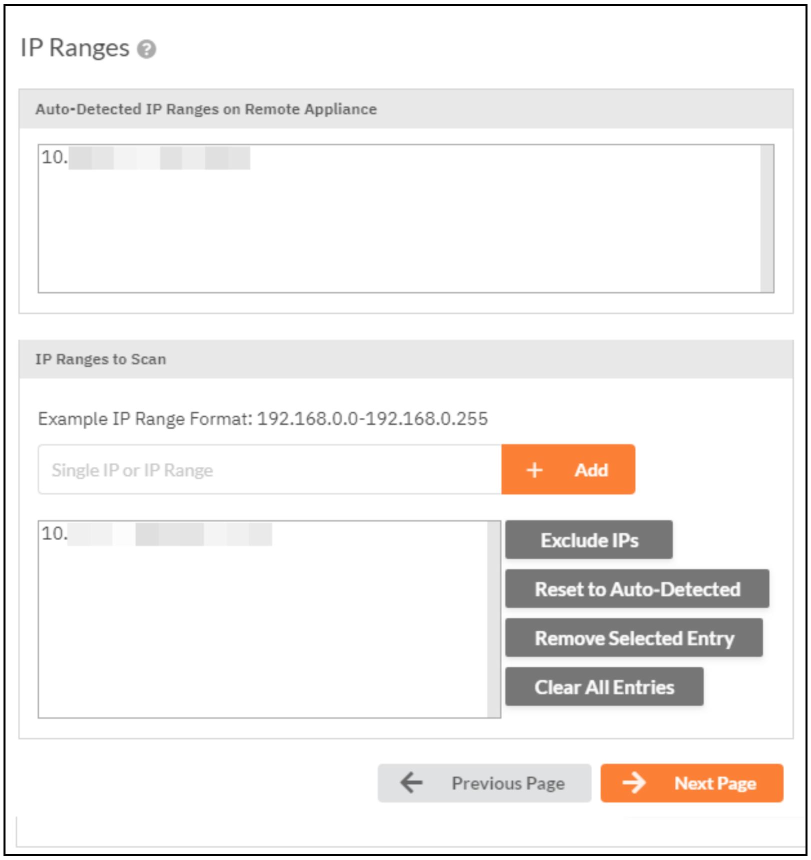
Username: username

Password: password

test.performanceit.com\jwadmin (AD user to be used first)

6. The **IP Ranges** screen will then appear. The **Cyber Hawk** 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**.

© 2024 RapidFire Tools, Inc. All rights reserved.



IP Ranges

Auto-Detected IP Ranges on Remote Appliance

10.[redacted]

IP Ranges to Scan

Example IP Range Format: 192.168.0.0-192.168.0.255

Single IP or IP Range

10.[redacted]

From this screen you can also:

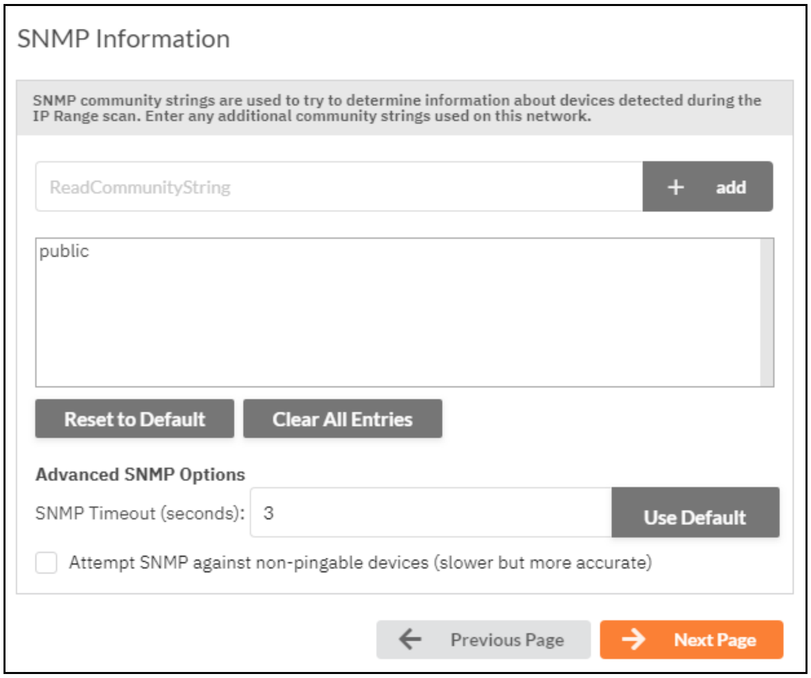
- Click **Reset to Default** to reset to the automatically suggested IP Range.
- **Exclude IPs** or IP ranges from the scan.

> **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.

Click **Next Page** once you have configured the IP ranges for the scan.

7. The **SNMP Information** window will appear. Enter any additional SNMP community strings used on the network. Click **Next Page**.

© 2024 RapidFire Tools, Inc. All rights reserved.



SNMP Information

SNMP community strings are used to try to determine information about devices detected during the IP Range scan. Enter any additional community strings used on this network.

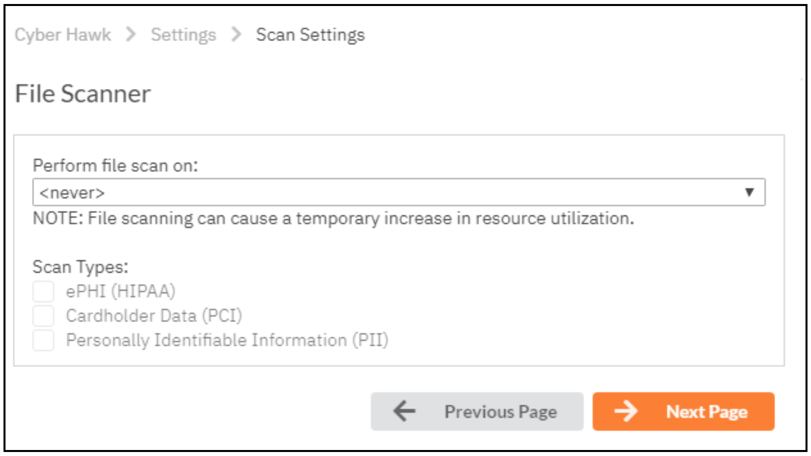
public

Advanced SNMP Options

SNMP Timeout (seconds): 3

□ Attempt SNMP against non-pingable devices (slower but more accurate)

8. The **File Scanner** window will appear. Choose what day of the week to perform the file scan. Select a day of the week from the drop-down menu. Next, select the Scan Types that will be performed:
    - **ePHI** (HIPAA) will scan for Electronic Protected Health Information
    - **Cardholder Data** (PCI) will scan for payment card numbers and other related information
    - **Personally Identifiable Information** (PII) will scan for information such as a person's name or social security number



Cyber Hawk > Settings > Scan Settings

File Scanner

Perform file scan on:

<never> ▾

NOTE: File scanning can cause a temporary increase in resource utilization.

Scan Types:

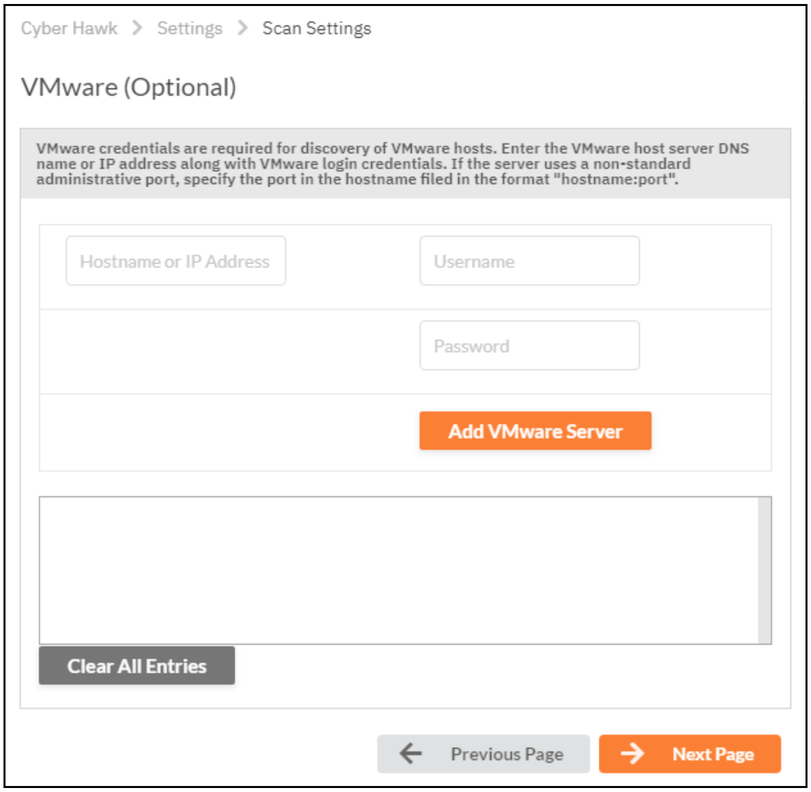
□ ePHI (HIPAA)

□ Cardholder Data (PCI)

□ Personally Identifiable Information (PII)

© 2024 RapidFire Tools, Inc. All rights reserved.

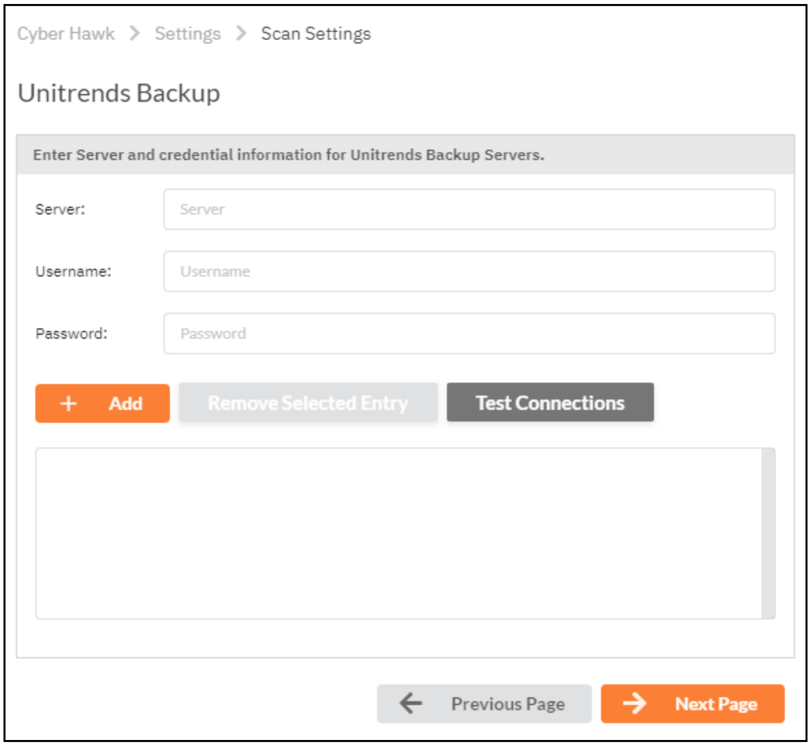
9. The optional **VMware** credentials window will appear. Enter the hostnames or IP Addresses of any VMware hosts that you wish to include in the scan. Likewise enter credentials needed to access the VMware hosts. Click **Next Page**.



VMware credentials are required for discovery of VMware hosts. Enter the VMware host server DNS name or IP address along with VMware login credentials. If the server uses a non-standard administrative port, specify the port in the hostname filed in the format "hostname:port".

10. The **Unitrends Backup** screen will appear. Enter the Unitrends Backup server name and login credentials.

© 2024 RapidFire Tools, Inc. All rights reserved.



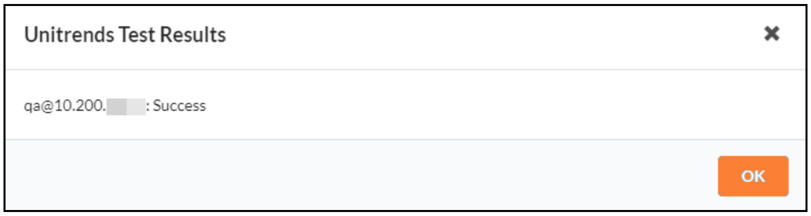
Enter Server and credential information for Unitrends Backup Servers.

Server: Server

Username: Username

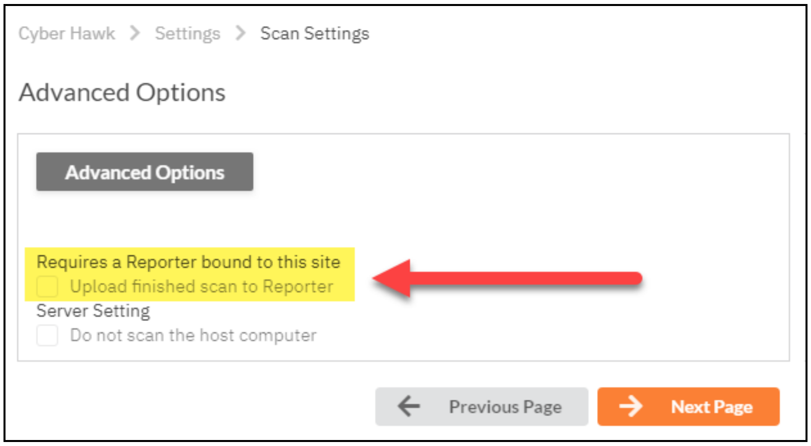
Password: Password

11. Click **Test Connection** to verify your Unitrends scan configuration.



qa@10.200.[redacted]: Success

12. If you are using a **Reporter** appliance, you can also choose whether to upload the finished scans to the Reporter. Click **Next Page**.



