Copyright © 2024 Kaseya Limited



# **USER GUIDE**

# Cyber Hawk (previously known as Detector)

Detecting and Responding to IT Security Policy Violations

**Kaseya**°





rapidfiretools.com



support@rapidfiretools.com

3/7/2024 3:09 PM

# Contents

Introduction to Cyber Hawk	8
Cyber Hawk Overview	8
Cyber Hawk Components	10
Setting Up Cyber Hawk	12
Initial Cyber Hawk Set Up	
Step 1 — Provision Cyber Hawk Appliance ID in Network Detective	12
Step 2 — Install Cyber Hawk and Create a New Site	13
Step 3 — Associate Cyber Hawk with a Site and Access Cyber Hawk Settings	14
Configure Cyber Hawk Using the Setup Wizard (Virtual Appliance)	
Step 1 — Configure Scan Settings	
Step 2 — Schedule Scans and Alert Notifications	
Tips for Scheduling the Level 2 Scan	
Step 3 — Configure Tech Email Groups	
Step 4 — Configure End User Email Groups	
Step 5 — Perform Pre-Scan Analysis	34
Step 6 — Perform Initial Cyber Hawk Scan	
Step 7 — Configure Policies	
Step 8 — Configure Notifications	40
Step 9 — Configure Smart Tags	41
Step 10 — Set Up RapidFire Tools Portal	43
Provisioning Additional Cyber Hawk Appliances for Deployment	44
Provisioning Additional Cyber Hawk Appliances for Deployment (Classic)	46
Provisioning Additional Detector Legacy Appliances for Deployment	49
Cyber Hawk Security Policy Violation Alerts	
Security Policy Violation Alert Notification Rule Actions	51
Set Up End User Alert Notifications	
More about End User Security Policy Violation Alert Notifications	54
Set Up Tech Group Alert Notifications	

Managing and Deleting "Ignore" Alert Rules	57
Cyber Hawk Security Alert Email Summaries	58
Security Policy Details	62
Cyber Hawk Alert Response Workflows	67
Create a Ticket from an Alert	67
Respond to an Alert Investigation Request (Tech Group)	68
Three Alert Response Scenarios using Cyber Hawk	71
#1: "Attempted access of system restricted to IT administrators only by a non-IT admin"	72
#2: "Unauthorized access to a computer in the Cardholder Data Environment (CE	)E)"72
#3: "New medium severity internal vulnerabilities were found"	73
Send the Tech Group an Alert Investigation Request (End User)	75
Request that the Tech Group Ignore an Alert (End User)	77
Process an Ignore Alert Request (Tech Group)	79
Using the RapidFire Tools Portal	83
<u>Alerts</u>	85
How Long Do Alerts Last in the Portal?	86
View and Process Alerts	86
Alert Item Statuses	87
Filter Alert Queue by Status	89
Revert Completed Alerts Back to the To Do Items	90
<u>To Dos</u>	94
How Long Do To Do Items Last in the Portal?	95
View and Process To Dos	95
Create To Do Items from Alerts	96
Set Up and Assign a Ticketing/PSA System Integration to a Site Using Cyber	
Hawk	98
Step 1 — Gather Credentials and Set Up your PSA System	98
Step 2 — Set Up a Connection to your Ticketing System/PSA	99
Step 3 — Map your Cyber Hawk's Site to a Ticketing System/PSA Connection	105
Set Up Autotask Integration	108

Set Up Autotask (SOAP) Integration	111
Set Up ConnectWise REST Integration	
Step 1 — Download and Install the ConnectWise Manage Internet Client Application	116
Step 2 — Select the ConnectWise Ticket System API Member Account to In with	tegrate
Create Minimum Permissions Security Role for API Member	
Table Setup Configuration	
Step 3 — Create an API Key in the ConnectWise Ticketing System	119
Step 4 — Configure Service Tables in ConnectWise	120
Step 5 — Remove "Disallow Saving" Flag from Company	
Set Up ConnectWise SOAP Integration	
Set Up Kaseya BMS Integration	
Set Up Portal Branding	
Set Custom Portal Theme	
Set Custom Portal Subdomain	
Set Custom Company Name	
Set Custom Company Logo	133
Set Up a Custom Subdomain to Access the RapidFire Tools Portal	
Set Up Custom SMTP Server Support	
Allow Clients to Access Portal and Manage Tickets	
Step 1 — Create Site Restricted User in Portal	
Step 2 — Assign User to Site	141
Step 3 — Assign User to Technician Role	
Manage Users (Global Level)	
Users and Global Access Roles	
Add User at Global Level	145
Edit User at Global Level	
RapidFire Tools Portal Site Roles	
Manage Site Data Collectors	
Data Collector Commands	153
Smart Tags	

Defining Smart Tags	156
Using Smart Tags	160
Add and Configure Smart Tags	161
Step 1 — Select the Site	161
Step 2 — Select Manage Cyber Hawk Appliance and Access the Cyber Hawk Setting	gs161
Step 3 — Access Smart Tags and Verify that Scan Data has been Downloaded	162
Step 4 — Select and Apply Recommended Tags	164
Step 5 — View Applied Tags	166
Step 6 — Select and Apply Additional Smart Tags from the Available Tags Window .	166
Export and Import Smart Tags	170
Export Smart Tags	170
Step 1 — Select the Site	170
Step 2 — Select Manage Cyber Hawk Appliance and Access the Cyber Hawk Settings	171
Step 3 — Access Smart Tags and Verify that Scan Data has been Downloaded	171
Step 4 — Export Smart Tags	172
Import Smart Tags	173
Step 1 — Select the Site	173
Step 2 — Select Manage Cyber Hawk Appliance and Access the Cyber Hawk Settings	173
Step 3 — Access Smart Tags and Verify that Scan Data has been Downloaded	174
Step 4 — Import a Smart Tags Configuration File	174
Delete Smart Tags	176
Step 1 — Open the Applied Tags Window and Select the Tag for Deletion	176
Step 2 — Select the Tag and Delete	176
Service Plans and Catalogs	178
Using the Service Plan Creator	178
Create Service Plans and Service Catalogs	179
Step 1 — Create a New Service Plan	179
Step 2 — Assign Security Policies to Your Service Plan	181
Step 3 — Define Reports Deliverables to be Included in the Service Plan	184
Step 4 — Create a Service Catalog	187

Generate a Service Catalog Document	190
Generate a Service Plan Matrix Document	191
Generate a Sample Master Services Agreement for a Service Plan	194
Step 1 — Opening Existing Network Detective Site that is Associated with your Cyb Hawk	er 194
Step 2 — Access the Cyber Hawk Settings	195
Step 3 — Select the Policy Configuration Option	195
Step 4 — Generate Master Service Agreement Option	196
Step 5 — Enter the MSP information, Customer information, and Service Plan Cost Details	197
Step 6 — Confirm Acceptance of the Disclaimer and Generate the Sample MSA	198
Managing Service Plans	199
Edit a Service a Plan	199
Delete a Service Plan	200
Managing Service Catalogs	202
Add Service Plans to a Catalog	202
Edit a Service Catalog	204
Remove (Delete) a Service Catalog from the List of Catalogs	205
Delete (Exclude) Service Plans from a Catalog	207
Default Cyber Hawk Service Plans	208
Appendices	212
Configure Cyber Hawk Using the Setup Wizard (RapidFire Tools Server)	213
Step 1 — Configure Scan Settings	214
Step 2 — Schedule Scans and Alert Notifications	222
Step 3 — Configure Tech Email Groups	223
Step 4 — Configure End User Email Groups	226
Step 5 — Perform Pre-Scan Analysis	228
Step 6 — Perform Initial Cyber Hawk Scan	231
Step 7 — Configure Policies	231
Step 8 — Configure Notifications	234
Step 9 — Configure Smart Tags	235
Step 10 — Set Up RapidFire Tools Portal	237

Additional Scan Host Configuration Options and Requirements	
Scan Host Diagram	
Scan Host Requirements	
Assigning Scan Hosts in a Domain Environment	
Pre-Scan Network Configuration Checklist	
Checklist for Domain Environments	
Checklist for Workgroup Environments	
RapidFire Tools Server vs. Virtual Appliance	
Sample Daily Alerts and Weekly Notices	
Sample Tech Alert	
Sample End User Alert	
Sample Weekly Notice	
Edit Policies Enforced at a Site	
Unitrends Backup Alerts	
Requirements for Unitrends Backup Alerts	
How to enable Unitrends Backup Alerts (Web Console)	
How to enable Unitrends Backup Alerts (Network Detective)	254
Audit Log	

# Introduction to Cyber Hawk

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

### 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.

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 and prevent the same "false-positive" from being generated again in the future

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.

• **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 Cyber Hawk Appliance software application installed on the target network. You have two install options. These include 1) installing the <b>RapidFire</b> <b>Tools Server</b> Windows Service, or 2) a <b>Virtual Appliance</b> that requires a user supplied Microsoft Hyper-V based system or a VMware based system.
Optional Small Form Factor Server Computer	This is an optional hardware component that can be purchased from RapidFire Tools to host and operate the Cyber Hawk Appliance. It is a small, portable server computer which plugs into the target network through an Ethernet connection.
Diagnostic Tool	This tool is used for configuring and troubleshooting the Cyber Hawk Appliance. The Diagnostic Tool should be run on the same network as the Cyber Hawk Appliance to perform diagnostics checks such as for Cyber Hawk Appliance connectivity.
Network Detective Application	This is the same Network Detective desktop application and report generator that is used with any other Network Detective modules. This application contains additional features to manage the Cyber Hawk Appliance remotely.
The Network Detective Service Plan Creator and the Service Catalog	Cyber Hawk users have access to Network Detective's unique "Service Plan Creator" tool that gives you the ability to modify our starter Service Plans, or create your own 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.

Cyber Hawk Component	Description
RapidFire Tools Portal	The RapidFire Tools Portal is 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:
	<ul> <li>transferring the requests to Ticketing/PSA Systems such as Autotask, ConnectWise, and Tigerpaw</li> </ul>
	<ul> <li>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</li> </ul>
	<ul> <li>creating Ignore Rules to address Alert False Positives</li> </ul>
	<ul> <li>completing a given Action Request</li> </ul>
	To access the RapidFire Tools Portal, visit the default web site URL of <u>https://www.youritportal.com</u> .
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 <u>"Set Up</u> and Assign a Ticketing/PSA System Integration to a Site Using Cyber Hawk" on page 98.

## Setting Up Cyber Hawk

Setting up Cyber Hawk consists of two parts:

- 1. Install Cyber Hawk on the target network and bind it to a Site in the Network Detective Application: "Initial Cyber Hawk Set Up" below
- 2. Configure Cyber Hawk scans and how it will enforce security policies on the target network: <u>"Configure Cyber Hawk Using the Setup Wizard (Virtual Appliance)" on page 17</u>

### Initial Cyber Hawk Set Up

Follow these steps to install Cyber Hawk and associate it with a Site in Network Detective.

### Step 1 — Provision Cyber Hawk Appliance ID in Network Detective

First ensure your account has an available Cyber Hawk **Appliance ID** to use during the install. To do this:

- 1. Visit <u>https://www.rapidfiretools.com/nd</u> to download and install the latest version of the **Network Detective Application**.
- 2. Run Network Detective and log in with your credentials.
- 3. Click **Appliances**.



4. Click Provision Cyber Hawk.

		/				
InFo	m	Appliance	<b>s</b> Conr	nector	Service Pla	ans
		Provision Cyber	Hawk Prov	vision Detec	tor Legacy	
es	Арр	liance Ovenide:			Downlo	ad Logs
		Appliance ID	Туре	Applia	nce Type	Site Na
	0	NDA1-	Virtual	Cyber	Hawk SDS	
	0	NDA1-	Server	Cyber	Hawk SDS	Pablo 1
	0	NDA1-	Virtual	Cyber	Hawk SDS	CDx (r
	0	NDA1-	Server	Cyber	Hawk SDS	

5. Select the number of appliances to activate.

Provision Cyber Hawk	×
Number of Cyber Hawk appliances to Activate: 1	-
OK Cancel	

6. Click **OK**. Your Cyber Hawk Appliance ID will be added to the list of appliances for your account.

The new appliance will appear with a gray button and will read "Not Activated."

0	NDA1-87	Virtual	Cyber Hawk SDS	Site	Activated	-
0	NDA1-73	Virtual	Cyber Hawk SDS		Not activated	-

7. Note the **Appliance ID** in the list. You will later select this ID during the install.

### Step 2 — Install Cyber Hawk and Create a New Site

- 1. Install Cyber Hawk on your client's network by either:
  - a. connecting the Cyber Hawk installed on the **Small Form Factor Server Computer** that you purchased from RapidFire Tools to your client's Network.
  - b. going to <u>https://www.rapidfiretools.com/nd</u> to download and install the **RapidFire Tools Virtual Appliance** on a computer operating within your client's network.

**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:** For more information about installing the Virtual Appliance, please download the <u>Virtual Appliance Installation Guide for Cyber Hawk</u>.

- 2. After successfully deploying Cyber Hawk, **run Network Detective** and **log in** with your credentials.
- 3. Create a new Site by clicking **New Site**.

New Site	Import Site	View 🔻	Refresh	
New Site				
All Network physical loc	Detective asses cation or a logica	ssments ar grouping,	e organized , such as a c	into Sites. A site can be a sustomer.
Type in Site	Name Here	-		
		Ok	Cancel	

4. Enter the **Site Name** and click **OK**.

# Step 3 — Associate Cyber Hawk with a Site and Access Cyber Hawk Settings

1. From within the Site Window, select the All selector symbol to expand the Site's Preferences in order to Add an Appliance.

|--|

2. Next, select the **Add** Appliance button. The Add Appliance window will be displayed.



3. Select the **Appliance ID** of the **Cyber Hawk** Appliance from the drop down menu.

Add Appliance	
Appliance ID: Site:	Customer A
	OK Cancel

**Note:** When users have purchased a Small Form Factor Server Computer, the Appliance ID can be found on a printed label on the Small Form Factor Server Computer itself.

After selecting the Appliance ID, select the **OK** button to continue.

4. After successfully adding a Cyber Hawk to the Site, its Appliance ID will appear under the Appliance bar in the Site Preferences window. The status of the Appliance will be indicated as Active.

V	Customer A	
	Appliances	Connectors Preferences
	$\nabla$	
	NDA	Active Kemove Appliance Up to Date
	Status	
	No queued tasks.	

**Important:** If you remove a Cyber Hawk from a Site, its configurations will be deleted.

When you have completed the two steps above, the Cyber Hawk will appear on the lefthand Site bar. Click on the Cyber Hawk icon to open the Cyber Hawk management screen:

	Customer / Edit Site Configure   Smart Tags		
	NDA1 Host Type: Vitual 💿 Active		
×	Settings		
	Policy Configuration: Modfy Scan Configuration: Modfy 7 Active Policies	Schedules: Mo	dify
	Email Configuration: Modify Comains: Al Domains: Al Domains: Primay Joinan Domains: Al Domains: IP Range(s): 10 200.10-10 200.1255	Level 1 Scan (Daily): Level 2 Scan (Weekl	(01C-05:0 1:00 AM (0 y): 1:00 AM o
V	Notification Rules Add Email Group Vew Ignored Alerts		
	Policy Name	Action	Group Name
	<ul> <li>Access Control</li> </ul>		
	Authorize New Devices to be Added to Restricted Networks	Email End User	<ul> <li>None</li> </ul>
	Restrict Access to Accounting Computers to Authorized Users	Email Tech	<ul> <li>None</li> </ul>
	Restrict Access to Business Owner Computers to Authorized Users	Create Ticket	<ul> <li>None</li> </ul>
	Restrict IT Administrative Access to Minimum Necessary	Create Ticket	<ul> <li>None</li> </ul>
_	Result: Users unat alle Not Huunonzed to Log into Multiple Computer Systems	Create Ticket	<ul> <li>None</li> </ul>
	Strictly Control the Addition of New Local Computer Administrators	Email Tech	<ul> <li>None</li> </ul>
	Strictly Control the Addition of New Users to the Domain	Email Tech	✓ None
	~	Customer       Edt Ste       Configure       Smart Tage         Image: Solution of the state of the sta	Customer       Est Ste       Configure       Smat Tage         Image: Solution of the state of the stat

Tip: When you first associate a Cyber Hawk with a Site, the **Cyber Hawk Initial Setup Wizard** will appear. The Wizard will guide you through each step of the Cyber Hawk configuration process.

Continue to the next step in setting up Cyber Hawk: <u>"Configure Cyber Hawk Using the</u> Setup Wizard (Virtual Appliance)" on the facing page.

# Configure Cyber Hawk Using the Setup Wizard (Virtual Appliance)

**Note:** This topic covers how to configure **Virtual Appliance** scans for Cyber Hawk using the Setup Wizard. If you are using the RapidFire Tools Server, see <u>"Configure</u> Cyber Hawk Using the Setup Wizard (RapidFire Tools Server)" on page 213.

**Tip:** See <u>"RapidFire Tools Server vs. Virtual Appliance" on page 247</u> for more info about the difference between the Virtual Appliance and RapidFire Tools Server.

After you have associated the Cyber Hawk with the Site, click on the Cyber Hawk icon:



The **Cyber Hawk Initial Setup Wizard** will appear. This wizard will guide you through the setup process and help you get the most out of your new Cyber Hawk. Click **Next** to begin the set up.

S Cyber Hawk Initial Setup Wizard	×
Welcome	
The Cyber Hawk initial setup wizard will walk you through the initial setup and config performed in this wizard can be accessed in the Cyber Hawk administrative interfac practice of setting up Cyber Hawk scans, policies, notifications, Smart Tags, and ak	guration process at this site. All actions e. This wizard walks through the best erting.
At any time, you may exit the wizard using the [Close] button and resume later. Althuse this wizard to guide you through the initial setup process, you can always configure select "Do not show again for this Site" before exiting the wizard.	ough it is hiqhly recommended to gure Cyber Hawk manually. Simply,
Do not show again for this Site	Back Next Close:

**Tip:** If you need to stop midway through the Cyber Hawk Initial Setup Wizard, don't worry. You can return to the Cyber Hawk screen for your Site and continue where you left off.

**Note:** This section of the guide walks you through the Initial Setup Wizard. This guide also contains seperate topics on configuring Cyber Hawk settings. Refer to these topics if you need to change Cyber Hawk after you have completed the initial set up process using the Wizard.

The steps below break down each part of the configuration process.

**Important:** For best results, the target network must be configured to allow for successful scans on all network endpoints. See <u>"Pre-Scan Network Configuration</u> <u>Checklist" on page 242</u> for configuration guidance for both Windows Active Directory and Workgroup environments.

### Step 1 — Configure Scan Settings

In this step you will configure the Scan Settings for the Cyber Hawk. Click Next.

Q Cyber Hawk Initial Setup Wizard		×
Configure Scan Settings		
Cyber Hawk will perform on-going scans using the settings provided in its Scan Co wizard will walk you through setting specific scan settings, including credentials, tai other options.	nfiguration. The Scan Configuratio rget network, domain, SNMP, and	n
Do not show again for this Site	Back Next Close	

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 <u>"Additional Scan Host</u> Configuration Options and Requirements" on page 239.

- 1. Enter the following information about the Scan Host(s):
  - a. One set of login credentials for all PCs that will serve as scan hosts
  - b. IP Address or Computer Name for the PCs that will serve as scan hosts

c. Domain name (NOT the name of the domain controller)

Scan Configuration Wizard		
Scan Hosts	Scan Hosts	
Merge Option	The values on this page will affect all tasks that require scar	hosts for this Appliance.
Active Directory	Usemame:	
ocal Domains	Password:	
Additional Credentials	Domain:	
Ranges	Scan Host	
NMP Information	chine to enter a new scan bost>	
ile Scanner		
Mware	]	
Initrends Backup	]	
onfirm	]	
	Clear All Scan Hosts	Test Scan Hosts

**Important:** Be sure that the computer you select to be a Scan Host meets the necessary Admin\$, WMI, File and Printer Sharing requirements and their respective firewall settings. The computer must also be operating Windows 8.1 or higher. We recommend that you assign at least two PCs to serve as scan hosts. This will allow scans to run even if one scan host becomes unavailable.

2. Click Test Scan Hosts.

Scan Hosts	Scan Hosts	
Merge Option	The values on this page will affect all tasks that require scan hosts for this Appliance.	
ctive Directory	leemame:	_
ocal Domains	Password:	4
dditional Credentials	Domain:	
<sup>o</sup> Ranges	Scan Host	
NMP Information	where to enter a new scan bests	
ïle Scanner		_
/Mware		
Jnitrends Backup		
Confirm		
		_
	Clear All Scan Hosts Test Scan Hosts	;

A message will appear indicating whether a connection can be established to each scan host. If the connection cannot be established, be sure the scan host meets the requirements – and that you have entered the correct credentials. See <u>"Scan Host Requirements" on page 240</u> for more information.

Test Scan Hosts	×
daedalus-pc: Success	
Close	

Click Next.

- 3. Select how you wish to treat computers that are not associated with Active Directory. You can treat them as:
  - part of the Primary Domain
  - part of a domain that you specify

• or choose not to treat them as part of a domain

💽 Scan Configuration Wizard	-		×
🖌 Scan Hosts	Merge Option		
Merge Option	How do you want to treat computers that are not associated with Active Directory?		
Active Directory	Treat them as part of the Primary Domain (*domain with most computers)		
Local Domains	Treat them as part of the specified domain:		
Additional Credentials	O Don't treat them as part of a domain		
IP Ranges			
SNMP Information			
File Scanner			
VMware			
Unitrends Backup			
Confirm			
	< Back Next >	Car	ncel

4. Enter credentials *with administrative rights* to connect to a Domain Controller with Active Directory. Click **Next** to test a connection with the Domain Controller and verify your credentials.

**Important:** Enter the username in the **domain\username** format. Use the full domain name.

5. If you are scanning a domain, choose whether to scan the entire domain or specific Organizational Units (OUs). Then click **Next**.

💽 Scan Configuration Wizard		-		×
🖌 Scan Hosts	Local Domains			
✓ Merge Option	Below is a list of the detected domains in the current forest of Active Directory.			
<ul> <li>Active Directory</li> </ul>	Gather information for ALL the domains detected.			
Local Domains	Gather information for only the Domains and OUs selected below.			_
Additional Credentials	۳ <u>.</u>			
IP Ranges				
SNMP Information				
File Scanner				
VMware				
Unitrends Backup				
Confirm				
	Expand All Collapse All Expand Selected			
	< Back Next	>	Can	cel

6. If you are scanning a Domain, enter any additional network scan credentials to connect to remote workstations. Then click **Next**.

Scan Configuration Wizard	_	□ ×
🖌 Scan Hosts	Additional Credentials (optional)	
✓ Merge Option	Network scan credentials are required to perform remote Windows data collection via WMI and Remote Registry. Use this screen to optionally add additional credentials to be used during the	
<ul> <li>Active Directory</li> </ul>	scan. Calls using the default credentials will always be attempted first.	
🖌 Local Domains		
Additional Credentials	Network Scan Credentials Usemame:	
IP Ranges	Password:	
SNMP Information	(AD userta he used first)	Add
File Scanner	(AD user to be used link)	
VMware		
Unitrends Backup		
Confirm		
	Clear Al < Back Next >	Cancel

7. From Scan Credentials, optionally add additional credentials to be used during the scan. Then click **Next**.

💽 Scan Configuration Wiz	ard — [	×
🖌 Scan Hosts	Scan Credentials	
✓ Merge Option	Network scan credentials are required to perform remote Windows data collection via WMI and Remote Registry. Use this screen to optionally add additional credentials to be used during the	
Active Directory	scan.	
Scan Credentials		
IP Ranges	Network Scan Credentials	
SNMP Information	Password:	
File Scanner		Add
VMware		
Confirm		
	Clear All	
	< Back Next >	Cancel

 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. Then click Next.

Scan Configuration Wizard			-			×
🖌 Scan Hosts	IP Ranges					_
🖌 Merge Option	Auto-Detected IP Ranges on Remote Appliance					
<ul> <li>Active Directory</li> </ul>	10.					
🖌 Local Domains						
🖌 Additional Credentials	IP Ranges to Scan					
IP Ranges	Single IP or IP Range	Add				
SNMP Information	10.					
File Scanner						
VMware						
Unitrends Backup						
Confirm			E	xclude IP	s	
			Reset to	o Auto-De	etected	j
			Import	from Tex	d File	
			Cle	ar All Entr	ies	
	< Bad	k	Next >		Canc	el

From this screen you can also:

### **RapidFireTools**°

- Click Exclude IPs to remove certain IP ranges from the scan.
- Click Reset to Auto-Detected to reset the automatically suggested IP Range.
- Click Import from Text File to import a predefined list or range of IP addresses.



Important: Scans may affect network performance.

9. A confirmation window will appear estimating the amount of time the scan will take for the designated IP Range. If the scan will take too much time, reduce the size of the IP range. Click **OK**.

