CYBER HAWK®
by RapidFire Tools

QUICK START GUIDE

Cyber Hawk Web Console

Detecting and Responding to IT Security Policy Violations

3/7/2024 2:43 PM

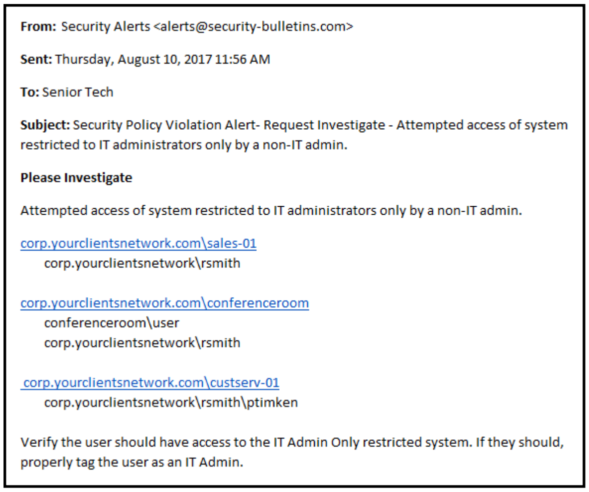
Kaseya®

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

Contents

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.



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

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

To: Senior Tech

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

Please Investigate

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

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

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

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

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

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 or prevent it from being generated again in the future

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

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

Setting Up Cyber Hawk

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

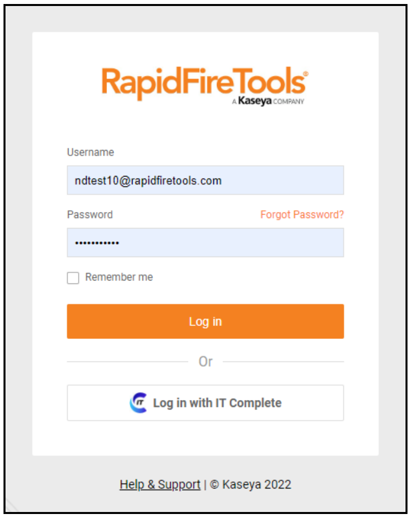
> **Note:** If you have previously set up Cyber Hawk Sites using the Network Detective app, you can access and manage those Sites in the Portal, too. This should NOT require any additional set up. See the topics in this guide for details on how to manage your Sites using the Cyber Hawk Web Console in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

Create a New Site

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

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

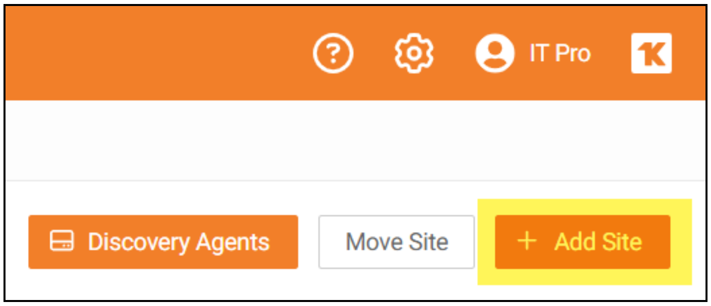
1. Access the RapidFire Tools Portal at https://www.youritportal.com and log in with your credentials.



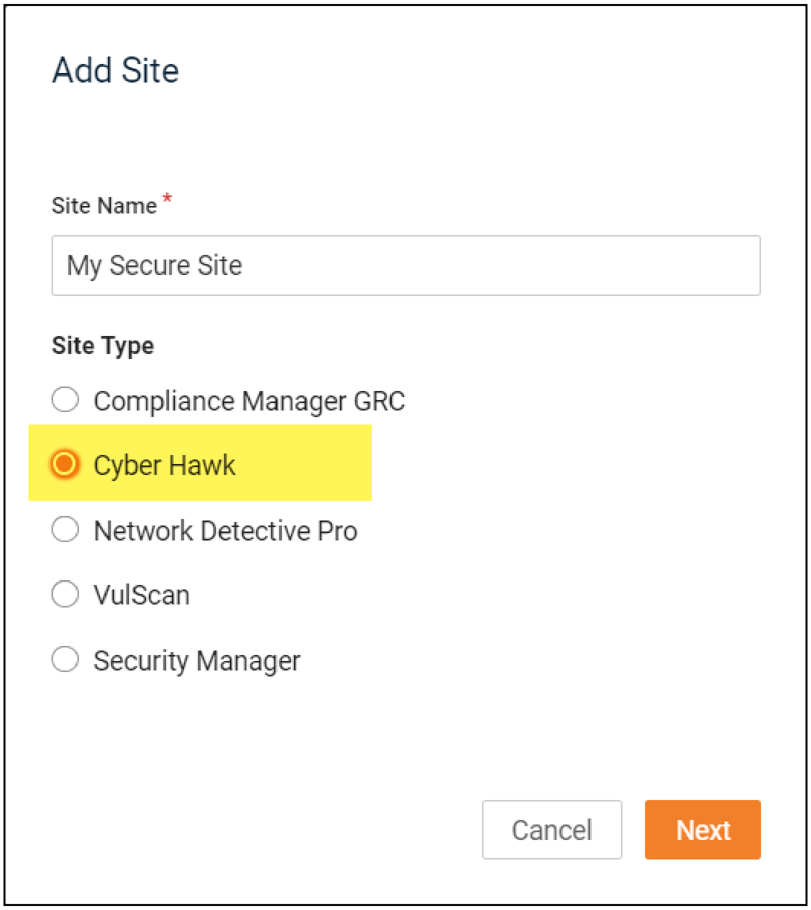
Username
ndtest10@rapidfiretools.com

Password •••••••••••

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



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



Add Site

Site Name *

My Secure Site

Site Type

○ Compliance Manager GRC

● Cyber Hawk

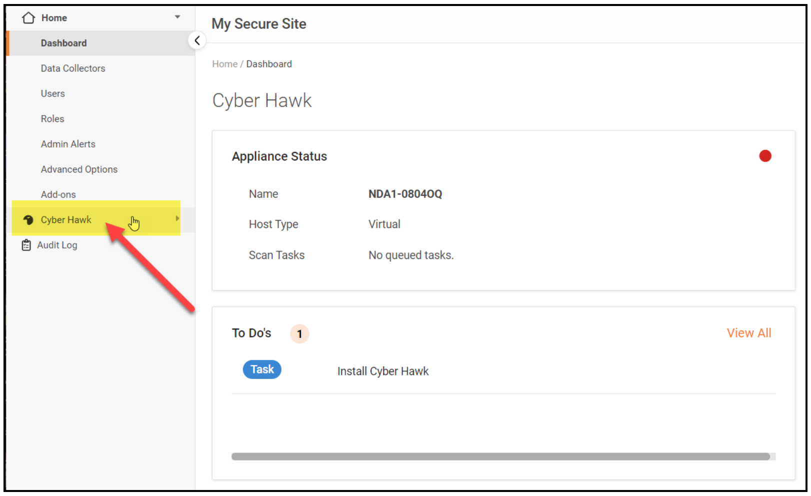
○ Network Detective Pro

○ VulScan

○ Security Manager

5. Click **Next**.

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



My Secure Site

Home / Dashboard

Cyber Hawk

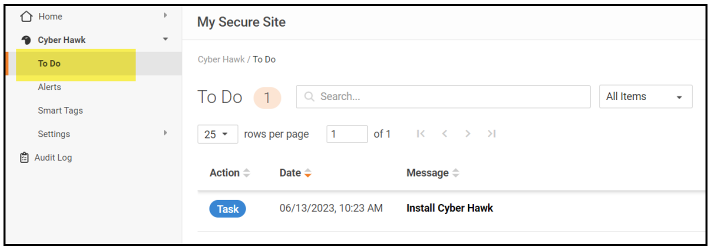
Appliance Status

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

To Do's 1 View All

Task Install Cyber Hawk

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



My Secure Site

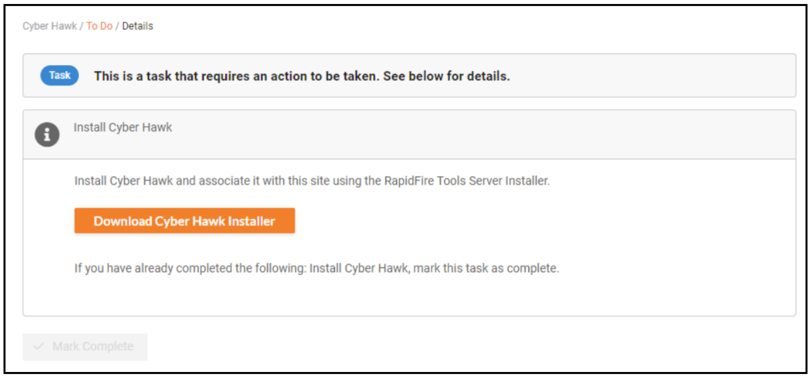
Cyber Hawk / To Do

To Do 1

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

Task 1 — Install Cyber Hawk

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



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

Install Cyber Hawk

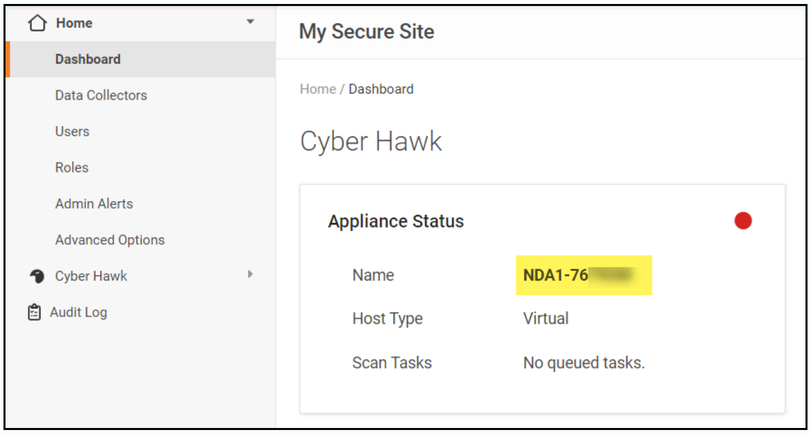
Install Cyber Hawk and associate it with this site using the RapidFire Tools Server Installer.