Requires a Reporter bound to this site

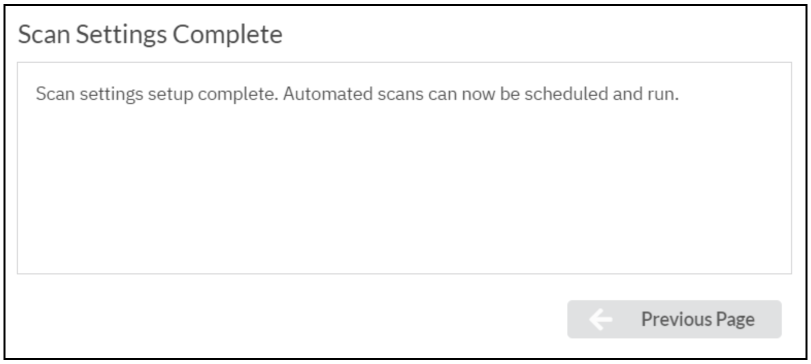
□ Upload finished scan to Reporter

Server Setting

□ Do not scan the host computer

© 2024 RapidFire Tools, Inc. All rights reserved.

13. Your scan settings will then be complete.



Scan Settings Complete

Scan settings setup complete. Automated scans can now be scheduled and run.

When you have finished entering the scan settings, return to the To Do list and click **Mark Complete** for the **Configure Scan Settings** To Do task.

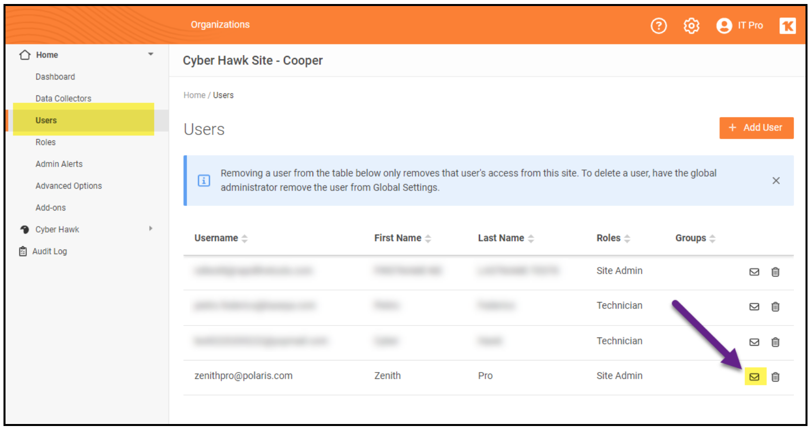
© 2024 RapidFire Tools, Inc. All rights reserved.

Invite Users to Cyber Hawk Site

You can send an email to invite site users to join your Cyber Hawk 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 Cyber Hawk 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.



Cyber Hawk Site - Cooper

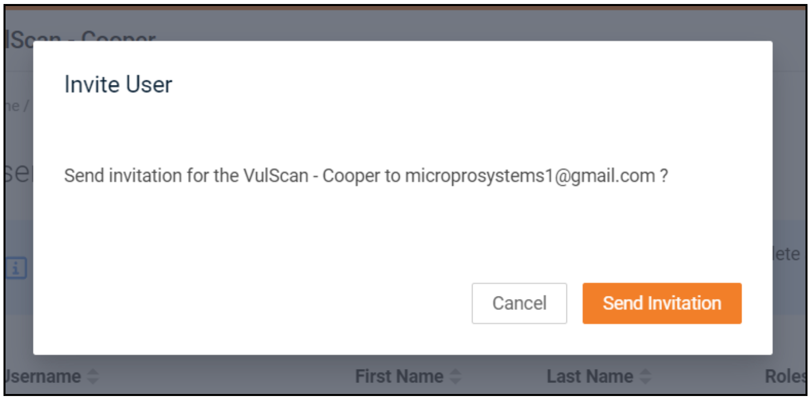
Home / Users

Users

Removing a user from the table below only removes that user's access from this site. To delete a user, have the global administrator remove the user from Global Settings.

Username	First Name	Last Name	Roles	Groups
[redacted]	[redacted]	[redacted]	Site Admin	
[redacted]	[redacted]	[redacted]	Technician	
[redacted]	[redacted]	[redacted]	Technician	
zenithpro@polaris.com	Zenith	Pro	Site Admin	

3. Click **Send Invitation**.

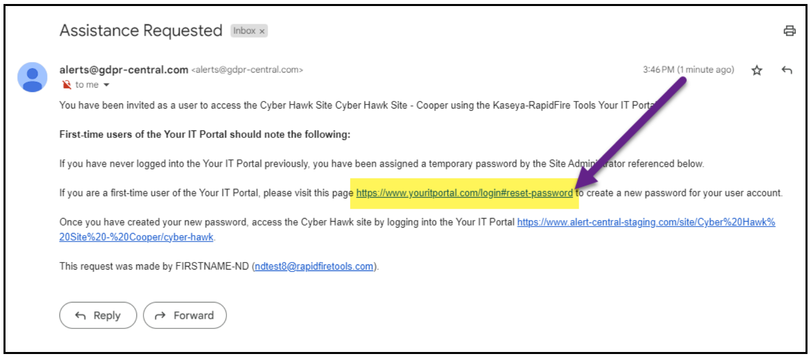


Invite User

Send invitation for the VulScan - Cooper to microprosystems1@gmail.com ?

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

© 2024 RapidFire Tools, Inc. All rights reserved.



Assistance Requested

alerts@gdpr-central.com <alerts@gdpr-central.com>
to me

3:46 PM (1 minute ago)

You have been invited as a user to access the Cyber Hawk Site Cyber Hawk Site - Cooper using the Kaseya-RapidFire Tools Your IT Portal

First-time users of the Your IT Portal should note the following:

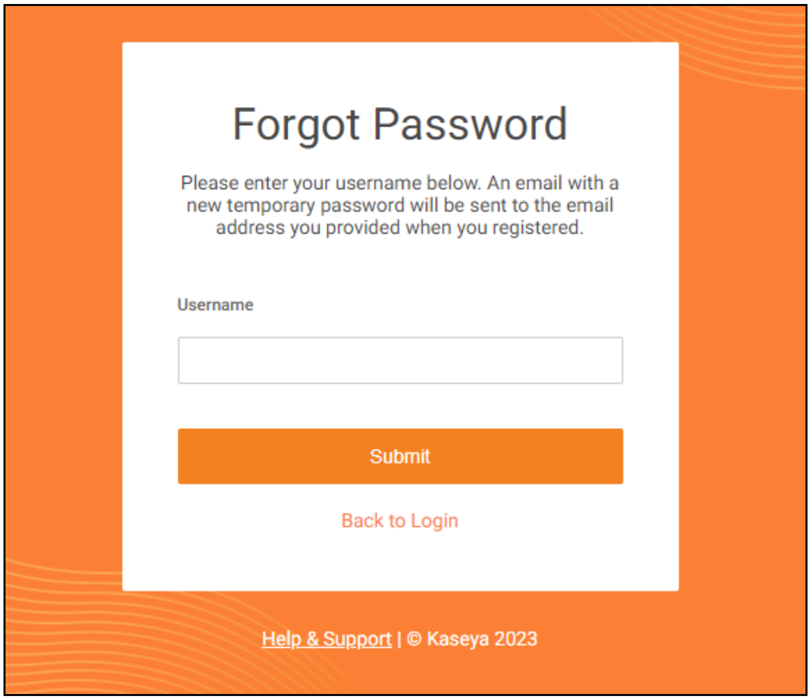
If you have never logged into the Your IT Portal previously, you have been assigned a temporary password by the Site Administrator referenced below.

If you are a first-time user of the Your IT Portal, please visit this page https://www.youritportal.com/login#reset-password to create a new password for your user account.

Once you have created your new password, access the Cyber Hawk site by logging into the Your IT Portal https://www.alert-central-staging.com/site/Cyber%20Hawk%20Site%20-%20Cooper/cyber-hawk.

This request was made by FIRSTNAME-ND (ndtest8@rapidfiretools.com).

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

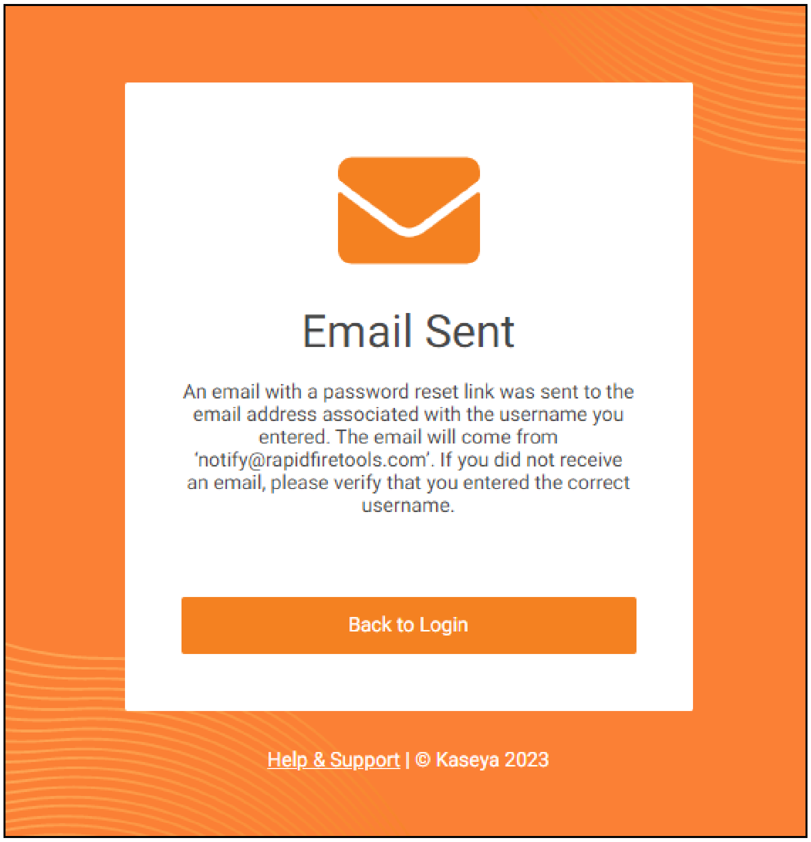


Forgot Password

Please enter your username below. An email with a new temporary password will be sent to the email address you provided when you registered.

Username

Help & Support | © Kaseya 2023

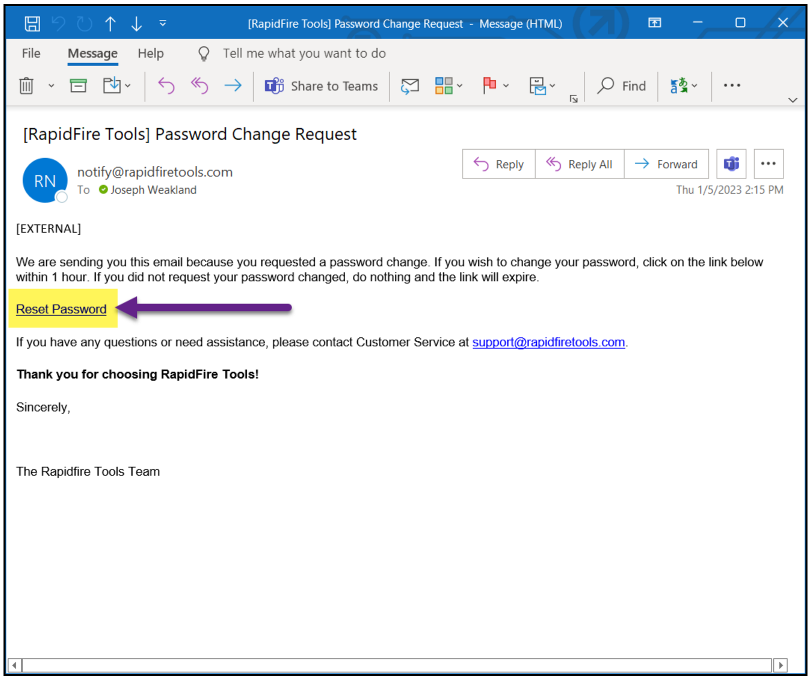


Email Sent

An email with a password reset link was sent to the email address associated with the username you entered. The email will come from ‘notify@rapidfiretools.com’. If you did not receive an email, please verify that you entered the correct username.

Help & Support | © Kaseya 2023

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



[RapidFire Tools] Password Change Request - Message (HTML)
File
Message
Help
Tell me what you want to do
Share to Teams
Find
Reply
Reply All
Forward

[RapidFire Tools] Password Change Request

RN notify@rapidfiretools.com

To Joseph Weakland

Thu 1/5/2023 2:15 PM

[EXTERNAL]

We are sending you this email because you requested a password change. If you wish to change your password, click on the link below within 1 hour. If you did not request your password changed, do nothing and the link will expire.

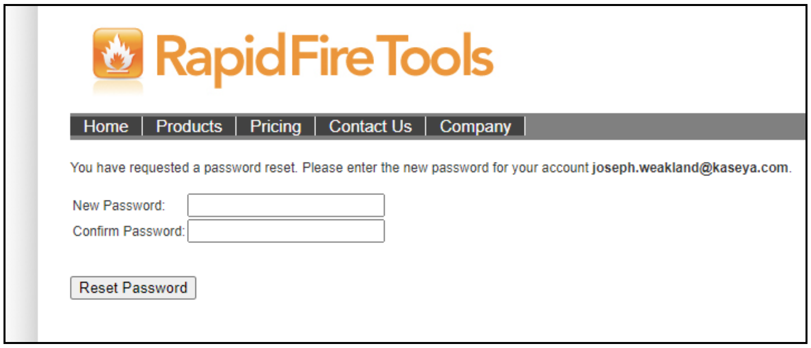
Reset Password

If you have any questions or need assistance, please contact Customer Service at support@rapidfiretools.com.