Confirm		×
×	You are currently about to scan 256 IP addresses. Large ranges can take long periods of time to complete.	
	Estimated Time: 1 hour(s)	
	Do you wish to continue?	
	OK Cancel	

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

Scan Configuration Wizard	- 0	×
🖌 Scan Hosts	SNMP Information	
🖌 Merge Option	SNMP community strings are used to try to determine information about devices detected during the IP Range scan. Enter any additional community	
Active Directory	strings used on this network.	,
🖌 Local Domains	Read Community String	Add
🖌 Additional Credentials	public	
🖌 IP Ranges		
SNMP Information	Reset to Default Import from Text File Clear All Entries	
File Scanner	Advanced CMMP Options	
VMware	SNMP Timeout (seconds): 10 Use Default	
Unitrends Backup	Attempt SNMP against non-pingable devices (slower but more accurate)	
Confirm		
	< Back Next > Car	ncel

- 11. 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 (HIPPA) 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

Scan Configuration Wizard	-	- 🗆	×
🖌 Scan Hosts	File Scanner		
✓ Merge Option	Perform file scan on: Sunday		
Active Directory	NOTE: File scanning can cause a temporary increase in resource utilization.		
🖌 Local Domains	Scan Types:		
🖌 Additional Credentials	ePHI (HIPAA)		
IP Ranges	Cardholder Data (PCI)		
SNMP Information	Personally Identifiable Information (PII)		
File Scanner			
VMware			
Unitrends Backup			
Confirm			
	< Back Next	> (	Cancel

Then click Next.

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**.

1	VMware (op	tional)				
Scan Hosts	VMware credent	ials are required for	discovery of VMware hosts. E	nter the		
Merge Option	VMware host ser If the server use	rver DNS name or IF s a non-standard ad	address along with VMware I	ogin credentials.		
Active Directory	hostname field in	the format "hostnar	ne port".			
🖌 Local Domains	Hostname or IP	Address	Username			
Additional Credentials			Password			
IP Ranges			Add VM	Iware Server		
SNMP Information						
Eile Seanner	Host	User				
VMware						
Unitrends Backup						
Confirm						
	Clear All En	tries				
				< Back Next >	Ca	ncel

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

**Note:** If you wish, you can use this screen to set up a connection between Cyber Hawk and your Unitrends Backup account. This will allow you to use Unitrends Backup security policies and alerts with Cyber Hawk.

💽 Scan Configuration Wizard		×
🖌 Scan Hosts	Unitrends Backup	
🖌 Merge Option	Enter server and credential information for any Unitrends Backup Servers.	
<ul> <li>Active Directory</li> </ul>	Server: Hostname or IP Address	
🖌 Local Domains	Username:	
🖌 Additional Credentials	Password: Password Add Unitrends Server	
🖌 IP Ranges	10.200	
SNMP Information		
🖌 File Scanner		
🗸 VMware		
Unitrends Backup		
Confirm		
	Clear All Entries Test Connections	
	< Back Next > 0	Cancel

14. Click Test Connection to verify your Unitrends Backup configuration.

Unitrends Test Results	×
qa@10.200. Success	
	ок

- 15. Click **Finish** to save your scan settings.
  - If you are using a **Reporter** appliance, you can also choose whether to upload the finished scans to the Reporter.
  - You can also select **Skip devices with all ports filtered**. Some devices use IPS (Intrusion Prevention Systems) that may prevent the Internal Vulnerability Scan from working as intended. If you know that an IPS is present on the network, select this option to avoid timed-out scans or false positives.

<b>Q</b> Scan Configuration Wizard		-		×
🖌 Scan Hosts	Confirm			
✓ Merge Option	Press Finish to save your settings. Use the Back button to go back and modify			
<ul> <li>Active Directory</li> </ul>	aounga.			
🖌 Local Domains				
🖌 Additional Credentials				
🖌 IP Ranges				
SNMP Information				
🖌 File Scanner	Advanced Options			
🗸 VMware	_			
🗸 Unitrends Backup	Upload finished scan to Reporter			
Confirm				
	Modify Settings < Back	Finish	Car	ncel

**Note: Skip devices with all ports filtered** is only available with the Cyber Hawk Virtual Appliance. It is not available with the RapidFire Tools Server or legacy Detector appliance.

### Step 2 — Schedule Scans and Alert Notifications

In this step you will configure the scanning and alert schedules for Cyber Hawk.



- 1. In the Schedule screen, enter the required information as in the image below:
  - a. Time Zone

- b. **Time for Level 1 Scan (Daily)**: This is the time for the daily Cyber Hawk scan. You can also choose whether to enable or disable the scan. It is Enabled by default.
- c. **Time for Level 2 Scan (Weekly)**: This is the time for the weekly Cyber Hawk scan. You can also choose whether to enable or disable the scan. It is Enabled by default.

**Important:** See <u>"Tips for Scheduling the Level 2 Scan" below</u> for tips on scheduling the scan at the best time to avoid affecting network performance.

- d. **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).
- e. **Weekly Notice**: This is the time that Cyber Hawk will send out a weekly notice to End Users and the Tech Group (default is Monday at 8:00am).

Schedule			×
Time Zone:	(UTC-05:00) I	Eastern Time (US & Canada) 🗸 🗸	
Level 1 Scan (Daily):	01:00 AM		
Level 2 Scan (Weekly):	01:00 AM	Saturday	
Daily Alert:	08:00 AM	🗘 🗹 Mon 🗹 Tue 🗹 Wed 🗹 Thu 🗹 Fri 🗌 Sat 🗌 Sun	
Weekly Notice:	08:00 AM	Monday ~	
		Save Discard	

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

### Tips for Scheduling the Level 2 Scan

Cyber Hawk's Level 2 Scan (Weekly) functionality relies on the use of an Internal Network Vulnerability scanner process to perform this 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:

- Level 2 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.

### Step 3 — Configure Tech Email Groups

In this step you will configure the email addresses and groups of users for your Technician Group. This is the group that will respond to security alerts sent by Cyber Hawk.

You can choose whether to use a pre-existing Global Tech Email Group, or a Site Specific Tech Email Group.

**Note:** If you choose to use a Global Email Group, you can select from among your pre-existing Global Email Groups or create a new one.

If you choose to create a Site-Specific email group, the list of Global Email Groups will be grayed-out.

Later, you can continue to create and edit Global Email Groups from **Preferences** > **Email Groups** at any time. You can also later create and edit site-specific email groups from the Cyber Hawk **Email Configuration** button at your specific Site.

Q Cyber Hawk Initial Setup Wizard	×
Configure Tech Email Groups	
Cyber Hawk can send notifications through email to both technicians and end-users. Email addresses are grouped together in Email Groups allowing for convenient management. Tech Email Groups receive requests through the "Emai Tech" workflow. These are typically notifications that go directly to your internal technicians and not specific end-users for verification.	il
You should always specify at least one Tech Email Group. The group can be global or specific to this site. If you have previously created Global Tech Email Group, you can skip this step.	
Use Global Tech Email Groups	
○ Create Site Specific Tech Email Groups	
🔿 Skip	
Do not show again for this Site Back Next Close	

- 1. Select an option and click Next.
- 2. To select an existing email group, click on a group from the menu and click **Save & Close**.

Add Email Groups  Add Email Group				×
Dolan and Mittel Tech	/ ×	Foosite User Group 💉 X Tech	Global Tech Group Tech	• × ^
Internal IT	/ ×	JD RFT Tech Group - 💉 🗙	JDolan Group	/ ×
<		Tech	1ech	
		Save & Close Discard & Close		

- 3. To add a new email group, click Add Email Group.
- 4. Enter information for the new email group. You will need to add each individual email address for the email group. You can do this by selecting from the list of existing users associated with your account.

Name:       Test User 1         Group Type:       ~         Designated Tech Group:       ~         To <type a="" address="" email="" enter="" new="" to=""></type>	💽 Add Email Group		×
Group Type:       ~         Designated Tech Group:       ~         To <type a="" address="" email="" enter="" new="" to=""></type>	Name:	Test User 1	
To <type a="" address="" email="" enter="" new="" to=""></type>	Group Type:		~
To <type a="" address="" email="" enter="" new="" to=""></type>	Designated Tech Group:		$\sim$
OK Cancel	To	<type a="" address="" email="" enter="" new="" to=""></type>	

#### **RapidFireTools**<sup>®</sup>

5. When you are finished, click **OK**.

### Step 4 — Configure End User Email Groups

Next you will configure the End User Email Group for your site.

**Note:** You cannot create Global End User Email Groups. You can only create site-specific end user email groups.

Over Hawk Initial Setup Wizard	×
Configure End User Email Groups	
End User Email Groups can receive some alert notifications directly. Certain policies are best sen triage purposes. You can setup end-user email groups now or later.	t to end-users first for
Create Site Specific End User Email Groups	
🔿 Skip	
Do not show again for this Site	Next Close:

1. To add a new email group, click Add Email Group.

💽 Add Email Group		Х
Name:	Test User 2	
Group Type:	End User	~
Designated Tech Group:	Test User 1	$\sim$
То	<type a="" address="" email="" enter="" new="" to=""></type>	
$\triangleright$	OK Cancel	

- 2. Enter information for the new email group. You will need to add each individual email address for the email group. You can do this by selecting from the list of existing users associated with your account. You can also type a new email address into the field.
- 3. When you are finished, click **OK**.

#### **RapidFireTools**<sup>®</sup>

4. Next configure how Cyber Hawk will handle Administrative emails. This includes errors related to scans or notifications. Enter the email addresses for the recipient(s) of Administrative emails. Then click **Next**.

Cyber Hawk Initial Setup Wizard	×
Administrative Emails	
Cyber Hawk can be configured to notify you of scan and notification errors. Configure the Admin Email settings below.	
To @rapidfiretools.com	
<type a="" address="" email="" enter="" new="" to=""></type>	
	_
Subject Prefix: %%SITE%%	
2 Snan Failed (eviniant: Innefini - Snan Failed)	
Notification Error (subject: <pre>subject: &lt;</pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre>	
✓ Scan Complete (subject: <pre>cprefix&gt; - Scan Complete)</pre>	
Do not show again for this Site Back Next Close	

5. Enter the configuration information for the email server. Choose whether to use the default configuration or your own custom SMTP server information. Click **Next**.

Q Cyber Hawk Initial	Setup Wizard			×
Email Server				
Cyber Hawk can	use the Default SMTP server securit	ty-bulletins.com or you	Ir own Custom SMTP server.	
Use Default SMTP	Server O Use Custom SMTP Server			
Alert From:	alerts@security-bulletins.com	Display Name:	Security Alerts	
Report From:	reports@security-bulletins.com	Display Name:	IT Security Reports	
Admin Notice From:	admin@security-bulletins.com	Display Name:	NDA1-32WR Admin	
Custom SMTP Settings				
Note: SMTP Server m	ust support TLS 1.2 or above.			
SMTP Server Address:				
Port:	465 🜲			
Security:	None			$\sim$
Usemame:				
Password:				
			Send Test E	mails
Do not show again fo	or this Site		Back Next Cl	ose

Step 5 — Perform Pre-Scan Analysis

Next you will **Perform a Pre-Scan Analysis** on the target network. This will show you any issues with your scan configuration. Click **Next**.



### The Pre-Scan Analysis will begin.

Over Hawk Initial Setup Wizard	×
Prescan Started	
The prescan has started. This typically only takes a few minutes depending on the size of the network.	
An email will be sent to the Administrative Email addresses you specified for this site when the prescan completes.	
Once the prescan completes, come back to this site to complete the Cyber Hawk setup process.	
Do not show again for this Site Back Next Close	

When the Pre-Scan Analysis finishes, the admin will receive an email summarizing any issues identified with your Cyber Hawk scan settings.



#### **RapidFireTools**°

Only one email saying that scan completed successfully	
From: notify@alert-central.com         Sent: Thursday, September 13, 2018 12:20 PM         To:       @rapidfiretools.com>         Subject: CH PreScan SS - sds alerts Scan Completed	
ADMINISTRATOR EVENT	
An administrative event has occured.	
Scan completed successfully.	

If the Pre-Scan Analysis identifies issues with your Cyber Hawk scan configuration, click Modify next to Scan Configuration and make the recommended changes.

Important: For best results, the target network must be configured to allow for successful scans on all network endpoints. See <u>"Pre-Scan Network Configuration</u> <u>Checklist" on page 242</u> for configuration guidance for both Windows Active Directory and Workgroup environments.
#### Step 6 — 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. To initiate the first scan, click **Next**.

Cyber Hawk Initial Setup Wizard	×
Initial Scan	
Before you can complete configuration of this Cyber Hawk, it must first perform its	irst scans.
Press Next to start the initial scan.	Back Next Close

Once the scan is completed, a confirmation message will appear. Click Next.



The scan will be downloaded automatically.

S Cyber Hawk Initial Setup Wizard	×
Downloading Scan	
Download Complete. Press Next to continue.	
Do not show again for this Site	Back Next Close

Click Next when the download is complete.

#### Step 7 — Configure Policies

You will then Configure Policies. In short, this is where you create the "Service Plan" that your MSP will offer to the client.

**Tip:** In the Wizard, you will select from one of several pre-defined service plans. However, you can modify or create your own custom service plan at any time. Tip: See "Using the Service Plan Creator" on page 178.

When you are ready to configure policies, click Next.



The Policy Configuration window will appear. Here you select the exact security policies that Cyber Hawk will enforce on the target network:

Rolicy Configuration	×
Select Policies	Generate
All rade Source     Advances to be readered to reasoned to re	Strictly control DNS on Locked Down Networks Description Charges DIS enties in networks had are bodied own should be strict) charges may indicate other issues including theft and should be investigated.
Stocky Control the Constion of New User Polities Stocky Control the Constion of New User Polities Computers Compute	Required Tags LOCKED DOWN DNS applied to an IP range
Control Sector:     Control Contect Control Contro Control Control Control Control Control Contro	
	Cancel Back Next

- 1. Select from a range of pre-defined service plans: *Bronze*, *Silver*, *Gold*, or *Platinum*. The higher the service level, the more Security Policies will be enforced.
- 2. **Review and select individual security policies from the list** of available policies. Use the check box to select or deselect a policy.
- 3. Click on a policy's name to read a description of that policy.
- 4. **Review the required Smart Tags** needed to enforce the policy (if applicable). Smart Tags help Cyber Hawk enforce security policies on specific PCs or parts of the network (such as an IP range).

5. When you have configured your security policy, click **Generate** to create a Managed Security Services Agreement (MSSA). This is an agreement between you (the MSP) and the client.



6. Enter your custom information for the MSSA.

OMSA Customization		Х
MSP Name:	PerformanceIT ]	
MSP State:	Georgia	
MSP Address:	1117 Perimeter Center West	~
Customer Name:		
Customer Address:	CUSTOMER ADDRESS	~
		$\sim$
Service Plan Monthly Charge (\$):	500	-
Additional Hourly Billing Rate (\$):	150	-
Hours per Month Included:	2	-
Emergency Authorized Limit (\$):	1000	-
Effective Date:	Thursday , March 15, 2018	
	OK Cancel	

7. Review the legal disclaimer.

#### **RapidFireTools**°



8. When you have generated and reviewed your MSSA, click Next.

Note: You can come back and modify the security policy at any time.

#### Step 8 — Configure Notifications

Next you will configure notifications. You can think of these as the "actions" that Cyber Hawk performs when it discovers a possible violation of a security policy.

ky Name	Action	Group Name	
Access Control			
Authorize New Devices to be Added to Restricted Networks	Email Tech	▼ None	
Restrict Access to Accounting Computers to Authorized Users	Email Tech	▼ None	3.
Restrict Access to Business Owner Computers to Authorized Users	Email Tech	▼ None	
Restrict Access to IT Admin Only Restricted Computers to IT Administrators	Email Tech	▼ None	-
Restrict IT Administrative Access to Minimum Necessary	Email Tech	▼ None	-
Restrict Users that are Not Authorized to Log into Multiple Computer Systems	Email Tech	▼ None	-
Strictly Control the Addition of New Local Computer Administrators	Email Tech	▼ None	-
Strictly Control the Addition of New Users to the Domain	Email Tech	▼ None	-
Strictly Control the Addition of Printers	Email Tech	▼ None	-
Computers			
Install Critical Patches on Network Computers within 30 Days	Email Tech	✓ None	-
Network Security			
Only Connect to Authorized Wireless Networks	Email Tech	▼ None	-

- 1. Review the specific **Policy** item.
- 2. Assign an **Action** to the policy item. This can 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



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

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

#### Step 9 — Configure Smart Tags

Next you will deploy **Smart Tags** within the network environment. Smart Tags help Cyber Hawk track behavior on the network in order to enforce the security policy.



#### EXAMPLE:

If a PC on your network should only be accessed by one user, you would assign that PC the *Single Desktop User* Smart Tag. This lets Cyber Hawk know to "lock down" that PC to only that user, and to send alert notifications when another user attempts to access it.

V	Recommended Tags Most common tags recommended for most envir	onments. Double-click to tag items from the latest scan.
	14 Tags GUEST NETWORK IP range	GUEST WIRELESS NETWORK IP range
	RESTRICTED NETWORK IP range	SINGLE DESKTOP USER User

Configure each Smart Tag by double clicking on it. Depending on the Smart Tag, a slightly different configuration screen will open. Below is an example:

ag Explorer										
🏮 si	NGLE DES	KTOP USE	R 1					Save	re & Close Discard &	Close
Applied T	0?		For Wh	at?			Why?			
This tag is app	lied to a User		Users that into other s	have a dedicated ystems directly.	desktop and sh	ould never log	Enhances have beer	detection of anoma n assigned a compu	alies by identifying which users uter.	2
Users			1							
Enter text t	to search			• Clear	3				Filters 4	<u>Clear Al</u>
									Active	<u>Clear Al</u>
Tagger	5 main	Name	Display Name	First	Last	Last Login	Active	Enabled	Ves No.	
				Blake		3/12/2018 1:	Yes	Yes	Enabled	Close M
				Marc		3/14/2018 11	Yes	Yes	Tapped	Clear Al
				chip		3/6/2018 2:0	Yes	Yes		Cicol 74
				D		3/6/2018 1:0	Yes	Yes	No No	
						3/15/2018 12	Yes	Yes	Local Accounts	Clear Al
						3/15/2018 1:	Yes	Yes	Include Local Acco	unts
				James		3/13/2018 10	Yes	Yes		
						2/15/2018 4:	Yes	Yes		
		-		Jabez						
				John		3/14/2018 10	Yes	Yes		
				John Joe		3/14/2018 10 3/15/2018 1:	Yes Yes	Yes Yes		
				John Joe Marianna		3/14/2018 10 3/15/2018 1: 3/14/2018 10	Yes Yes Yes	Yes Yes Yes		
				John Joe Marianna Pablo		3/14/2018 10 3/15/2018 1: 3/14/2018 10 3/14/2018 12 2/14/2018 12	Yes Yes Yes Yes	Yes Yes Yes Yes		

On the Smart Tag configuration screen you can find:

- 1. The name of the smart tag
- 2. A description of the smart tag, including the part of the network environment to which it is applied, its purpose, and the benefit of employing the smart tag
- 3. Search for specific network components to which to assign tags (in this case, users)
- 4. Filter the list of available network components
- 5. Check the box to assign smart tags to specific network components

The Wizard will present you with a list of recommended smart tags to deploy within the network based on the specific Security Policies you decided to enforce in the earlier step.

When you have assigned all recommended smart tags to network components, click **Next**.

**Tip:** See the section <u>"Smart Tags" on page 156</u> in this guide for more detailed information.

#### Step 10 — Set Up RapidFire Tools Portal

Congratulations! You've configured Cyber Hawk on the target network! Your End Users and Tech Group will now receive daily alerts whenever Cyber Hawk discovers suspicious activity on the network.

**Now it's time to set up the RapidFire Tools Portal**. The Portal is where your endusers and technicians respond to alerts sent out by Cyber Hawk to enforce the security policy. It is also used to configure branding and integrate with your preferred ticketing system/PSA.

Click Close to dismiss the Cyber Hawk Initial Setup Wizard.



See these topics to set up the RapidFire Tools Portal:

- <u>"Set Up and Assign a Ticketing/PSA System Integration to a Site Using Cyber</u> Hawk" on page 98
- "Set Up Portal Branding" on page 128
- "Set Up a Custom Subdomain to Access the RapidFire Tools Portal" on page 134
- "Set Up Custom SMTP Server Support" on page 137

#### **RapidFireTools**<sup>®</sup>

## Provisioning Additional Cyber Hawk Appliances for Deployment

With Cyber Hawk, you have the ability to self-provision and deploy an unlimited number of Cyber Hawk Appliances using the RapidFire Tools Portal. If you wish to provision and set up your sites using Network Detective instead, see <u>"Provisioning Additional Cyber Hawk Appliances for Deployment (Classic)" on page 46</u>.

Follow these steps to provision a Cyber Hawk Appliance:

- 1. Run Network Detective and log in with your credentials.
- 2. Select the **Appliance** icon on the ribbon bar.



The Appliances window will be displayed.

3. Select the **Provision Cyber Hawk** button to begin the Cyber Hawk provisioning process.



The Provision Cyber Hawk window will be displayed.

👤 Provision new Cyber Hawk		>
To provision a new Cyber Hav	vk site, log into the YourITPortal and selec	ct Add Site.
For Non-EU customers: For EU customers:	https://secure.youritportal.com https://secure.youritportal-eu.com	
		Classic Provisioning
	Cancel	

- 4. Access the RapidFire Tools Portal and log in to create a site and continue the provision process.
  - If you are a non-EU customer, click https://secure.youritportal.com.
  - If you are an EU customer, click https://secure.youritportal-eu.com.
- 5. Log in to the Portal and click **Add Site**. Continue provisioning the new Site in the Rapid Fire Tools Portal.

🖷 < 🧧 RapidFire Tools Portal X +	$\vee$		-		×
$\leftrightarrow$ $\rightarrow$ O $\textcircled{a}$ $\textcircled{https://secure.y}$	puritportal.com/login	□ ☆ 1	¢≡ <i>l</i> ~	È	
Kaseya	unitportal.com/login RapiclFireTools Welcome Back @rapidfiretools.com			K	
	соруну	it © 2019 Raseya Linned   Heij	r & Suppor	v.De	` v

	@ @	IT Pro Ҟ
Discovery Agents	Move Sit	te + Add Site

Tip: Once you create the new Site, the new Cyber Hawk appliance will be provisioned automatically. However, you will still need to install it.

**Note:** See the <u>Cyber Hawk Web Console User Guide</u> for complete instructions on using Cyber Hawk for all of your sites completely within the RapidFire Tools Portal.

# Provisioning Additional Cyber Hawk Appliances for Deployment (Classic)

With Cyber Hawk, you have the ability to self-provision and deploy an unlimited number of Cyber Hawk Appliances. Use this process to provision a new appliance if you do not wish to use the RapidFire Tools Portal to create the new appliance.

Follow these steps to provision a Cyber Hawk Appliance:

- 1. Run Network Detective and login with your credentials.
- 2. Select the Appliance icon on the ribbon bar.



The Appliances window will be displayed.

3. Select the **Provision Cyber Hawk** button to begin the Cyber Hawk provisioning process.



The Provision Cyber Hawk window will be displayed.

If you wish to provision a Cyber Hawk without using the RapidFire Tools Portal to create a site, click **Classic Provisioning**.

Appliance Type	Site Name	Activated	Running Tasks	Qu
Reporter		Activated	0	0
Audit Guru		Not activated	0	0
Audit Guru		Not activated	0	0
Reporter	Provision new Cyber Hawk		×	0
Reporter			~	0
Cyber Hawk SDS	To provision a new Cyber Hawk site, log into the YourlTPortal and select Add Site.			-
Reporter				0
Cyber Hawk SDS				0
Reporter	For Non-EU customers: <u>https://secure.youritportal.com</u>			0
Reporter				0
Reporter	For EU customers: https://secure.youritportal-eu.com			0
Cyber Hawk SDS	Clas	sic Provisionina		0
Reporter				0
Audit Guru	Cancel			0
Cyber Hawk SDS				0
Cyber Hawk SDS	Detect Suspicious Behavior 2 (remote)	Activated	0	0
All	Detect Suspicious Behavior for Linux (remote)	Activated	0	0
All	Detect Suspicious Behavior for RFTS (remote)	Activated	0	0
All	Detect Suspicious Behavior for Windows (remote)	Activated	0	0

4. Select the number of Cyber Hawk you want to activate and select the OK button to continue.

Q Provision Cyber Hawk		
Number of Cyber Hawks to Activate: 1		
OK Cancel		

The Cyber Hawk Provisioned window will be displayed to indicate that the Cyber Hawk(s) have been provisioned for use.



5. Select the OK button to view the newly provisioned Cyber Hawk in the Appliances window.

The newly provisioned Cyber Hawk will be displayed in the Appliances window and provisioned as Not Activated.