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

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

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

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



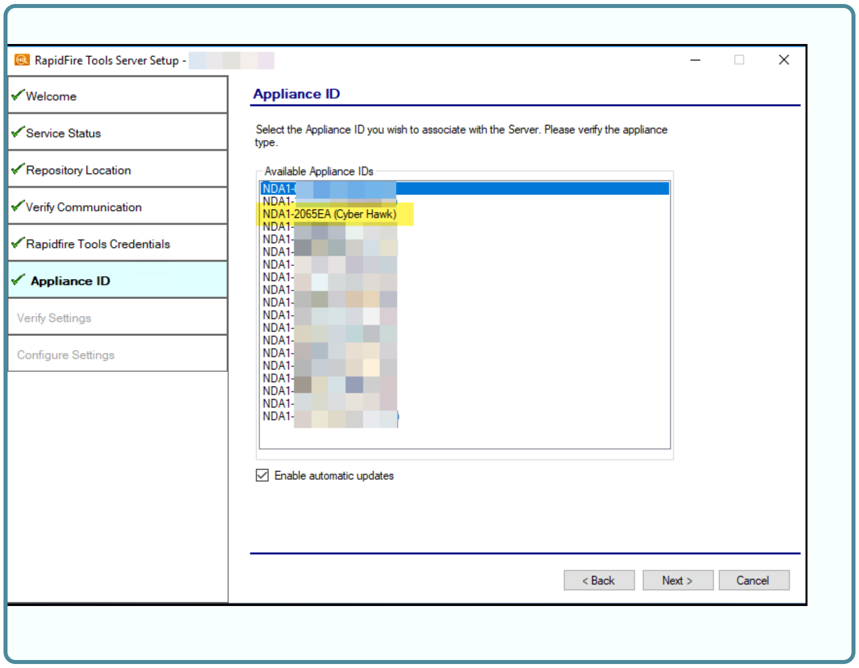
Appliance Status

Name NDA1-76[redacted]

Host Type Virtual

Scan Tasks No queued tasks.

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



Appliance ID

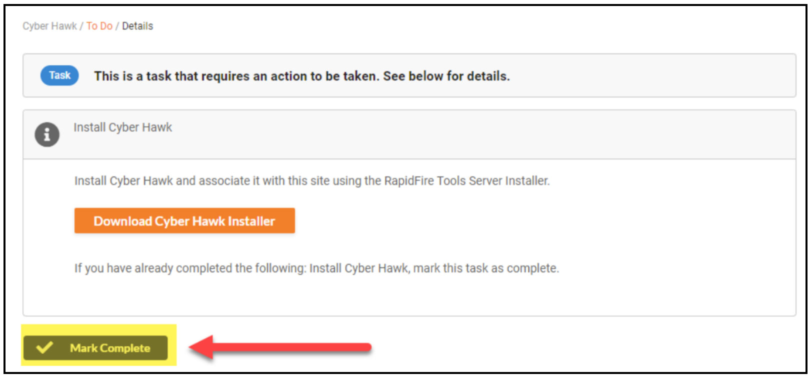
Select the Appliance ID you wish to associate with the Server. Please verify the appliance type.

Available Appliance IDs

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

☑ Enable automatic updates

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



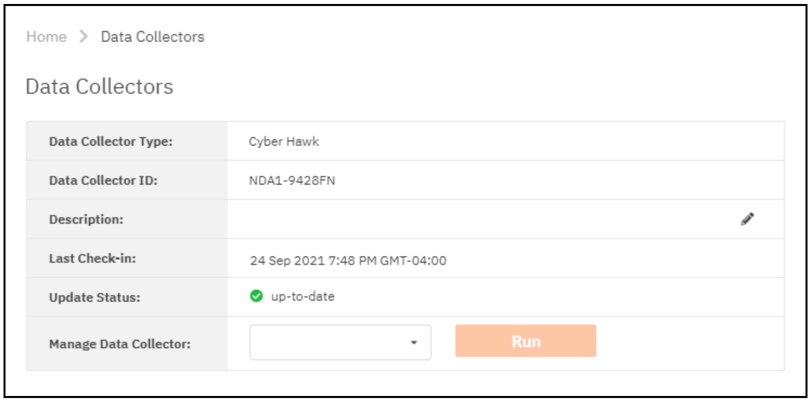
This is a task that requires an action to be taken. See below for details.

Install Cyber Hawk

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

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

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



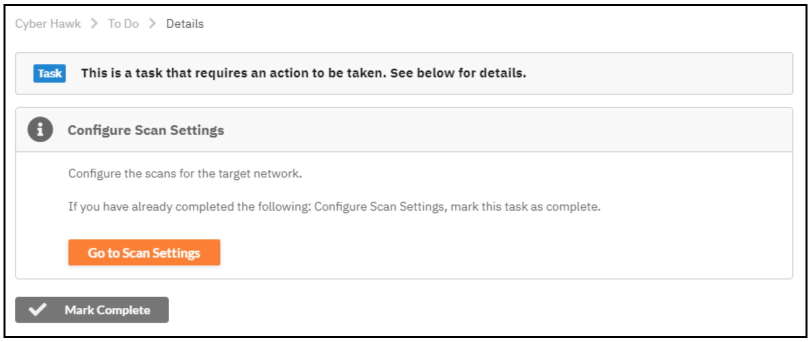
Home > Data Collectors

Data Collectors

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

Task 2 — Configure Scan Settings

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



Cyber Hawk > To Do > Details

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

Configure Scan Settings

Configure the scans for the target network.

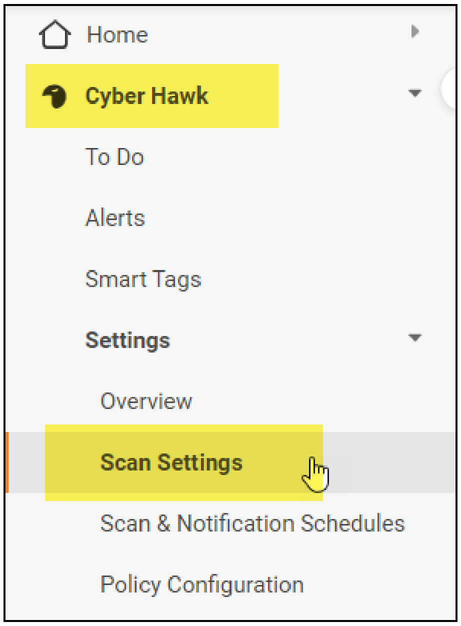
If you have already completed the following: Configure Scan Settings, mark this task as complete.

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

- Look here to "Configure Scan Settings for Active Directory Domain" below
- Look here to "Configure Scan Settings for Workgroup" on page 20

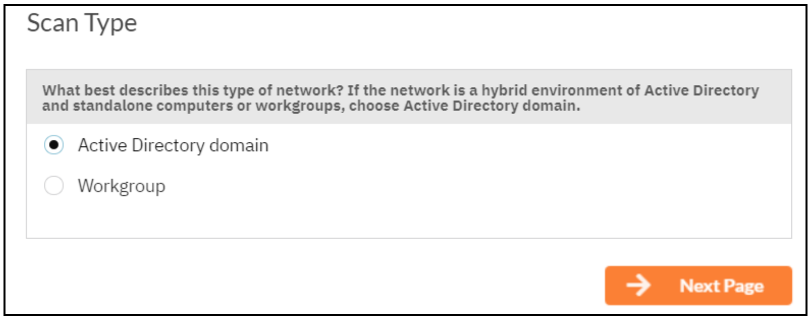
Configure Scan Settings for Active Directory Domain

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



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

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



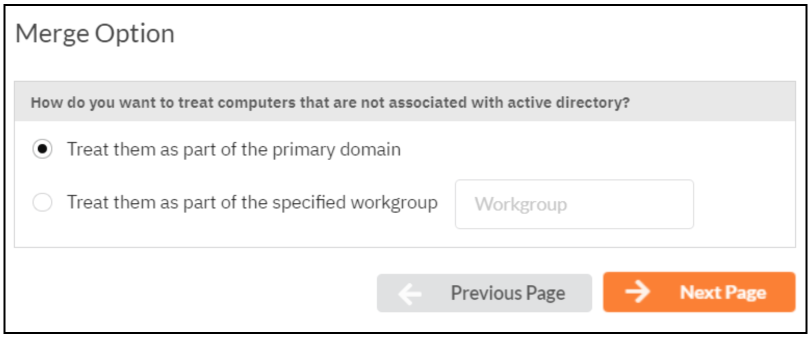
Scan Type

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

● Active Directory domain

○ Workgroup

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



Merge Option

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

● Treat them as part of the primary domain

○ Treat them as part of the specified workgroup Workgroup

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

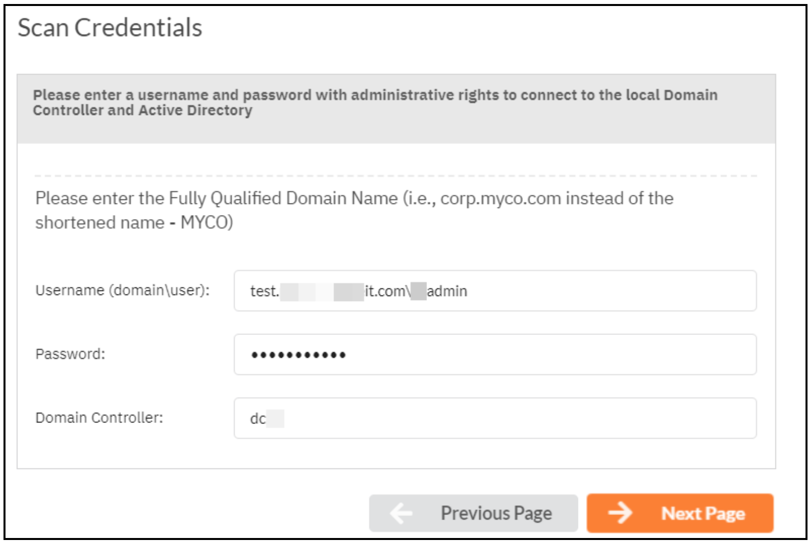
> **Tip:** Use this feature to tell Cyber Hawk how to handle computers that are not connected to the domain. This affects how they appear in alerts and reports.