Thank you for choosing RapidFire Tools!

Sincerely,

The Rapidfire Tools Team



You have requested a password reset. Please enter the new password for your account **joseph.weakland@kaseya.com**.

New Password:

Confirm Password:

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

© 2024 RapidFire Tools, Inc. All rights reserved.

Enable VulScan Integration with Cyber Hawk for Internal Vulnerability Scanning

If you use VulScan to perform internal vulnerability scans, you can import these scans into your Cyber Hawk site. Simply set up internal scans in VulScan, and enable the integration in Cyber Hawk. You can then generate Cyber Hawk security alerts for detected internal vulnerabilities.

The integration requires that you have a VulScan site with an internal appliance that is performing scheduled internal scan tasks.

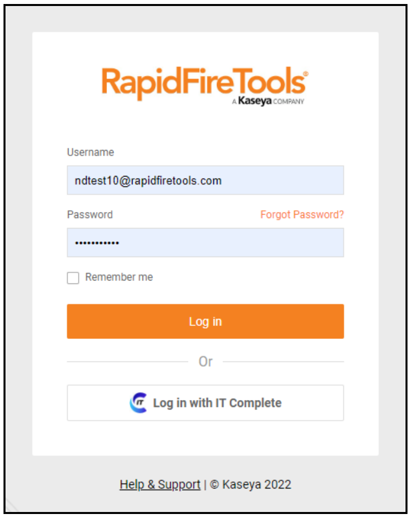
Follow these steps to enable the integration of VulScan with Cyber Hawk:

Step 1 – Set Up VulScan Site

This step covers how to set up a VulScan site. if you already have a VulScan site set up to perform internal scans in the same organization as your Cyber Hawk site, you can skip to "Step 4 – Configure Cyber Hawk Internal Vulnerability Scan using VulScan" on page 260.

To create a VulScan site:

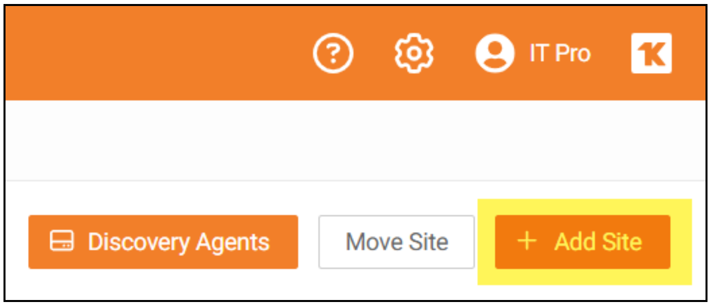
1. Access the RapidFire Tools Portal at https://www.youritportal.com and log in with your credentials.



Username: ndtest10@rapidfiretools.com

Password: ···········

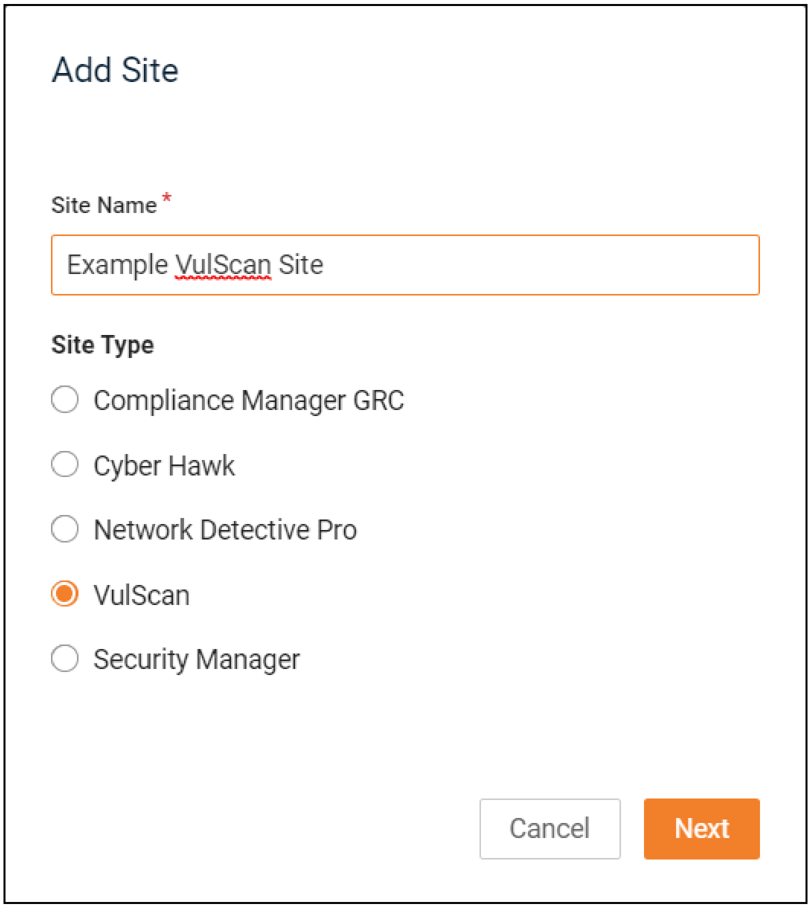
2. From the Sites page, click **Add Site**.



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**.


Add Site

Site Name *

Example VulScan Site

Site Type

○ Compliance Manager GRC

○ Cyber Hawk

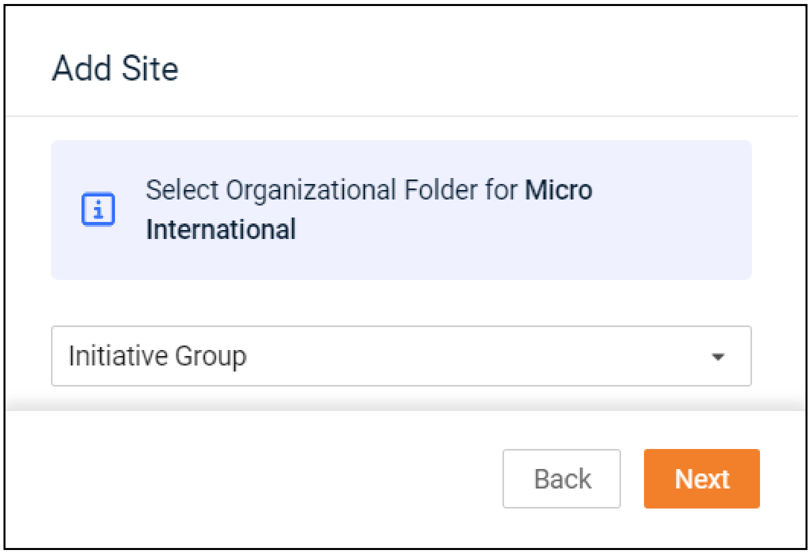
○ Network Detective Pro

● VulScan

○ Security Manager

5. Click **Next**. Choose an Org Folder for the site and click **Next**. Be sure to place your VulScan site in the **same organization** as your Cyber Hawk site.

© 2024 RapidFire Tools, Inc. All rights reserved.

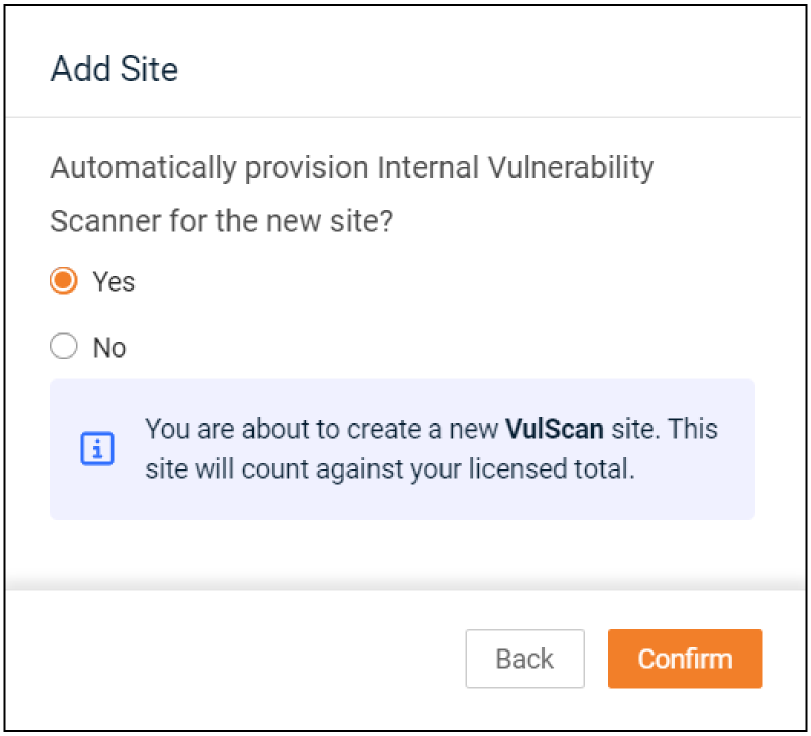


Add Site

Select Organizational Folder for **Micro International**

Initiative Group

6. Select **Yes** to provision an Internal Vulnerability Scanner appliance for the new site. Then click **Confirm**.



Add Site

Automatically provision Internal Vulnerability Scanner for the new site?

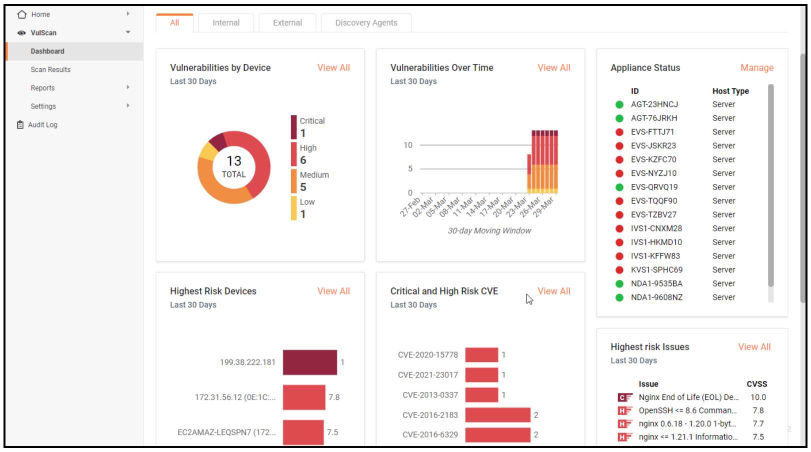
● Yes

○ No

You are about to create a new **VulScan** site. This site will count against your licensed total.

The VulScan site dashboard will appear. This dashboard will populate with data once you begin performing scans.

© 2024 RapidFire Tools, Inc. All rights reserved.



	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

	Issue	CVSS
C	Nginx End of Life (EOL) De...	10.0
H	OpenSSH <= 8.6 Comman...	7.8
H	nginx 0.6.18 - 1.20.0 1-byt...	7.7
H	nginx <= 1.21.1 Informatio...	7.5

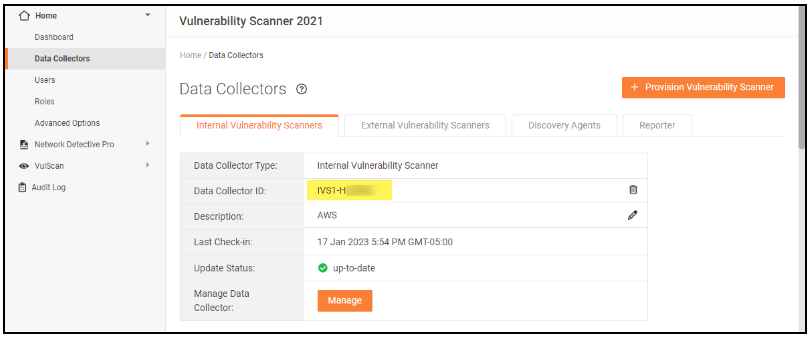
Step 2 – Install VulScan Appliance

Next, install the VulScan virtual appliance that you provisioned in Step 1 onto the target network to be scanned. This should be the same network where you have deployed Cyber Hawk.

Download the **VulScan Virtual Appliance Installer** at https://www.rapidfiretools.com/vs-downloads.

For detailed instructions, see Virtual Appliance Installation Guide for VulScan.

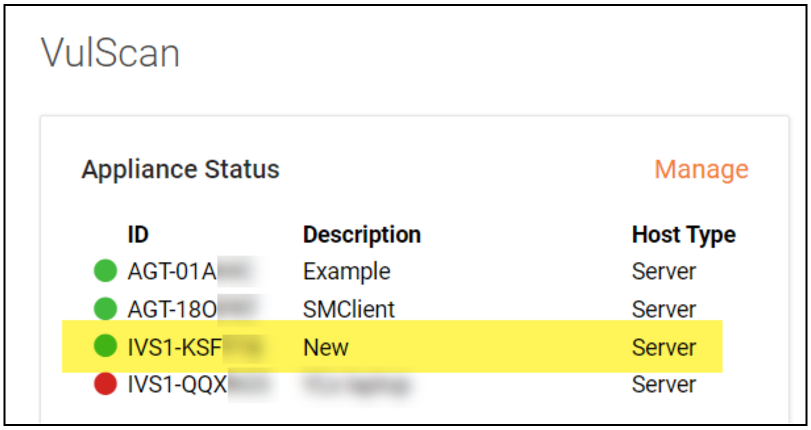
During the install, be sure to associate the appliance with the correct site. During the install process, you will need to choose the correct **Data Collector ID** for the site. You can find ID for the "IVS" (Internal Vulnerability Scanner) for the site either from the site dashboard or from **[Your Site]** > **Home** > **Data Collectors**, as in the image below.