Appliances Appliance Override:			Down	nload Logs Manage Scans	Manage Reports	Health Check	Maintenar	nce	
( An	Appliance ID	Type	Appliance Type	Site Name			Activated	٠	Т
	O NDA1-	Virtual	Cyber Hawk				Activated		-
All Appliances	NDA1	Virtual	Cyber Hawk				Not activate	ed	-

**RapidFireTools**<sup>®</sup>

6. To complete the Cyber Hawk Activation process, go to <u>www.rapidfiretools.com/nd</u> and download and install the Cyber Hawk Virtual Appliance on a Hyper-V or VMware enabled computer operating within your client's network.

**Note:** For more information about installing the Virtual Appliance, please download the <u>Virtual Appliance Installation Guide for Cyber Hawk</u>.

## Provisioning Additional Detector Legacy Appliances for Deployment

**Note:** Note that this workflow is currently in the process of being phased out in favor of new functionality. See <u>"Provisioning Additional Cyber Hawk Appliances for</u> <u>Deployment" on page 44</u> for instructions on the new workflow.

Follow these steps to provision a Legacy Detector Appliance:

- 1. Run Network Detective and login with your credentials.
- 2. Select the **Appliance** icon on the ribbon bar.

💽 Network De	tective		
			- <u>-</u>
Home	InForm	Appliances	Connector

The Appliances window will be displayed.

3. Select the **Provision Legacy Detector** button to begin the appliance provisioning process.



The Provision Legacy Detector window will be displayed.

4. Select the number of Detectors you want to activate, select the Authorization check box, and select the OK button to continue.



The Detector Provisioned window will be displayed to indicate that the Detector(s) have been provisioned for use.

**RapidFireTools**<sup>®</sup>



5. Select the OK button to view the newly provisioned Detector in the Appliances window.

The newly provisioned Detector will be displayed in the Appliances window and provisioned as Not Activated.

Appliances	Appliance Override:		Dow	nload Logs Manage Scans	Manage Reports	Health Check	Maintenan	nce
( An	Appliance ID	Type	Appliance Type	Site Name		A	ctivated	* T
-	O NDA1-	Virtual	Cyber Hawk			A	ctivated	-
Al Appliances	MDA1	Virtual	Cyber Hawk			N	ot activate	sd -

6. To complete the Detector Activation process, go to <u>www.rapidfiretools.com/nd</u> and download and install the Detector Virtual Appliance on a Hyper-V or VMware enabled computer operating within your client's network.

**Note:** For more information about installing the Virtual Appliance, please download the Virtual Appliance Installation Guide for Cyber Hawk.

## 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	<ol> <li>Send your technicians an <i>Alert Notification</i> directing them to investigate the issue.</li> <li>Create an Alert item in the Portal.</li> </ol>
2. Email End User	<ol> <li>Send an <i>End User Alert Notification</i> to End User(s) in your client's company.</li> <li>The End User can then decide how your technicians respond to the Alert. End Users can direct your company's technicians to:         <ul> <li><i>Investigate the Alert</i>. The Tech Group will then receive an Alert Notification, and an Alert item will be created in the Portal.</li> <li><i>Set up an Ignore Rule</i> 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.</li> </ul> </li> </ol>
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 Using Cyber Hawk" on page 98.
4. None	Take no action.

#### **RapidFireTools**<sup>®</sup>

### 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, click the Cyber Hawk icon to open the Cyber Hawk management screen.



2. If necessary, click the chevron button **I** to expand the **Notification Rules** panel.



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

O Add Email Group	Σ
Name:	Your Client Company Group
Group Type:	End User 🔹
Designated Tech Group:	Cust A - Tech Team 💌
To	business.owner @yourclientcompany.com
	OK Cancel

Enter the email addresses for the End User Group. Click **To...** to select from users assigned to your Network Detective account. You can also type in the addresses manually. Click **OK**.

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.

Action	Group Name
	A
Email Tech	Cust A - Tech Team 🔹
Email Tech	Cust A - Tech Team 🔹
Email Tech	Cust A - Tech Team 🔹
None	None
None	Cust A - Tech Team 🔹
Email End User	Cust A - Tech Team 🔹
Create Ticket	Cust A - Tech Team 🔹
Email Tech	Cust A - Tech Team 🔹

**Note:** The list of policy names displays the list of security policies currently being enforced at the Site. To modify the policy configuration, see <u>"Edit Policies</u> <u>Enforced at a Site" on page 251</u>.

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

Action	Group Name	
		*
Email Tech	r Cust A - Tech Team 🔻	
Email Tech	r Cust A - Tech Team 🔻	
Email Tech	r Cust A - Tech Team 🔹	
Email End User	r Customer A	
Email Tech	Customer A	Ш
Email Tech	Your Client Company Group	J
Email Tech	r Cust A - Tech Team 🔻	
Email Tech	r Cust A - Tech Team 🔹	

#### **RapidFireTools**<sup>®</sup>

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.
<ul> <li>myclientsnetwork.com\dc09</li> <li>mcn\rsmith</li> </ul>
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?
Yes No

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, click the Cyber Hawk icon to open the Cyber Hawk management screen.



2. If necessary, click the chevron button loss to expand the **Notification Rules** panel.



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 ).

💽 Add Email Group		×
Name:	Example Tech Group	
Group Type:	Tech	$\sim$
Designated Tech Group:		$\sim$
To	<type a="" address="" email="" enter="" new="" to=""></type>	
	OK Cancel	

Enter the email addresses for the Tech User Group. Click **To...** to select from users assigned to your Network Detective account. You can also type in the addresses manually. Click **OK**.

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.

Action		Group Name	
Email End User	•		•
Email Tech	•		•
None		None	•
Email End User		None	•
Create Ticket		None	•
Email Tech	Ŧ	None	•
Email Tech	•	None	•

**Note:** The list of policy names displays the list of security policies currently being enforced at the Site. To modify the policy configuration, see <u>"Edit Policies</u> <u>Enforced at a Site" on page 251</u>.

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

Action		Group Name		
Email End User	•		•	
Email Tech	-		•	
Create Ticket	•	Global Tech Group	٠	l
Create Ticket	•	Internal IT		
Create Ticket	•	My MSP Technicians New Group Global		
Email Tech	•			
Email Tech	•		U	
			*	

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

## 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. Run Network Detective and log in with your credentials.
- 2. Open your Site associated with your Cyber Hawk and view the Cyber Hawk Settings.
- 3. Select the **View Ignored Alerts** button located on the Daily Alerts bar in the Cyber Hawk Settings window.



4. The Ignored Alerts window will be displayed.

Alert Type	Alert Details	Ignored Recipient
New profile		All recipients
New profile		All recipients
New profile (Business Owner's comp	uter)	All recipients
Critical patches not applied timely		
Critical patches not applied timely		
Critical patches not applied timely		
Critical patches not applied timely		
Unusual logon time by user		
Unusual logon time by user		
Unusual logon time by user		
Unusual logon time by user		
New High Severity Internal Vulnerab	ity 1.3.6.1.4.1.25623.1.0.807574	
New profile (Business Owner's comp	uter)	

5. Select the X icon next to the Ignore Alert rule that you would like to delete.

Alert Type	Alert Details	Ignored Recipient
New profile	Select the X to Disable the Ignore	Al recipients
New profile	Alert Rule after you Save and Close	All recipients
New profile (Business Owner's computer)	the ignored wents window	Al recipients
Critical patches not applied timely		
Critical patches not applied timely		
Critical patches not applied timely		
Critical patches not applied timely		
Unusual logon time by user		
Unusual logon time by user		
Unusual logon time by user		
Unusual logon time by user		
New High Severity Internal Vulnerability	1.3.6.1.4.1.25623.1.0.807574	
New profile (Business Owner's computer)		
	Save & Oten Decard & Oten	

- 6. Selected Ignore Alert rules will be grayed out indicating that these rules will be deleted after the Alert Rule settings are saved.
- 7. After selecting the Ignore Alert rules that you want to delete, select the **Save & Close** button in the Ignored Alerts window.

🖲 lgi	rored Alerts		×
	Alert Type	Aiert Details	Ignored Recipient
3	New profile		All recipients
$\odot$	New profile		All recipients
Θ	New profile (Business Owner's computer)		All recipients
$\odot$	Critical patches not applied timely		
0	Critical patches not applied timely		
0	Critical patches not applied timely		
3	Critical patches not applied timely		
0	Unusual logon time by user		
Θ	Unusual logon time by user		
$\odot$	Unusual logon time by user		
Θ	Unusual logon time by user		
3	New High Severity Internal Vulnerability	1.3.6.1.4.1.25623.1.0.807574	
$\odot$	New profile (Business Owner's computer)		
		Save & Close Discard & Close	

## 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
Security Issues - Week over Week

To configure Weekly and Monthly Security Alert Summaries:

- 1. Open Cyber Hawk from your Site.
- 2. Click Email Configuration.
- 3. Click the **Summary Emails** tab.



4. Choose whether to enable **Weekly** and **Monthly** Summaries. Select the Recipient Email Group from the **To:** drop down menu.

#### **RapidFireTools**°

SMTP Serve	Email Groups	Email Subjects	Summary Emails	]	
	Entail Groups	Email Subjects			
- Weekly Sum	mary				
Summary of a	lerts and changes	sents every week (	on Moanday at 8 A	М.	
Enabled					
To: -I	Please Select -			•	
Subject:					
	Send Now				
Monthly Sun	mary				
Summary of a	lerts and changes	sents every month	on the first day of t	he month at 8 A	М.
· ·	-				
Enabled					
Enabled					
To:	Please Select -			•	
To: - Subject:	Please Select -			•	
To: Subject:	Please Select - Send Now			•	
To: -	Please Select - Send Now			•	
To: Subject:	Please Select -			•	

- 5. Enter a **Subject** line for the email.
- 6. Click Save & Close.

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)

#### What's in the Cyber Hawk Alert Summaries?

Group security policy changes

Network changes (such as the addition of new devices)

#### **RapidFireTools**\*

## Security Policy Details

The table below documents each Security Policy, including the <u>"Smart Tags" on page 156</u> 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;

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 Usersauthorized 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       Notify if users account is promoted to Administrator access rights         Access to Minimum Necessary       Notify if users account is promoted to Administrator access rights		n/a	n/a
Restrict Users that are Not       Notify if a user logs into more than one computer         Authorized to Log into Multiple       Computer Systems		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

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)	Investigate all backup failures (Unitrends)Notify if Unitrends server backup fails (requires Unitrends credentials in scan configuration)		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

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

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

## 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 <u>"Security Policy</u> <u>Violation Alert Notification Rule Actions" on page 51</u>.)

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 <u>"Set Up and Assign a Ticketing/PSA System</u> Integration to a Site Using Cyber Hawk" on page 98.
- 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.

## 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 Network Detective Site that is used to manage your Cyber Hawk Appliance.

**Note:** To learn more, see <u>"Set Up and Assign a Ticketing/PSA System Integration to a</u> <u>Site Using Cyber Hawk" on page 98</u>.

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.

Cyber Hawk 📏	Alerts				
Alerts 141	Q Search		To Do	*	All
Status 🌲	Date 🖨	Message 💠			
Ticket	7/19/19, 6:05 AM	A user that typically uses only one computer t	vas found to have logged into	multiple sy	stems.
Ticket	7/19/19, 6:05 AM	A user that typically uses only one computer t	vas found to have logged into	multiple sy	stems.
Ticket	7/19/19, 6:05 AM	Unauthorized access to a computer in the Car	dholder Data Environment (CE	DE).	
Ticket	7/19/19, 6:05 AM	Unauthorized access to a computer in the Car	dholder Data Environment (CC	DE).	
Ticket	7/19/19, 6:05 AM	Unauthorized access to a computer in the Car	dholder Data Environment (CI	DE).	

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.

Ticke	This alert was sent to the ticketing system. You may also create a To Do item from it.
8	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 enterpu backup solution.
Alert	Object(s)
D AP	P01 )

## 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.



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

RapidF	ireTools <sup>®</sup>
Username	
Password	Forgot Password?
Remember me	
L	og in
	Or
Ҡ Log in	with KaseyaOne
Learn More a	bout KaseyaOne

After you log in, the Alert Item will appear.

Cyber Hawk > Alerts > Details	
Investigate Please investigate and remediate if required.	Additional Information
Attempted access of system restricted to IT administrators only by a non-IT	History
admin.	Recommended Response Plans *
Verify the user should have access to the IT Admin Only restricted system. If they should, properly tag the user as an IT Admin.	Non Admin Access Alert
Select the items to act on below:	
testcom/desktop-f0	
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 TiterRaw (Sensice Board: Help Desk)	
NO OP (Debug Only)	
at Submit Action a Mark Complete	
and mark complete and take no action	
Constant and this alter for the selected items again Optive completely).     Crasts a fourt in TypePrev Greek Backet Help Desk     No OP (Debug Chip)     More Anton     Select Complete     Mark Complete     Mark Complete     Mark Complete     Mark Complete	

**RapidFireTools**<sup>°</sup>

**Note:** Click I 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.	Additional Information
Attempted access of system restricted to IT administrators only by a non-IT	History
admin.	Recommended Response Plans *
Verify the user should have access to the IT Admin Only restricted system. If they should, properly tag the user as an IT Admin.	F Non Admin Access Alert
Select the items to act on below:	
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)	
Schrötzgrung:	-

- 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.

ction(s):	
Add "IT ADMIN" tag to the Do not send this alert for Create a ticket in TigerPa	he Users selected above. r the selected items again (ignore completely) aw (Service Board: Help Desk)
Submit Action	Mark Complete

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.		
	Back	Confirm

A confirmation message will appear.

ОК		
Your	changes have bee	en processed.
<b>&gt;</b>	Continue	

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

To Do <mark>1315</mark>	Q Search		All Items
Action \$	Date ¢	Site ¢	Message \$
Complete	<del>2/26/19, 3:44 PM</del>	New-CyberHawk Site	Install Cyber Hawk
Complete	2/26/19, 12:53 PM		Configure Smart Taga
Complete	2/26/19, 12:53 PM		Configure Policies and Notifications
Complete	2/26/19, 12:50 PM		Perform Initial Sean
Complete	2/26/19, 12:35 PM		Review Pre-sean Analysis Results and Recommendations

#### 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:

<b>B</b> A	
	Attempted access of system restricted to IT administrators only by a non-IT admin.
V	- /erify the user should have access to the IT Admin Only restricted system. If they should, properly tag the user as an IT Admin.
elect th	e items to act on below:
🕑 🖵 t	test
	test comv
	test test'
ction(s):	test test
Ction(s): Add "I	T ADMIN" tag to the Users selected above.
Ction(s): Add "I" Create	TADMIN" tag to the Users selected above.       send this alert for the selected items again (ignore completely).       a ticket in TigerPaw (Service Board: Help Desk)

- 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.

**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:

Inve	sligate Please investigate and remediate if required.
6	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.j t.com\desktop-
	J test. i .com/desktop-
Action(	J test,com\desktop
Action(	test, .com\desktop-
Action(	
Action( Add	
Action( Add Ren Dor Creat	

- 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.

#### #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 T system.	his alert has not been proce			
		essed. You may convert it int	o a To Do item, or send it strai	ght to your ticketing
Ð	New medium severity inte Medium severity vulnerabilitie possible.	rnal vulnerabilities were fo	und. network security and should be a	iddressed as quickly as
Alert Obj	ject(s)			
CVSS: 4	.3 - SSL/TLS: Report Weak Cip	oher Suites (1.3.6.1.4.1.25623.1	.0.103440)	view details

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)	
Action(s): Do not send this alert for the selected items again (ignore completely).	
🛪 Submit 🗸 Mark Complete	
	-
Diagnostic details will appear as a result of the Cyber Hav	/k scan. This includes

A Medium CVSS: 5	OID: 1.3.6.1.4.1.25623.1.0.10736	Port: 135 / tcp	
NVT Name			
Summary	numeration Reporting		
Distributed Computing Environ host can be enumerated by com	nment / Remote Procedure Calls (DCE/RPC) or nnecting on port 135 and doing the appropri	MSRPC services running on the remote ate queries.	
Affected Nodes			
Impact			
An attacker may use this fact	t to gain more knowledge about the remote h	ost.	
Controll			
Filter incoming traffic to the Vulnerability Detection Result Here is the list of DCE/RPC of	nis ports. or MSRPC services running on this host via	the TCP protocol:	
Filter incoming traffic to the Vulnerability Detection Result Here is the list of DCE/RPC of Port:	nis ports. or MSRPC services running on this host via Je	the TCP protocol:	
Filter incoming traffic to the Vulnerability Detection Result Here is the list of DCE/RPC of Port: . Name of issue . Issue summ	ns ports. or MSRPC services running on this host via Le ary	the TCP protocol:	
Filter incoming traffic to the Vulnerability Detection Result Here is the list of DCE/RPC / Port: Name of issue Issue summ Affected Noo	ue ary des	the TCP protocol:	
Filter incoming traffic to the Vulnerability Detection Result Here is the list of DCE/RPC / Port: Name of issue Issue summ Affected Noo Impact	ue ary des	the TCP protocol:	
Filter incoming traffic to the Vulnerability Detection Result Here is the list of DCE/RPC / Port: Name of issue Issue summ Affected Noo Impact Proposed So	ue ary des	the TCP protocol:	

# 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.



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.

0	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.	Recommended Response Plans                                   Image: The set of the set
- -	and the second sector of the	
Notes (Optio	onal)	
Q R	equest Investigation	

**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.



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



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

## 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.



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**.



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.



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



## 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.



**RapidFireTools**°

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

RapidFireTools				
Username				
Password	Forgot Password?			
Remember me				
Lo	og in			
	Or			
K Log in	with KaseyaOne			
Learn More al	bout KaseyaOne			

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



**Note:** Click I 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:
  - 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:



- 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.



#### **RapidFireTools**\*

**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.
- 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.		
	Back	Confirm

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

ОК		
Your	hanges have bee	en processed.
<b>&gt;</b>	Continue	

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

To Do 1315	Q Search		All Items 🔹 🗌 Hide Related
Action ¢	Date ¢	Site ‡	Message ¢
Complete	2/26/19, 3:44 PM	New GyberHawk Site	Install Cyber Hawk
Complete	<del>2/26/19, 12:53 PM</del>		Configure Smart Tags
Complete	2/26/19, 12:58 PM		Configure Policies and Notifications
Complete	<del>2/26/19, 12:50 PM</del>		Perform Initial Sean
Complete	<del>2/26/19, 12:35 PM</del>		Review Pre-sean 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.

Alerts	85
How Long Do Alerts Last in the Portal?	86
View and Process Alerts	86
Alert Item Statuses	87
Filter Alert Queue by Status	89
Revert Completed Alerts Back to the To Do Items	90
To Dos	94
How Long Do To Do Items Last in the Portal?	95
View and Process To Dos	
Create To Do Items from Alerts	96
Set Up and Assign a Ticketing/PSA System Integration to a Site Using Cyber Hawk	98
Step 1 — Gather Credentials and Set Up your PSA System	98
Step 2 — Set Up a Connection to your Ticketing System/PSA	99
Step 3 — Map your Cyber Hawk's Site to a Ticketing System/PSA Connection	105
Set Up Autotask Integration	108
Set Up Autotask (SOAP) Integration	111
Set Up ConnectWise REST Integration	116
Set Up ConnectWise SOAP Integration	. 125
Set Up Kaseya BMS Integration	127
Set Up Portal Branding	128
Set Custom Portal Theme	130
Set Custom Portal Subdomain	131
Set Custom Company Name	132
Set Custom Company Logo	133
Set Up a Custom Subdomain to Access the RapidFire Tools Portal	134
Set Up Custom SMTP Server Support	137
Allow Clients to Access Portal and Manage Tickets	140
Step 1 — Create Site Restricted User in Portal	140
Step 2 — Assign User to Site	141
Step 3 — Assign User to Technician Role	142

Manage Users (Global Level)	
Users and Global Access Roles	
Add User at Global Level	
Edit User at Global Level	
RapidFire Tools Portal Site Roles	
RapidFire Tools Portal Site Roles Manage Site Data Collectors	

## Alerts

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



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.

Darrien Site								
=		Cyber Hawk 💙 J	Alerts					
A Home	~	Alerts 185	Q. Search		All Alerts	*	Past 7 Days	•
InDoc	~							
Cyber Hawk	^	Status 💠	Date ‡	Message ¢				
🔲 To Do		Complete	7/11/19, 10:40 PM	A user that typically uses only one comput	er was found to have logger	d into multipl	e systems.	
Alerts		To Do	7/11/19, 10:41 PM	Unauthorized access to an accounting con	aputer.			
<ul> <li>Smart Tags</li> <li>Settings</li> </ul>	~	Complete	7/11/19,10:41 PM	Unauthorized access to an accounting con	aputer.			
Audit Log		To Do	7/11/19, 10:41 PM	Unauthorized access to an accounting com	iputer.			
		To Do	7/11/19, 10:41 PM	Unauthorized access to an accounting con	iputer.			
		Complete	7/11/19, 10:41 PM	Unauthorized access to an accounting com	nputer.			
		Complete	7/11/19, 10:41 PM	Unauthorized access to an accounting com	aputer.			

#### **RapidFireTools**°

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 89
- <u>"Create To Do Items from Alerts " on page 96</u>
- "Revert Completed Alerts Back to the To Do Items" on page 90

### View and Process Alerts

To view and process Alert items:

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

RapidF	-ireTools'
Username	
Password	Forgot Password
Remember me	
L	.og in
	Or
Ҟ Log in	with KaseyaOne
Learn More a	about KasevaOne

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

Darrien Site	
≡	Cyber Hawk 📏 Alerts
👚 Home 🗸 🗸	Alerts 185 Q Sear
🗄 InDoc 🗸 🗸	
Cyber Hawk	Status 🗢 🛛 Date 🖨
📃 To Do	New 7/18/19
🛕 Alerts	New 7/18/19
Smart Tags	
Settings 🗸 🗸	New 7/18/19
Audit Log	<b>New</b> 7/18/19

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

Cyber Hawk 📏	Alerts					
Alerts 185	Q Search		All Alerts	*	Past 7 Days	*
Status 🖨	Date 💠	Message \$				
To Do	7/16/19, 6:05 AM	Unauthorized access to a computer containing	ePHI.			
To Do	7/16/19, 6:05 AM	Unauthorized access to a computer containing	ePHI.			
To Do	7/16/19, 6:05 AM	Unauthorized access to a computer containing	ePHI.			
To Do	7/16/19, 6:05 AM	Unauthorized access to a computer containing	ePHI.			
To Do	7/16/19, 6:05 AM	Unauthorized access to a computer containing	ePHI.			
To Do	7/16/19, 6:05 AM	Unauthorized access to a computer in the Car	dholder Data Environment (G	CDE).		
To Do	7/16/19, 6:05 AM	Unauthorized access to a computer in the Car	dholder Data Environment ((	CDE).		

## Alert Item Statuses

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

These statuses are:



**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.

## Filter Alert Queue by Status

1. Select the Alerts view.



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

Cyber Hawk 义	Alerts						
Alerts 185	Q. Search		All Aler	rts	•	Past 7 Days	*
			All Al	erts			
Status 🖨	Date \$	Message \$		New			
To Do	7/16/19, 6:05 AM	Unauthorized access to a computer containing	ge 📕 1	Fo Do			
			<b>E</b>	End User			
To Do	7/16/19, 6:05 AM	Unauthorized access to a computer containing	;e	Complete			
To Do	7/16/19, 6:05 AM	Unauthorized access to a computer containing	;e 🔳 1	licket .			
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

#### Status you selected.

Cyber Hawk 🗦	Alerts		
Alerts 31	Q Search	End User - All	*
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.	
End User	7/8/19, 6:18 PM	Attempted access of system restricted to IT administrators only by a non-IT admin.	
End User	7/8/19, 6:18 PM	Attempted access of system restricted to IT administrators only by a non-IT admin.	
End User	7/8/19, 6:18 PM	Attempted access of system restricted to IT administrators only by a non-IT admin.	
End User	7/8/19, 6:18 PM	Attempted access of system restricted to IT administrators only by a non-IT admin.	
End User	7/8/19, 6:18 PM	Attempted access of system restricted to IT administrators only by a non-IT admin.	

## 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:

1. Select the **Alerts** view.

Darrien Site	
≡	Cyber Hawk 义 Alerts
A Home	✓ Alerts 185 Q Sear
InDoc	~
Cyber Hawk	∧ Status ≎ Date ≎
🔲 To Do	New 7/18/19
🛕 Alerts	New 7/18/19
Smart Tags	
Settings	New 7/18/19
Audit Log	New 7/18/19

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

Cyber Hawk 🗦	Alerts	
Alerts 15	Q Search	Complete 👻
Status 🗢	Date 🜩	Message \$
Complete	7/19/19, 6:05 AM	Unauthorized access to a computer in the Cardholder Data Environment (CDE).
Complete	7/19/19, 6:05 AM	Unauthorized access to a computer in the Cardholder Data Environment (CDE).
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

#### **RapidFireTools**°

yber H	awk > Alerts > Details
	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.
Aler	t Object(s)
້ <b>.</b> ງ	test\ Revert

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

Alert Object(s)	
<b></b> ♀ ♀	
C Revert	

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.