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

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

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

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



Scan Credentials

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

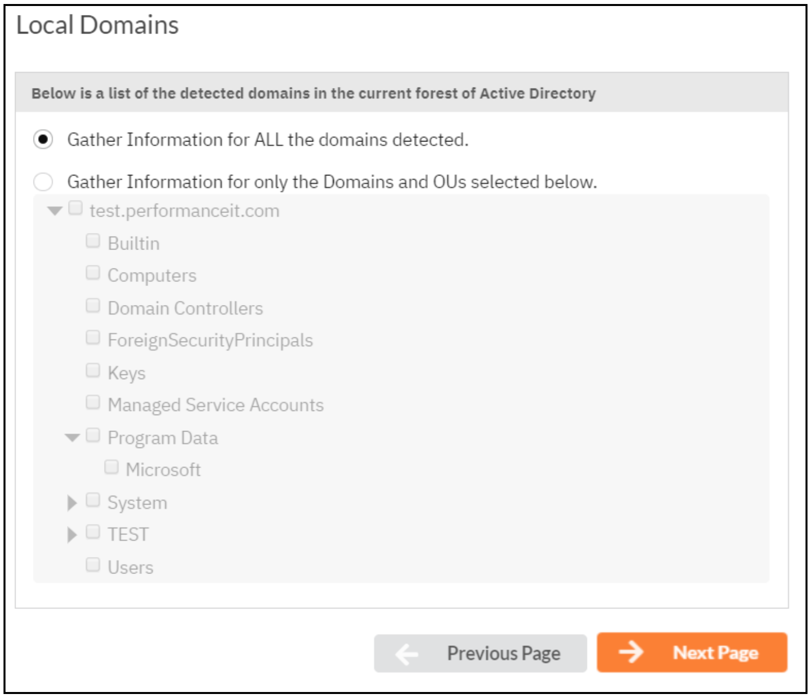
Please enter the Fully Qualified Domain Name (i.e., corp.myco.com instead of the shortened name - MYCO)

Username (domain\user): test.[redacted]it.com\[redacted]admin

Password: •••••••••••

Domain Controller: dc[redacted]

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



Local Domains

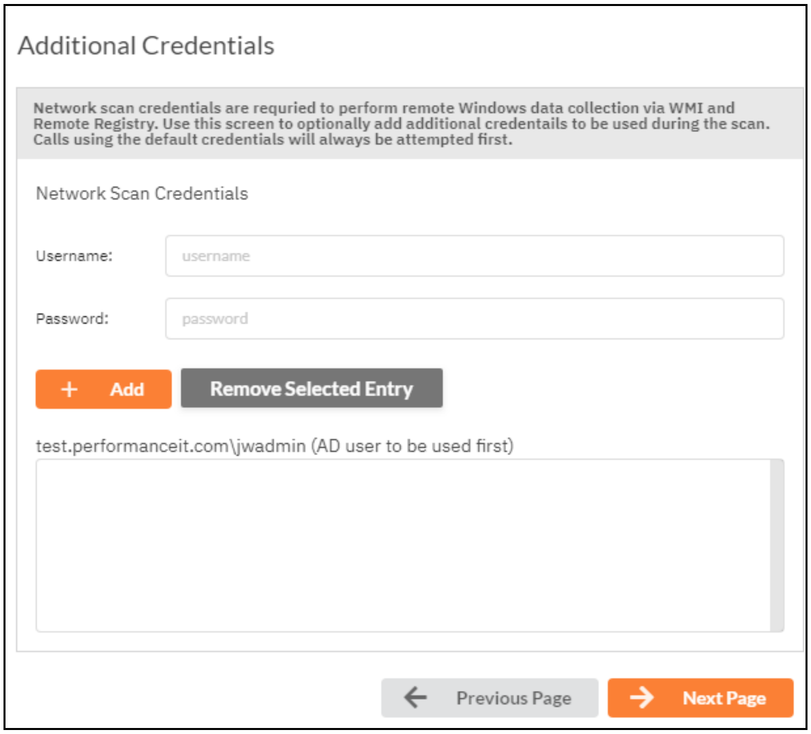
Below is a list of the detected domains in the current forest of Active Directory

● Gather Information for ALL the domains detected.

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

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

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



Additional Credentials

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

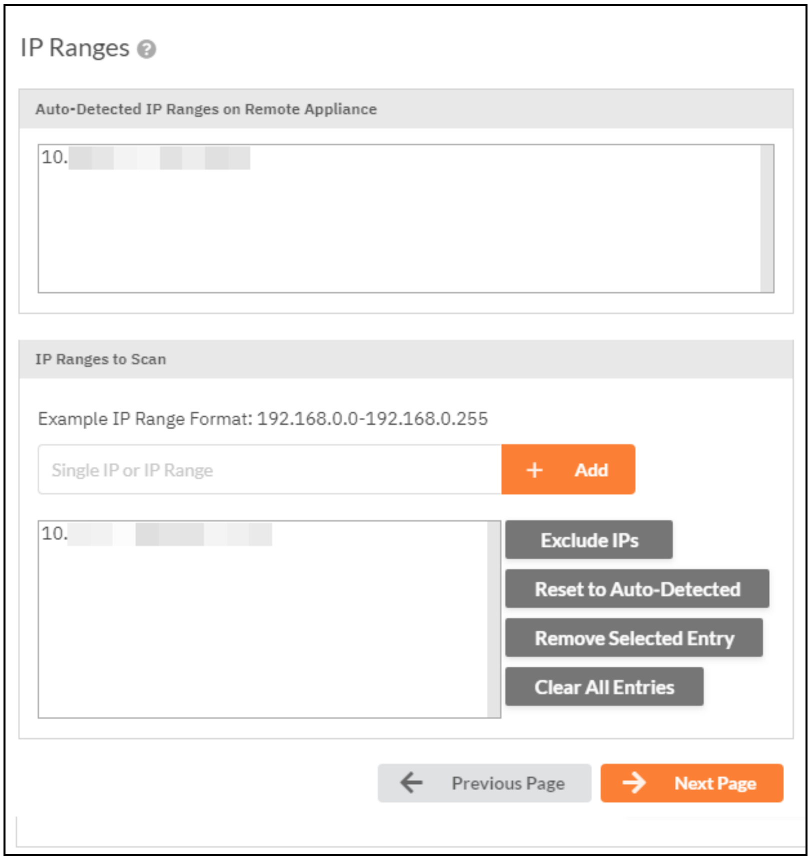
Network Scan Credentials

Username: username

Password: password

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

7. The **IP Ranges** screen will then appear. The Cyber Hawk appliance will automatically suggest an IP Range for the scan. If you do not wish to scan the default IP Range, select it and click **Clear All Entries**. Use this screen to enter additional IP Addresses or IP Ranges and click **Add**.



10.[redacted]

Example IP Range Format: 192.168.0.0-192.168.0.255

10.[redacted]

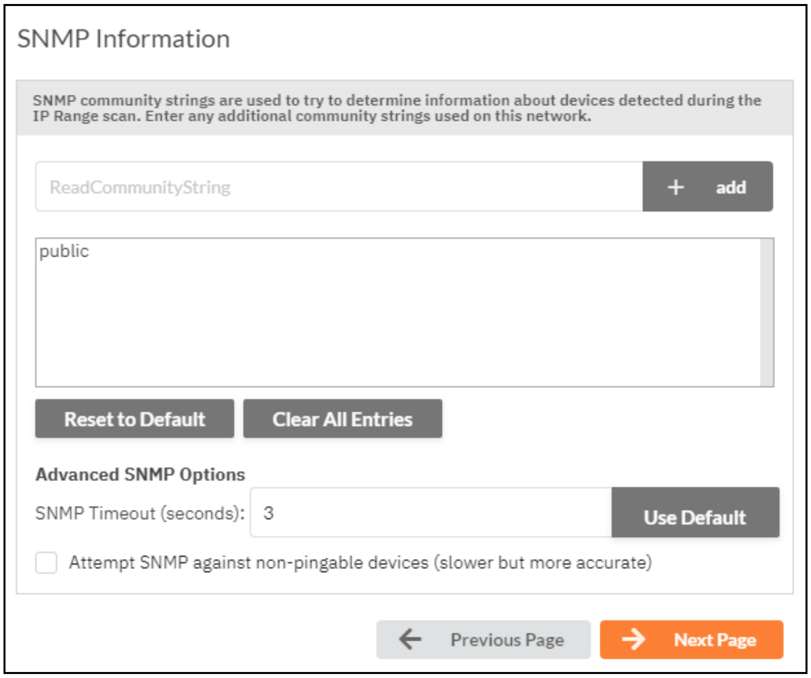
From this screen you can also:

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

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

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

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



SNMP Information

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

ReadCommunityString

public

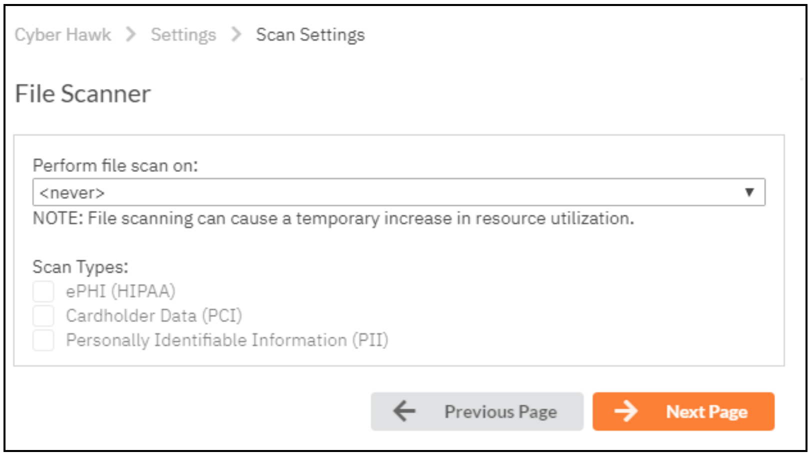
Advanced SNMP Options

SNMP Timeout (seconds): 3

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

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

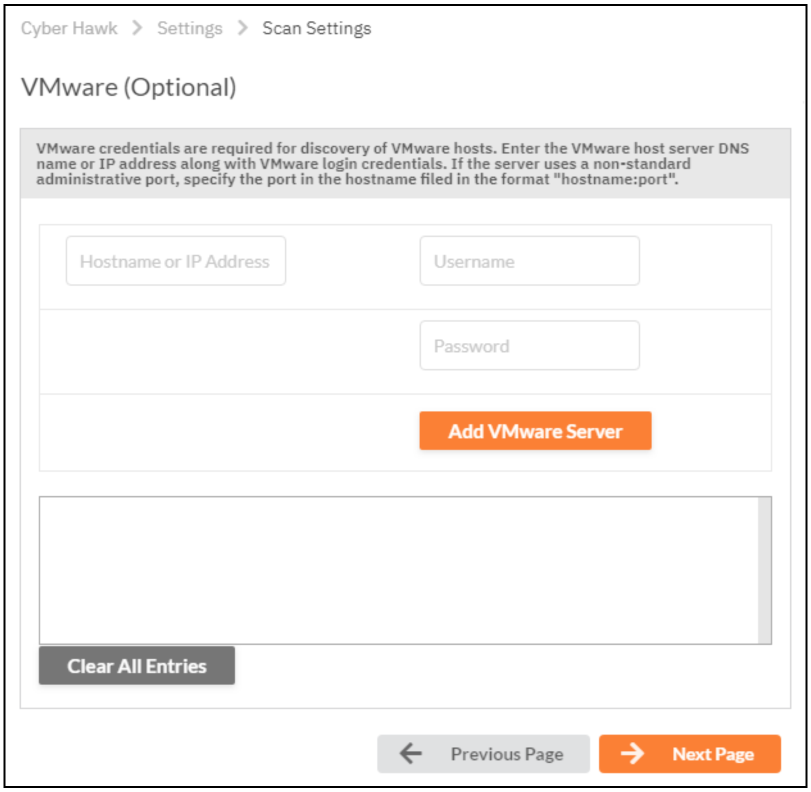
person's name or social security number



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

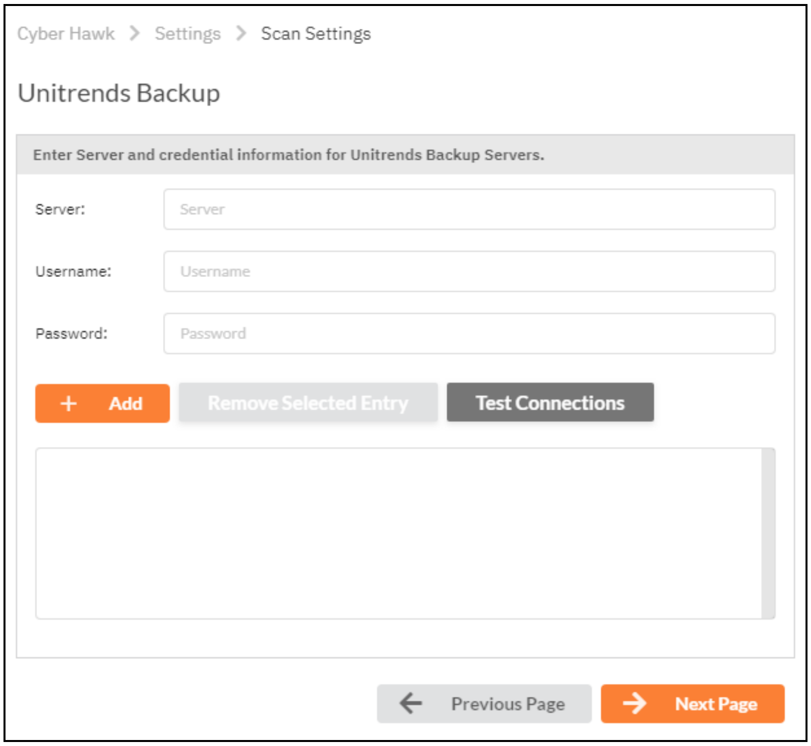
Scan Types:
□ ePHI (HIPAA)
□ Cardholder Data (PCI)
□ Personally Identifiable Information (PII)

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



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

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

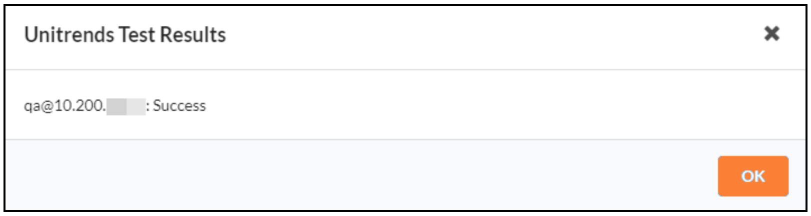


Cyber Hawk > Settings > Scan Settings

Unitrends Backup

Enter Server and credential information for Unitrends Backup Servers.

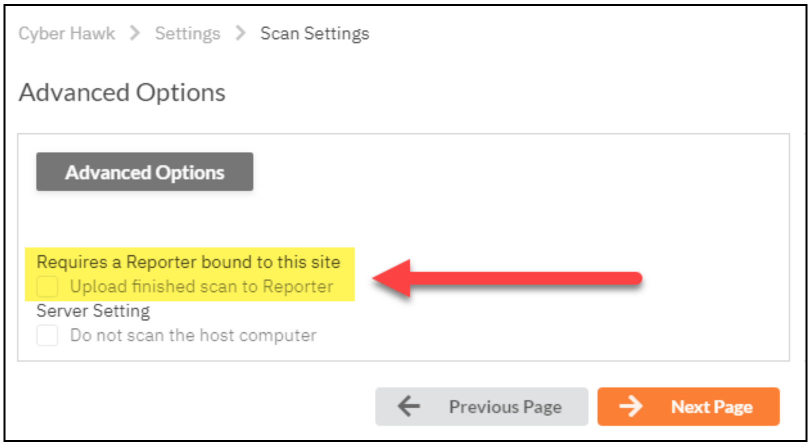
12. Click **Test Connection** to verify your Unitrends scan configuration.



Unitrends Test Results

qa@10.200.[redacted]: Success

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



Cyber Hawk > Settings > Scan Settings

Advanced Options

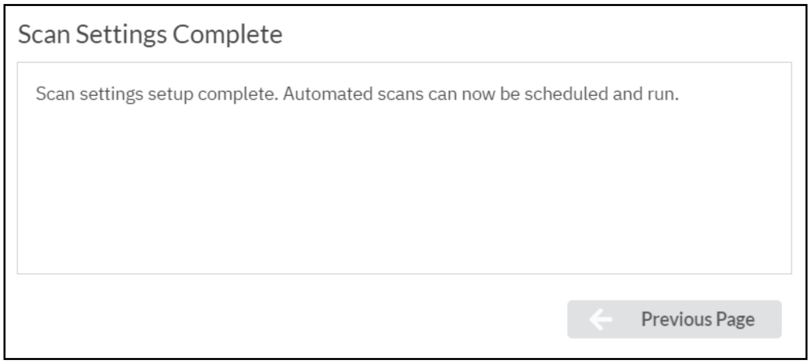
Requires a Reporter bound to this site

□ Upload finished scan to Reporter

Server Setting

□ Do not scan the host computer

14. Your scan settings will then be complete.



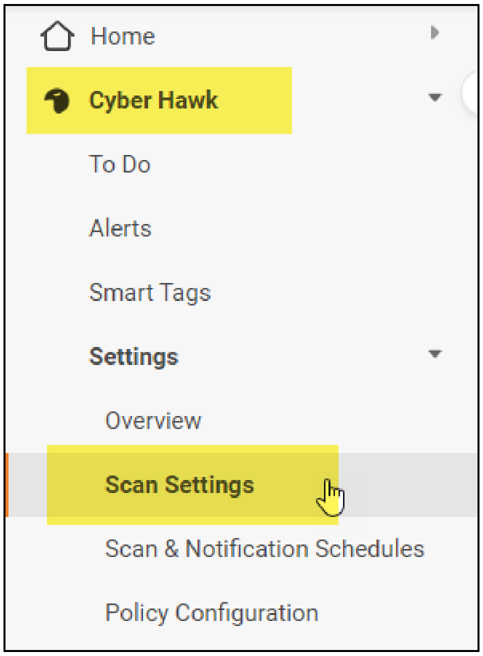
Scan Settings Complete

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

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

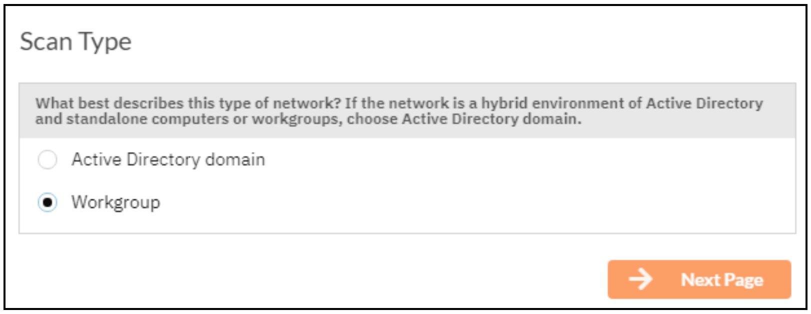
Configure Scan Settings for Workgroup

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



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

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



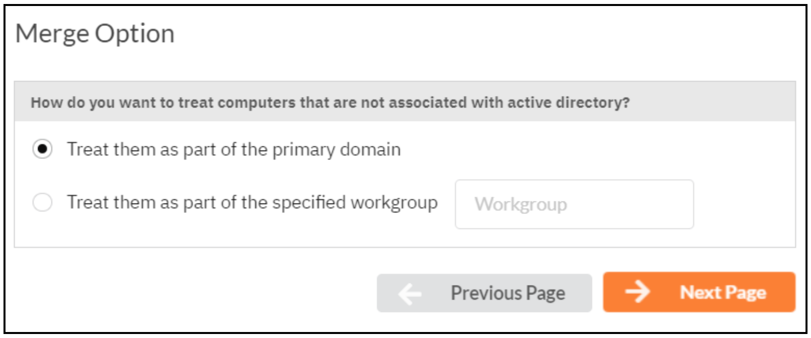
Scan Type

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

○ Active Directory domain

● Workgroup

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



Merge Option

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

● Treat them as part of the primary domain

○ Treat them as part of the specified workgroup Workgroup

a. Treat them as part of the primary domain

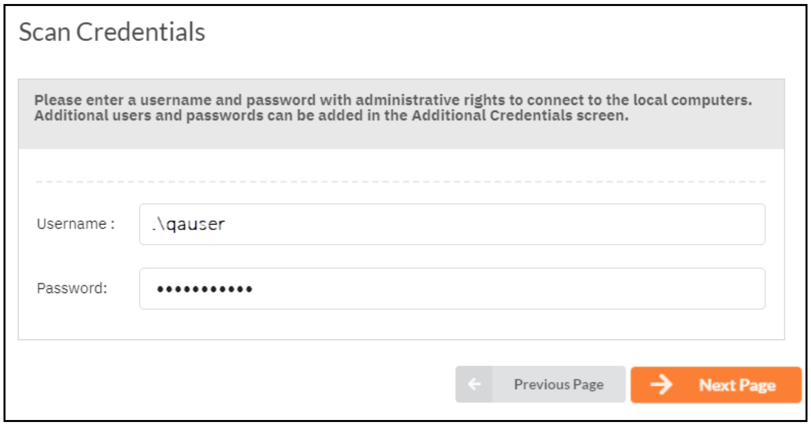
b. Treat them as part of a specific workgroup by entering a workgroup name

c. Don't treat them as part of a domain (non-domain assets will appear separately in alerts and reports)