Data Collector Type:	Internal Vulnerability Scanner
Data Collector ID:	IVS1-H[redacted]
Description:	AWS
Last Check-in:	17 Jan 2023 5:54 PM GMT-05:00
Update Status:	✓ up-to-date
Manage Data Collector:	Manage

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**.

© 2024 RapidFire Tools, Inc. All rights reserved.



VulScan

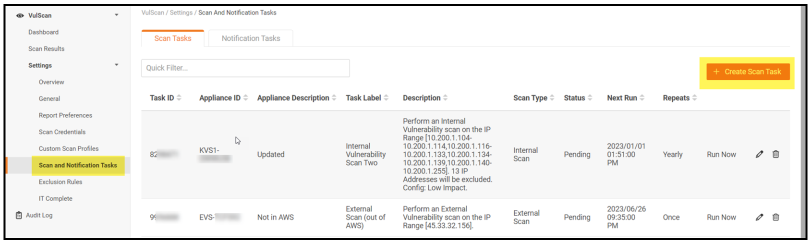
Appliance Status

	ID	Description	Host Type
●	AGT-01A[redacted]	Example	Server
●	AGT-18O[redacted]	SMClient	Server
●	IVS1-KSF[redacted]	New	Server
●	IVS1-QQX[redacted]	[redacted]	Server

Step 3 – Create and Schedule VulScan Scan Task

In order for VulScan 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:

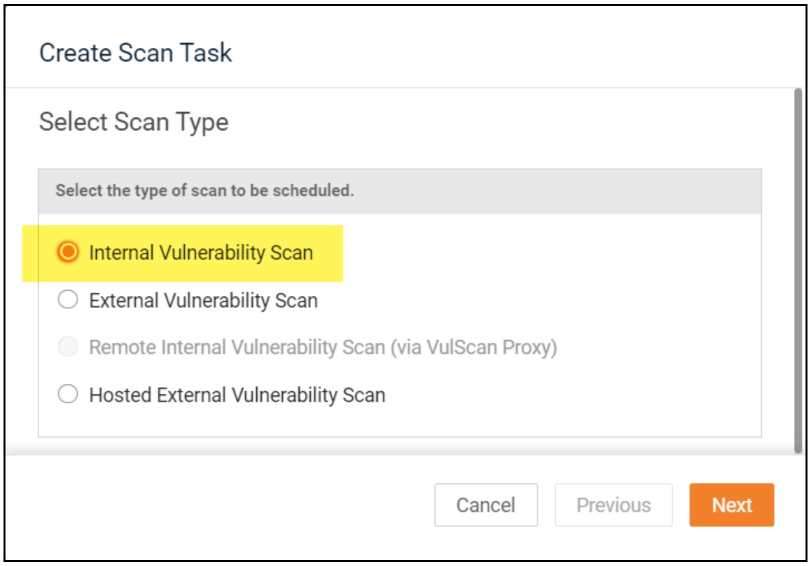
1. From your site, go to **VulScan** > **Settings** > **Scan and Notification Tasks**.
2. From the **Scan Tasks** tab, click **Create Scan Task**.



Task ID	Appliance ID	Appliance Description	Task Label	Description	Scan Type	Status	Next Run	Repeats		
82[redacted]	KVS1-[redacted]	Updated	Internal Vulnerability Scan Two	Perform an Internal Vulnerability scan on the IP Range [10.200.1.104-10.200.1.114,10.200.1.116-10.200.1.133,10.200.1.134-10.200.1.139,10.200.1.140-10.200.1.255]. 13 IP Addresses will be excluded. Config: Low Impact.	Internal Scan	Pending	2023/01/01 01:51:00 PM	Yearly	Run Now	✎ 🗑
9[redacted]	EVS-[redacted]	Not in AWS	External Scan (out of AWS)	Perform an External Vulnerability scan on the IP Range [45.33.32.156].	External Scan	Pending	2023/06/26 09:35:00 PM	Once	Run Now	✎ 🗑

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

© 2024 RapidFire Tools, Inc. All rights reserved.



Create Scan Task

Select Scan Type

Select the type of scan to be scheduled.

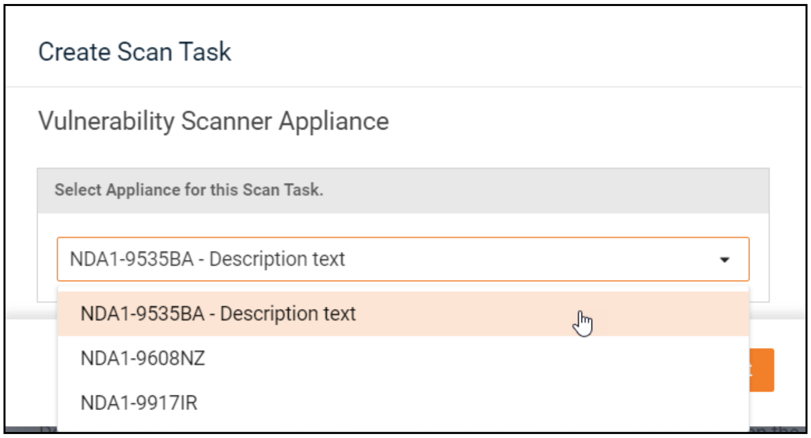
● Internal Vulnerability Scan

○ External Vulnerability Scan

○ Remote Internal Vulnerability Scan (via VulScan Proxy)

○ Hosted External Vulnerability Scan

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



Create Scan Task

Vulnerability Scanner Appliance

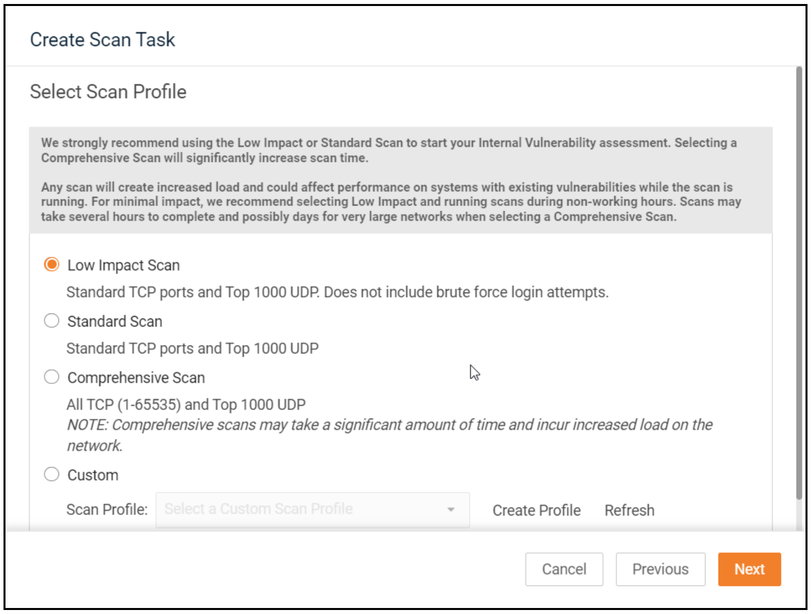
Select Appliance for this Scan Task.

NDA1-9535BA - Description text

- NDA1-9535BA - Description text
- NDA1-9608NZ
- NDA1-9917IR

5. Select the **Scan Profile**. You can select from the available profiles, or you can use your own Custom Scan Profile. See the VulScan User Guide for complete details.

© 2024 RapidFire Tools, Inc. All rights reserved.



Create Scan Task

Select Scan Profile

We strongly recommend using the Low Impact or Standard Scan to start your Internal Vulnerability assessment. Selecting a Comprehensive Scan will significantly increase scan time.

Any scan will create increased load and could affect performance on systems with existing vulnerabilities while the scan is running. For minimal impact, we recommend selecting Low Impact and running scans during non-working hours. Scans may take several hours to complete and possibly days for very large networks when selecting a Comprehensive Scan.

● Low Impact Scan

Standard TCP ports and Top 1000 UDP. Does not include brute force login attempts.

○ Standard Scan

Standard TCP ports and Top 1000 UDP

○ Comprehensive Scan

All TCP (1-65535) and Top 1000 UDP
NOTE: Comprehensive scans may take a significant amount of time and incur increased load on the network.

○ Custom

Scan Profile: Select a Custom Scan Profile

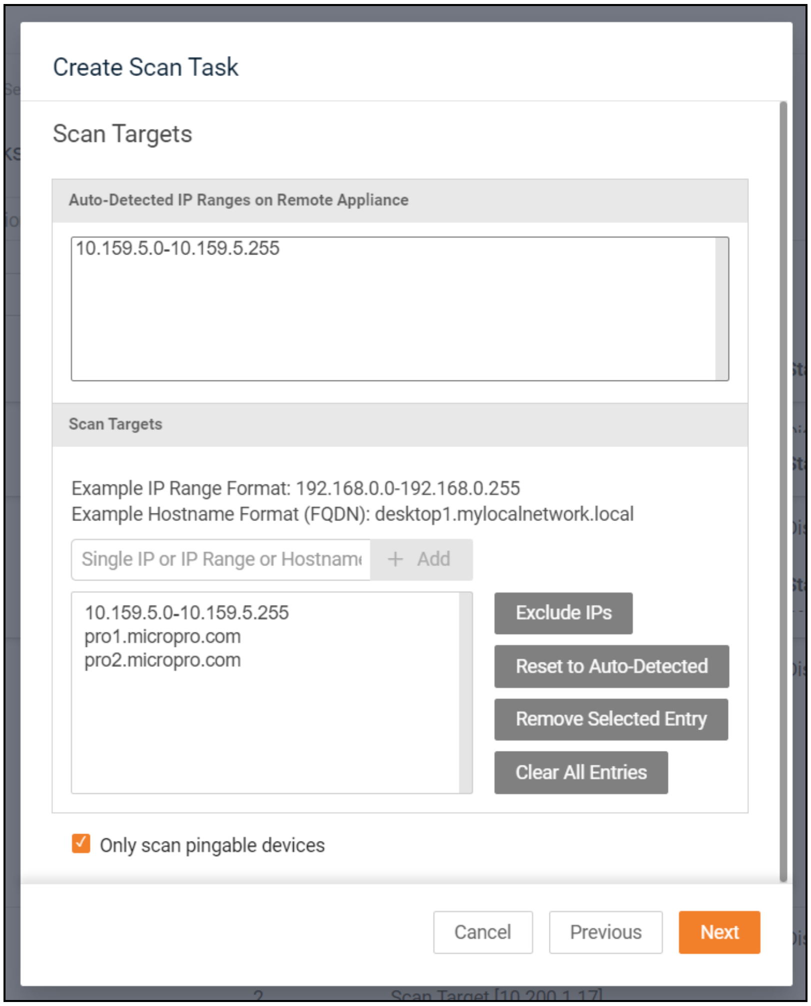
The available options are in the table below. Click **Next**.

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 select **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**.

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

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.


Create Scan Task

Scan Targets

Auto-Detected IP Ranges on Remote Appliance

10.159.5.0-10.159.5.255

Scan Targets

Example IP Range Format: 192.168.0.0-192.168.0.255
Example Hostname Format (FQDN): desktop1.mylocalnetwork.local

10.159.5.0-10.159.5.255
pro1.micropro.com
pro2.micropro.com

☑ Only scan pingable devices

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.

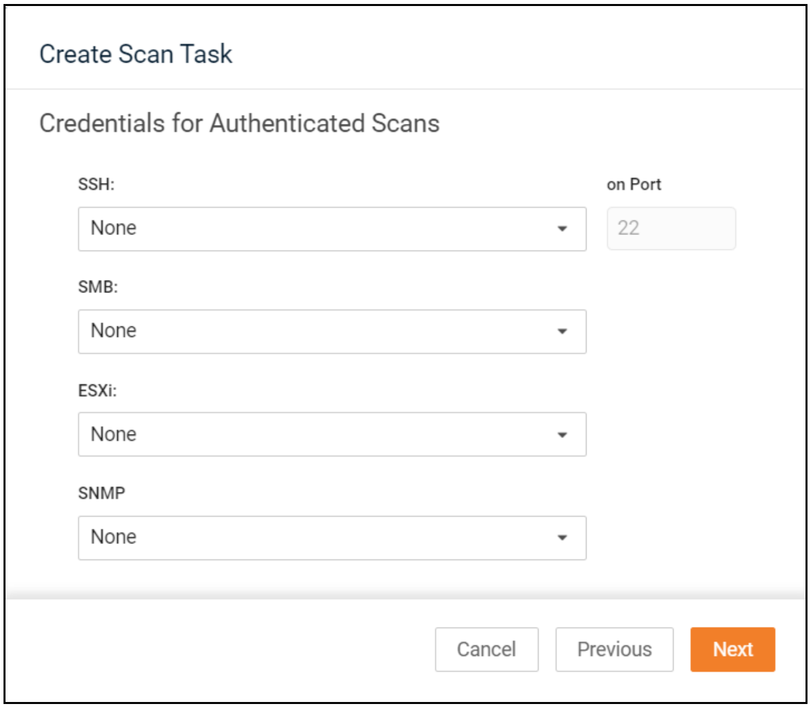
> **Note:** Key network component IP addresses should be excluded in order to prevent scans being performed from impacting the performance of a device when it is being scanned. For example, a company might want to

© 2024 RapidFire Tools, Inc. All rights reserved.

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. See the VulScan User Guide for more detail on credentialed scans.