Ð	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.
lect	the items to act on below:
lect	the items to act on below: I test.performanceit.com\desktop-f0m1o27 L test\dadmin
elect	the items to act on below: test.performanceit.com\desktop-f0m1o27 test\dadmin
lect	the items to act on below:  I test.performanceit.com\desktop-f0m1o27  test\dadmin  PCI / CDE AUTHORIZED USER" tag to the Users selected above.
tion(s	the items to act on below:  I test.performanceit.com\desktop-f0m1o27  test\dadmin  : : "PCI / CDE AUTHORIZED USER" tag to the Users selected above. ove "PCI / CDE COMPUTER" tag from the Computers selected above.

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

#### **RapidFireTools**\*

## To Dos

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

To Do	11	
<b>T</b> Filter	All Items 🔹	Search
Action	Date	Message *
Investigate	3/17/2018, 12:00 PM	Unauthorized access to a computer containing ePHI.
Investigate	3/20/2018, 12:00 PM	New device found on a restricted network.
Investigate	3/20/2018, 12:01 PM	DNS record added on Locked Down network.
Investigate	3/30/2018, 12:01 PM	Computer that should not have direct Internet access not properly restricted.

**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.

RapidFireTools		Organizations					
Home	) V	Granite Partne	Granite Partners				
To Do		Ace Group / Granite Pa	artners / Cyber Hawk / To Do				
Alerts Smart Tags		To Do 13 Q Search All Ite			All Items 🗸		
Settings		Action $\diamondsuit$	Date 🔷	Message 🌲			
🗟 Audit Log		Investigate	01-Mar-2024, 9:01 PM	Unauthorized connection to a wir KaseyaWireless	eless network.		
		Investigate	01-Mar-2024, 9:01 PM	Unauthorized connection to a wir itswifi 2.4	eless network.		

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 <u>"Set Up Tech Group Alert Notifications" on page 55</u>)
- 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 <u>Set Up End</u> <u>User Alert Notifications</u>)

Note: End Users do not receive To Dos.

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 <u>https://www.youritportal.com</u> and log into the RapidFire Tools Portal using your login credentials.

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

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

RapidFireTools		Organizations		
Home	) _	Granite Partne	rs	
To Do		Ace Group / Granite P	artners / Cyber Hawk / <b>To Do</b>	
Alerts Smart Tage		To Do 13	Q Search	All Items 🗸
Settings	Settings		Date 🔶	Message ≑
💼 Audit Log		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.

#### **RapidFireTools**<sup>®</sup>

## 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".

Cyber Hawk > Alerts							
Alerts 34	Q Search		New	•			
			New				
Status \$	Date 🗢	Message ¢	To Do				
New	7/22/19, 6:04 AM	Backup all Windows servers (Unitrends).	End User				
			Complete				
New	7/22/19, 6:04 AM	Backup all Windows servers (Unitrends).	Ticket				
New	7/22/19, 6:04 AM	Backup all Windows servers (Unitrends).	Task				



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



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							
🔚 Create To Do 🔲 🖼 Create Ticket							

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.

# Set Up and Assign a Ticketing/PSA System Integration to a Site Using Cyber Hawk

To successfully configure the Autotask, ConnectWise, or Tigerpaw 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 Login Credentials for Network Detective
- A Network Detective "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 Network Detective with multiple PSA accounts, gather credentials for each PSA account)
- Other prerequisites specific to your chosen PSA system (refer to the table below)

Tip: If you're having trouble, see the **Appendices** section in the <u>Network Detective</u> <u>User Guide</u> for more detailed information on how to configure your PSA to integrate with RapidFire Tools products.

PSA System	PSA Prerequisites
Autotask	<ul> <li>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.</li> <li>Autotask Username</li> <li>Autotask Password</li> </ul>

PSA System	PSA Prerequisites
SOAP (Deprecated)	<ul> <li>Autotask API Username</li> <li>Autotask API Password</li> </ul>
REST Connec+Wise	<ul> <li>ConnectWise REST Public Key</li> <li>ConnectWise REST Private Key</li> <li>ConnectWise Company ID</li> <li>ConnectWise PSA URL</li> </ul>
SOAP Connec+Wise™	<ul> <li>ConnectWise Username</li> <li>ConnectWise Password</li> <li>ConnectWise Company ID</li> <li>ConnectWise PSA URL</li> </ul>
Tigerpaw	<ul> <li>Tigerpaw Username</li> <li>Tigerpaw Password</li> <li>Tigerpaw API URL</li> </ul>

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

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

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



**Note:** In order to configure the Settings in the Portal, you must be a **Master** user in your company's Network Detective account.

2. Click global Settings (Admin)



3. Click Connections.



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

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

5. In the Setup New Connection window, select the **Connection Type** by selecting the Autotask, ConnectWise, ConnectWise REST, or Tigerpaw system.

	Connecting to other systems enable workflo integrations with your RapidFire Tools modu a Connection Type below to get started	w les. Choose
onnection - Choose	<b>Type *</b> e Connection Type –	•
Autotas	sk tWise	
	tWise REST	
Connec		շիդ
Kaseya	BMS	$\bigcirc$
Kaseya TigerPa	BMS	$\cup$

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

This information will include:

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

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

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

#### **RapidFireTools**\*

B Ticket Details Specify how tickets should I	e created in the ticketing system.	
Work Type *	Assigned Resource	
Maintenance	▼ Da }rown	•
Pole	Due Date/Time *	
Standard MS Engineer	* Now + 5	Minutes
Issue Type	Sub-Issue Type	
Maintenance	vvorkstation	•
Queue	Priority *	
Level I IT Management	▼ Medium	•
Status *	Source	
New	* Email	•
Test ticket will be created in th	e account selected below.	
Q Account Name		
Account *		
		Ŧ

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

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

🖌 🖉 Confirm [	Details					
<ul> <li>Please confirm the information below before saving your new Connection.</li> <li>Connection</li> </ul>						
LW TP 532019 Prod						
Туре		TigerPaw				
Login		Performanceit				
Ticketing						
ervice Board	Help Desk	Service Type	Break/Fi:			
ccount	Performance It	Representative	Ian Alexande			

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

GI	obal Settings > Connections onnections					
Your Connections + Add						
	Name 💠	Туре 💠	Login 💠			
	AT	Autotask	dbrown@.com	1		
	BMS	Kaseya BMS	mw	/	ii ii	

## Step 3 — Map your Cyber Hawk's Site to a Ticketing System/PSA Connection

Follow these steps to map a Ticketing System/PSA Connection to the Network Detective Site associated with your Cyber Hawk.

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



2. Select the Network Detective **Site** you want to assign to this Ticketing System/PSA Integration.

Site Site below and a Connection to use to create tickets for that Site.     Image: Site Site for Customer ABC   Image: Site Site Site Site Site Site Site Site	Map Site to Connection	×
Site   Site for Customer ABC   ConnectWise   Company Lookup   C   C   Select Company*   Customer ABC	Select a Site below and a Connection	on to use to create tickets for that Site.
Site for Customer ABC       ConnectWise         Company Lookup         C       Q         Select Company*         Customer ABC	🛱 Site	5 <sup>5</sup> Connection
Company Lookup C Q Select Company* Customer ABC ~	Site for Customer ABC 🔹	ConnectWise •
C Q Select Company* Customer ABC ~		Company Lookup
Select Company* Customer ABC		c Q
Customer ABC -		Select Company *
		Customer ABC 🔹
Cancel Save		Cancel Save

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

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

#### **RapidFireTools**°

## Set Up Autotask Integration

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

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

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

<b>*</b> <sup>3</sup>	Connecting to other systems enable workflow integrations with your RapidFire Tools modules. Choose a Connection Type below to get started.
Additior specific	al setup may be necessary to configure the API user in the ticketing system. Please refer to the configuration documentation
Connection Ty	pe *
– Choose C	onnection Type 🗸 🗸
Autotask S	OAP
	_[اس
Autotask	
Autotask ConnectWi	se
Autotask ConnectWi ConnectWi	se REST
Autotask ConnectWi ConnectWi Kaseya BM	se REST S
4. Click Authenticate in Autotask.

***	Add New Connection Connecting to other systems enable workflow integration with your RapidFire Tools modules. Choose a Connection	S
	Type below to get started.	
Connection T	īvne *	
Autotask	162	~
Authoriz	e in Autotask 🕝	

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

Autotask
Username
Remember me
Continue
Or
K Log In with KaseyaOne
Help & Support   © Kaseya 2024

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



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

	Ticket Details Specify how ticke system.	ets sho	ould be created in the ticke	eting
Autotask Orga	nization*		Ticket Category *	Learn more
- Choose Organization 🗸		~	– Choose Category –	~
Ticket Type *			Status*	
– Choose T	icket Type –	~	– Choose Status –	~
Priority *				
– Choose P	riority	~		

## Set Up Autotask (SOAP) Integration

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

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



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



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



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

Admin	
Account Settings & Users Features & Settings Automation	Activations Extensions & Integrations
Expand All Collapse All	
<ul> <li>Your Organization</li> </ul>	
Resources/Users (HR) Resources/Users (HR)	
Resources/Users (HR)	
Resources/Users Manage user account (for people in your organization who have	Time Off Policies Manage the time off categories and the number of days or hours
Resources/Users Manage user account for people in your organization who have an Autotask login.	Time Off Policies Manage the time off categories and the number of days or hours in each category your resources are entitled to at each length of service tier.
Resources/Users Manage user accoult 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.	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.

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

≡ Autota	ask	Search	Q	Dashboards	Create	Му	Calendar
🔶 Reso	ources						
+ New -	🕹 Import/Ir	mport History	🕹 📃 Sho	w Inactive Fi	nd Resource		
New Resou	irce ser	Resource ID 🚖	Default Depar	tment Security	Level 🌲	License Ty	rpe 🌲 🛛 C
				•	•		•
	_						
	-						
	Section Page						

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

Add API User	0
Save & Close S Cancel	Review Terms and Conditions for API Use
General	í
Eizet Name *	Security Level *
Last Name*	Date Format
	MM/dd/yyyy
Email Address*	Time Format
	hh:mm a 🔻
Active	Number Format
Locked	x,xxx.xx
	Primary Internal Location *
	· · · · ·
Credentials	
C Generate Key	G Generate Secret
	Password (Secret)*
AFT fracking identifier	
API version 1.6 & later require the user of an API tracking identifier. C	nce assigned, this cannot be changed.
Custom (Internal Integration)	
RapidFire Tools - Network Detective	
	I
LINE OT BUSINESS	I
A line of business can be used to grant access or prevent access to Not Associated	data associated with Contracts, Tickets, Projects, etc.
	A330010100
	+
	v
Resource can view items with no assigned Line of Busines	ŝ

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

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

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

Add API User	0
🖹 Save & Close 🛞 Cancel	Review Terms and Conditions for API Use
Credentials	•
$\bigcirc$ Generate Key	
Username (Key) *	Password (Secret) *
API Tracking Identifier API version 1.6 & later require the user of an API tracking identifier. ( Integration Vendor Custom (Internal Integration) Integration Vendor* Tapidfice	Drice assigned, this cannot be changed.
Perspectium - Middleware (ServiceNow) PropelYourMSP Li Pulseway - RMM Quickpass - Password Management Quoter Software Inc Quoter QuoteWerks - Quotes, Proposals, and Procurement RapidFire Tools - Email2Ticket RapidFire Tools - Network Detective	ssociated with Contracts, Tickets, Projects, etc. Associated
Red Cactus - Bubble CRM Integrations Relokia - Data Migration Resale Partners - Telephony	· · · ·

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

## Set Up ConnectWise REST Integration

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

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

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

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

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

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



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

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

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

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

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

### 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					1
	Company				All
	Maintenance				
	Configurations	All	All		All
	Contacts	All	All		All
Service Desk	κ				
	Service Tickets	All	All		All
System					
	API Reports				All
	Table Setup*	All			All
	*Customized Table Setup: Allow Company / Company Status, Company / Configuration, Opportunities / Opportunity Status, Opportunity Status, Opportunity Type (See <u>"Table Setup</u> <u>Configuration" below</u> below for an extended explanation)				

## Table Setup Configuration

From Table Setup, click **customize**.

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

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

ow Access to these		Disallow Access to these		
Company / Company Status		Activities / Activity Status-CRM		
Company / Configuration		Activities / Activity Type	1	
Opportunities / Opportunity Status	>	Agreements / Agreement Type		
Opportunities / Opportunity Type	Ŕ	Agreements / Batch		
	×	Company / Address Formats		
	«	Company / Company Type		
		Company / Configuration Status		
		Company / Country		
		Company / Currency		-
		4	F.	

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

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



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

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

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

## Step 4 — Configure Service Tables in ConnectWise

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

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

1. Service Board

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

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

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

Board	Statuses	Types	Subtypes	Items	Auto Templates	Teams

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

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

## Step 5 — Remove "Disallow Saving" Flag from Company

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

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

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

Setup Ta	bles		
Setup Ta	bles		
SEARCH	CLEAF	2	
Category		Table ^	Description
Company	$\sim$	<u> </u>	
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.

Setup T Compar	able ny S	es > Compa Status List	any Status List			
< +	-	SEARCH	CLEAR			
Descriptio	n		Default	Inactive	Notify	Custom Note
<u>Active</u>						
Inactive					$\checkmark$	
Imported					$\checkmark$	
Credit Hold	<u>+</u>				$\checkmark$	
<u>Problem</u>					$\checkmark$	
not-Approv	<u>ed</u>		$\checkmark$		$\checkmark$	
<u>Solid</u>						
Attention r	ieed	ded			$\checkmark$	
may Leave					$\checkmark$	
Delinquent					$\checkmark$	

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

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

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

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

(	Company Search <b>Micro Pro</b>	> Com	pany > C	ompany Finan	ce Detail			
<	Summary	Rec	ар	Invoices 0	Time	e O	Expens	ses O
<		રુ	<b>⋴</b> ∨	History 🗸	Links	~		
	Company: Mi	cro Pro						
	Company: *	Micro	Pro				Pho	one:
	Company ID: *	123					Fax	C
	Status: *	not-Ap	proved			$\sim$	🛱 We	b Site:
	Type: *							
	Prospect $\chi$							
Ĩ	Finance Detai	ls			र्भ	È>		

## 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 Ta Setup Ta	bles bles	
SEARCH	CLEAR	
Category	Table 个	Description
	✓ integrator	
General	Integrator Login	Setup Integrator Access

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

Integra	tor Login	5 5	
Setup	Logs		
<	+ 🗄 🗄 🔂 +	HISTORY 🗸 🔟	
Userr api	name*		
Pass	word		
	ss Level Records created by Integra	tor O All Records	
Selec	t the available API integrat	lion(s) you wish to enable and configure below	
$\Box$	API Name		
	Activity	Callback URL	Use legacy of
	Agreement	Callback URL	Use legacy o
	Company	Callback URL	

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

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

## Set Up Kaseya BMS Integration

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

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

#### **RapidFireTools**<sup>®</sup>



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

ß	CRM Manager	CRM Manager
Ø	Project Manager	Project Manager
Ø	Service Desk Manager	Service Desk Manager
C	Administrator	Administrator

4. Click the Role Users tab.

✓ Security Ro	le Information	
Name: *	tor	
Status:		
Active		
Permissions	Role Users	

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

# Set Up Portal Branding

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

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

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

Rapidi	-ire loois
Username	
Password	Forgot Password?
Remember me	
	Log in
	Or
Ҟ Log ir	n with KaseyaOne
Learn More	about KaseyaOne

2. Click global Settings (Admin) > Users.



3. Click Branding.

Micro Consulting	Organizations
(2) General	Global Settings / General
🖌 Branding	
➔ Connections	General
Admin Alerts	Time Zone ③
O Users	(UTC-05:00) Eastern Time (US & Canada)
🕲 Compliance Manager GRC 🔹 🕨	
🔍 Network Detective Pro	Date Format ③
VulScan	dd-MMM-yyyy
Service Plans	

From this page, you can then:

- "Set Custom Portal Theme" below
- "Set Custom Portal Subdomain" on the facing page
- <u>"Set Custom Company Name" on page 132</u>
- <u>"Set Custom Company Logo" on page 133</u>

## Set Custom Portal Theme

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

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

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

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



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

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

## Set Custom Portal Subdomain

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

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

<b>Site</b> 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.

÷	$\rightarrow$	C	(	greystone.alert-central-dev.com/login	
					Username Password Pasemore Pas

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

## Set Custom Company Name

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

Micro Consulting	Organizations
🙆 General	Global Settings / Branding
🖌 Branding	
<ul> <li>Connections</li> </ul>	Branding ③
🗘 Admin Alerts	Theme
<b>O</b> Users	(Click to Preview)

To do this:

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

🙆 General					
🖌 Branding		Custom Branding			
➔ Connections		Company Name			
🗘 Admin Alerts		Displayed in top left of menu bar			
<b>2</b> Users		Micro Consulting			
© Compliance Manager GRC	•				
Q Network Detective Pro	Þ				
VulScan	Þ				
E Service Plans	Þ				
Email Groups					

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

## Set Custom Company Logo

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

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



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

#### **RapidFireTools**<sup>®</sup>

#### login screen.

G Pro	areystone ofessionals
Username	
Password	Forgot Password?
Remember me	
	Log in
Learn N	Nore about KaseyaOne

Set Up a Custom Subdomain to Access the RapidFire Tools Portal

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

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

RapidFireTools <sup>®</sup>				
Username				
Password	Forgot Password?			
Remember me				
Lo	g in			
(	Dr			
🗙 Log in w	vith KaseyaOne			
Learn More ab	out KaseyaOne			

2. Click global Settings (Admin)



3. Click Branding.



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

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

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



# 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. In the Cyber Hawk Settings window, select the Email Configuration Modify button to access the Email Configuration options window.

V	Settings	
	Policy Configuration: 23 Active Policies	Modify
	Email Configuration:	Modify

The Email Configuration window will be displayed.

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

SMTP Server						
Use Default SMTP Server     O Use Custom SMTP Server						
Alert From:	youre	mailaddress@your	domain.com	Display Name:	Security Alerts	
Report From:	youre	mailaddress@your	domain.com	Display Name:	IT Security Reports	
Admin Notice F	rom: youre	mailaddress@your	domain.com	Display Name:	Your Admin Notices	
Custom SMTP	Settings					
SMTP Server Address: smtp.yourdomain.com						
Port: 587 🚖						
Security: SSL				▼		
Usemame:	Username: youremailaddress@yourdomain.com					
Password:						
Send Test Emails						

4. Select the Send Test Email button to test the SMTP email Server configuration and email addresses.

α	Email Configu	iration					×	
5	SMTP Server	Email Gr	oups Email Subjects Summary Emails					
	O Use Default	SMTP S	erver	Ose Custom S	SMTP Server			
	Alert From:		yourer	mailaddress@yourd	domain.com	Display Name:	Security Alerts	
	Report From:		yourer	mailaddress@yourd	domain.com	Display Name:	IT Security Reports	
	Admin Notice Fr	rom:	yourer	mailaddress@yourd	domain.com	Display Name:	Your Admin Notices	
	Custom SMTP S	Settings –						
	SMTP Server A	ddress:	smtp.y	vourdomain.com				
	Port:		5	587 🌲				
	Security:		SSL				•	
	Usemame:		yourer	mailaddress@yourd	domain.com	_		
	Password:							
	Send Test Emails							
	Save & Close Discard & Close							

5. Select the Send button in the Send Test Emails window. The status of the email test is displayed in the Send Test Emails window.

Send Test En	Send Test Emails					
Email To: Subject:	youremailaddress@youritcompany.com SMTP Test Email					
	Send					
Alert email t Email sent. Report ema Email sent. Admin emai	est result: il test result: I test result:					
	Close					

After a successful test has been completed, select the Close button to close the Send Test Emails window.

6. To complete the setup process, select the Save & Close button in the Email Configuration window to save the Custom SMTP Server Email Configuration settings.

# 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.

Add User					
Email Address *	Email Address *				
your-client-user@client.com					
First Name * Last Name *					
Client	User				
Password *					
•••••					
Confirm Password *					
•••••					
Global Access Role *					
Site Restricted		•			
	Close	🖌 Add			

6. Click Add.

Note: Look here for a complete breakdown of	"Users and Global Access Roles"
<u>on page 144</u> .	

## Step 2 — Assign User to Site

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

Darrien Site					
≡	Home > Users				
A Home ^	Users 😰			+ Ad	d User
Dashboard				_	
Appliance	Removing a user have the global adminis	from the table below only ren strator remove the user from (	noves that user's access from t Global Settings.	his site. To delete a u	iser,
👱 Users	University &	First Name A	Last Marca	Deles +	
Roles	Username 🗸	Filst Name 🗸	Last Name 🗸	Client	
Admin Alerts	-				-
Advanced Options				Client	•
Add-ons				Site Admin	Î
 InDoc ✓				Client	Î

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**.

Darrien Site					
≡		Home > Roles			
A Home	^	Roles @			
Dashboard		Site Admin	+ Add User	Technician	+ Add User
Data Collectors			î		Ξ.
Lusers					
🚢 Roles					
Admin Alerts					
Advanced Options		Client View	Add User		
Add-ons			ĩ		
InDoc	~		ĩ		
Oyber Hawk	~		1		
📋 Audit Log					

**Note:** Look here for more details on <u>"RapidFire Tools Portal Site Roles" on</u> page 150.

- 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 (<u>https://www.youritportal.com</u>).

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

# Manage Users (Global Level)

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



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

Micro Consulting		Organizations	
🙆 General		Global Settings / Users	
🖌 Branding		<u>.</u>	
<ul> <li>Connections</li> </ul>		Users ③	
🇘 Admin Alerts		Search	
O Users			
Scompliance Manager GRC	Þ	licemame 📥	Display Name 🚔
Q Network Detective Pro	Þ	osemane 🗸	
VulScan	Þ	writertech527@gmail.com	100.000
Service Plans	Þ		14/11/
Email Groups		wgipson@microconsulting.com	Gibson
🗔 Data Collectors			
C IT Complete		and plane and	1000

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	ø	Û
bv-admin@microsolutions.com		Admin	All / (Site Admin), Test CIS V8 IG1 site (Site Admin)	No	ø	Û
chuckp@microconsulting.com	Chuck Palahniuk	Site Restricted	Micro Consulting MSP (Unassigned)	No	Ø	Ô
example-user@rapidfiretools.com	Example User 1	Site Restricted	Sample HIPAA Assessment (Unassigned)	No	Ø	Û

#### **RapidFireTools**<sup>\*</sup>

## 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 <i>Site Settings</i> and <i>Global Settings</i> . Can access API Keys from Global Settings.
	Who should I assign this level to?
	IT Managers within your operation who have your highest level of trust, and who will:
	<ul> <li>be the "primary" admin for the RapidFire Tools Portal</li> </ul>
	<ul> <li>handle sensitive data for all of your clients</li> </ul>
	<ul> <li>purchase and provision additional RapidFire Tools Products</li> </ul>
	<ul> <li>create and assign the appropriate security permissions for users within — and outside — of your operation who access the Portal</li> </ul>
ADMIN	Has global access to multiple sites. Has access to <i>Site Settings</i> and <i>Global Settings</i> .
	Who should I assign this level to?
	<ul> <li>Users you trust within your operation to be "secondary" admins for the RapidFire Tools Portal</li> </ul>
	<ul> <li>Users you trust with sensitive data for all of your clients</li> </ul>
Global Access Role	Description
--------------------	--
	<ul> <li>Users you trust to create and assign the appropriate security permissions for users within — and outside — of your operation who access the Portal</li> </ul>
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?
	<ul> <li>Techs or others in your operation who should only access specific Sites as a Site Admin or Technician</li> </ul>
	<ul> <li>Techs or others in your operation who should also access sites in the Network Detective application</li> </ul>
	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 <b>Site Redistricted</b> 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?
	<ul> <li>Techs who should only access specific Sites as a Site Admin or Technician</li> </ul>
	<ul> <li>Client users working with your team to perform IT or compliance assessments in the role of Technician, Internal Auditor, or SME</li> </ul>

From the Users page, you can also:

- "Add User at Global Level" below
- "Edit User at Global Level" on page 148

## Add User at Global Level

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

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

1. Click Add User.

Global Settings / Users						
Users ③			_	<b>—</b>	+ Add U	ser
Search	All	- Z Re	quire Two-Factor Authent r All Accounts	ication Z Enable Dis for All Use	scovery Ag	gents
Username 🔶	Display Name 💠	Global Access Level 💠	Site Level Access ≑	2FA 💠		
billfoyers@itsolutions.com	Bill Foyers	Site Restricted	Salient Industries (Client)	Yes	ø	Û
bv-admin@microsolutions.com	ΒV	Admin	All / Bobs VulScan Site (Site Admin), Test CIS V8 IG1 site (Site Admin)	No	Ø	Û

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

Last Name: *
Pro
•

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

3. Choose a Global Access Role for the User.

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

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

#### **RapidFireTools**<sup>°</sup>

Global Access Role	Description		
	application.		
	Who should I assign this level to?		
	<ul> <li>Techs or others in your operation who should only access specific Sites as a Site Admin or Technician</li> </ul>		
	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 <b>Site Redistricted</b> 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?		
	<ul> <li>Techs who should only access specific Sites as a Site Admin or Technician</li> </ul>		
	<ul> <li>Client users working with your team to perform IT or compliance assessments in the role of Technician, Internal Auditor, or SME</li> </ul>		

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

## Edit User at Global Level

**Note:** Only *Master* and *Admin* users can edit users. And only Master users can edit other Master users. See <u>"Manage Users (Global Level)" on page 143</u> for more details.