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

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

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



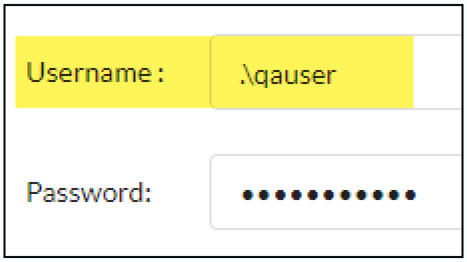
Scan Credentials

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

Username : .\qauser

Password: •••••••••••

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



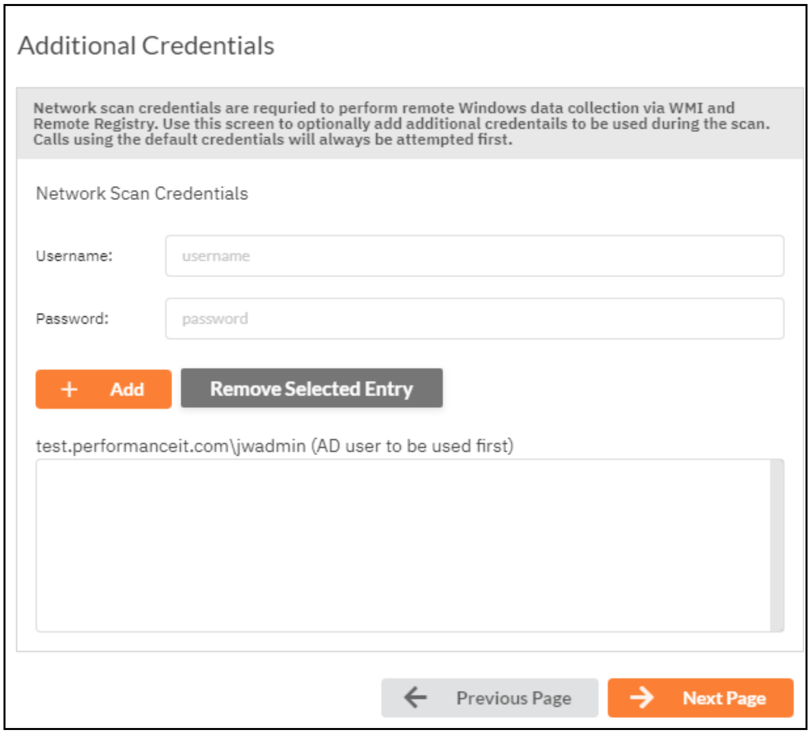
Username : .\qauser

Password: ●●●●●●●●●●●

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

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

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



Additional Credentials

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

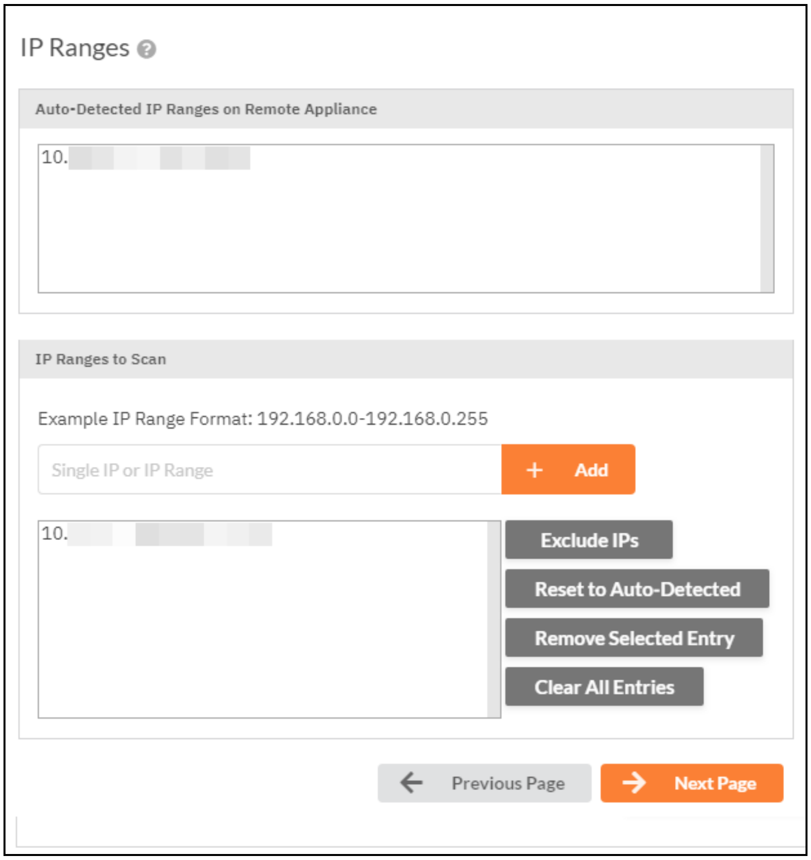
Network Scan Credentials

Username: username

Password: password

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

5. The **IP Ranges** screen will then appear. The **Cyber Hawk** appliance will automatically suggest an IP Range for the scan. If you do not wish to scan the default IP Range, select it and click **Clear All Entries**. Use this screen to enter additional IP Addresses or IP Ranges and click **Add**.



IP Ranges

Auto-Detected IP Ranges on Remote Appliance

10.[redacted]

IP Ranges to Scan

Example IP Range Format: 192.168.0.0-192.168.0.255

10.[redacted]

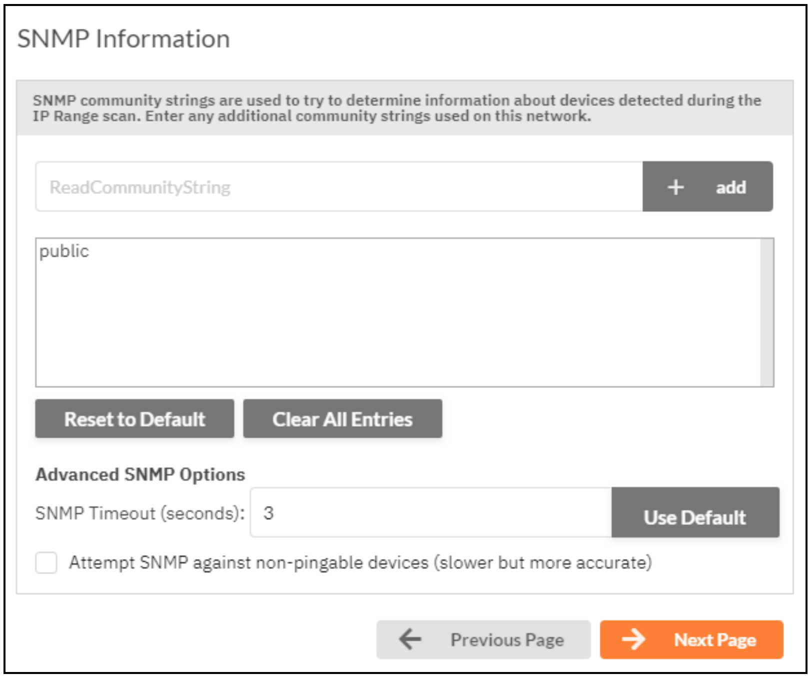
From this screen you can also:

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

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

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

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



SNMP Information

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

public

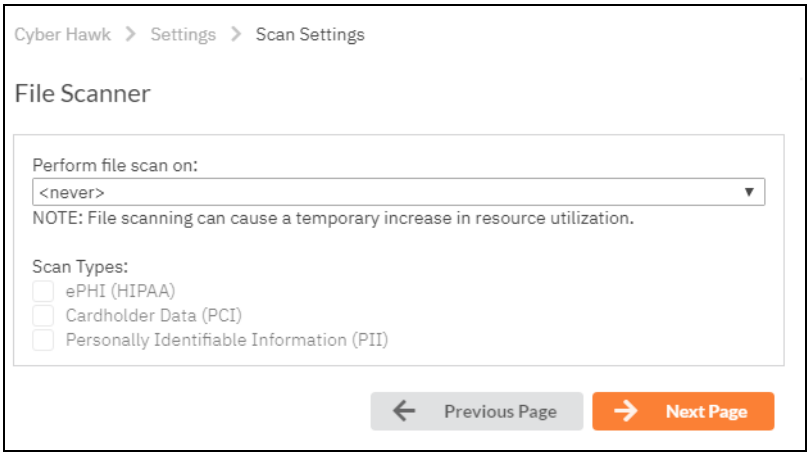
Advanced SNMP Options

SNMP Timeout (seconds): 3

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

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

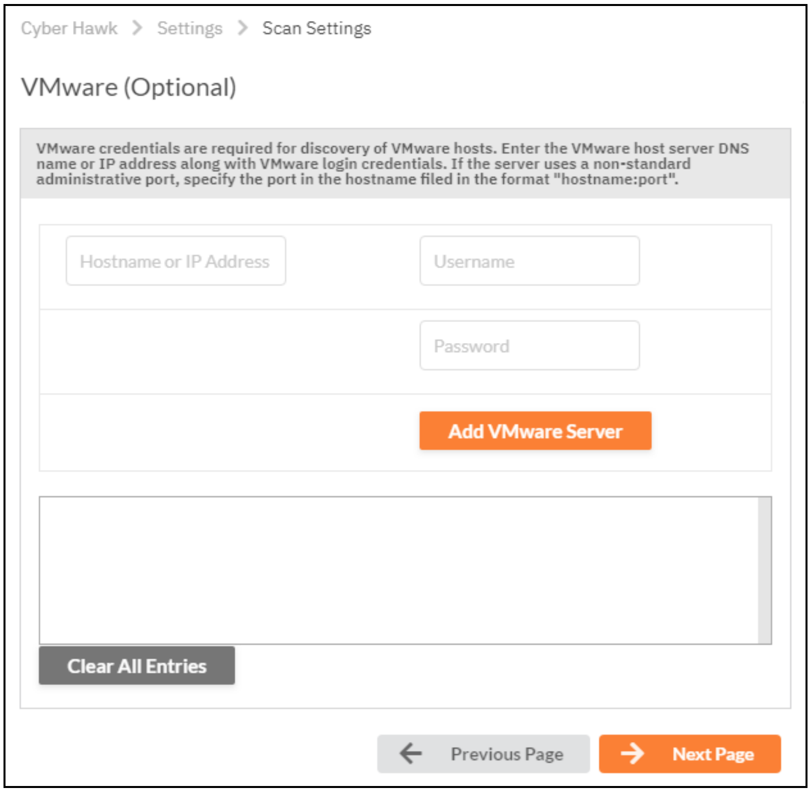
person’s name or social security number



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

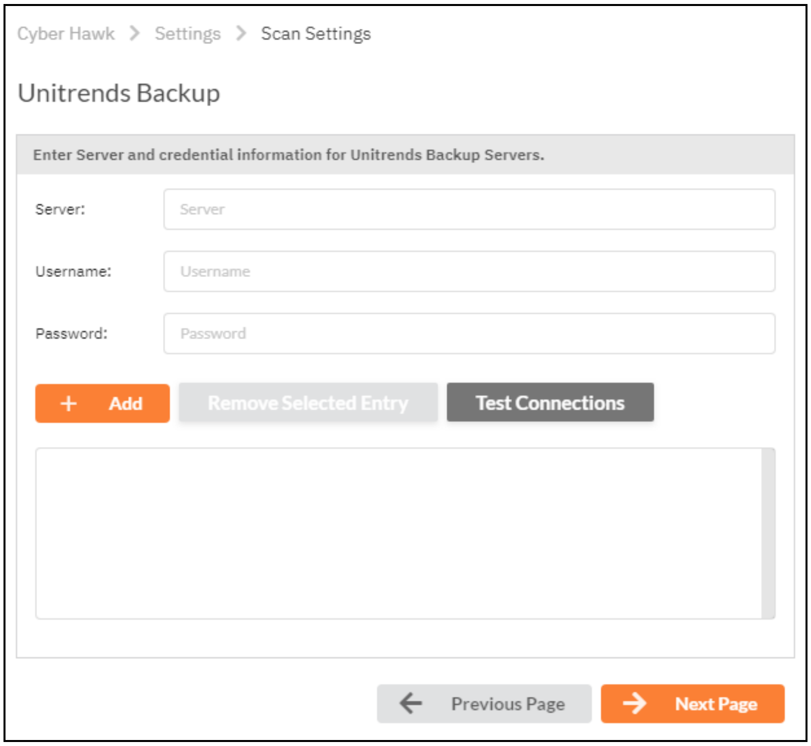
Scan Types:
☐ ePHI (HIPAA)
☐ Cardholder Data (PCI)
☐ Personally Identifiable Information (PII)

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



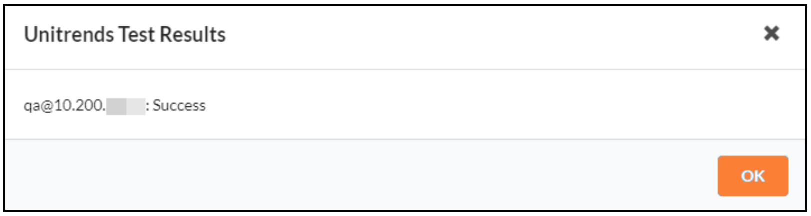
VMware credentials are required for discovery of VMware hosts. Enter the VMware host server DNS name or IP address along with VMware login credentials. If the server uses a non-standard administrative port, specify the port in the hostname filed in the format "hostname:port".

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



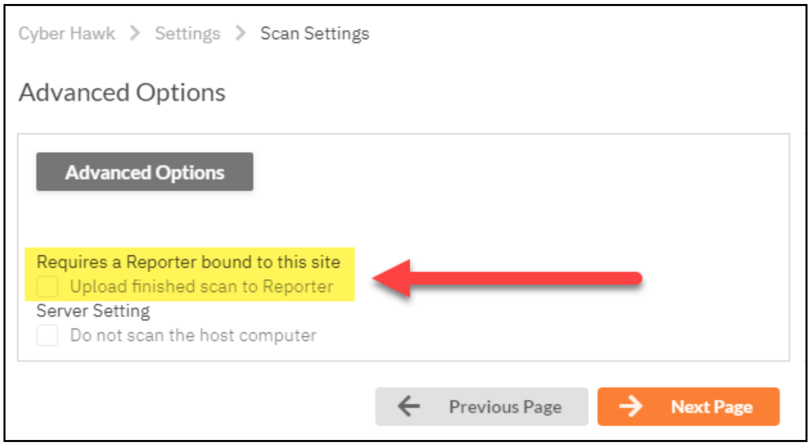
Enter Server and credential information for Unitrends Backup Servers.

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



qa@10.200.[redacted]: Success

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



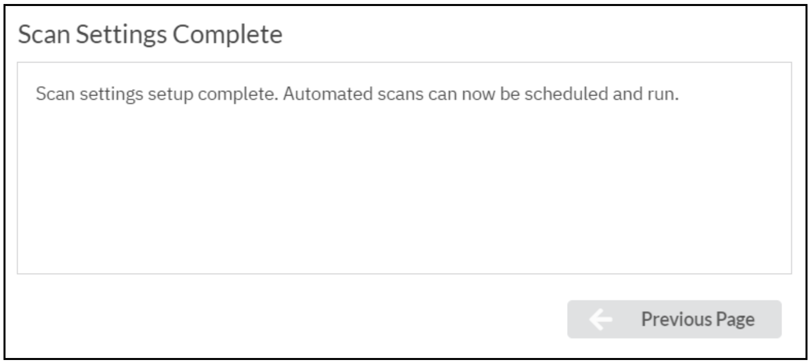
Requires a Reporter bound to this site

□ Upload finished scan to Reporter

Server Setting

□ Do not scan the host computer

12. Your scan settings will then be complete.

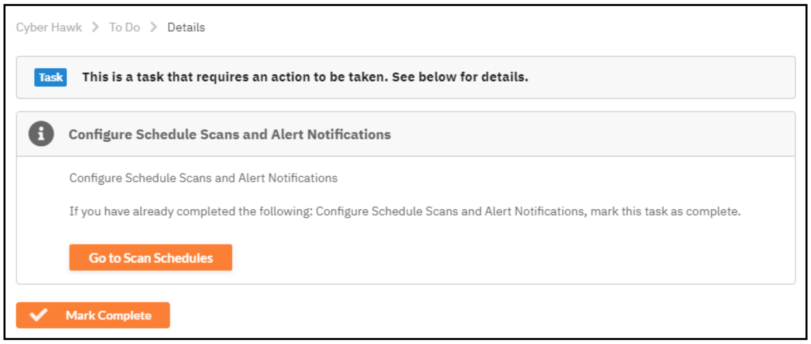


Scan settings setup complete. Automated scans can now be scheduled and run.

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

Task 3 — Configure Schedule Scans and Alert Notifications

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


Cyber Hawk > To Do > Details

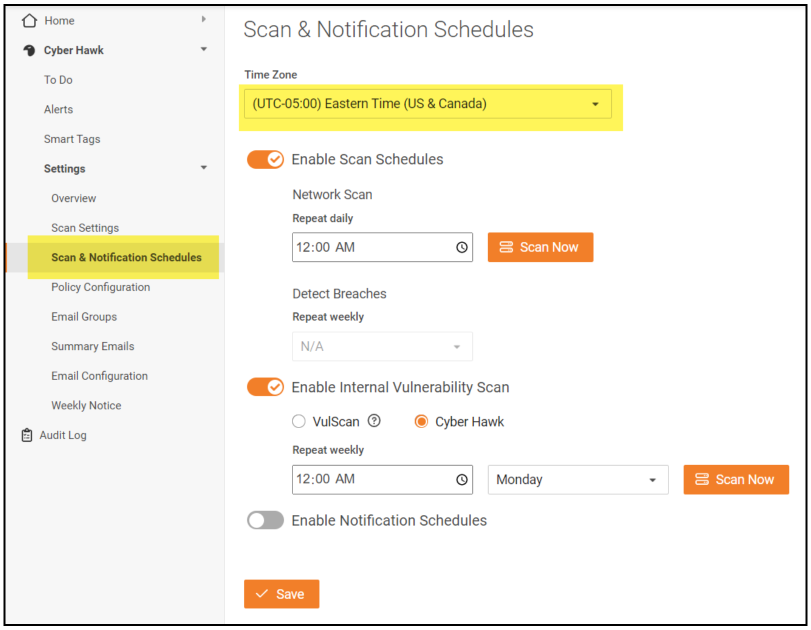
Task This is a task that requires an action to be taken. See below for details.