Create Scan Task

Credentials for Authenticated Scans

SSH: None on Port 22

SMB: None

ESXi: None

SNMP None

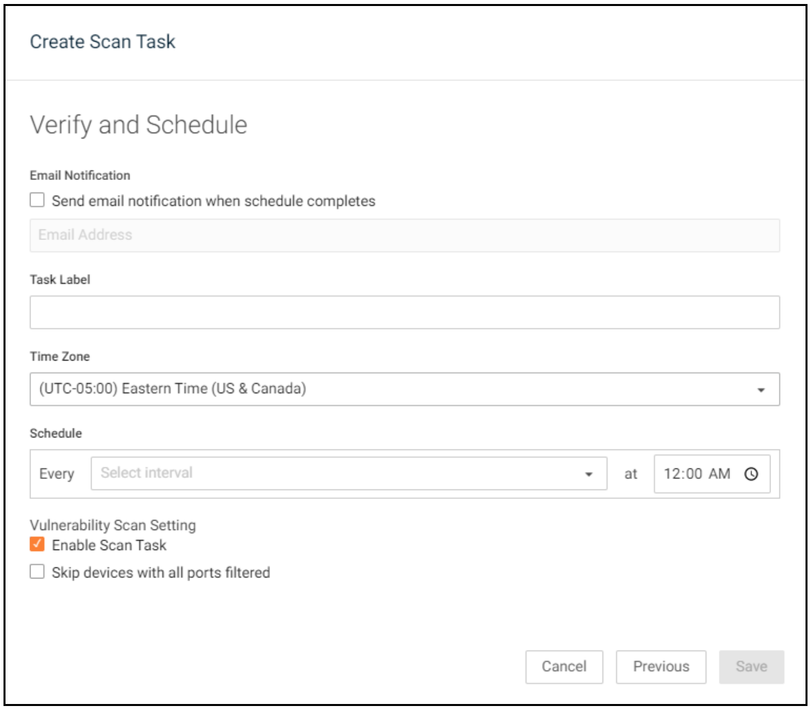
For each protocol, select the credentials you wish to use from the drop-down menu. When you're finished, click **Next**.

- **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.

© 2024 RapidFire Tools, Inc. All rights reserved.

- **SNMP**: Use this protocol to scan for devices such as switches, bridges, routers, access servers, computer hosts, hubs, and printers.

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



Create Scan Task

Verify and Schedule

Email Notification

□ Send email notification when schedule completes

Email Address

Task Label

Time Zone

(UTC-05:00) Eastern Time (US & Canada)

Schedule

Every Select interval at 12:00 AM

Vulnerability Scan Setting

☑ Enable Scan Task

□ Skip devices with all ports filtered

   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.

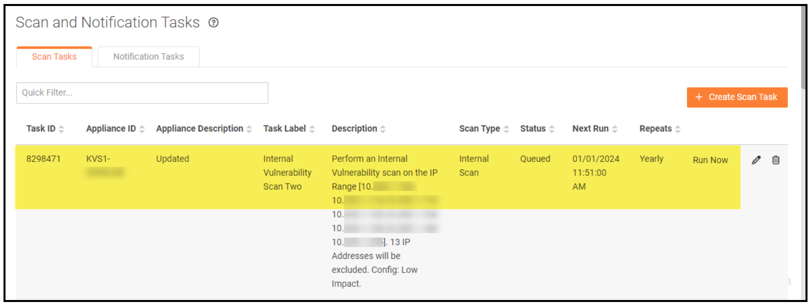
   e. **Enable** or **disable** scan task; you can then later edit the scan task to enable/disable at any time.

   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.

© 2024 RapidFire Tools, Inc. All rights reserved.

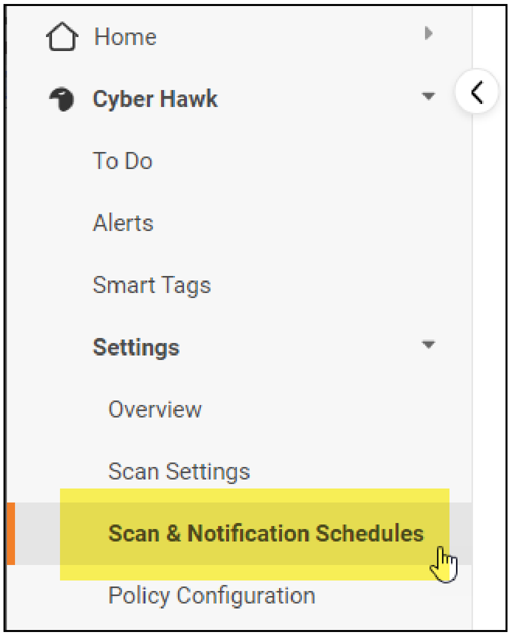

Scan and Notification Tasks

Task ID	Appliance ID	Appliance Description	Task Label	Description	Scan Type	Status	Next Run	Repeats		
8298471	KVS1-[redacted]	Updated	Internal Vulnerability Scan Two	Perform an Internal Vulnerability scan on the IP Range [10.[redacted] 10.[redacted] 10.[redacted] 10.[redacted] 10.[redacted]]. 13 IP Addresses will be excluded. Config: Low Impact.	Internal Scan	Queued	01/01/2024 11:51:00 AM	Yearly	Run Now	

Step 4 – Configure Cyber Hawk Internal Vulnerability Scan using VulScan

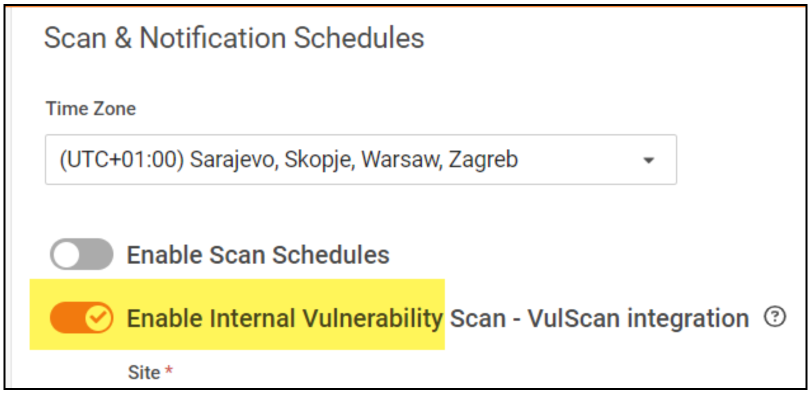
Once you 1) create a VulScan site, 2) install the internal scan appliance, and 3) schedule an internal vulnerability scan, return to your Cyber Hawk site. In this step, you will configure Cyber Hawk to import internal scans from VulScan.

1. From your Cyber Hawk Site, navigate to **Cyber Hawk** > **Settings** > **Scan & Notification Schedules**.



2. Click the slider to **Enable Internal Vulnerability Scan**.

© 2024 RapidFire Tools, Inc. All rights reserved.



Scan & Notification Schedules

Time Zone

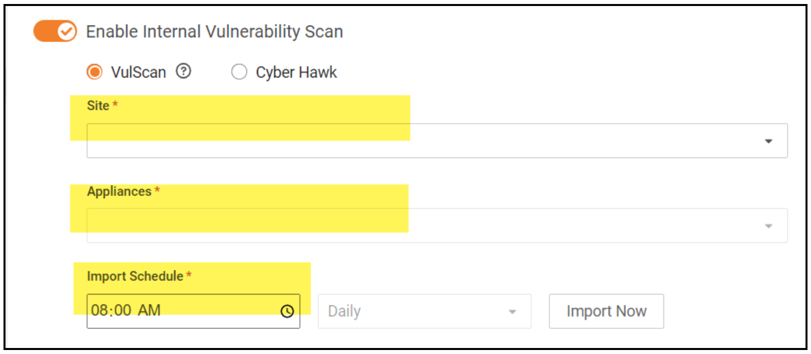
(UTC+01:00) Sarajevo, Skopje, Warsaw, Zagreb

○ Enable Scan Schedules

● Enable Internal Vulnerability Scan - VulScan integration

Site *

3. Select **VulScan**. (This step is only required if you also have a Cyber Hawk Virtual Appliance associated with your site.)
4. From **Site**, select your VulScan site from the drop-down menu. Your VulScan site **must be in the same organization** as your Cyber Hawk site.



● Enable Internal Vulnerability Scan

● VulScan ○ Cyber Hawk

Site *

Appliances *

Import Schedule *

08:00 AM Daily Import Now

5. From **Appliances**, select the VulScan appliance(s) from which to import internal vulnerability scans. **BE SURE YOU HAVE A SCHEDULED INTERNAL VULNERABILITY SCAN TASK SET UP FOR YOUR VULSCAN SITE.**
6. From **Import Schedule**, set the time and interval to import the results of VulScan internal vulnerability scans.

> **Note:** Set the import time to occur **after** your VulScan internal vulnerability scans will have completed.

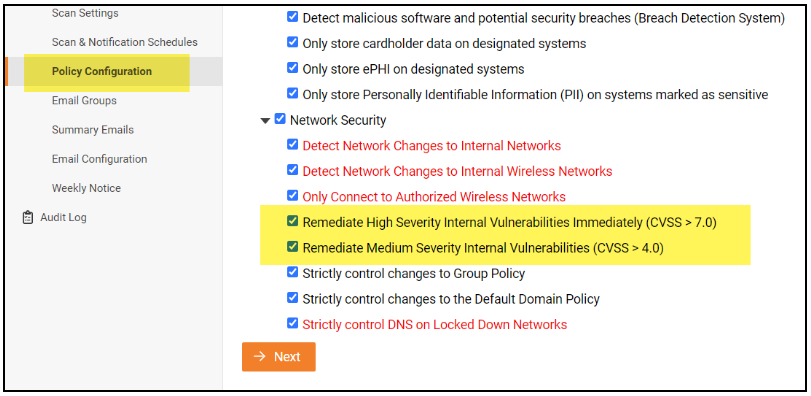
You can also click **Import Now** to import scans immediately.

Step 5 – Enable Remediate Internal Vulnerability Policies

Finally, be sure you have enabled the appropriate **Policies** from **Policy Configuration**.

© 2024 RapidFire Tools, Inc. All rights reserved.

1. Navigate to **Cyber Hawk** > **Settings** > **Policy Configuration**.
2. Ensure that the Remediate Medium and High Severity Internal Vulnerabilities policies are selected.



☑ Detect malicious software and potential security breaches (Breach Detection System)
☑ Only store cardholder data on designated systems
☑ Only store ePHI on designated systems
☑ Only store Personally Identifiable Information (PII) on systems marked as sensitive
☑ Network Security
☑ Detect Network Changes to Internal Networks
☑ Detect Network Changes to Internal Wireless Networks
☑ Only Connect to Authorized Wireless Networks
☑ Remediate High Severity Internal Vulnerabilities Immediately (CVSS > 7.0)
☑ Remediate Medium Severity Internal Vulnerabilities (CVSS > 4.0)
☑ Strictly control changes to Group Policy
☑ Strictly control changes to the Default Domain Policy
☑ Strictly control DNS on Locked Down Networks

3. When 1) your scheduled VulScan import completes, and 2) your Cyber Hawk Alert Notifications are sent, you will receive alerts for internal vulnerabilities detected by VulScan.

© 2024 RapidFire Tools, Inc. All rights reserved.

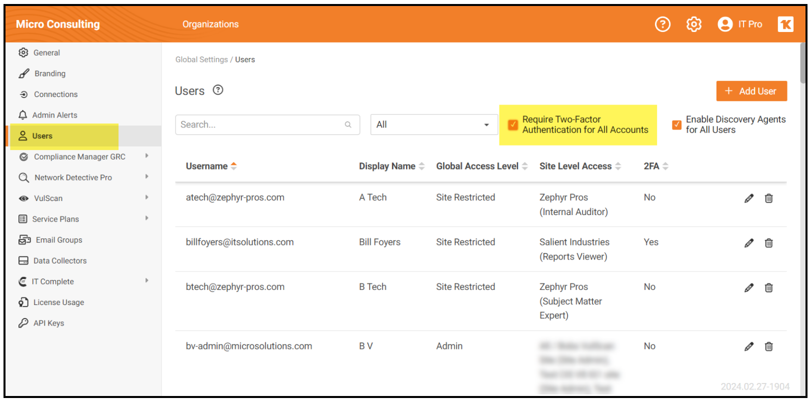
Enable Global Two-Factor Authentication (2FA) for Portal Users

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.



☑ Require Two-Factor Authentication for All Accounts

☑ Enable Discovery Agents for All Users

Username	Display Name	Global Access Level	Site Level Access	2FA
atech@zephyr-pros.com	A Tech	Site Restricted	Zephyr Pros (Internal Auditor)	No
billfoyers@itsolutions.com	Bill Foyers	Site Restricted	Salient Industries (Reports Viewer)	Yes
btech@zephyr-pros.com	B Tech	Site Restricted	Zephyr Pros (Subject Matter Expert)	No
bv-admin@microsolutions.com	B V	Admin	[redacted]	No

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

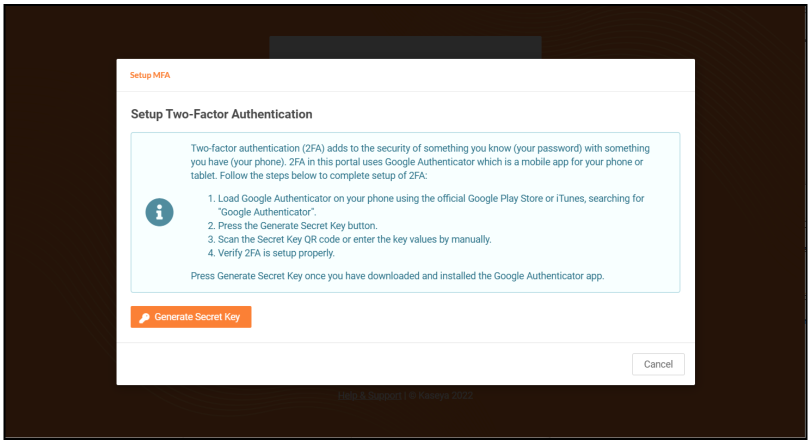
Step 2 — Portal user logs in and sets up 2FA Access

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.