To edit users:

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

fs-admin@foresight.com	Foresight Admin	All	All	No	0	۵
globalteam@itsolutions.com	Global Team	Site Restricted	Salient Industries (Unassigned)	No	0	ŵ
itpro@prodynamics.com	IT Pro	All	All	No	0	ŵ
itpro@tech-dynamism.net	Tech Pro	Site Restricted	Salient Industries (Site Admin)	No	0	ŵ

3. Click Save.

#### **RapidFireTools**\*

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

#### RapidFireTools®

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.

Micro Consulting	Organizations		ি	) 🔞 🔒 IT Pro 🔣
Home •	Granite Dynamics			
Data Collectors	Micro Professionals / Granite Dyna	mics / Home / Data Collectors		
Users Roles	Data Collectors ©	)	+ Pr	ovision Vulnerability Scanner
Advanced Options	Internal Vulnerability Scan	ners External Vulnerability Scanners	Discovery Agents	
	Data Collector Type:	Internal Vulnerability Scanner		
	Data Collector ID:	IVS1-YRVY83	1	
	Description:		0	
	Last Check-in:	Never		
	Update Status:	unknown		
	Manage Data Collector:	(Data Collector Offline)		
				2024.02.27-1904

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.

Home	*	Data Collectors	)	+ Provision V	ulnerability Scanner
Data Collectors		Internal Vulnerability Scar	ners External Vulnerability Scanners Discovery Agents	Reporter	
Users					
Roles		Data Collector Type:	Internal Vulnerability Scanner		
Advanced Options		Data Collector ID:	IVS1-	0	
Network Detective Pro	•	Description:	AWS	ø	
VulScan	+	Last Check-In:	17 Jan 2023 5:54 PM GMT-05:00		
E Addit Log		Update Status:	🥥 up-to-date		
		Manage Data Collector:	(Data Collector Offline)		
		Data Collector Type:	Internal Vulnerability Scanner		
		Data Collector ID:	KVS1-	Û	
		Description:	La li lu le lo La li lu le lo	0	
		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 <u>"Data Collector Commands " below</u> from the drop-down menu. If the Data Collector is not available, "Data Collector Offline" will appear.

## Data Collector Commands

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

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

**RapidFireTools**°

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

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

#### **RapidFireTools**<sup>°</sup>

Manage Scans	view and								
	Manage Data Collecto	r Scans - NDA1-0333N	NC						
								1 /1 >	> view 10 *
	ID ¢	Assessment	Scan Type 💠		Size (MB)	Start Date UTC	¢	End Date UTC \$	Status ¢
	11270906		Network Assessment (Cyb	oer Hawk)	3.18	null 04:24:38 F	M	null 04:34:22 PM	Done
	11270941		Push Deploy (ZIP)		40.74	null 04:42:15 F	м	null 05:15:39 PM	Done
	11307821		Push Deploy (ZIP)		4.93	null 05:37:15 F	м	null 05:48:56 PM	Done
	11411856		Network Assessment (Cyb	per Hawk)	3.09	null 01:21:13 F	м	null 01:31:02 PM	Done
	11411857		Push Deploy (ZIP)		43.55	null 01:21:13 F	м	null 02:04:22 PM	Done
	11432840		Network Assessment (Cyb	per Hawk)	3.02	null 04:46:26 F	м	null 04:56:15 PM	Done
	11432841		Push Deploy (ZIP)		43.22	null 04:46:26 F	M	null 05:29:30 PM	Done
	👲 Download	i Selected	Delete Selected	Remove from	Queue	O Cancel Sel	ected		
									Close
	• Downloa • Delete co • Remove	d scan omplete queued	files ed scans and scans	d their a	ssoci	iated fil	es		
Manage Reports (Reporter only)	• Downloa • Delete co • Remove • Cancel s Access ar	d scan omplete queued cans in nd mana	files ed scans and scans progress age reports s	d their a	ssoci	e Report	es ter ap	opliance	
Vanage Reports (Reporter only)	<ul> <li>Downloa</li> <li>Delete co</li> <li>Remove</li> <li>Cancel s</li> <li>Access ar</li> </ul>	nd scan for complete queued cans in nd mana	files ed scans and scans progress age reports s	d their a	ssoci	Report	es ter ap	opliance	).
/anage Reports Reporter only)	Downloa     Delete co     Remove     Cancel s     Access ar	d scan omplete queued cans in nd mana	files ed scans and scans progress age reports s	d their a	ssoci	iated fil	es ter ap	opliance	).
lanage Reports Reporter only)	Downloa     Delete co     Remove     Cancel s     Access ar	id scan for the sc	files ed scans and scans progress age reports s	d their a	ssoci	e Report	es ter ap	opliance	).
lanage Reports Reporter only)	Downloa     Delete co     Remove     Cancel s     Access ar	id scan omplete queued cans in nd mana	files ed scans and scans progress age reports :	d their a stored o	on the	e Report	es ter ap	opliance	<u>.</u>
lanage Reports Reporter only)	Downloa     Delete co     Remove     Cancel s     Access ar	nd scan for omplete queued cans in nd mana	files ed scans and scans progress age reports a mereter to a	d their a stored o	ssoci	Report	es ter ap	opliance	
lanage Reports Reporter only)	Downloa     Delete cc     Remove     Cancel s     Access ar	d scan formplete queued cans in nd mana	files ed scans and scans progress age reports s age reports scans age reports scans age reports	d their a stored o	ssoci	tated fil     tate fil     tate fil     tate fil     tate fil     tate fil	es ter ap	opliance	<u>.</u>
lanage Reports Reporter only)	Downloa     Delete co     Remove     Cancel s     Access ar	d scan formplete queued cans in nd mana	files ed scans and scans progress age reports a age reports Revertes a Area trail Reordeo 20 Peerflorato	d their a stored of size size of size of o Deriv o Deriv o Deriv		tated fil     tate     fil	es ter ap	opliance	).
lanage Reports Reporter only)	Downloa     Delete co     Remove     Cancel s  Access ar  Mage Reports - NOX  Report Set ID  Assessmet- A	ad scan formplete queued cans in nd mana	files ed scans and scans progress age reports a age reports breverter age control of the second breverter age control of the second brever	Stored of           \$	ssoci on the on the official site official site official site official site official site official	Report     1     1/4     1/4     1/4	es ter ap	opliance	<u>)</u> .
lanage Reports Reporter only)	Downloa     Delete co     Remove     Cancel s  Access an  Mage Repet: - KOX  Repet Set D  Assumet- Assumet	ad scan formplete queued cans in nd mana Agorts Agorts Agorts Agorts	files ed scans and scans progress age reports a age reports age reports compared Mays doc 20 Paret Marga doc	Stored of Stored of Stored of Stored of Stored of Stored S	ssoci on the site official site official site official site official site official	A Report	es ter ap <u>*</u> <u>*</u> <u>*</u> <u>*</u> <u>*</u>	pliance	<u>).</u>
anage Reports Reporter only)	Downloa     Delete co     Remove     Cancel s  Access ar  Knee Reports - ROX  Report Set 10  Assement- Assement	ad scan for mana and mana	files ed scans and scans progress age reports a age reports scans scans scans scans age reports scansc	Stored of         Ster           Stored of         Ster           Stored of         Ster           Stored of         Deriv           0         Deriv           179782         Deriv           4398         Deriv           216610         Deriv	ssoci on the site official site official site official site official site official site official	Control C	es ter ap با باهر عام با با ب	pliance	).
anage Reports Reporter only)	Downloa     Delete co     Remove     Cancel s  Access ar  Mage Repets - NDA  Repet Set D  Assement- A	ad scan formplete queued cans in ad mana ad mana ad mana	files ed scans and scans progress age reports a age reports age reports age age age age age age age age age age age age age	Stored of         Stored of           0         Series           0         Derrid           1266912         Derrid           1379752         Derrid           212110         Derrid           232101         Derrid           232101         Derrid           232101         Derrid           232101         Derrid           232101         Derrid	ssocial on the con the	term of fill     t	es ter ap * 'view 10 *	pliance	<u>.</u>
anage Reports eporter only)	Downloa     Delete co     Remove     Cancel s  Access ar  Mage Repers - NDA  Repert Set D  Assessment- Assess	ad scan formplete queued cans in ad mana ad mana ad mana agerts agerts agerts agerts agerts agerts agerts agerts agerts agerts	files ed scans and scans progress age reports a age reports age Reports age Reports age age age age age age age age age age age age age age age age age age	Stored         Stored<		t          1         1         1	× viev 20 ± ± ± ± ± ± ± ± ± ± ± ± ±	pliance	<del>.</del>
Aanage Reports Reporter only)	Downloa     Delete co     Remove     Cancel s  Accesss ar  Kassmet- Assamet- As	ad scan for polete queued cans in and mana and	files ed scans and scans progress age reports a age reports age Reports BReek-Avgentage Caretak Reportage Caretak Reportage	Stored         Stored<	SSOCI	A Report	× view 10 • • • • • • • • • • • • • • •	ppliance	<u>.</u>
Vanage Reports (Reporter only)	Downloa     Delete co     Remove     Cancel s     Cancel s     Access an	ad scan for polete queued cans in and mana and	files ed scans and scans progress age reports a age reports age Preveninger Credited Meagement Plander Credited Meagement Plander Mill Deal Megordar	Stored         Stered           0         Set           0         Set           0         Set           1366912         Derri           136692         Derri           4398         Derri           963298         Derri           435396         Derri	SSOCI on the on the site 06/13 site 06/13 site 06/13 site 06/13 site 06/13 site 06/13 site 06/13 site 06/13 site 06/13	A Report	× view 10	pliance	<u>.</u>
Janage Reports Reporter only)	Downloa     Delete co     Remove     Cancel s     Access ar	ad scan for poleter queued cans in and mana	files ed scans and scans progress age reports a age reports age Reports BRPereferinger Clerchashegerdec BRPereferinger Clerchashegerdec Considered Nationation Considered Nationation C	Stored c	SSOCI on the on the site 06/13 nite 06/13 ni	A Report	es ter ap	opliance	<u>.</u>

#### **RapidFireTools**\*

# 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."

Тад	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

Here are some of the Smart Tags available for use:

Тад	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

Тад	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

Тад	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

#### RapidFireTools®

## 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

Double click your mouse pointer on the Site that you are configuring automated scan, alerts, and reports to be performed upon in order to view and access the Site.



# Step 2 — Select Manage Cyber Hawk Appliance and Access the Cyber Hawk Settings

After the Site has been opened, select the Cyber Hawk icon located within the Site bar.



The Cyber Hawk Settings window will be displayed.

#### **RapidFireTools**<sup>®</sup>

Customer A	Configure   Smart Tags   Notifications
NDA	Host Type: Virtual 🜔 Active
∧ 🍓 Settings	
Daily Alerts	Add Recipient
Weekly Notice	Add Recipient
Reports	Add Delivery Schedule

# Step 3 — Access Smart Tags and Verify that Scan Data has been Downloaded

Select the Smart Tags link within the Cyber Hawk's Settings window.

Customer A		Configure   Smart Tags
NDA	Host Type: Virtual 🧶	Active
∧ 🍓 Settings		
Daily Alerts	Add Recipient	
Weekly Notice	Add Recipient	
Reports	Schedule Report	

If no scans have been performed by the Cyber Hawk, the following message will be presented by Network Detective.

Customer A	Configure   Smart Tags   Notifications
Smart Tags	No scan data found. A scheduled scan must be completed before tagging can occur.
No scan data found. A scheduled scan mu	ist be completed before tagging can occur.
Tagging improves detection of anomalies a	and threats by providing knowledge of the environment to the Detector.
Once the Detector has scanned your netw	ork for the first time, you can explore the data and apply tags to entities like computers and users.

After scans have been performed, select the Smart Tags link and download the scan as instructed.

Customer A		Configure	Ι	Smart Tags
Smart Tags				
Downloading Scan Data	772			

Once the scans have been downloaded, the completion of the process will be confirmed by the presentation of the Smart Tags options consisting of Applied Tags, Recommended Tags, and Available Tags as presented to the right.

Cu	stomer A		Configure	Smart Tag	js
	Smart Tags	Up to Date			
▲ 🗐	Applied Tags				
∧ 🖵	Recommended Tags				
∧	Available Tags				

Once the Smart Tags are "Up to Date", you can access, view, and use the settings for Applied Tags, Recommended Tags, and Available Tags.

**Note:** When starting a Site using the Cyber Hawk, then attempting to view or update the Smart Tags configuration, you may be prompted to update the scan data with the latest scan per a notice as presented to the right.

Customer A		Configure   Smart Tags
Smart Tags	New Detector Scan Available	Download Update

Depending on the number of changes in Users and Computers on your client's network, you may wish download the updated scan to ensure the latest User identity and Computer information is available for use when setting Smart Tag configurations.

## Step 4 — Select and Apply Recommended Tags

1. To add a Smart Tag from the Recommended Tags list, select the Recommended Tags option by selecting the A selector on the Recommended Tags bar.

	Cus	stomer A		Configure	Smart Tags
		Smart Tags	Up to Date		
^		Applied Tags			
^	J	Recommended Tags			
^		Available Tags			

The Recommended Tags window will be displayed.

	Customer A	Configure Se	nart Tags   Notifications							
	Smart Tags Up to	Date								
^	Applied Tags									
V	Recommended Tags									
	8 Tags									
	AUTHORIZED PRINTER Printer	AUTHORIZED SSID SSID	BUSINESS OWNER User	BUSINESS OWNER PC Computer						
	GUEST NETWORK IP range	GUEST WIRELESS NETWORK IP range	User User	RESTRICTED IT ADMIN ONLY Computer						

2. Next, select the Smart Tag that you would like to configure and apply.

For example, select the IT Admin tag by double-clicking on the IT Admin User Smart Tag Icon.



This action will display the Tag Explorer window for this Smart Tag.

Within the Tag Explorer window, instructions are presented that detail:

- what the Tag is to be "Applied To" (i.e. users or computers)
- the "For What" purpose the Tag can be used
- the "Why" reason to use the Tag

Tag Explorer			X
			Save & Close Discard & Close
Applied To?		For What?	Why?
This tag is applied to a User		IT Administrators typically have more access to network resources than the typical user.	Identifies who should have this elevated level of access
Filters	Users		
Active <u>Clear Al</u> Yes No	Enter text t	o search	ar
Enabled Clear Al			

**Tip:** There are a number of Smart Tags that should be used as logical "pairs". For example, the IT Admin User tag should be used with the Restricted IT Admin Computer Only tag. Using this pair of Smart Tags will enable you to define all of the IT Admin users, and the computer endpoints that are to be only accessible by IT Admin users. Alerts will be generated when non-IT Admin users access the computers designated as Restricted IT Admin Computers Only.

3. Next, define which network Users are IT Admin Users by selecting the Users that should be designated as IT Administrators in the Tag Explorer window presented for the IT Admin Users tag.

Tag Explorer											×
	IN							Save & C	lose	Discard & Close	
Applied To?			For Whi	st?			Why?				
This tag is applied to a U	loor		IT Administr resources th	ators typically hav an the typical us	ve more access to nel er.	twork	Identifies with	to should have this eld	vated level of	access.	
Filters	Clear Al	Users									
Mo Yes						• Cle	ar 🛛				
Enabled	Clear AL										
Yes		Tagged	Domain	Name	Display Name	Fint	Last	Last Login	Active	Enabled	
I NO								(never)	No	Yes	
Tagged	Cear Al							5/28/2015 1	No	No	
Yes Yes								5/10/2016 6:	Yes	Yes	
m 110		1						5/11/2016 5:	Yes	Yes	
								4/15/2013 2:	No	No	
								7/7/2014 12:	No	No	*

To specify the IT Admin Users, select the Check Box next to Users that should be designated as IT Admin Users from the list presented in the Tag Explorer window.

4. Next, select the Save & Close button to save the Smart Tag settings for the IT Admin User Smart Tag.

>	Ap	oplied Tags	
	9 Tags	(176 Applied)	
		IT ADMIN 2 users tagged	<b>Î</b>

When the IT Admin Tag is configured and Applied, the IT Admin Tag will be available for updating in the Applied Tags section of the Smart Tags options window.

### Step 5 — View Applied Tags

To view the Smart Tags that have been Applied from the Applied Tags list, select the Applied Tags option by selecting the Applied Tags bar.

Customer A		Configure   Smart Tags
Smart Tags	Up to Date	
Applied Tags		

The Smart Tags that have been applied to the Cyber Hawk configuration for the Site will be listed in the Applied Tags window as seen below.

V	Ap	plied Tags	
	9 Tags	(176 Applied)	
		IT ADMIN 2 users tagged	Û

You can double click on the Smart Tag to view the tag's settings.

# Step 6 — Select and Apply Additional Smart Tags from the Available Tags Window

1. To add a Smart Tag from the Available Tags list, select the Available Tags option by selecting the Available Tags bar.

Cu	stomer A	Configure	Smart Tags	
	Smart Tags	Up to Date		
▲ 🗐	Applied Tags			
^ 🖯	Recommended Tags			
	Available Tags			

The Smart Tags available for use will be displayed.

Y	Tags without	vailable Tags it items associated. Double-click to tag ite	ems from t	he latest scan.				
	17 Tag	s						
		ACCOUNTING COMPUTER Computer		ACCOUNTING USER User		DATABASE SERVER Computer		DMZ COMPUTER Computer
		HIPAA / ePHI AUTHORIZED USER User	J	HIPAA / ePHI COMPUTER Computer	J	IGNORE COMPUTER CHANGES Computer	J	IGNORE NETWORK CHANGES IP range
	•	IGNORE USER CHANGES User	•	LOCKED DOWN Computer	J	NO DIRECT INTERNET ACCESS Computer		PCI / CDE AUTHORIZED USER User
		PCI / CDE COMPUTER Computer		RESTRICTED NETWORK IP range		SINGLE DESKTOP USER User		VIRTUAL MACHINE Computer

2. Double click on the Smart Tag that you want to use and the Tag Explorer window for the selected tag will open. Configure the Tag by selecting the Users or Computers listed in the Tag Explorer window that you want to designate as being "Tagged" within the Tag as displayed below.

RESTRICTED IT A	DMIN O	NLY			s	rve & Close	Discard & Close	
Applied To?		For What?			Why?			
This tag is applied to a Computer		Some computers directly by IT Adm	typically servers) should or inistrators.	nly be accessed	Allows alerting when access	occurs by	non-IT Admins.	
Filters	Comput	lers						
Operating Systems Clear Al								
<none detected=""></none>	Calma have	the second			1			
Hyper-V Server 2012	Enter tex	t to search		•	Jear			
Windows 10 Enterprise								
Windows 10 Pro Insider Preview	Tacord	Domain	Computer	IP Address	05	Active	Last Login	
Windows 2000 Server	Taggeu	Domain	Computer	IF Address	Wadawa 0.1 Dec	Vee	E (11 (2010 A 24-50 AM	-
Windows 7 Enterprise		_		_	Windows 6.1 Pro	Tes	3/11/2016 4:24:30 PM	-
Windows / Professional					windows server 20	IVO	10/1/2014 6/43/32 PM	
Windows 8 Pro					Windows Server 20	NO	10/29/2014 5:22:50 AM	
Windows 8.1 Enterprise	×				Windows 8.1 Pro	Yes	5/11/2016 4:14:21 AM	
Windows 8.1 Pro					Windows Server 20	No	2/11/2015 11:49:29 PM	
Windows 8.1 Pro with Media Center	$\checkmark$				Windows 10 Pro	Yes	5/11/2016 4:27:41 AM	
Windows Server 2003					Windows 10 Pro	Yes	5/11/2016 4:42:25 AM	
Windows Server 2008 R2 Datacenter					Windows 10 Pro	No	4/6/2016 2:06:33 PM	
Windows Server 2008 R2 Standard					Windows 7 Enterpris	e No	7/24/2014 4:11:58 PM	
Windows Server 2012 Datacenter					Windows 8.1 Pro	No	9/23/2015 6:26:14 AM	
Windows Server 2012 R2 Datacenter					Windows 10 Pm Inc	No	10/15/2015 1-57-20 AM	
Windows Server 2012 R2 Standard	1				Mindows 9 Extensio		5/11/2016 4-50/21 AM	
Windows Server 2012 Standard					Windows 7 Esterni	e 100	E/11/2010 E-14-EE AM	
Windows Server 2016 Technical Prev					Whows 7 Enterpre	e les	3/11/2016 3.14.33 PM	
Windows Server 2016 Technical Prev					Windows 8.1 Enter.	. No	1/15/2016 7:15:48 PM	
					Windows 10 Pro	Yes	5/10/2016 9:50:37 PM	
Active Clear Al	×				Windows 8.1 Enter.	. Yes	5/11/2016 1:09:53 AM	
No					Windows Server 20	Yes	5/11/2016 5:15:57 AM	
					Windows Server 20	Yes	4/20/2016 3:50:26 PM	
Tagged Clear Al					Windows 8 Enterpris	e No	12/18/2014 1:55:53 PM	
Yes	×				Windows 10 Pro	Yes	5/11/2016 4:39:36 AM	
No					Windows 10 Pm	Yes	5/10/2016 11:28:05 PM	

3. Next, select the Save & Close button to save the Smart Tag settings for the selected Smart Tag.

When the Tag you selected is configured and Applied, the Tag will be available for updating in the Applied Tags section of the Smart Tags options window.

4. Verify that the Tag you configured and Applied is in the Applied Tags window.

To view the Smart Tags that have been Applied from the Applied Tags list, select the Applied Tags option by selecting the selector on the Applied Tags bar.

Customer A		Configure   Smart Tags
Smart Tags	Up to Date	
Applied Tags		

The Applied Tags will be displayed to enable you to confirm that the Smart Tag you selected and configured has been Applied.

V	Applied Tags			
	11 Tags (151 Applied)			
	ACCOUNTING COMPUTER	ACCOUNTING USER	AUTHORIZED PRINTER	AUTHORIZED SSID
	4 computers tagged	1 user tagged	2 printers tagged	5 SSIDs tagged
	BUSINESS OWNER	BUSINESS OWNER PC	DATABASE SERVER	HIPAA / ePHI AUTHORIZED USER
	1 user tagged	1 computer tagged	4 computers tagged	1 user tagged

#### **RapidFireTools**\*

# Export and Import Smart Tags

Before associating a new Network Detective Site file to a Cyber Hawk that has already been configured for use with another Site to detect Anomalies, Changes, and Threats (ACT) on a network, you may want to Export and reuse the original site's Smart Tag settings.

Customer A			Configure	I	Smart Tags		Notifications
NDA	Host Type: Virtual	Active					
🔨 🍓 Settings							
A Daily Aler	ts Add Recipient						
N Weekly N	Add Recipient						
Reports	Add Delivery Schedule						

The use of the Export Smart-Tags feature must be done before associating a new Site with your Cyber Hawk if the Cyber Hawk is to be used to detect ACT events on the same network.

Once a Cyber Hawk and its associated Site have been configured to operate with a given network, switching the Site file to be used with your Cyber Hawk will trigger a deletion of the Smart Tag settings associated with the original Site used to configure and apply the Smart Tag settings to your Cyber Hawk.

If there is a requirement to save the Smart Tags from the current Site's Cyber Hawk configuration for reuse in a different Site associated with your Cyber Hawk that is to be connected to the same network as the original Site was used, you must use the Smart Tags Export and Import options to save and reuse the tags for later use in your new Site file used to set up the Cyber Hawk's configuration.

## **Export Smart Tags**

#### Step 1 — Select the Site

After starting Network Detective, double click your mouse pointer on the Site that you are configuring the automated scan and alerts to be performed upon in order to view and access the Site's Settings.



# Step 2 — Select Manage Cyber Hawk Appliance and Access the Cyber Hawk Settings

After the Site has been opened, select the Cyber Hawk icon located within the Site bar.