Configure Schedule Scans and Alert Notifications

Configure Schedule Scans and Alert Notifications

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

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



Scan & Notification Schedules

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

Enable Scan Schedules

Network Scan

Repeat daily: 12:00 AM

Detect Breaches

Repeat weekly: N/A

Enable Internal Vulnerability Scan

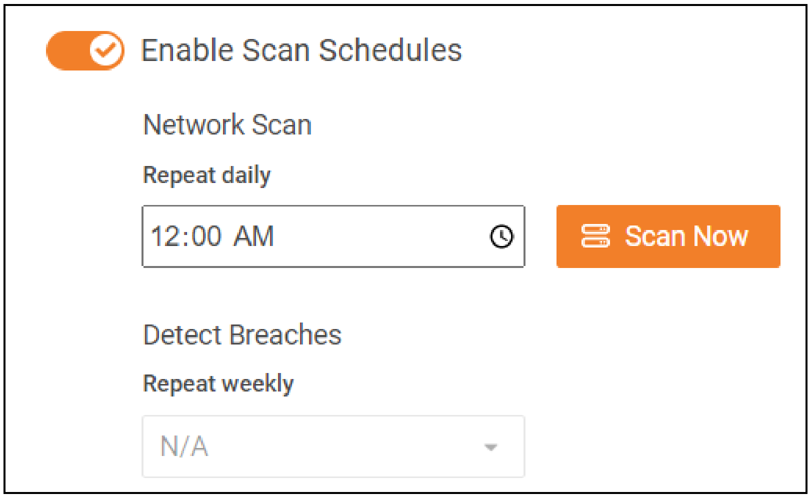
○ VulScan ● Cyber Hawk

Repeat weekly: 12:00 AM Monday

Enable Notification Schedules

Enable Scan Schedules

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



Enable Scan Schedules

Network Scan

Repeat daily

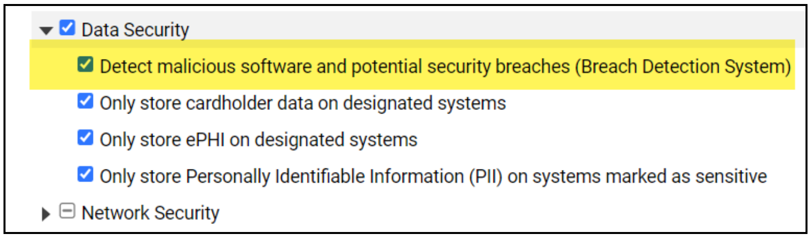
12:00 AM

Detect Breaches

Repeat weekly

N/A

1. **Network Scan**: Set the time for the daily Cyber Hawk (Level 1) Network Scan. This scan will check for anomalies, changes, and threats as per your settings in "Task 8 — Configure Policies and Notifications" on page 41. You can also click **Scan Now** to begin a scan immediately.
2. **Detect Breaches**: Set the time for a malicious software and breach detection scan. This requires that you first activate the **Breach Detection System** policy from **Policy Configuration** > **Data Security**.

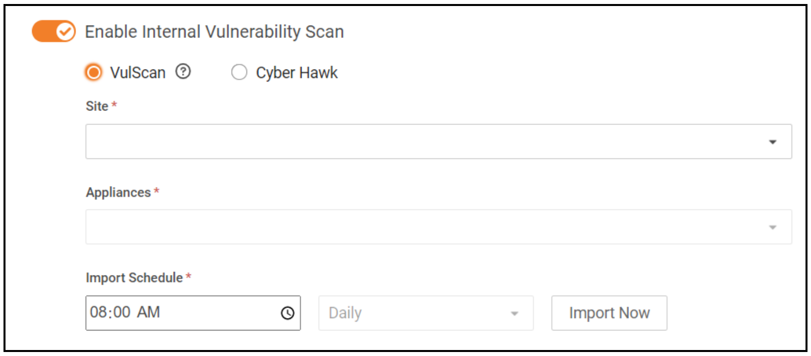


- ☑ Data Security
  - ☑ Detect malicious software and potential security breaches (Breach Detection System)
  - ☑ Only store cardholder data on designated systems
  - ☑ Only store ePHI on designated systems
  - ☑ Only store Personally Identifiable Information (PII) on systems marked as sensitive
- ⊟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

Enable Internal Vulnerability Scan

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

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


Enable Internal Vulnerability Scan

● VulScan ○ Cyber Hawk

Site *

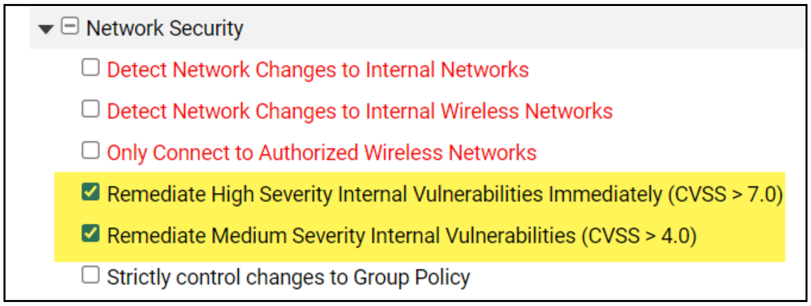
Appliances *

Import Schedule *

08:00 AM

Daily

In order to generate alerts regarding internal vulnerabilities, ensure you have selected these policies from **Settings** > **Policy Configuration** > **Network Security**. You will set up these policies later in "Task 8 — Configure Policies and Notifications" on page 41.


Network Security

☐ Detect Network Changes to Internal Networks

☐ Detect Network Changes to Internal Wireless Networks

☐ Only Connect to Authorized Wireless Networks

☑ Remediate High Severity Internal Vulnerabilities Immediately (CVSS > 7.0)

☑ Remediate Medium Severity Internal Vulnerabilities (CVSS > 4.0)

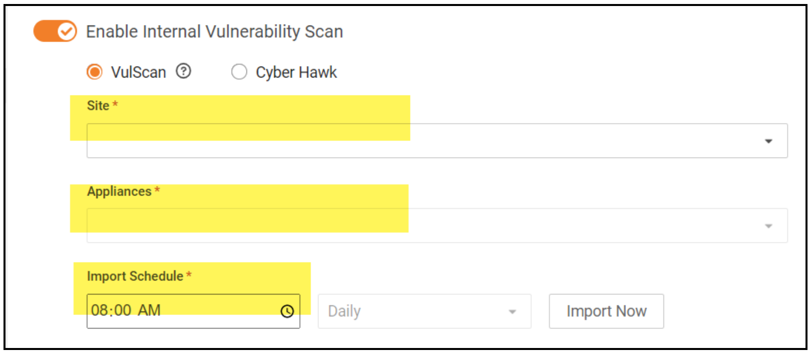
☐ Strictly control changes to Group Policy

Enable Internal Vulnerability Scanning using VulScan Import

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

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

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



☑ Enable Internal Vulnerability Scan

● VulScan ⓘ ○ Cyber Hawk

Site *

Appliances *

Import Schedule *

08:00 AM Daily

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

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

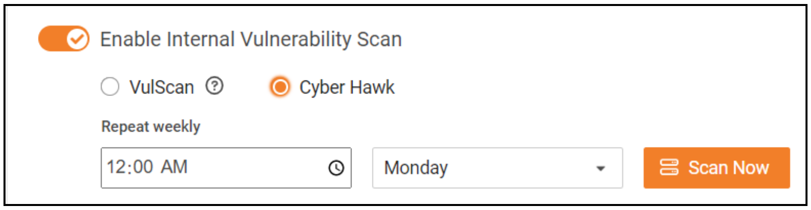
You can also click **Import Now** to import scans immediately.

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

Enable Cyber Hawk Internal Vulnerability Scan

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

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



☑ Enable Internal Vulnerability Scan

○ VulScan ● Cyber Hawk

Repeat weekly

12:00 AM Monday

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

Tips for Scheduling the Internal Vulnerability Scan

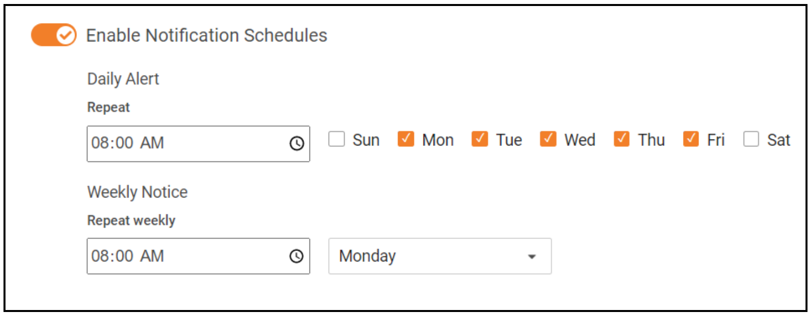
Internal Network Vulnerability scans are intentionally designed to be aggressive and comprehensive in nature. At Internal Network Vulnerability scan run time, there are instances where these scans can impact network performance and access to computer endpoints by network users during the time a scheduled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

It is recommended that:

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

Enable Notification Schedules

Activate the slider to enable Notification Schedules.



Enable Notification Schedules

Daily Alert

Repeat

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

Weekly Notice

Repeat weekly

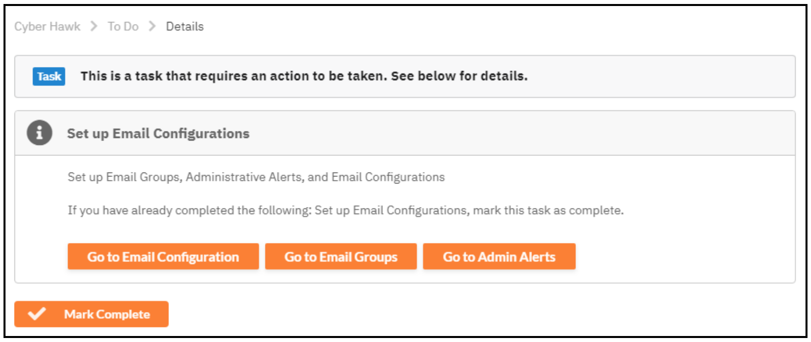
08:00 AM Monday

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

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

Task 4 — Set up Email Configurations

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



Cyber Hawk > To Do > Details

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

Set up Email Configurations

Set up Email Groups, Administrative Alerts, and Email Configurations

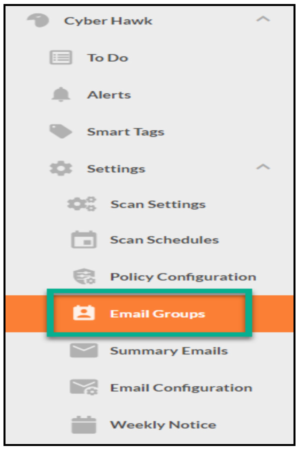
If you have already completed the following: Set up Email Configurations, mark this task as complete.