© 2024 RapidFire Tools, Inc. All rights reserved.

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



Setup Two-Factor Authentication

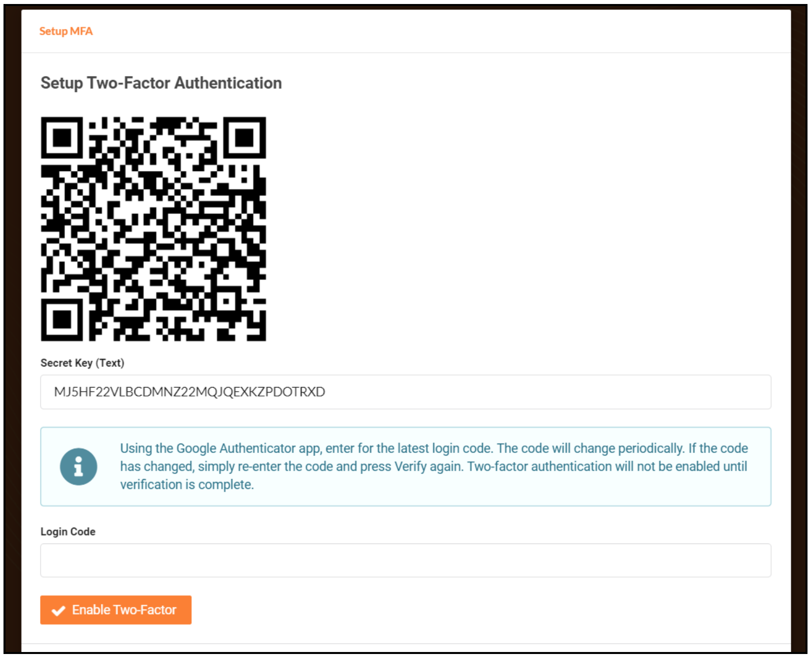
Two-factor authentication (2FA) adds to the security of something you know (your password) with something you have (your phone). 2FA in this portal uses Google Authenticator which is a mobile app for your phone or tablet. Follow the steps below to complete setup of 2FA:

1. Load Google Authenticator on your phone using the official Google Play Store or iTunes, searching for "Google Authenticator".
2. Press the Generate Secret Key button.
3. Scan the Secret Key QR code or enter the key values by manually.
4. Verify 2FA is setup properly.

Press Generate Secret Key once you have downloaded and installed the Google Authenticator app.

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

3. From the app, click **+** to add a new 2FA account.
4. Select **QR code**, and use your mobile device to scan the QR code that appears in the Portal.



Setup Two-Factor Authentication

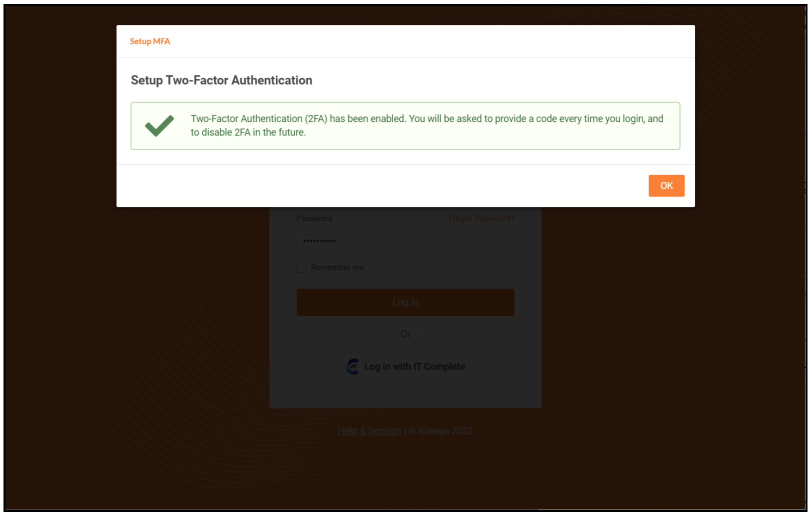
Secret Key (Text)

MJ5HF22VLBCDMNZ22MQJQEXKZPDOTRXD

Using the Google Authenticator app, enter for the latest login code. The code will change periodically. If the code has changed, simply re-enter the code and press Verify again. Two-factor authentication will not be enabled until verification is complete.

Login Code

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



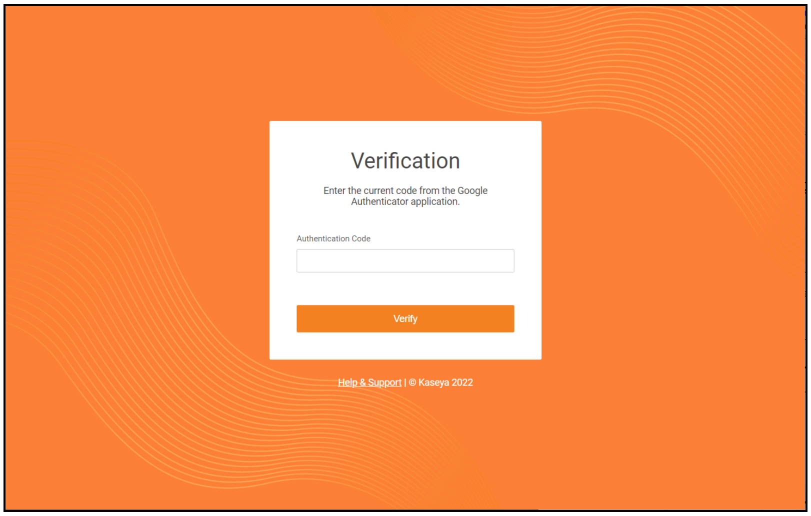
Setup MFA

Setup Two-Factor Authentication

Two-Factor Authentication (2FA) has been enabled. You will be asked to provide a code every time you login, and to disable 2FA in the future.

Step 3 — Portal Users enter Authentication Code after initial login

Once both the Master admin and individual portal users enable 2FA access, **all portal users must enter a one-time Authentication Code to access the Portal**. In this way, you can greatly enhance the security of the portal experience for all users.



Verification

Enter the current code from the Google Authenticator application.

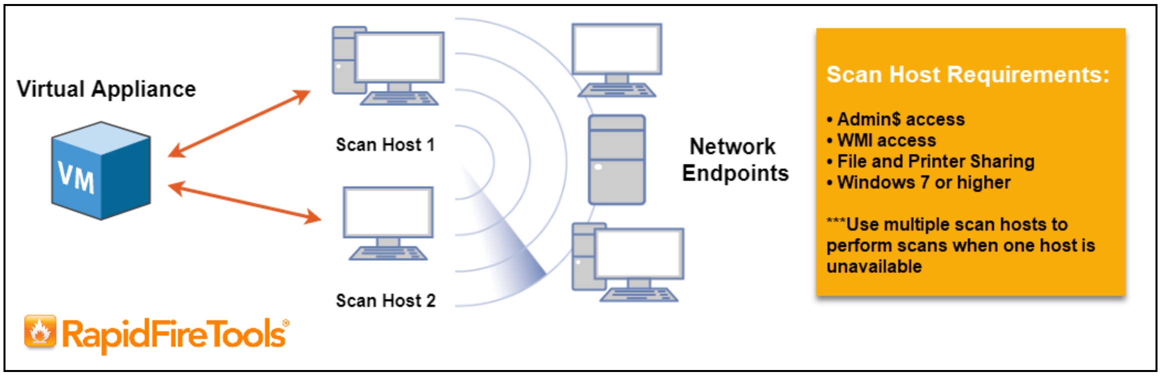
Authentication Code

Additional Scan Host Details

The Cyber Hawk Appliance requires access to at least one separate, additional PC on the client’s network. This computer is called the “Scan Host.” The Scan Host is used to initiate scans.

Scan Host Diagram

For your reference, the image below shows the relationship between the Cyber Hawk Virtual Appliance and the PCs that serve as scan hosts.



Scan Host Requirements:

- Admin$ access
- WMI access
- File and Printer Sharing
- Windows 7 or higher

***Use multiple scan hosts to perform scans when one host is unavailable

The RapidFire Tools **Virtual Appliance** is a virtual machine installed on the target network. The Appliance:

- communicates with the Scan Host
- pushes scans to the Scan Host, which are then pushed to the network
- communicates with the RapidFire Tools Servers (outbound on port 443)

The **Scan Host** is a computer on the target network. The Scan Host allows scans to be performed using a computer that is part of the existing network. The Scan Host:

- pushes scan tasks from the Virtual Appliance to the endpoints on the target network
- communicates with the Virtual Appliance

Note: Multiple Scan Hosts allow for scans to continue even if one scan host is unavailable.

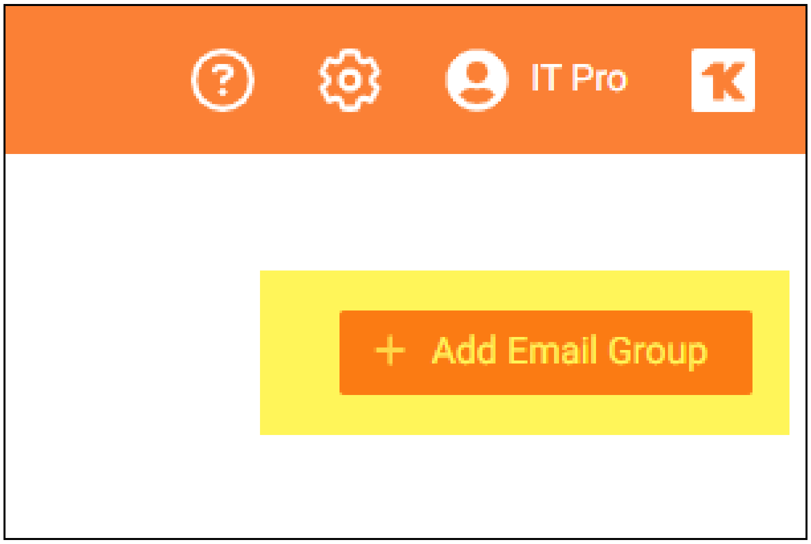
© 2024 RapidFire Tools, Inc. All rights reserved.

Create Global Email Groups

You can create global level Email Groups for use with all of your Cyber Hawk sites. This allows you to quickly assign email groups for the notification actions that you set up in "Task 8 — Configure Policies and Notifications" on page 48.

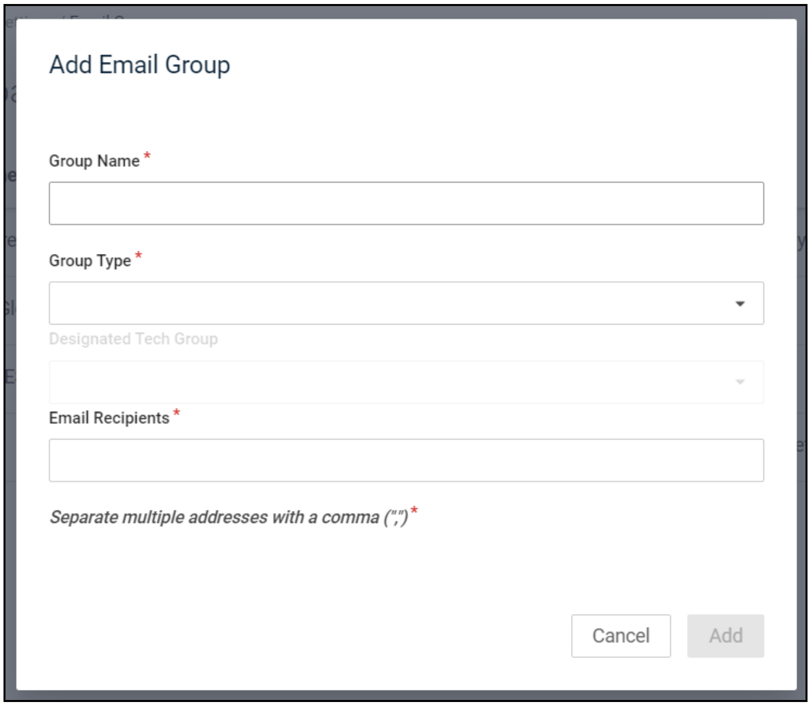
Here's how to set up global Email Groups:

1. From the RapidFire Tools Portal, navigate to global **Settings (Admin)** ⚙ > **Email Groups**.
2. Click **Add Email Group**.



3. Enter a **Group Name** to help your team understand the purpose of the Email Group.

© 2024 RapidFire Tools, Inc. All rights reserved.