The Cyber Hawk Settings window will be displayed.

# Step 3 — Access Smart Tags and Verify that Scan Data has been Downloaded

Select the Smart Tags link within the Cyber Hawk's Settings window.

#### **RapidFireTools**<sup>®</sup>

Customer A	Configure   Smart Tags
NDA NDA	Host Type: Virtual O Active
∧ 🍓 Settings	
Daily Alerts	Add Recipient
Weekly Notice	Add Recipient
Reports	Schedule Report

#### Step 4 — Export Smart Tags

Select the Export option to export the Smart Tags configuration.



Your will be prompted to save the Smart Tags export file in a location of your choice.

	Expo	ort Detector Smart Tag Co	nfiguration			
) 🕀 🝷 🕇 🚺	► This PC ► Downloads		v د	Search Downloads		p
rganize 👻 Ne	w folder				8:: •	6
	Name	^	Date modified	Туре	Size	
This PC Desktop		No items m	atch your search.			
Documents						
🗼 Downloads						
Music 📗						
Pictures						
Videos						
C Drive (C:)						
Potwork Asse	ssm 🗸 z					
File name:	SmartTag_autosave_2016-05-20.xml					
Save as type:	XML Files (*.aml)					
Hide Folders				Zarve	Cancel	

Select the folder you want to save the Smart Tags Configuration file in, name the file, and select the Save button to export the file.

## Import Smart Tags

#### Step 1 — Select the Site

Double click your mouse pointer on the Site that you are configuring automated scan, alerts, and reports to be performed upon in order to view and access the Site.

All Sites	Customer A - Inspector Assessment Created: 1/28/2016 1:31 PM Modified: 2/11/2016 11:15 AM Assessment Status: In Progress Checklist: 0/2	Customer A - Network Assessment Created: 12/29/2015 2:50 PM Modified: 2/2/2016 8:09 AM Assessment Status: In Progress Checklist: 1/2	Customer A - PCI Assessment Created: 12/10/2015 2:53 PM Modified: 12/28/2015 8:23 PM Assessment Status: In Progress Checklist: 0/4
	Customer A - Security Assessment Created: 11/24/2015 11:34 AM Modfied: 2/10/2016 8:26 PM Assessment Status: In Progress Checklist: 3/3	Customer A - SQL Server Assessment Created: 11/27/2015 4:52 PM Modfied: 1/23/2016 7:45 PM Assessment Status: In Progress Checklist: 1/1	Customer A Created: 7/16/2015 9:11 PM Modified: 2/11/2016 11:18 AM Assessment: Status: In Progress Checklist: 0/2

# Step 2 — Select Manage Cyber Hawk Appliance and Access the Cyber Hawk Settings

After the Site has been opened, select the Cyber Hawk icon located within the Site bar.



The Cyber Hawk Settings window will be displayed.

#### **RapidFireTools**<sup>\*</sup>

	Cus	stomer A			Configure		Smart Tags		Notifications
		NDA	Host Type: Virtual 🥚	Active					
^	٠	Settings							
^	V_01	Daily Alerts	Add Recipient						
^		Weekly Notice	Add Recipient						
^	2	Reports	Add Delivery Schedule						

# Step 3 — Access Smart Tags and Verify that Scan Data has been Downloaded

Select the Smart Tags link within the Cyber Hawk's Settings window.

Customer A			Configure	Smart Tags
NDA NDA	Host Type: Virtual 🧕	Active		
∧ 🍓 Settings				
Daily Alerts	Add Recipient			
Weekly Notice	Add Recipient			
Reports	Schedule Report			

### Step 4 — Import a Smart Tags Configuration File

Select the Import option to import a Smart Tags configuration file.

Smart Tags	Import	Export
------------	--------	--------

A prompt will be presented requesting verification from you in order to continue the Import of the Smart Tags Configuration File.

	Import Smart Tag Warning	×
<u>^</u>	Importing a Smart Tag Configuration will remove all applied tags. Do you want to continue?	
	Yes No	

Select the Yes button to continue.

The Import Cyber Hawk Smart Tag Configuration window will be displayed.



Select the Smart Tag Configuration File name and select the Open button to perform the Smart Tag Import process.

## **Delete Smart Tags**

Use the following steps to delete a Smart Tag

### Step 1 — Open the Applied Tags Window and Select the Tag for Deletion

To access the Smart Tags that have been Applied from the Applied Tags list, select the Applied Tags option by selecting the Applied Tags bar.



The Applied Tags window will be displayed.

V	Applied Tags			
	11 Tags (151 Applied)			
	BUSINESS OWNER 1 user tagged	BUSINESS OWNER PC 1 computer tagged	DATABASE SERVER 4 computers tagged	HIPAA / ePHI AUTHORIZED USER 1 user tagged
	HIPAA / ePHI COMPUTER 122 computers tagged	NO DIRECT INTERNET ACCESS 3 computers tagged	VIRTUAL MACHINE 7 computers tagged	

### Step 2 — Select the Tag and Delete

Right click the mouse pointer on the tag to be deleted. A Remove Tag menu option will be presented.



Select the Remove Tag menu option and the tag will be deleted and removed from the Applied Tags window.



#### **RapidFireTools**°

# 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 the Network Detective 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 and Service Catalogs

To create a new Service Plan, follow these steps:

### Step 1 — Create a New Service Plan

- 1. After successfully deploying Cyber Hawk, visit <u>www.rapidfiretools.com/nd</u> to download and install the latest version of the Network Detective Application. Then run Network Detective and login with your credentials.
- 2. Select the Service Plans icon.



3. Select Create New Service Plan.

		Create New Service P	lan			
Service Plar	าร	Manage Plans				
	^	Silver (Silve	Silver (Silver)			
Manage Plans	ш	Sites	Policies	Scheduled Reports		
		1 •	12 •	0 🔻		
Manage Catalogs	+					

4. Enter the name and display name for your Service Plan.

Create New Service Plan	×
Enter a name for the Service Plan:	Zinc
Enter a display name for the Service Plan:	Zinc
ОК С	ancel

#### **RapidFireTools**°

Select **OK** to generate the basic Service Plan template. The modify Service Plan screen will appear.

Modify Service Plan						
Service Plan:	Zinc			Sa	ive	Delete
Display Name:	Zinc					
Description:						^
						$\vee$
Detector Po	odify		Scheduled Repo	orts	Modify	
0 of 33 policies selected 0 reports				) reports		
Plan Pricing Details						
Service Plan Monthly Charge (\$):		500	•			
Additional Hourly Billing Rate (\$):		150	÷			
Hours per Month Included:		2	*			
Emergency Auth	1000	<b>+</b>				
Plan Usage	•					
Site					Modifie	d

Before assigning the Service Plan to a Network Detective Site that is associated with a Cyber Hawk, you will need to specify the Service Plan's Policies and Scheduled Reports requirements.

Your Service Plan template will also be available within the Manage Plans window.
		Create New Service Plan			
Service Plans		Manage Plans			
Manage Plans	<b>^</b>	YourIT Company's Svc Plan 💉 >			
	E	Sites	Policies	Scheduled Reports	
Manage Catalogs	-	0 •	0 •	0 •	

**Note:** The default Service Plan template does not have any Network Detective Sites, Security Policies, or Scheduled Reports specified.

## Step 2 — Assign Security Policies to Your Service Plan

1. From the Modify Service Plan screen, click **Modify** next to Cyber Hawk policies.

Modify Ser	vice Plan				
Service Plan:	Zinc			Save	Delete
Display Name:	Zinc				
Description:					^
					~
Detector Po	olicies M	odify	Schedule	d Reports	Modify
0 of 33 policies s	selected		0 reports		
Plan Pricin	g Details				
Service Plan Mo	onthly Charge (\$):	500	÷		
Additional Hourly	y Billing Rate (\$):	150	÷		
Hours per Month	Included:	2	<b>+</b>		
Emergency Auth	norized Limit (\$):	1000	<b>+</b>		
Plan Usage	•				
Site				Modifie	ed

**RapidFireTools**<sup>®</sup>

Note: From the main Service Plan screen, you can access the Modify Service Plan screen by clicking the Edit Service Plan option  $\checkmark$ . **YourIT Company's Svc Plan**  $\checkmark$ Sites 0  $\checkmark$  Policies 0  $\checkmark$  0  $\checkmark$  0  $\checkmark$ 

2. Select the Security Policies tab and select the policies that you want to assign to your Service Plan.



3. As you select the Policies, be sure to familiarize yourself with the Smart Tags descriptions presented.



For each Security Policy that requires a Smart Tag set up to be performed, the Tags associated with a given security policy will need to be configured to fully enable the Cyber Hawk's Security Policy Violation detection.

- 4. After completing the selection of the Policies that you want associated with your Service Plan, click **Next**.
- 5. Next configure the notifications and actions for each security policy. Also assign email groups for those who will receive the notifications (End Users and/or your Tech Group(s). This tells Cyber Hawk what to do when it discovers a policy violation.

💽 Cyber Hawk Policies - Cadmium (Cadmium)	
Configure Notifications Add Global Email Group	Assign actions and groups to receive notifications
Policy Name	Action Group Name
<ul> <li>Access Control</li> </ul>	
Authorize New Devices to be Added to Restricted Networks	Email Tech 🔻 None
Investigate Suspicious Logons by Users	Email Tech 🔻 None
Investigate Suspicious Logons to Computers	Email Tech 🔻 None
Restrict Access to Accounting Computers to Authorized Users	Email Tech 🔻 None
Restrict Access to Business Owner Computers to Authorized Users	Email Tech 🔻 None
Restrict Access to Computers Containing ePHI to Authorized Users	Email Tech 🔹 None
Restrict Access to IT Admin Only Restricted Computers to IT Administrators	Email Tech 🔻 None
Restrict Access to Systems in the Cardholder Data Environment (CDE) to Authorized Users	Email Tech 🔻 None
Restrict IT Administrative Access to Minimum Necessary	Email Tech 🔻 None
Restrict Users that are Not Authorized to Log into Multiple Computer Systems	Email Tech 🔹 None

6. Click Finish.

## Step 3 — Define Reports Deliverables to be Included in the Service Plan

You have the ability to include references to one or more Network Assessment and Security Assessment Reports to be included as a part of your Service Plan deliverables to your customer.

The Reports you select to be included in the Service Plan deliverables will be referenced in three places within Network Detective:

- the Service Plan Scheduled Reports window
- the Service Catalog\* document generated by Network Detective
- the Service Plan Matrix document generated by Network Detective

**Note:** The Service Catalog document will enable you to present an overview of your company's Service Plan(s) to your clients.

**Important:** While the reports will be referenced as part of the Service Plan in the documents listed above, these reports are not generated automatically. You can generate them using the Network and/or Security Assessment modules. You can also generate them automatically using the Reporter appliance. See the <u>Reporter User</u> <u>Guide</u>.

Follow these steps to define the Reports deliverables for your Service Plan.

1. Select the Scheduled Reports tab to plan and document the Scheduled Report runs associated with a given Service Plan.



2. Select the Schedule Report button to define the Reports that should be part of the Service Plan you are creating.

	^	🔍 Manage Report Tasks	
Scheduled Reports Mor	dify	Schedule Report Reports	

You can define which Reports should be generated and at which Intervals (daily, weekly, monthly, etc.) the reports are to be generated.

3. Select from the Network and Security Reports listed in the Schedule Reports Wizard window, and select the Next button.

Network	Security	
🖂 🕽 A	l Network	Assessment Reports
	🦷 Standa	ard Reports
[	🗌 🗋 Cli	ent Risk Report (.docx)
	Ne 🗋	etwork Management Plan (.docx)
	🗌 📄 Fu	ll Detail Report (.docx)
[	🗌 🗋 Ex	cel Export (xlsx)
[	w	indows Patch Assurance Report (.docx) - BETA
	w	indows Patch Assurance Change Report (.docx) - BETA
[	🗌 📄 Sit	e Diagram (.docx)
[	🗌 📄 Sit	e Diagrams Export to Microsoft Visio (.zip)
[	🗌 📄 As	set Detail Report (.docx)
[	🗆 🚺 IT	SWOT Analysis Report (.docx)
[	🗌 🗋 Ne	etwork Assessment PowerPoint (.pptx)
[	w	indows Service Account Report (.docx)
[	🛛 🛶 La	yer 2-3 Diagram Report (.docx)
[	🗋 🚄 La	ver 2-3 Diagram Export to Microsoft Visio (.zip)

4. Using the Every list control, select the frequency from the choices available (i.e. day, week, month, year, or once). Select the Finish button once your selections are complete.

O Schedule Re	eport Wizard			X
Schedule				
Time Zone:	(UTC-05:00) Eastern Tim	e (US & Canada)		-
Every	month  day week	on the 28th	▼ at	12:00 AM 🗘
	month year once	Back	Next	Finish

After you have selected the Reports that are a part of the Service Plan, and have assigned the frequency of Report generation, these reports will be listed in the Scheduled Reports window.

When a Service Plan has been assigned to a Network Detective Site used with a Cyber Hawk, you can use the Reporter Appliance to schedule the actual automatic Report generation tasks to generate the reports deliverables for your service plans.

Manage Report Tasks	<
Schedule Report	
Reports Repeats	
😢 NetworkAssessment-Client Risk Report Weekly	
😢 NetworkAssessment-Network Management Plan 🛛 Weekly	
😢 NetworkAssessment-Full Detail Change Report Monthly	
😢 NetworkAssessment-Quarterly Business Review Monthly	

**Note:** When selecting a particular Report, or a group of Reports to be included in a Service Plan, you will need to define how frequently that the Reports are to be generated by your team as part of delivering your company's security service associated with the Service Plan.

5. Select the Save button to save your Service Plan Reports selections and configurations.

Modify S	ervice Plan	
Service Plan:	YourIT Company's Svc Plan	Save Delete

The Manage Plans window will list your newly created Service Plan and present the details associated with the plan.

anage Plan	S				
Silver		/ ×	Gold		× ×
Sites	Policies	Scheduled Reports	Sites	Policies	Scheduled Reports
0 •	10 •	2 •	1 v 18 v		1 •
YourIT Co	mpany's Svc	Plan 💉 🗙	Platinum		× ×
YourIT Co	mpany's Svc Policies	Plan 💉 🗙 Scheduled Reports	Platinum Sites	Policies	Scheduled Reports

The details include the number of:

- Network Detective Sites that use the plan
- Security Policies assigned to the plan itself
- Reports that are to be generated and delivered to the customer as part of a particular Service Plan

## Step 4 — Create a Service Catalog

1. Select the Service Plans icon.



2. Select the Manage Catalogs Icon.

#### **RapidFireTools**°

	Create New Service P	Plan				
Service Plans	Manage Plans	5				
	Silver (Silve	ər)	/ ×	Gold (Gold	I)	/ ×
Manage Plans	Sites 1 ▼	Policies 12	Scheduled Reports 0 ▼	Sites 2 •	Policies 18	Scheduled Reports 0 ▼
Manage Catalogs	Platinum (F	Platinum)	/ ×	Titanium (1	litanium)	/ ×
	Sites	Policies 23	Scheduled Reports	Sites	Policies	Scheduled Reports 22 ▼

All of the available Service Catalogs will be available within the Catalog Name drop down list found within the Service Catalog window.

Service Plans	Manage Catalogs Generate
Manage Plans	Catalog Name: All Plans           All Plans         Clone         Remove         Include All Plans           All Plans         Silver Gold Platinum Catalog 1         Catalog 1         Catalog 1         Catalog 1
Manage Catalogs	New Variant Catalog Security Services Catalog Description SMB Service Catalog HIPAA Services Mike SMB Silver Gold Variant 1 Managed Services Offerings
	Authorize N Super Small SMBs stricted Networks PCI Service Catalog
	Install Critic MyClient Company Service Plan Small Office Solution ters within 30 Days

3. To create a new Service Catalog, select the default Catalog named "All Plans" and select the Clone button.

Service Plans	Manage Catalogs Generate
Manage Plans	Catalog Name: All Plans Clone
Manage Catalogs	Description

4. Enter in the Catalog Name and select the OK button to create the new catalog.



5. Select the Exclude option to hide each of the plans you do not want to be included in the Service Catalog document to be generated.

Service Plans	Manage Catalogs	Generate	)		
	Catalog Name: Your IT Company	y Catalog 🗸	Clone Remov	/e Include All Pl	ans
Manage Plans	Description	Silver (Silver) Exclude	YourIT Company's Svc Plan (YourIT Company's Svc Plan) <u>Exclude</u>	Gold (Gold) Exclude	Platinum (Platinum) Exclude

6. The remaining Service Plans not excluded from your new Service Catalog will be contained within the catalog.

Service Plans	Manage Catalogs Generate			
	Catalog Name: Your IT Company Catalog 🔽 Clone Remo	ve Include All Pl	ans	
Manage Plans	Description	Yourl T Company's Svc Plan (Yourl T Company's Svc Plan) Exclude	Gold (Gold) Exclude	Platinum (Platinum) Exclude
	Authorize New Devices to be Added to Restricted Networks	*	*	*

The Service Catalog you created will be automatically saved for future use.

## Generate a Service Catalog Document

After you have created a Service Catalog, you can use Network Detective to 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 and Procedures, and a list of Reports deliverables.

To generate the Service Catalog document, follow these steps:

1. Select the Service Plans icon.

💽 Network Det	tective			
		/		
Home	InForm	Appliances	Connector	Service Plans

2. Select the Manage Catalogs Icon.

Service Plans	Manage Catalogs Gene	erate			
	Catalog Name: All Plans	Clone	e Remove Inc	lude All Plans	
Manage Plans	Description	Silver (Silver)	Gold (Gold)	Platinum (Platinum)	Titanium (Titanium)
Manage Catalogs	Authorize New Devices to be Added to Restricted Networks	*	*	*	1

3. All of the Catalogs will be presented in the Catalog Name list.

Service Plans	Manage Ca	talogs Generate				
Marrow Direct	Catalog Name:	All Plans	Clone	Remove	lude All Plans	
Manage rians	Descriptio	Silver Gold Platinum Catalog 1 New Variant Catalog	r r)	Gold (Gold)	Platinum (Platinum)	Titanium (Titanium)
Manage Catalogs	Authorize N Added to R	Security Services Catalog SMB Service Catalog HIPAA Services Mike SMB		*	~	*
	Install Critic Network Co Days	Silver Gold Variant 1 Managed Services Offerings Super Small SMBs PCI Service Catalog MyClient Company Service Plan		*	*	*
	Only Conne	Small Office Solution		×	<b>~</b>	<b>~</b>

4. To generate the Service Catalog document, select the name of the Catalog from the Catalog Name list.

Service Plans	Manage Catalogs	Generate
	Catalog Name: Silver Gold Pla	Service Plan Catalog Plan Matrix
Manage Plans		

5. Select the Generate and then select the Service Plan Catalog menu option to generate the Service Catalog document.

Service Plans	Manage Catalogs	Generate
Manage Plans	Catalog Name: Silver Gold Platin	um

6. Network Detective will generate the Service Catalog document and open Microsoft Word so that you may edit and print the document.



## Generate a Service Plan Matrix Document

After you have created a Service Plan, you can use Network Detective to generate a Service Plan Matrix document in Microsoft Word format.

The Service Plan Matrix document will contain a list of the Security Policies you have assigned to your Service Plan(s) along with a list of Reports deliverables.

To generate the Service Plan Matrix document, follow these steps:

1. Select the Service Plans icon.



2. Select the Manage Catalogs Icon.

Service Plans	Manage Catalogs Generate					
	Catalog Name: All Plans	Clone	e Remove Inc	lude All Plans		
Manage Plans	Description	Silver (Silver)	Gold (Gold)	Platinum (Platinum)	Titanium (Titanium)	
Manage Catalogs	Authorize New Devices to be Added to Restricted Networks	*	*	*	*	

3. All of the Catalogs will be presented in the Catalog Name list.

Service Plans	Manage Catalogs Generate				
	Catalog Name: All Plans	Clon	e Remove Inc	lude All Plans	
Manage Plans	Descriptio Catalog 1 New Variant Catalog Servity: Service Catalog	er 11)	Gold (Gold)	Platinum (Platinum)	Titanium (Titanium)
Manage Catalogs	Authorize N SMB Service Catalog Added to R HIPAA Services Mike SMB		*	~	
	Silver Gold Install Critic Variant 1 Network Co Managed Services Offerings Super Small SMBs Days PCI Service Catalog Mc/Citer Company Service Plat		~	*	~
	Only Conne Small Office Solution		×	×	×

4. To generate the Service Plan Matrix document for a specific Catalog, select the name of the Catalog from the Catalog Name list.

Service Plans	Manage Catalogs	Generate
Manage Plans	Catalog Name: Silver Gold Platin	num 🔽

5. Select the Generate and then select the Plan Matrix menu option to generate the Plan Matrix document.

Service Plans	Manage Catalogs	Generate
	Catalog Name: Silver Gold Pla	Service Plan Catalog Plan Matrix
Manage Plans		

6. Network Detective will generate the Plan Matrix document and open Microsoft Word so that you may edit and print the document.

Policy	YourIT Company's Svc Plan
Install Critical Patches on Network Computers within 30 Days	1
Investigate Suspicious Logons by Users	×
Investigate Suspicious Logons to Computers	1
Authorize New Devices to be Added to Restricted Networks	×
Only Connect to Authorized Printers	×
Remediate High Severity Internal Vulnerabilities Immediately (CVSS > 7.0)	×
Restrict Access to Accounting Computers to Authorized Users	1
Restrict Access to IT Admin Only Restricted Computers to IT Administrators	×
Restrict Access to Business Owner Computers to Authorized Users	1
Restrict IT Administrative Access to Minimum Necessary	×
Restrict Users that are Not Authorized to Log into Multiple Computer Systems	1
Strictly Control the Addition of New Local Computer Administrators	~
Strictly Control the Addition of New Users to the Domain	1
Users Should Only Access Authorized Systems	~
Changes on Locked Down Computers Should be Strictly Controlled	1
Install Critical Patches for DMZ Computers within 30 Days	-
Only Connect to Authorized Wireless Networks	~
Remediate Medium Severity Internal Vulnerabilities (CVSS > 4.0)	~
Detect Network Changes to Internal Networks	1
Restrict Access to Computers Containing ePHI to Authorized Users	
Restrict Internet Access for Computers that are Not Authorized to Access the Internet Directly	r
Detect Network Changes to Internal Wireless Networks	

- 7. The Security Policies associated with the Plan are in the document.
- 8. And a list of Reports deliverables associated with the plan are referenced the Report Tasks section of the Service Plan's Matrix.

Repor	t Tasks	
Scheduled Reports		YourIT Company's Svc Plan
Weekly	Network Assessment-Client Risk Report	✓
Weekly	Network Assessment-Network Management Plan	✓
Monthly	Network Assessment-Full Detail Change Report	✓
Monthly	Network Assessment-Quarterly Business Review	✓

# Generate a Sample Master Services Agreement for a Service Plan

After you have created a Service Plan, you can use Network Detective to generate a sample Master Services Agreement (MSA) document in Microsoft Word format.

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:

## Step 1 — Opening Existing Network Detective Site that is Associated with your Cyber Hawk

- 1. Start the Network Detective application.
- 2. Select the Site that that is Associated with your Cyber Hawk Appliance.



3. To open the Site, double-click on the Site name.

## Step 2 — Access the Cyber Hawk Settings

After opening the Site associated with your Cyber Hawk Appliance, select the Cyber Hawk Settings icon located on the left side of the Network Detective window to view the Cyber Hawk's Settings.



## Step 3 — Select the Policy Configuration Option

The Policy Configuration option enables you to configure Cyber Hawk to detect violations of Access Control, Computer, and Network Security policies that take place within the network.

Within the Policy Configuration window, you have the option to generate the Sample Master Service Agreement that is associated with the selected Service Plan's Security Policies that you have defined for your Cyber Hawk.



In the Cyber Hawk Settings window, select the Policy Configuration Modify button to access the Policy Configuration options window.

The Policy Configuration window will be displayed.



## Step 4 — Generate Master Service Agreement Option

1. Select the Generate button in the Policy Configuration window.



2. Next, select the Master Service Agreement Option.

3. The MSA Customization window will be displayed.

MSA Customization		×
MSP Name:	YourIT Company From Company Info Tab	
MSP State:	Enter Your State's Name Here	
MSP Address:	Enter Your Address Here	*
		Ψ.
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	*
Emergency Authorized Limit (\$):	1000	-
Effective Date:	Thursday , April 20, 2017	
	OK Cancel	

## Step 5 — Enter the MSP information, Customer information, and Service Plan Cost Details

- 1. In the MSA Configuration window, enter the MSP Name, State, and Address along with the Customer Name and Address.
- 2. Next, enter the Service Plan Monthly Charge, Additional Hourly Billing Rate, Hours per Month Included, Emergency Authorized Limit, and the Effective Date to be referenced in the sample MSA.
- 3. After entering the MSA Configuration information, select the OK button.

4. The Disclaimer notification and confirmation window will be displayed.



## Step 6 — Confirm Acceptance of the Disclaimer and Generate the Sample MSA

Select the OK button in the Disclaimer window to generate the Sample MSA in Word format.

Network Detective will generate the Master Services Agreement document and open Microsoft Word so that you may edit and print the document.



## Managing Service Plans

The instructions below detail the processes used to Modify and Delete Service Plans.

#### Edit a Service a Plan

**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.

To edit a Service Plan, follow these steps:

1. Select the Service Plans icon.



2. Select the Edit icon on the Service Plan that you would like to edit.

Manage Plans	;	
Silver		✓ ×
Sites	Policies	Scheduled Reports
0 🔻	10 🔻	2 •
YourIT Con Sites 0 •	Policies	Plan 💉 × Scheduled Reports 4 🔻

#### **RapidFireTools**°

3. The Modify Service Plan window will be displayed.



4. Change the Cyber Hawk Security Policies, the plan's Scheduled Reports settings, or the Name of the plan, and select the Save button.

#### Delete a Service Plan

**Important:** When you delete a Service Plan, any Sites using that plan will have their plan updated to "Custom" and the configuration for those Sites will be retained. You can later go to those Sites and apply a different plan to them if you wish.

To Delete a Service Plan, follow these steps:

1. Select the Service Plans icon.



2. Select the Edit icon on the Service Plan that you would like to Delete.

Manage Plans				
Silver		/ ×		
Sites	Policies	Scheduled Reports		
0 •	10 🔻	2 •		
YourIT Com Sites 0 ▼	Policies 19 V	Plan 🖍 🔀 Scheduled Reports 4 🔻		

3. Confirm the deletion of the Service Plan you selected.



4. The selected Service Plan is deleted and is removed from the Manage Plans window.

#### **RapidFireTools**°



## **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. Select the Service Plans icon.



2. Select the Manage Catalogs icon.

Service Plans	Manage Plans	;	
	Silver (Silve	× ×	
Manage Plans	Sites	Policies	Scheduled Reports
	3 🔻	12 🔻	0 🔻
Manage Catalogs			

3. Select Service Catalog Name for the Catalog that you would like to edit.



4. The selected Service Catalog will be displayed in the Manage Catalogs window. This Catalog will include the Service Plans previously added to the Catalog.

Manage Catalogs Generate			
Catalog Name: Your IT Company Catalog V Clone Remove Include All Plans			
Description	YourlT Company's Svc Plan (YourlT Company's Svc Plan) Exclude	Gold (Gold) Exclude	
Authorize New Devices to be Added to Restricted Networks	~	×	

5. Select the Include All Plans button.

#### **RapidFireTools**<sup>®</sup>

Manage Catalogs Generate	
Catalog Name: Silver Gold Platinum	Clone Remove Include All Plans
Description	

- 6. This action will add all of the other Service Plans that are currently not listed within the Catalog's Service Plan list.
- 7. 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.

Manage Catalogs Generate							
	Catalog Name: Silver Gold Platinum	Clone Remo	ve Include All Pla	ins			-
	Description	Silver (Silver) Exclude	YourIT Company's Svc Plan (YourIT Company's Svc Plan) Exclude	Gold (Gold) Exclude	Platinum (Platinum) Exclude	Titanium (Titanium) Exclude	
	Authorize New Devices to be Added to Restricted Networks	~	~	~	~		
	Install Critical Patches on Network Computers within 30 Days	•	~	•	~	•	

8. After you have Excluded the Services Plans that are not required, exit the Service Plan Creator.

### Edit a Service Catalog

To edit a Service Catalog, follow these steps:

1. Select the Service Plans icon.



2. Select the Manage Catalogs icon.

Service Plans	Manage Plans	;	
	Silver (Silve	× ×	
Manage Plans	Sites	Policies	Scheduled Reports
	3 🔻	12 🔻	0 🔻
Manage Catalogs			

3. Select Service Catalog Name for the Catalog that you would like to edit.



4. The selected Service Catalog will be displayed in the Manage Catalogs window.

Manage Catalogs Generate		
Catalog Name: Your IT Company Catalog Clone Remove Include All Plans		
Description	YourIT Company's Svc Plan (YourIT Company's Svc Plan) Exclude	Gold (Gold) Exclude
Authorize New Devices to be Added to Restricted Networks	×	×

At this point in the process, you may:

- Add Service Plans to a Catalog
- Exclude Service Plans from a Catalog
- Remove the selected Catalog entirely from the Service Plan Creator

### Remove (Delete) a Service Catalog from the List of Catalogs

To Remove (delete) an entire Service Catalog, follow these steps:

1. Select the Service Plans icon.



2. Select the Manage Catalogs icon.

Service Plans	Manage Plans			
	Silver (Silve	/ ×		
Manage Plans	Sites	Policies	Scheduled Reports	
	3 🔻	12 🔻	0 🔻	
Manage Catalogs				

3. Select Service Catalog Name for the Catalog that you would like to Remove.

Service Plans	Manage Catalogs Generate
	Catalog Name: Silver Gold Platinum Clone Remove
Manage Plans	Silver Gold Platinum Small Office Solution Description Your IT Company Catalog Titanium
Manage Catalogs	Authorize New Devices to be Added to Restricted Networks

The selected Service Catalog will be displayed in the Manage Catalogs window.

Manage Catalogs Generate		
Catalog Name: Your IT Company Catalog V Clone Remove Include All Plans		
Description	YourlT Company's Svc Plan (YourlT Company's Svc Plan) Exclude	Gold (Gold) Exclude
Authorize New Devices to be Added to Restricted Networks	×	×

4. Select Remove button to delete the Catalog from the Service Plan Creator.



5. The Catalog that you Removed will no longer be present in the Catalog Name list.

Catalog Nam	e: Your IT Company Catalog	~	Clone	Remove	Include All Plans
	Silver Gold Platinum Titanium				
Descripti	on				
Authorize	New Devices to be Added	to Re	stricted	Networks	

## Delete (Exclude) Service Plans from a Catalog

To delete a Service Plan from a Service Catalog, follow these steps:

1. Select the Service Plans icon.



2. Select the Manage Catalogs icon.



3. Select Service Catalog Name for the Catalog that you would like to edit.

Service Plans	Manage Catalogs Generate
Manage Plans	Catalog Name: Silver Gold Platinum  Clone Remove All Plans Silver Gold Platinum Small Office Solution
Manage Catalogs	Description         Your IT Company Catalog           Titanium         Titanium

4. The selected Service Catalog will be displayed in the Manage Catalogs window. This Catalog will include the Service Plans previously added to the Catalog.

Manage Catalogs Generate		
Catalog Name: Your IT Company Catalog V Clone Remove Include All Plans		
Description	YourIT Company's Svc Plan (YourIT Company's Svc Plan) Exclude	Gold (Gold) Exclude
Authorize New Devices to be Added to Restricted Networks	×	×

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.

Catalog Name: Your IT Company Catalog V Clone Remove Include All Plans				
Description	YourIT Company's Svc Plan (YourIT Company's Svc Plan) Exclude	Gold (Gold) Exclude	Platinum (Platinum) Exclude	
Authorize New Devices to be Added to Restricted Networks	~	*	~	

- 6. Select the Exclude Link to remove the specific Service Plan selected from the Service Catalog.
- 7. The Excluded Service Plan will no longer be listed within the Service Catalog user interface unless re-added in the future.

## 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		✓	✓	✓
Users Should Only Access Authorized Systems		✓	√	✓
Changes on Locked Down Computers should be Strictly Controlled			✓	✓
Install Critical Patches for DMZ Computers within			✓	✓

#### **RapidFireTools**\*

Security Policy Description	Bronze	Silver	Gold	Platinum
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				
Enable automatic screen lock on computers with sensitive information				
Enable automatic screen lock for users with access to sensitive information				

Security Policy Description	Bronze	Silver	Gold	Platinum
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)				

#### **RapidFireTools**\*

## Appendices

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

Configure Cyber Hawk Using the Setup Wizard (RapidFire Tools Server)	
Step 1 — Configure Scan Settings	
Step 2 — Schedule Scans and Alert Notifications	
Step 3 — Configure Tech Email Groups	
Step 4 — Configure End User Email Groups	
Step 5 — Perform Pre-Scan Analysis	
Step 6 — Perform Initial Cyber Hawk Scan	
Step 7 — Configure Policies	231
Step 8 — Configure Notifications	
Step 9 — Configure Smart Tags	
Step 10 — Set Up RapidFire Tools Portal	
Additional Scan Host Configuration Options and Requirements	
Scan Host Diagram	
Scan Host Requirements	
Assigning Scan Hosts in a Domain Environment	
Pre-Scan Network Configuration Checklist	242
Checklist for Domain Environments	242
Checklist for Workgroup Environments	
RapidFire Tools Server vs. Virtual Appliance	
Sample Daily Alerts and Weekly Notices	
Sample Tech Alert	
Sample End User Alert	
Sample Weekly Notice	
Edit Policies Enforced at a Site	
Unitrends Backup Alerts	
Requirements for Unitrends Backup Alerts	
How to enable Unitrends Backup Alerts (Web Console)	
How to enable Unitrends Backup Alerts (Network Detective)	
Audit Log	

# Configure Cyber Hawk Using the Setup Wizard (RapidFire Tools Server)

**Note:** This topic covers how to configure Cyber Hawk after you have installed the Cyber Hawk **RapidFire Tools Server** on the target network. If you are using the Cyber Hawk **Virtual Appliance** instead, see <u>"Configure Cyber Hawk Using the Setup Wizard (Virtual Appliance)" on page 17</u>.

After you have associated the Cyber Hawk with the Site, click on the Cyber Hawk icon:



The **Cyber Hawk Initial Setup Wizard** will appear. This wizard will guide you through the setup process and help you get the most out of your new Cyber Hawk. Click **Next** to begin the set up.

Q Cyber Hawk Initial Setup Wizard	×
Welcome	
The Cyber Hawk initial setup wizard will walk you through the initial setup and com performed in this wizard can be accessed in the Cyber Hawk administrative interfa practice of setting up Cyber Hawk scans, policies, notifications, Smart Tags, and a	iguration process at this site. All actions ce. This wizard walks through the best lerting.
At any time, you may exit the wizard using the [Close] button and resume later. Alt use this wizard to guide you through the initial setup process, you can always con select "Do not show again for this Site" before exiting the wizard.	hough it is highly recommended to figure Cyber Hawk manually. Simply,
Do not show again for this Site	Back Next Close

**Tip:** If you need to stop midway through the Cyber Hawk Initial Setup Wizard, don't worry. You can return to the Cyber Hawk screen for your Site and continue where you left off.

**Note:** This section of the guide walks you through the Initial Setup Wizard. This guide also contains separate topics on configuring Cyber Hawk settings. Refer to these topics if you need to change Cyber Hawk after you have completed the initial set up process using the Wizard.

The steps below break down each part of the configuration process.

**Important:** For best results, the target network must be configured to allow for successful scans on all network endpoints. See <u>"Pre-Scan Network Configuration</u> <u>Checklist" on page 242</u> for configuration guidance for both Windows Active Directory and Workgroup environments.

## Step 1 — Configure Scan Settings

In this step you will configure the Scan Settings for the Cyber Hawk. Click Next.

Q Cyber Hawk Initial Setup Wizard	×
Configure Scan Settings	
Cyber Hawk will perform on-going scans using the settings provided in its Scan Co wizard will walk you through setting specific scan settings, including credentials, tar other options.	nfiguration. The Scan Configuration get network, domain, SNMP, and
Do not show again for this Site	Back Next Close

- 1. Select how you wish to treat computers that are not associated with Active Directory. You can treat them as:
  - part of the Primary Domain
  - part of a domain that you specify

Important: Do not select the "Don't treat them as part of a domain".

This will re	sult in Alerts not being sent.
Scan Configuration Wiza	rd — — X
Merge Option	Merge Option
Active Directory	How do you want to treat computers that are not associated with Active Directory?
Local Domains	Treat them as part of the Primary Domain ("domain with most computers)
Additional Credentials	O Treat them as part of the specified domain:
IP Ranges	
SNMP Information	
File Scanner	
VMware	
Unitrend Backup	
Confirm	
	< Back Next > Cancel

2. Enter credentials *with administrative rights* to connect to a Domain Controller with Active Directory. Click **Next** to test a connection with the Domain Controller and verify your credentials.

**Important:** Enter the username in the **domain\username** format. Use the Fully Qualified Domain Name (FQDN).

/ Marra Oakan	Active Directory	
Active Directory	Please enter a usemame and password with administrative rights to connect to	
Local Domains	<ul> <li>If you are scanning a workgroup environment, enter credentials which can access the individual workstations as a local administrator.</li> </ul>	
Additional Credentials	I want to scan	
IP Ranges	Active Directory domain     Workgroup (no domain)	
SNMP Information	Active Directory Credentials     If in a domain, please enter the Fully Qualified Domain Name (i.e.,	
File Scanner	Corpunyco.com instead or the shortened name - MTCO)	1.4
/Mware	Password:	] (domain \user)
Jnitrend Backup	Domain Controller: dc	]
Confirm		
		_

3. If you are scanning a domain, choose whether to scan the entire domain or specific Organizational Units (OUs). Then click **Next**.

Scan Configuration Wizard		-		×
Verge Option	Local Domains			
<ul> <li>Active Directory</li> </ul>	Below is a list of the detected domains in the current forest of Active Directory.			
Local Domains	Gather information for ALL the domains detected.			
Additional Credentials	Gather information for only the Domains and OUs selected below.			۱ ۲
IP Ranges				
SNMP Information				
File Scanner				
VMware				
Unitrend Backup				
Confirm				
	Expand All Collapse All Expand Selected			-
	< Back N	ext >	Cano	el

4. If you are scanning a Domain, enter any additional network scan credentials to connect to remote workstations. Then click **Next**.
| 💽 Scan Configuration Wizard          | -  |        |
|--------------------------------------|--|--------|
| ✓ Merge Option                       | Additional Credentials (optional)  |        |
| <ul> <li>Active Directory</li> </ul> | Network scan credentials are required to perform remote Windows data collection via WMI and<br>Remote Benistry. Use this screen to ontionally add additional credentials to be used during the |        |
| 🖌 Local Domains                      | scan. Calls using the default credentials will always be attempted first.  |        |
| Additional Credentials               |  |        |
| IP Ranges                            | Network Scan Credentials   |        |
| SNMP Information                     | Password:  |        |
| File Scanner                         |  | Add    |
| VMware                               |  |        |
| Unitrend Backup                      |  |        |
| Confirm                              |  |        |
|                                      |  |        |
|                                      |  |        |
|                                      |  |        |
|                                      | Clear All  |        |
|                                      |  |        |
|                                      | < Back Next >  | Cancel |
|                                      |  |        |

5. From Scan Credentials, enter credentials *with administrative rights* to perform remote Windows data collection via WMI and Remote Registry. Use this screen to optionally add additional credentials to be used during the scan. Then click **Next**.

Scan Configuration Wizard	-	□ ×
✓ Merge Option	Scan Credentials	
<ul> <li>Active Directory</li> </ul>	Network scan credentials are required to perform remote Windows data collection via WMI and Remote Registry. Use this screen to optionally add additional credentials to be used during the	
Scan Credentials	scan.	
IP Ranges		
SNMP Information	Network Scan Credentials	
File Scanner	Password:	
VMware		Add
Unitrend Backup		
Confirm		
	Clear All	
	< Back Next >	Cancel

6. 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**. Then click **Next**.

🔍 Scan Configuration Wizard			_		×
Verge Option	IP Ranges				
Active Directory	Auto-Detected IP Ranges on Remote Appliance				
🖌 Local Domains	10255				
🖌 Additional Credentials					
IP Ranges	IP Ranges to Scan				
SNMP Information	Single IP or IP Range Add	1			
File Scanner	10. 255	1			
VMware					
Unitrend Backup					
Confirm					
		L.	Exclu	ude IPs	
			Reset to Ar	uto-Detect	ted
			Import fro	m Text File	e
			Clear A	VI Entries	
	< Back	1	Next >	Car	ncel
J					

From this screen you can also:

- Click Exclude IPs to remove certain IP ranges from the scan.
- Click **Reset to Auto-Detected** to reset the automatically suggested IP Range.
- Click **Import from Text File** to import a predefined list or range of IP addresses.



7. A confirmation window will appear estimating the amount of time the scan will take for the designated IP Range. If the scan will take too much time, reduce the size of the IP range. Click **OK**.



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

💽 Scan Configuration Wizard	- 🗆 X
✓ Merge Option	SNMP Information
Active Directory	SNMP community strings are used to try to determine information about devices detected during the IP Bange scan. Enter any additional community
🖌 Local Domains	strings used on this network.
🖌 Additional Credentials	Read Community String Add
IP Ranges	public
SNMP Information	
File Scanner	Reset to Default Import from Text File Clear All Fritries
VMware	Advanced SNIMD Options
Unitrend Backup	SNMP Timeout (seconds): 3 Use Default
Confirm	Attempt SNMP against non-pingable devices (slower but more accurate)
	< Back Next > Cancel

- 9. 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 (HIPPA) 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

💽 Scan Configuration Wizard	- 0	×
✓ Merge Option	File Scanner	
<ul> <li>Active Directory</li> </ul>	Perform file scan on: <a href="https://www.englight.com">www.englight.com</a>	
🖌 Local Domains	NOTE: File scanning can cause a temporary increase in resource utilization.	
🖌 Additional Credentials	Scan Types:	
🗸 IP Ranges	ePHI (HIPAA)	
SNMP Information	Cardholder Data (PCI)	
File Scanner		
VMware		
Unitrend Backup		
Confirm		
		_

Then click Next.

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**.

🔍 Scan Configuration Wizard				-		×
✓ Merge Option	VMware (optic	onal)				
Active Directory	VMware credential VMware host serve	s are required for er DNS name or If	discovery of VMware hosts. Enter the <sup>o</sup> address along with VMware login creder	itials.		
🖌 Local Domains	If the server uses a hostname field in th	a non-standard ad ne format "hostnar	ministrative port, specify the port in the ne:port".			
Additional Credentials	Hostname or IP A	Address	Username			
✓ IP Ranges			Password			
SNMP Information			Add VMware Serve	er		
🖌 File Scanner	Used	User				
VMware	Host	User				
Unitrend Backup						
Confirm						
	Clear All Entri	es				
			< Back	Next >	Car	ncel

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

**Note:** If you wish, you can use this screen to set up a connection between Cyber Hawk and your Unitrends Backup account. This will allow you to use Unitrends Backup security policies and alerts with Cyber Hawk.

💽 Scan Configuration Wizard				-		×
🖌 Merge Option	Unitrend E	Backup				
Active Directory	Enter server a	and crendtial infomration for any Unitrends B	ackup Servers.			
🖌 Local Domains	Server:	Hostname or IP Address				
🖌 Additional Credentials	Usemame:	Username				
🗸 IP Ranges	Password:	Password	Add Unitrends Server			
SNMP Information	qa@10.200.	.1.150				
🗸 File Scanner						
🗸 VMware						
Unitrend Backup						
Confirm						
	Clear Al	Entries Test Connections				
			< Back Ne	xt >	Can	cel

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

Unitrends Test Results	×
qa@10.200. Success	
	ок

13. Click **Finish** to save your scan settings. If you are using a **Reporter** appliance, you can also choose whether to upload the finished scans to the Reporter.

🔍 Scan Configuration Wizard	-		×
✓ Merge Option	Confirm		
Active Directory	Press Finish to save your settings. Use the Back button to go back and modify settings		
🖌 Local Domains			
Additional Credentials			
/ IP Ranges			
SNMP Information			
File Scanner			
VMware	Advanced Options At least one advanced option is enabled.		
/ Unitrend Backup			
Confirm	Upload trinshed scan to Reporter Server Setting     Do not scan the host computer		
	Modify Settings < Back Finish	Ca	ncel

# Step 2 — Schedule Scans and Alert Notifications

In this step you will configure the scanning and alert schedules for Cyber Hawk.

Q Cyber Hawk Initial Setup Wizard	×
Configure Schedules	
Cyber Hawk will perform both Daily and Weekly scans and notifications. The next configuration for a typical Cyber Hawk. You may adjust the scan and notification d scans need to be performed before alerts and notices can be sent.	dialog will show the default ay and time if desired. Be aware that
Press Next to launch the scan scheduling dialog.	
Do not show again for this Site	Back Next Close

- 1. In the Schedule screen, enter the required information as in the image below:
  - a. Time Zone
  - b. **Time for Level 1 Scan (Daily)**: This is the time for the daily Cyber Hawk scan. You can also choose whether to enable or disable the scan. It is Enabled by default.
  - c. **Time for Level 2 Scan (Weekly)**: This is the time for the weekly Cyber Hawk scan. You can also choose whether to enable or disable the scan. It is Enabled by default.
  - d. **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).

e. **Weekly Notice**: This is the time that Cyber Hawk will send out a weekly notice to End Users and the Tech Group (default is Monday at 8:00am).

Schedule			×
Time Zone:	(UTC-05:00)	Eastern Time (US & Canada)	~
Level 1 Scan (Daily):	01:00 AM	Enabled	
Level 2 Scan (Weekly):	01:00 AM	🗘 Saturday	
Daily Alert:	08:00 AM	🗘 🗹 Mon 🗹 Tue 🗹 Wed 🗹 Thu 🗹 Fri	Sat Sun
Weekly Notice:	08:00 AM	🗘 Monday 🗸 🗸	
		Save Discard	

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

# Step 3 — Configure Tech Email Groups

In this step you will configure the email addresses and groups of users for your Technician Group. This is the group that will respond to security alerts sent by Cyber Hawk.

You can choose whether to use a pre-existing Global Tech Email Group, or a Site Specific Tech Email Group.

**Note:** If you choose to use a Global Email Group, you can select from among your pre-existing Global Email Groups or create a new one.

If you choose to create a Site-Specific email group, the list of Global Email Groups will be grayed-out.

Later, you can continue to create and edit Global Email Groups from **Preferences** > **Email Groups** at any time. You can also later create and edit site-specific email groups from the Cyber Hawk **Email Configuration** button at your specific Site.



- 1. Select an option and click **Next**.
- 2. To select an existing email group, click on a group from the menu and click **Save & Close**.

Dolan and Mittel	2 X	Foosite User Group	Global Tech Group	▲ ×
Tech		Tech	Tech	
Internal IT Tech	• ×	JD RFT Tech Group - 💉 X Global Tech	JDolan Group Tech	<i>i</i> ×
			¢	

- 3. To add a new email group, click Add Email Group.
- 4. Enter information for the new email group. You will need to add each individual email address for the email group. You can do this by selecting from the list of existing users associated with your account.

💽 Add Email Group		×
Name:	Test User 1	
Group Type:		~
Designated Tech Group:		$\sim$
To	<type a="" address="" email="" enter="" new="" to=""></type>	
	OK Cancel	

5. When you are finished, click **OK**.

**Note:** Once you complete the Setup Wizard, see <u>"Allow Clients to Access Portal and Manage Tickets" on page 140</u> for more options on setting up Cyber Hawk for users outside of your organization.

# Step 4 — Configure End User Email Groups

Next you will configure the End User Email Group for your site.

**Note:** You cannot create Global End User Email Groups. You can only create site-specific end user email groups.

Cyber Hawk Initial Setup Wizard	×
Configure End User Email Groups	
End User Email Groups can receive some alert notifications directly. Certain policies are best sent to en triage purposes. You can setup end-user email groups now or later.	d-users first for
Create Site Specific End User Email Groups	
🔿 Skip	
Do not show again for this Site	Close

1. To add a new email group, click Add Email Group.

💽 Add Email Group		×
Name:	Test User 2	
Group Type:	End User	~
Designated Tech Group:	Test User 1	$\sim$
To	<type a="" address="" email="" enter="" new="" to=""></type>	
$\searrow$	OK Cancel	

- 2. Enter information for the new email group. You will need to add each individual email address for the email group. You can do this by selecting from the list of existing users associated with your account. You can also type a new email address into the field.
- 3. When you are finished, click **OK**.

4. Next configure how Cyber Hawk will handle Administrative emails. This includes errors related to scans or notifications. Enter the email addresses for the recipient(s) of Administrative emails. Then click **Next**.

**Tip:** The Administrative Emails recipient will also receive the results of the prescan 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.

💽 Cyber	Hawk Initial Set	up Wizard		×
Admi	nistrative E	mails		
Cyber H Configu	lawk can be c ire the Admin	onfigured to notify you of scan and notification errors. Email settings below.		
То	8	@rapidfiretools.com		
	<type td="" to<=""><td>enter a new email address&gt;</td><td></td><td></td></type>	enter a new email address>		
	Subject Prefix:	%%SITE%%		
	Core Failer	d (a birst) confine Cons Fridad)		
	Notification	From (subject: construct - Notification From)		
	Scan Com	elet (subject: <pretix> - Scan Complete)</pretix>		
	E cour com	inte (august, grants, estat complete)		
Do not	t show again for t	his Site	Back Next	Close

5. Enter the configuration information for the email server. Choose whether to use the default configuration or your own custom SMTP server information. Click **Next**.