Add Email Group

Group Name *

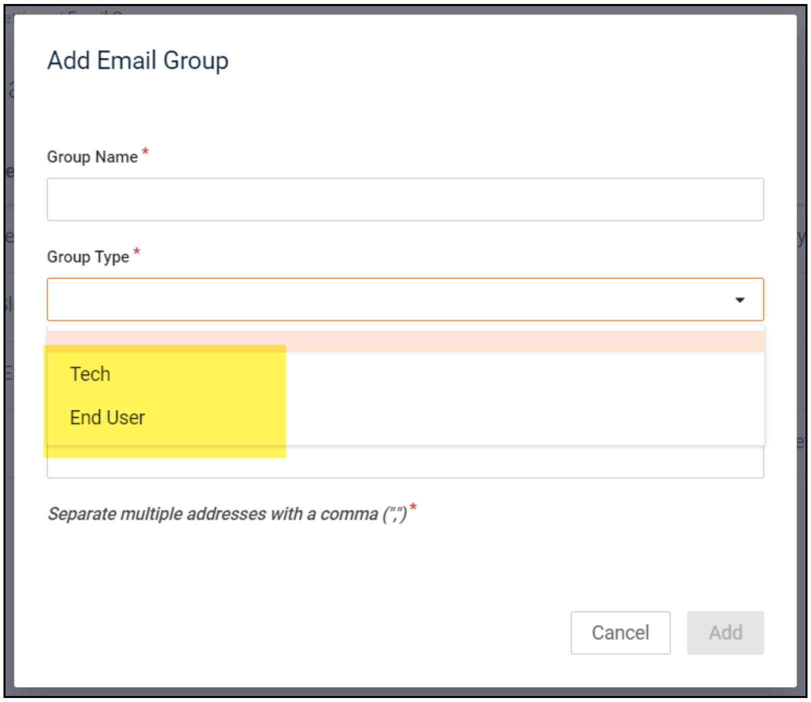
Group Type *

Designated Tech Group

Email Recipients *

Separate multiple addresses with a comma (",") *

4. Select a **Group Type**: **Tech** or **End-user**.



Add Email Group

Group Name *

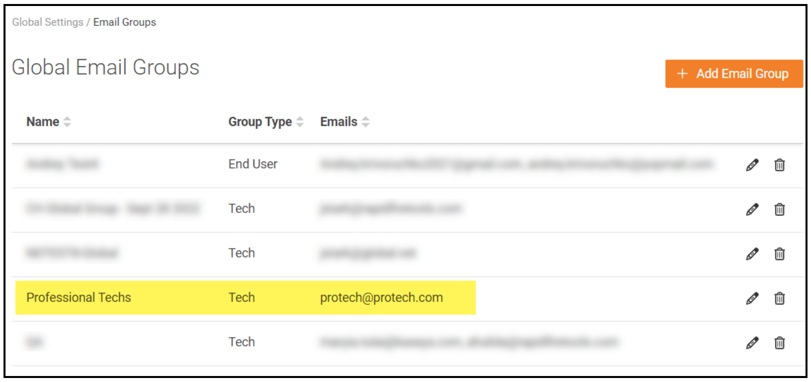
Group Type *

Separate multiple addresses with a comma (",") *

5. Enter the **Email Recipients** for the group.

© 2024 RapidFire Tools, Inc. All rights reserved.

6. Click **Add** when you are finished configuring the group. The group will appear in the list of Email Groups. You can then select this group for each of your Cyber Hawk sites as you complete "Task 8 — Configure Policies and Notifications" on page 48.



Global Settings / Email Groups

Global Email Groups

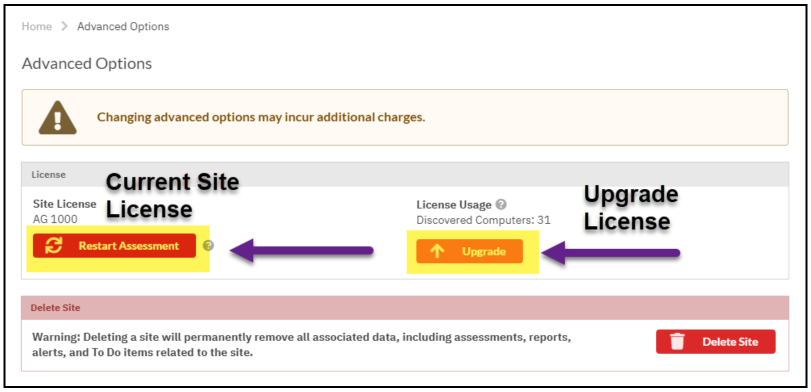
Name	Group Type	Emails
[redacted]	End User	[redacted]
[redacted]	Tech	[redacted]
[redacted]	Tech	[redacted]
Professional Techs	Tech	protech@protech.com
[redacted]	Tech	[redacted]

Upgrade your Site License (MSPs Only)

Note: Only MSP account users can upgrade an individual site license. If you are a direct-to-customer or SMB user, please contact your account representative to upgrade your license.

Your site must be licensed for the number of computers on the target network. If the network scan discovers more computers on the site network than are covered in your license, you will need to upgrade your license to continue the assessment. To do this:

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



Changing advanced options may incur additional charges.

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

Note: Subscriptions cannot be downgraded or canceled until the end of the subscription period.

3. Click **Upgrade**.
4. Select a license from the **Available Licenses** tab.

If you have a license violation, it will be removed and you can continue with your assessment. See below for more information on the available licenses.

Site License Options

Note: You have an unlimited number of **250 Licenses** as part of your Cyber Hawk subscription. If you wish to upgrade your license, you will be billed extra. Contact your Sales Representative for more details.

© 2024 RapidFire Tools, Inc. All rights reserved.

Account-wide License Options (MSP and SMB)

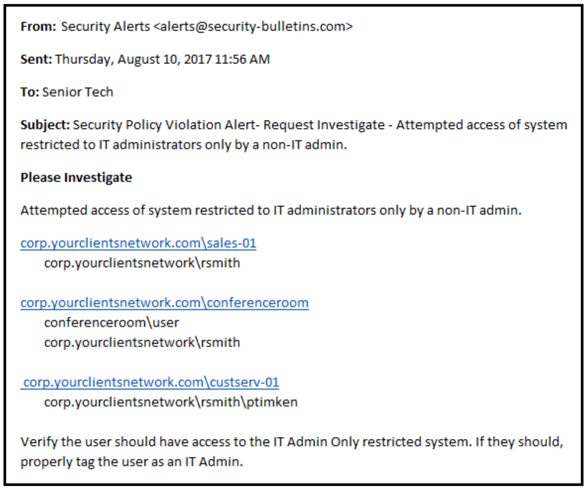
There are two licensing "models" for RapidFire Tools accounts:

- **MSP**: For resellers who offer managed services to clients. License upgrades are purchased site-by-site.
- **SMB**: For end-users who are deploying services on their own networks/sites. Account-wide license covers a certain number of sites and computers. Contact account representative to upgrade.

Sample Daily Alerts and Weekly Notices

Below are samples of email messages that present a Tech Alert and End User Alert Notifications and a Weekly Notice.

Sample Tech Alert



From: Security Alerts <alerts@security-bulletins.com>

Sent: Thursday, August 10, 2017 11:56 AM

To: Senior Tech

Subject: Security Policy Violation Alert- Request Investigate - Attempted access of system restricted to IT administrators only by a non-IT admin.

Please Investigate

Attempted access of system restricted to IT administrators only by a non-IT admin.

corp.yourclientsnetwork.com\sales-01
corp.yourclientsnetwork\rsmith

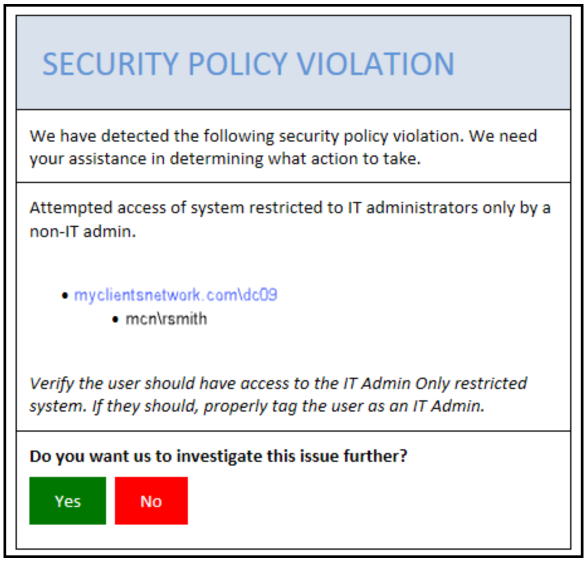
corp.yourclientsnetwork.com\conferenceroom
conferenceroom\user
corp.yourclientsnetwork\rsmith

corp.yourclientsnetwork.com\custserv-01
corp.yourclientsnetwork\rsmith\ptimken

Verify the user should have access to the IT Admin Only restricted system. If they should, properly tag the user as an IT Admin.

© 2024 RapidFire Tools, Inc. All rights reserved.

Sample End User Alert



SECURITY POLICY VIOLATION

We have detected the following security policy violation. We need your assistance in determining what action to take.

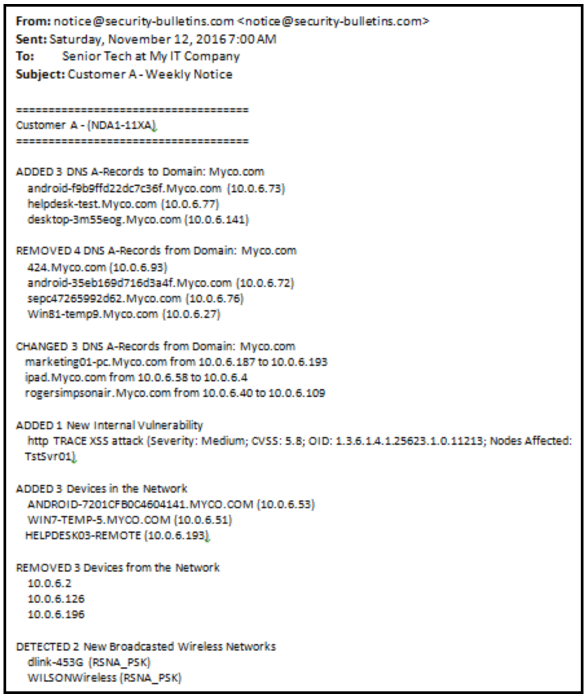
Attempted access of system restricted to IT administrators only by a non-IT admin.

- myclientsnetwork.com\dc09
  - mcn\rsmith

Verify the user should have access to the IT Admin Only restricted system. If they should, properly tag the user as an IT Admin.

Do you want us to investigate this issue further?

Sample Weekly Notice



From: notice@security-bulletins.com <notice@security-bulletins.com>
Sent: Saturday, November 12, 2016 7:00 AM
To: Senior Tech at My IT Company
Subject: Customer A - Weekly Notice

```
====================================
Customer A - (NDA1-11XA)
====================================

ADDED 3 DNS A-Records to Domain: Myco.com
   android-f9b9ffd22dc7c36f.Myco.com (10.0.6.73)
   helpdesk-test.Myco.com (10.0.6.77)
   desktop-3m55eog.Myco.com (10.0.6.141)

REMOVED 4 DNS A-Records from Domain: Myco.com
   424.Myco.com (10.0.6.93)
   android-35eb169d716d3a4f.Myco.com (10.0.6.72)
   sepc47265992d62.Myco.com (10.0.6.76)
   Win81-temp9.Myco.com (10.0.6.27)

CHANGED 3 DNS A-Records from Domain: Myco.com
  marketing01-pc.Myco.com from 10.0.6.187 to 10.0.6.193
  ipad.Myco.com from 10.0.6.58 to 10.0.6.4
  rogersimpsonair.Myco.com from 10.0.6.40 to 10.0.6.109

ADDED 1 New Internal Vulnerability
   http TRACE XSS attack (Severity: Medium; CVSS: 5.8; OID: 1.3.6.1.4.1.25623.1.0.11213; Nodes Affected:
  TstSvr01)

ADDED 3 Devices in the Network
   ANDROID-7201CFB0C4604141.MYCO.COM (10.0.6.53)
   WIN7-TEMP-5.MYCO.COM (10.0.6.51)
  HELPDESK03-REMOTE (10.0.6.193)

REMOVED 3 Devices from the Network
   10.0.6.2
   10.0.6.126
   10.0.6.196

DETECTED 2 New Broadcasted Wireless Networks
   dlink-453G (RSNA_PSK)
   WILSONWireless (RSNA_PSK)
```

© 2024 RapidFire Tools, Inc. All rights reserved.

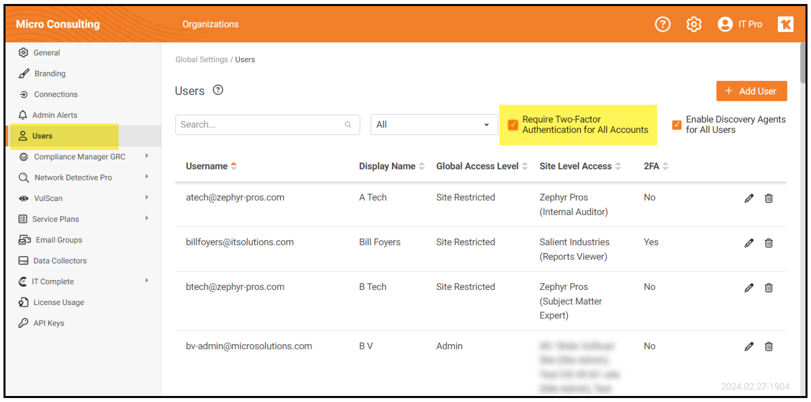
Enable Global Two-Factor Authentication (2FA) for Portal Users

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.



☑ Require Two-Factor Authentication for All Accounts

☑ Enable Discovery Agents for All Users

Username	Display Name	Global Access Level	Site Level Access	2FA
atech@zephyr-pros.com	A Tech	Site Restricted	Zephyr Pros (Internal Auditor)	No
billfoyers@itsolutions.com	Bill Foyers	Site Restricted	Salient Industries (Reports Viewer)	Yes
btech@zephyr-pros.com	B Tech	Site Restricted	Zephyr Pros (Subject Matter Expert)	No
bv-admin@microsolutions.com	B V	Admin	[redacted]	No

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

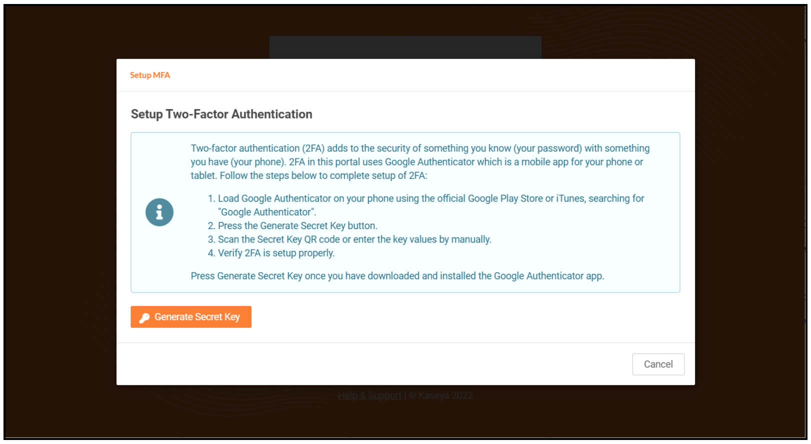
Step 2 — Portal user logs in and sets up 2FA Access

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.

© 2024 RapidFire Tools, Inc. All rights reserved.

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



Setup MFA

Setup Two-Factor Authentication

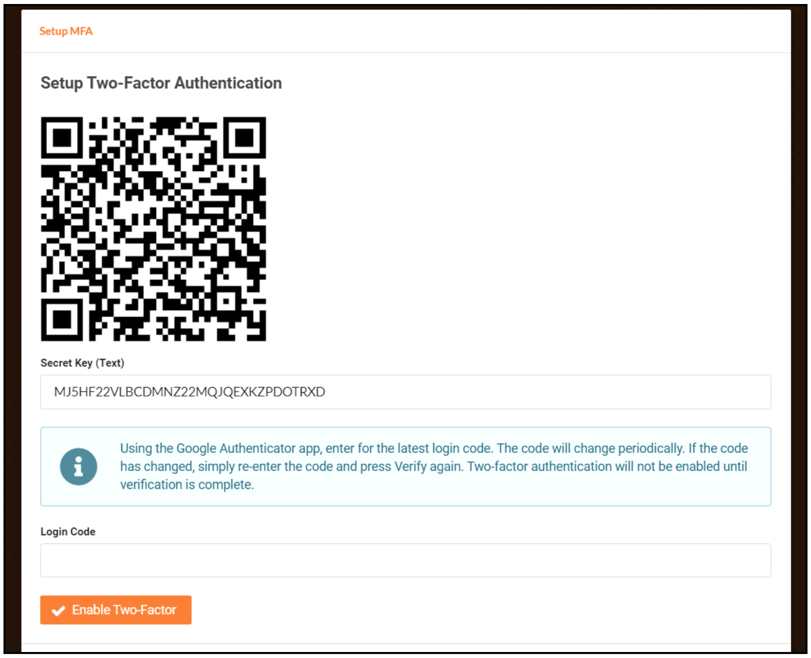
Two-factor authentication (2FA) adds to the security of something you know (your password) with something you have (your phone). 2FA in this portal uses Google Authenticator which is a mobile app for your phone or tablet. Follow the steps below to complete setup of 2FA:

1. Load Google Authenticator on your phone using the official Google Play Store or iTunes, searching for "Google Authenticator".
2. Press the Generate Secret Key button.
3. Scan the Secret Key QR code or enter the key values by manually.
4. Verify 2FA is setup properly.

Press Generate Secret Key once you have downloaded and installed the Google Authenticator app.

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

3. From the app, click **+** to add a new 2FA account.
4. Select **QR code**, and use your mobile device to scan the QR code that appears in the Portal.



Setup MFA

Setup Two-Factor Authentication

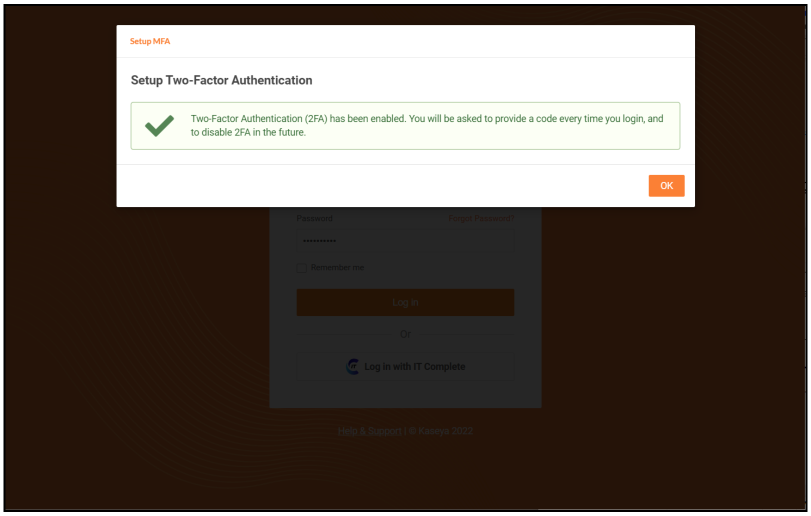
Secret Key (Text)

MJ5HF22VLBCDMNZ22MQJQEXKZPDOTRXD

Using the Google Authenticator app, enter for the latest login code. The code will change periodically. If the code has changed, simply re-enter the code and press Verify again. Two-factor authentication will not be enabled until verification is complete.

Login Code

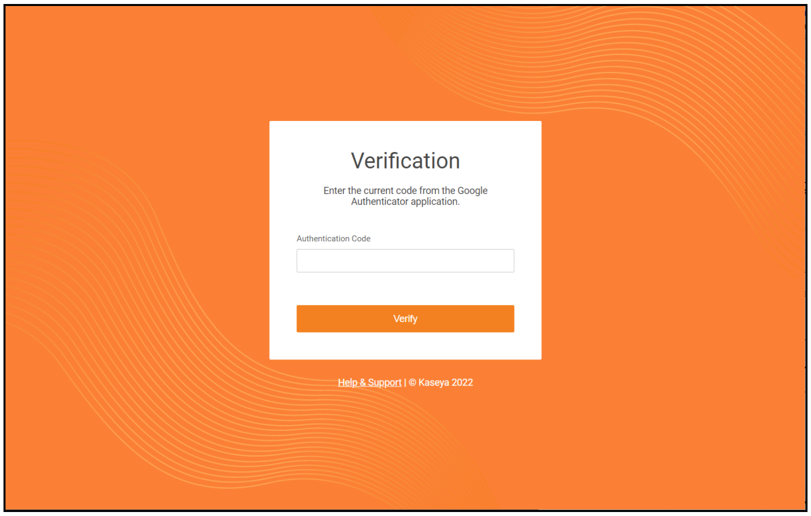
5. A setup confirmation modal will appear. Click **OK**.



Two-Factor Authentication (2FA) has been enabled. You will be asked to provide a code every time you login, and to disable 2FA in the future.

Step 3 — Portal Users enter Authentication Code after initial login

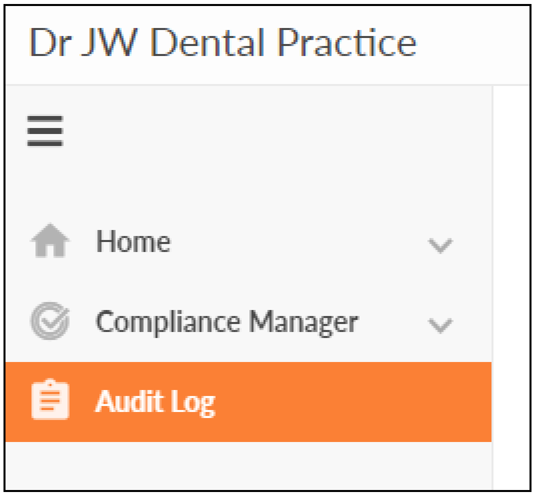
Once both the Master admin and individual portal users enable 2FA access, **all portal users must enter a one-time Authentication Code to access the Portal**. In this way, you can greatly enhance the security of the portal experience for all users.



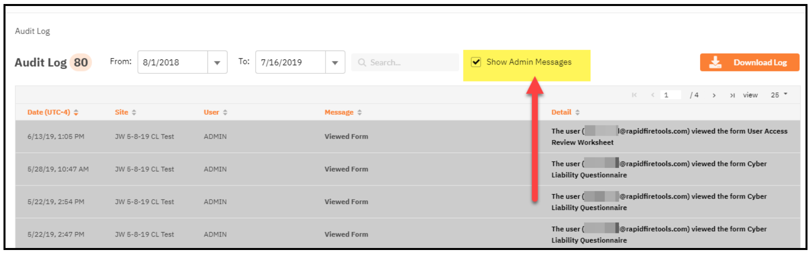
Enter the current code from the Google Authenticator application.

Audit Log

The **Audit Log** allows you to see all of the activity in the RapidFire Tools Portal.



Click **Show Admin Messages** to see even more detail. This includes notices that scans were started, completed, failed, etc.



Audit Log

Audit Log 80 From: 8/1/2018 To: 7/16/2019 Search... ☑ Show Admin Messages Download Log

1 / 4 view 25

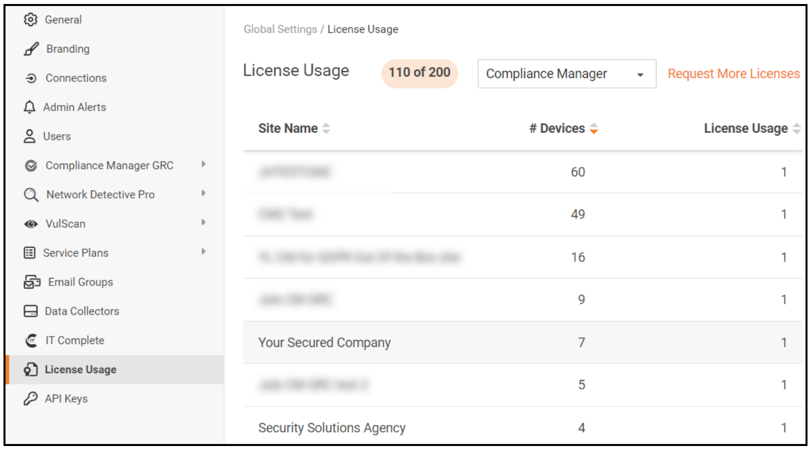
Date (UTC-4)	Site	User	Message	Detail
6/13/19, 1:05 PM	JW 5-8-19 CL Test	ADMIN	Viewed Form	The user ([redacted]@rapidfiretools.com) viewed the form User Access Review Worksheet
5/28/19, 10:47 AM	JW 5-8-19 CL Test	ADMIN	Viewed Form	The user ([redacted]@rapidfiretools.com) viewed the form Cyber Liability Questionnaire
5/22/19, 2:54 PM	JW 5-8-19 CL Test	ADMIN	Viewed Form	The user ([redacted]@rapidfiretools.com) viewed the form Cyber Liability Questionnaire
5/22/19, 2:47 PM	JW 5-8-19 CL Test	ADMIN	Viewed Form	The user ([redacted]@rapidfiretools.com) viewed the form Cyber Liability Questionnaire

© 2024 RapidFire Tools, Inc. All rights reserved.

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.

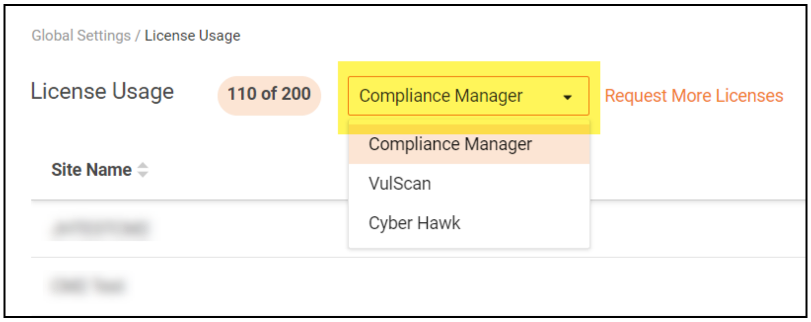


Site Name	# Devices	License Usage
[redacted]	60	1
[redacted]	49	1
[redacted]	16	1
[redacted]	9	1
Your Secured Company	7	1
[redacted]	5	1
Security Solutions Agency	4	1

A Site License will be automatically consumed whenever the number of detected devices exceeds 250. For example:

- When 0 to 250 devices are detected, one Site License will be used
- When 251 Devices are detected, a second Site License will be used
- When 501 Devices are detected, a third Site License will be used, and so on

Use the drop-down menu to filter between Compliance Manager GRC, VulScan, and Cyber Hawk site license usage.



Site Name
[redacted]
[redacted]

User Control Tests

Several RapidFire Tools data collection tools employ **User Control Tests** to analyze the security of potential web browsing activity on a device. As part of the test, the data collector will attempt to access certain risk-prone websites directly from a device. User Control Tests can thus help determine how much access a user has to potentially risky websites, and can highlight the need for additional controls on web browsers.

RapidFire Tools Data Collectors that employ User Control Tests include:

- Network/Security Data Collector (using Security scan on local device)
- Push Deploy Tool (using Security Scan)
- Remote Data Collector (using Security Scan and/or Push Deploy Scan)
- Discovery Agents
- Cyber Hawk Level 1 Scan

Below you can find a list of the websites that User Control Tests will attempt to access:

Important: If you are using an anti-virus or other tool that monitors suspicious web browsing, note that you may receive alerts from such systems related to this activity. Refer to the list of websites below, as well as the time of such alerts compared with the time of data collector activity, to determine whether such alerts are false positives that result from User Control Tests.

- http://www.facebook.com/
- https://plus.google.com/
- http://www.myspace.com/
- http://www.youtube.com/
- http://mail.yahoo.com/
- http://gmail.google.com/
- http://espn.go.com/
- http://thepiratebay.se/
- http://isohunt.to/
- http://www.playboy.com/
- http://www.youporn.com/
- http://download.cnet.com/
- http://www.tucows.com/

© 2024 RapidFire Tools, Inc. All rights reserved.