Alert From:	alerts@security-bulletins.com	Display Name:	Security Alerts	
Report From:	reports@security-bulletins.com	Display Name:	IT Security Reports	
Admin Notice From:	admin@security-bulletins.com	Display Name:	NDA1-32WR Admin	
Port: Security:	465 🜩			
Usemame:				
Password:				

**Note:** Once you complete the Setup Wizard, see <u>"Allow Clients to Access Portal and</u> <u>Manage Tickets" on page 140</u> for more options on setting up Cyber Hawk for users outside of your organization.

# Step 5 — Perform Pre-Scan Analysis

Next you will **Perform a Pre-Scan Analysis** on the target network. This will show you any issues with your Cyber Hawk scan configuration before the final client deployment. Click **Next** to continue.



The pre-scan analysis will begin. Click **Close** to dismiss the wizard. You'll be able to return to Cyber Hawk and continue setup once the pre-scan analysis is complete.



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

From: notify@alert-central.com < notify@alert-central.com>         Sent: Thursday, September 13, 2018 1:03 PM         To:       @rapidfiretools.com>         Subject: CH SS PreScan - sds alerts Scan Completed
ADMINISTRATOR EVENT
An administrative event has occured.
Scan completed with failure. The following errors were encountered during the most recent scan: - [SCAN FAILED] [NO DATA] No computers, network devices, or users were found during the scan. This is a possible indication of a misconfiguration or network issue.
Only one email saying that scan completed successfully
From: notify@alert-central.com <notify@alert-central.com> Sent: Thursday, September 13, 2018 12:20 PM To: @rapidfiretools.com&gt;</notify@alert-central.com>
Subject: CH PreScan SS - sds alerts Scan Completed
ADMINISTRATOR EVENT

An administrative event has occured.

Scan completed successfully.

If the pre-scan analysis identifies issues with your Cyber Hawk scan configuration, click **Modify** next to **Scan Configuration** and make the recommended changes. You can find this under **Settings** in the Cyber Hawk dashboard.



Important: For best results, the target network must be configured to allow for successful scans on all network endpoints. See <u>"Pre-Scan Network Configuration</u> <u>Checklist" on page 242</u> for configuration guidance for both Windows Active Directory and Workgroup environments.

# Step 6 — 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. To initiate the first scan, click **Next**.

O Cyber Hawk Initial Setup Wizard	×
Initial Scan	
Before you can complete configuration of this Cyber Hawk, it must first perform its	first scans.
Press Next to start the initial scan.	Back Next Close

Once the scan is completed, a confirmation message will appear. Click Next.



The scan will be downloaded automatically.

S Cyber Hawk Initial Setup Wizard	×
Downloading Scan	
Download Complete. Press Next to continue.	
Do not show again for this Site	Back Next Close

Click Next when the download is complete.

# Step 7 — Configure Policies

You will then Configure Policies. In short, this is where you create the "Service Plan" that you will offer to the client.

**Tip:** In the Wizard, you will select from one of several pre-defined service plans. However, you can modify or create your own custom service plan at any time. See <u>"Using the Service Plan Creator" on page 178</u>.

**RapidFireTools**<sup>®</sup>

When you are ready to configure policies, click Next.



The Policy Configuration window will appear. Here you select the exact security policies that Cyber Hawk will enforce on the target network:



- 1. Select from a range of pre-defined service plans: *Bronze*, *Silver*, *Gold*, or *Platinum*. The higher the service level, the more Security Policies will be enforced.
- 2. **Review and select individual security policies from the list** of available policies. Use the check box to select or deselect a policy.
- 3. Click on a policy's name to read a description of that policy.
- 4. **Review the required Smart Tags** needed to enforce the policy (if applicable). Smart Tags help Cyber Hawk enforce security policies on specific PCs or parts of the network (such as an IP range).
- 5. When you have configured your security policy, click Generate.

6. Then click **Managed Security Services Agreement (MSSA)** from the drop down menu. This will create an agreement between you and the client.



7. Enter your custom information for the MSSA.

OMSA Customization	×
MSP Name:	PerformanceIT ]
MSP State:	Georgia
MSP Address:	1117 Perimeter Center West
Customer Name:	
Customer Name.	
Customer Address:	CUSTOMER ADDRESS
	~
Service Plan Monthly Charge (\$):	500
Additional Hourly Billing Rate (\$):	150
Hours per Month Included:	2
Emergency Authorized Limit (\$):	1000
Effective Date:	Thursday , March 15, 2018
	OK Cancel

8. Review the legal disclaimer.



## RapidFireTools<sup>®</sup>

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

H	5-0	;									uzk2j	dyz.k02 [Cor
File	Home	Insert	Design	Layout	References	Mailings	Review	View	Q Tell	me what you w	vant to do	
Paste •	X Cut E Copy ✓ Format Pa Clipboard	Aria Inter	I <u>U</u> ,	$\mathbf{x} = 11 \mathbf{x} \mathbf{A}$ also $\mathbf{x}_2 \mathbf{x}^2$ Font	A Aa - Aa	<ul> <li></li> <li><!--</th--><th>}≣ • '•∏•  ≡≡  Parag</th><th> </th><th>2↓   ¶ • ⊞ •</th><th>AaBbCcDa Emphasis</th><th>AaBbC Heading 1</th><th>AaBbC 1 Heading</th></li></ul>	}≣ • '•∏•  ≡≡  Parag		2↓   ¶ • ⊞ •	AaBbCcDa Emphasis	AaBbC Heading 1	AaBbC 1 Heading
				MAN	AGED SECU	JRITY SEF	VICES A	GREEME	NT			
	This by a	MASTER S and between	BERVICES	AGREEMEN	IT (the " <u>Agreem</u> ed Security Se	<u>nent</u> ") is <u>ente</u> rvice Provide	ed into and r ("MSSP"),	effective as a Georgia (	of 10/11/2 Corporation	018 (the "Effec with principal of	<u>tive Date</u> "), offices at	
	111 MS	7 Perimeter SP and Cus	Center We tomer are s	st, and CUS cometimes re	FOMER NAME ferred to individ	, located at, ( lually as a "P	CUSTOMER arty" and col	ADDRESS lectively as	the "Partie	ier"). In this Ag is."	reement,	
			Bac	kground:			applic	able fees	and ch	arges and (	Customer's	
	MS sec inve net bas	SP is in the urity service stigation and work resource ed upon accent	ne busines ces, inclue nd remedia ces occurrir reement a	s of providi ding best ation of misung behind the nd implement	ng outsourced efforts detect ise and abuse corporate fire itation of a se	IIT tion, e of wall et of	compl Agree agree least currer	nance with ment. Eit ment upor 30 days pri 1t term.	n terms her Party written r or to the e	and condition / may termi notice of non-i expiration date /	s or this inate this renewal at of the then	
	bes	t practices s	ecurity Poli Agr	icies & Proce reement:	dures.		<ol> <li>RATE month Any a hourly</li> </ol>	S AND CH Ily basis for dditional w rate of X	ARGES. S Xcurrency ork outside currencySy	Services will be SymbolX\$500 of the scope w mbolX\$150.	billed on a per month. /ill be at an /ISSP may	

10. When you have generated and reviewed your MSSA, click Next.

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

# Step 8 — Configure Notifications

Next you will configure notifications. You can think of these as the "actions" that Cyber Hawk performs when it discovers a possible violation of a security policy.

onfigure Notifications Add Email Group			
icy Name	Action	Group Name	
Access Control			
Authorize New Devices to be Added to Restricted Networks	Email Tech	✓ None	
Restrict Access to Accounting Computers to Authorized Users	Email Tech Z	✓ None	3
Restrict Access to Business Owner Computers to Authorized Users	Email Tech	<ul> <li>None</li> </ul>	-
Restrict Access to IT Admin Only Restricted Computers to IT Administrators	Email Tech	✓ None	
Restrict IT Administrative Access to Minimum Necessary	Email Tech	✓ None	
Restrict Users that are Not Authorized to Log into Multiple Computer Systems	Email Tech	▼ None	
Strictly Control the Addition of New Local Computer Administrators	Email Tech	▼ None	
Strictly Control the Addition of New Users to the Domain	Email Tech	✓ None	
Strictly Control the Addition of Printers	Email Tech	▼ None	
Computers			
Install Critical Patches on Network Computers within 30 Days	Email Tech	▼ None	
Network Security			
Only Connect to Authorized Wireless Networks	Email Tech	▼ None	

- 1. Review the specific **Policy** item.
- 2. Assign an **Action** to the policy item. This can 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



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

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

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

# Step 9 — Configure Smart Tags

Next you will deploy **Smart Tags** within the network environment. Smart Tags help Cyber Hawk track behavior on the network in order to enforce the security policy.



#### **RapidFireTools**<sup>®</sup>

#### EXAMPLE:

If a PC on your network should only be accessed by one user, you would assign that PC the *Single Desktop User* Smart Tag. This lets Cyber Hawk know to "lock down" that PC to only that user, and to send alert notifications when another user attempts to access it.



Configure each Smart Tag by double clicking on it. Depending on the Smart Tag, a slightly different configuration screen will open. Below is an example:

g Explorer											
🚽 si	NGLE DE	SKTOP USE	R U					Save	e & Clos	e Discard	& Close
Applied T	0?		For Wh	at?			Why?				
This tag is applied to a User			Users that into other s	have a dedicated ystems directly.	d desktop and	should never log	Enhance: have bee	s detection of anoma n assigned a compu	alies by i .ter.	dentifying which users	2
lleore											_
Users					- 3						
Enter text	o search			• Clear					F	Filters 4	Clear
	_								E	Active	Clear
Tagger	5 main	Name	Display Name	First	Last	Last Login	Active	<sup>♥</sup> Enabled		Yes	
				Blake		3/12/2018 1:	Yes	Yes	Œ	Enabled	Clear
				Marc		3/14/2018 11	Tes	Tes	E	Tagged	Clear
				D		3/6/2018 1:0	Yes	Yes		Yes	
				-		3/15/2018 12	Yes	Yes		No No	
						3/15/2018 1:	Yes	Yes	= =	Local Accounts	Clear
				James		3/13/2018 10	Yes	Yes		Include Local Ac	counts
				Jabez		2/15/2018 4:	Yes	Yes			
				John		3/14/2018 10	Yes	Yes			
				Joe		3/15/2018 1:	Yes	Yes			
				Marianna		3/14/2018 10	Yes	Yes			
				Pablo		3/14/2018 12	Yes	Yes			
1000				1.1		2/14/2010 10	14				

On the Smart Tag configuration screen you can find:

- 1. The name of the smart tag
- 2. A description of the smart tag, including the part of the network environment to which it is applied, its purpose, and the benefit of employing the smart tag

- 3. Search for specific network components to which to assign tags (in this case, users)
- 4. Filter the list of available network components
- 5. Check the box to assign smart tags to specific network components

The Wizard will present you with a list of recommended smart tags to deploy within the network based on the specific Security Policies you decided to enforce in the earlier step.

When you have assigned all recommended smart tags to network components, click **Next**.

**Tip:** See the section <u>"Smart Tags" on page 156</u> in this guide for more detailed information.

# Step 10 — Set Up RapidFire Tools Portal

Congratulations! You've configured Cyber Hawk on the target network! Your End Users and Tech Group will now receive daily alerts whenever Cyber Hawk discovers suspicious activity on the network.

**Now it's time to set up the RapidFire Tools Portal**. The Portal is where your endusers and technicians respond to alerts sent out by Cyber Hawk to enforce the security policy. It is also used to configure branding and integrate with your preferred ticketing system/PSA.

Click Close to dismiss the Cyber Hawk Initial Setup Wizard.



See these topics to set up the RapidFire Tools Portal:

- <u>"Set Up Portal Branding" on page 128</u>
- "Set Up a Custom Subdomain to Access the RapidFire Tools Portal" on page 134
- "Set Up Custom SMTP Server Support" on page 137
- "Set Up and Assign a Ticketing/PSA System Integration to a Site Using Cyber Hawk" on page 98
- "Allow Clients to Access Portal and Manage Tickets" on page 140

# Additional Scan Host Configuration Options and Requirements

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.



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.

#### **RapidFireTools**°

## Scan Host Requirements

Before proceeding to set up the Scan Host, ensure that the following requirements are met:

- The Scan Host PC must have Windows 8.1 or higher.
- WMI, Admin\$, and File and Printer Sharing must be enabled on the network along with their respective firewall settings.

Note that in order to initiate the scans, the Scan Host PC must also:

- be turned on
- be connected to the network

## Assigning Scan Hosts in a Domain Environment

You assign Scan Hosts in the first step of the Scan Configuration Wizard. We recommend that you assign at least two PCs to serve as scan hosts. This will allow scans to run even if one scan host becomes unavailable.

To assign or modify Scan Hosts:

1. In the Cyber Hawk Settings window, click **Modify** next to Scan Configuration.

y Configuration:	Modify	Scan Configuratio	
ve Policies	_		on, woury
		Local Scan Merge:	Primary Domain
I Configuration:	Modly	Domains:	Corp.PerformanceIT.com
	il Configuration:	il Configuration: Modly	il Configuration: Mosty Local Scan Merge: Domains: IP Range(s):

The Scan Configuration Wizard will appear.

- 2. Click Modify Settings if you wish to modify a previously configured scan.
- 3. The Scan Hosts window will appear. Next assign scan hosts:
  - a. Enter one set of login credentials to access the PCs that you wish to designate as scan hosts.
  - b. Enter the name of the domain (NOT the name of the domain controller).

c. Enter the IPs or computer names of the computers that will initiate the scans.



- 4. 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 above, B) that you have entered the values correctly as detailed in the image above.
- 5. Continue through the Scan Configuration Wizard and enter all required fields.

# 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)
	<ul> <li>Allow Windows Management Instrumentation (WMI) service to operate through Windows Firewall</li> <li>This includes the following rules: <ul> <li>Windows Management Instrumentation (ASync-In)</li> <li>Windows Management Instrumentation (WMI-In)</li> <li>Windows Management Instrumentation (DCOM-In)</li> </ul> </li> </ul>
	<ul> <li>Allow <i>File and printer sharing</i> to operate through Windows Firewall</li> <li>This includes the following rules:</li> <li>File and Printer Sharing (NB-Name-In)</li> <li>File and Printer Sharing (SMB-In)</li> <li>File and Printer Sharing (NB-Session-In)</li> </ul>
	Enable <i>Remote Registry</i> "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 <i>Internet Control Message Protocol (ICMP)</i> 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:
	<ul> <li>operating a Kaseya-RapidFire Tools product network data collector to issue ICMP echo request messages to be sent to Windows computers and network devices</li> </ul>
	<ul> <li>to send ICMP echo reply messages in response to an ICMP echo request</li> </ul>
	Note: ICMP requests are used to detect active Windows computers and network devices to scan.
	GPO Configuration for Windows Services
	<i>Windows Management Instrumentation (WMI)</i> • 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)

### **RapidFireTools**\*

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\syst
em /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-accountcontrol-and-remote-restrictions-in-windows

 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-wmiremotely-starting-with-vista

 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
	• <i>Admin</i> \$ 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
	<ul> <li>Ensure the Windows Services below are running and allowed to communicate through Windows Firewall:</li> <li>Windows Management Instrumentation (WMI)</li> <li>Windows Update Service</li> <li>Remote Registry</li> <li>Remote Desktop</li> <li>Remote Procedure Call</li> </ul>
	<ul> <li>Workgroup computer administrator user account credentials.</li> <li>Note: Before configuring scan settings for workgroups, prepare a list of the workgroup computer(s) administrator user account credentials for entry into the scan settings wizard.</li> </ul>
	Enable the <i>Internet Control Message Protocol (ICMP)</i> 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:

#### **RapidFireTools**<sup>\*</sup>

Complete?	Workgroup Configuration
	<ul> <li>operating a Kaseya-RapidFire Tools product network data collector to issue ICMP echo request messages to be sent to Windows computers and network devices</li> </ul>
	<ul> <li>to send ICMP echo reply messages in response to an ICMP echo request</li> </ul>
	Note: ICMP requests are used to detect active Windows computers and network devices to scan.

# RapidFire Tools Server vs. Virtual Appliance

**Reporter**, **Cyber Hawk**, and **Audit Guru** require that you install either the A) **RapidFire Tools Server** or B) **Virtual Appliance** on the target network to be assessed.

- The **RapidFire Tools Server** is a Windows service installed on a PC on the target network. It is quick and simple to install, *but it cannot perform an internal vulnerability scan* on the target network. Nonetheless, the Server can still identify a great number of security issues within the assessment environment.
- The RapidFire Tools **Virtual Appliance** is a virtual machine that must be installed on a PC on the target network using Hyper-V or VMWare. It takes slightly more time to install, but it can perform an internal vulnerability scan on the target network. The internal vulnerability scan identifies potential technical risks on the network that might be exploited by an attacker **from within** the network.

**Tip:** In general, we recommend deploying the **RapidFire Tools Server** for its ease of use. However, if you require an *Internal Vulnerability Scan* of the target network, you should use the Virtual Appliance. Refer to the table below for a quick breakdown of the Server's pros and cons (as compared to the Virtual Appliance).

Features	RapidFire Tools Server	Virtual Appliance
Easier/faster to install	$\checkmark$	-
Less configuration to collect consistent scan data	$\checkmark$	-
Lower system requirements	$\checkmark$	-
Requires scan hosts on the target network	-	$\checkmark$
Can perform internal vulnerability scan	-	$\checkmark$

#### **RapidFireTools**°

# 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



# Sample End User Alert



# Sample Weekly Notice

From: notice@security-hulletins.com < notice@security-hulletins.com>
Sent: Saturday, November 12, 20167-00 AM
To: Senior Tech at My IT Company
Subject: Customer A - Weekly Notice
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-7201CF80C4604141.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)

#### **RapidFireTools**°

RapidFireTools

# Edit 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.
- 2. Open the Cyber Hawk management screen.
- 3. Under Settings, click **Modify** next to Policy Configuration.



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

:ui	Select Po	blicies
4	Service Plan:	Plutoninum (Modified)
		zies
_		cess Control
ər		Authorize New Devices to be Added to Restricted Networks Investigate Suspicious Logons by Users
ca		Investigate Suspicious Logons to Computers Restrict Access to Accounting Computers to Authorized Users
m		Restrict Access to Business Owner Computers to Authorized Users
R		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
il (		Restrict II 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
tv		Strictly Control the Removal of Users from the Domain

- 5. Make any changes to the Notification Rules for the policies.
- 6. Click **Finish**. The policy changes will take effect when Cyber Hawk next performs a scan and sends out alerts.

# Unitrends Backup Alerts

Maintaining backups of all servers is an essential component from both a *backup disaster recovery* point of view and an *incident recovery* point of view. Cyber Hawk integrates with **Unitrends Backup** in order to help you ensure that servers on the network are protected and can be recovered.

When you integrate Cyber Hawk with Unitrends Backup, you will receive **Unitrends Backup Alerts** as in the example alert below:

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.	
Aler	t Object(s)	
	им	

**Backup Alerts** can help notify you when new servers come online within the network that need to be protected. You can also receive alerts when scheduled backups fail for whatever reason. You can enable and receive alerts for the following Unitrends Backup Policies:

- Backup all Hyper-V servers
- Backup all VMware servers
- Backup all Windows servers
- Investigate all backup failures

You can use and configure Unitrends Backup Alerts in both the Cyber Hawk Web Console and the Cyber Hawk appliance in Network Detective.

## **Requirements for Unitrends Backup Alerts**

In order to use Unitrends Backup Alerts, you must:

- Deploy and configure Unitrends Backup on the target network (see <u>Unitrends</u> <u>Backup</u> documentation)
  - You will need Unitrends Backup login credentials to set up Backup Alerts
• Deploy and configure Cyber Hawk for your Site(s)

You can then enable Unitrends Backup Alerts as below:

## How to enable Unitrends Backup Alerts (Web Console)

- 1. Navigate to your Cyber Hawk Site in either Cyber Hawk or the Portal.
- 2. Go to the **Cyber Hawk tab > Settings > Scan Settings**.
- 3. Using the Scan Configuration Wizard, navigate through each screen until you reach **Unitrends Backup**.

Cyber Hawk > Settings > Scan Settings							
Unitrends Backup							
Enter Server and	credential information for Unitrends Backup Servers.						
Server:	Server						
Username:	Username						
Password:	Password						
+ Add	Remove Selected Entry Test Connections						
	← Previous Page → Next Page						

4. Enter the Unitrends Backup server name and login credentials. Click **Test Connection** to verify your configuration.

Unitrends Test Results	×
qa@10.200. Success	
	ок

- 5. Save the Scan Settings.
- 6. Next, enable Unitrends Backup Alerts in the Cyber Hawk Policy Configuration.

**RapidFireTools**°



7. Repeat this process for each Site that will use Backup Alerts.

**Note:** Next time scans are performed and alerts are generated, the Site will receive Backup Alerts. Refer to these alerts to see which systems need to be backed up.

ew This alert has not stem.	been processed. You may convert it into a To Do item, or send it straight to your ticketing	
Backup all Window	s servers (Unitrends).	
Maintaining backups of recovery point of view. solution.	all server is an essential component from both a backup disaster recovery point of view and an incident Ensure that all Windows servers on the network are properly backed up using an enterprise backup	
Alert Object(s)		
, RWW		

How to enable Unitrends Backup Alerts (Network Detective)

- 1. Navigate to your Cyber Hawk Site in either Cyber Hawk or the Portal.
- 2. Open the Site Scan Settings.
- 3. Using the Scan Configuration Wizard, navigate through each screen until you reach **Unitrends Backup**.

Scan Configuration Wizard					-		×
🖌 Scan Hosts	Unitrends	Backup					
✓ Merge Option	Enter server	and credential informa	ation for any Unitre	nds Backup Servers.			
Active Directory	Server:	Hostname or IP Add	tress				
✓ Local Domains	Usemame:	Username					
✓ Additional Credentials	Password:	Password		Add Unitrends Server			
✓ IP Ranges	qa@10.200	.1.150					
SNMP Information							
✓ File Scanner							
🖌 VMware							
Unitrends Backup							
Confirm							
	Clear A	Entries Tes	t Connections				
-				< Back	Next >	Can	cel

4. Enter the Unitrends Backup server name and login credentials. Click **Test Connection** to verify your configuration.

ι	Unitrends Test Results — 🗆 🗙								
	For any failed Unitrends S 1. The login credentials 2. The IP Address or Host 3. The Unitrends Server is	iervers, please ver tname s online and availa	ify the following: ble on the netwo	rk					
	User	Server	Result						
	ga	10.200.1.150	Success						
	40	10.200.1100	000000						
	L								
		View	/ full details	Close					

- 5. Save the Scan Settings.
- 6. Next, enable Unitrends Backup Alerts in the Cyber Hawk Policy Configuration.

## **RapidFireTools**<sup>°</sup>

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							
Backup all Hyper-V servers (Unitrends)							
Backup all VMware servers (Unitrends)							
Backup all Windows servers (Unitrends)							
Investigate all backup failures (Unitrends)							
Changes on Locked Down Computers should be Strictly Controlled							
Enable automatic screen lock for users with access to sensitive information							
Enable automatic screen lock on computers with sensitive information							
Install Critical Patches for DMZ Computers within 30 Days							

7. Repeat this process for each Site that will use Backup Alerts.

**Note:** Next time scans are performed and alerts are generated, the Site will receive Backup Alerts. Refer to these alerts to see which systems need to be backed up.

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)  RMM	teer This alert has not been processed. You may convert it into a To Do item, or send it straight to your ticketing ystem.	
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.	Backup all Windows servers (Unitrends).	
Alert Object(s) ⊒ RMM	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.	
⊋ RMM	lert Object(s)	
	RMM	

## 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 🔻 Q. Search	Show Admin Messages	🛓 Download Log
Date (UTC-4) 💠	Site ¢	User ¢	Nessage ¢	Detail ¢	К < 11. /4 > н view 25 *
6/13/19, 1:05 PM	JW 5-8-19 CL Test	ADMIN	Viewed Form	The user ( Review Work	I@rapidfiretools.com) viewed the form User Access isheet
5/28/19.10:47 AM	JW 8-8-19 CL Test	ADMIN	Viewed Form	The user ( Liability Que	⊗rapidfiretools.com) viewed the form Cyber stionnaire
5/22/19, 2:54 PM	JW 5-8-19 CL Test	ADMIN	Viewed Form	The user ( Liability Que	@rapidfiretools.com) viewed the form Cyber stionnaire
6/22/19, 2:47 PM	JW 5-8-19 CL Test	ADMIN	Viewed Form	The user ( Liability Que	Srapidfiretools.com) viewed the form Cyber stionnaire