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

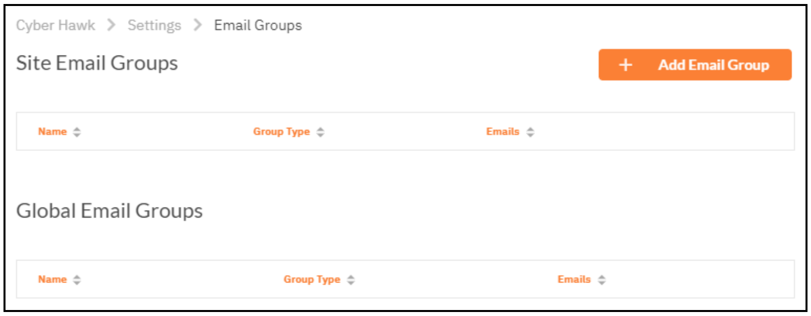
Set Up Email Groups

To set up Email Groups:

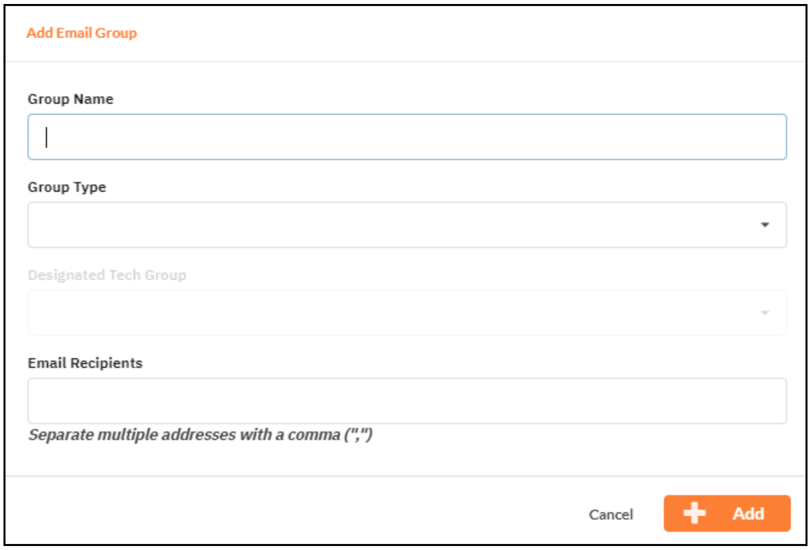
1. From the To Do item, click **Go to Email Groups** or go to the **Cyber Hawk tab** > **Settings**.
2. Click **Email Groups** from the Settings options on the left-hand side of the screen.



3. Click **Add Email Group**.



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



Add Email Group

Group Name

|

Group Type

Designated Tech Group

Email Recipients

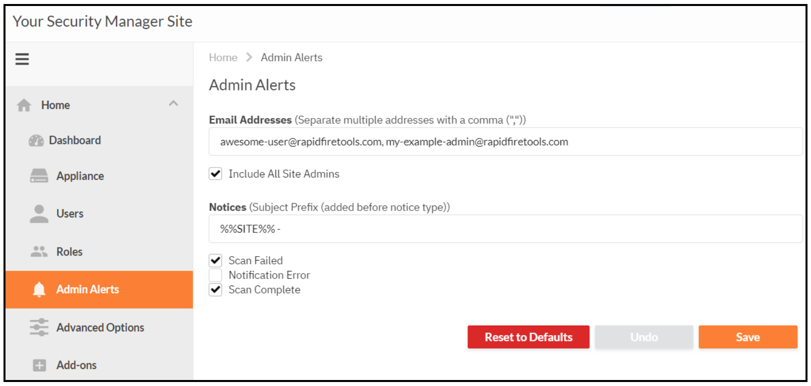
Separate multiple addresses with a comma (",")

> **Note:** For *Group Type*:
> • Select **Tech** for Alerts that will be sent to your Technicians.
> • Select **End User** for Alerts that you wish to send to on-site users for feedback before involving your Technicians.
> You will configure which Alerts go to which Group Type later in the Policy Configuration set up process.

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

Set Up Admin Alerts

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



Your Security Manager Site

Admin Alerts

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

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

☑ Include All Site Admins

Notices (Subject Prefix (added before notice type))

%%SITE%% -

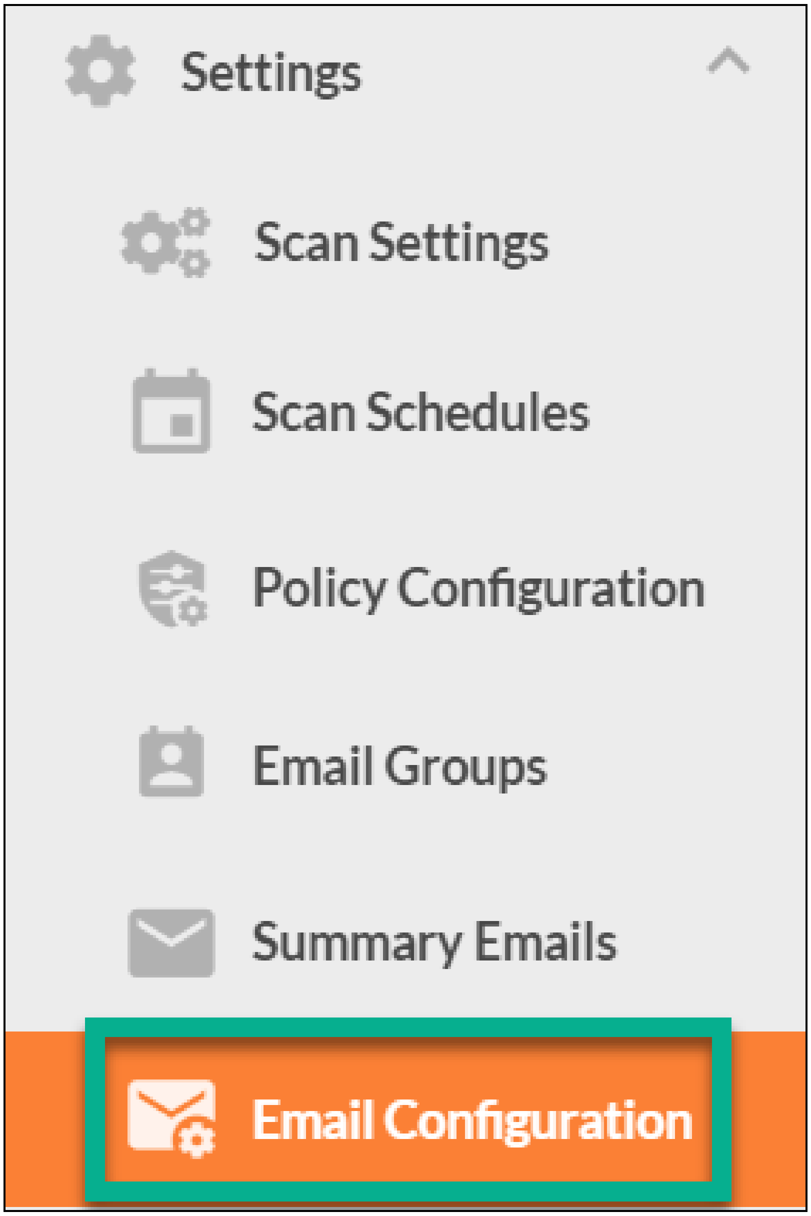
☑ Scan Failed
□ Notification Error
☑ Scan Complete

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

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

Set Up Email Configuration

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

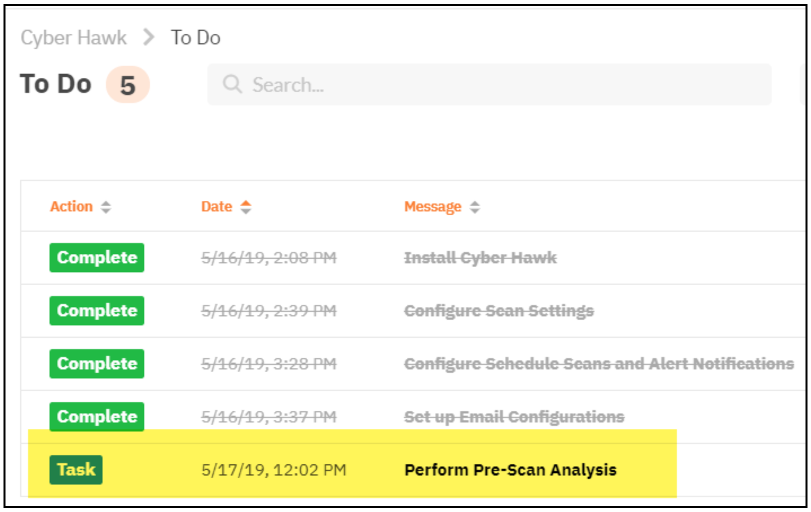


4. When you are finished, return to the To Do item and click **Mark Complete**.

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

Task 5 — Perform Pre-Scan Analysis

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

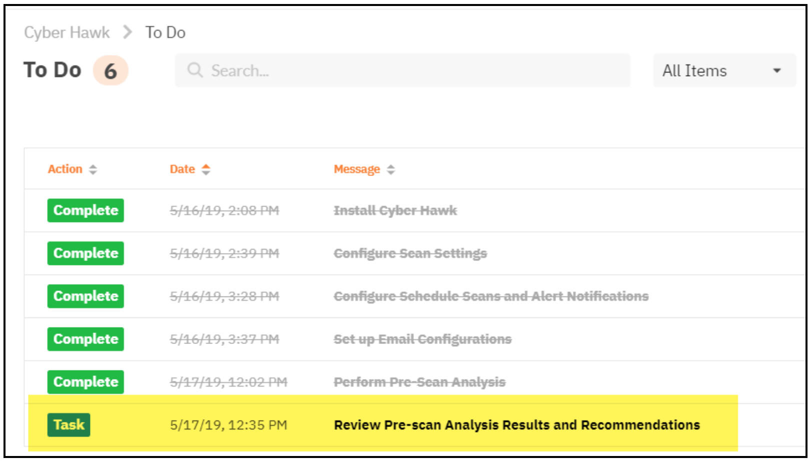


Action	Date	Message
Complete	~~5/16/19, 2:08 PM~~	~~Install Cyber Hawk~~
Complete	~~5/16/19, 2:39 PM~~	~~Configure Scan Settings~~
Complete	~~5/16/19, 3:28 PM~~	~~Configure Schedule Scans and Alert Notifications~~
Complete	~~5/16/19, 3:37 PM~~	~~Set up Email Configurations~~
Task	5/17/19, 12:02 PM	**Perform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

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

Task 6 — Review Pre-Scan Analysis Results and Recommendations

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



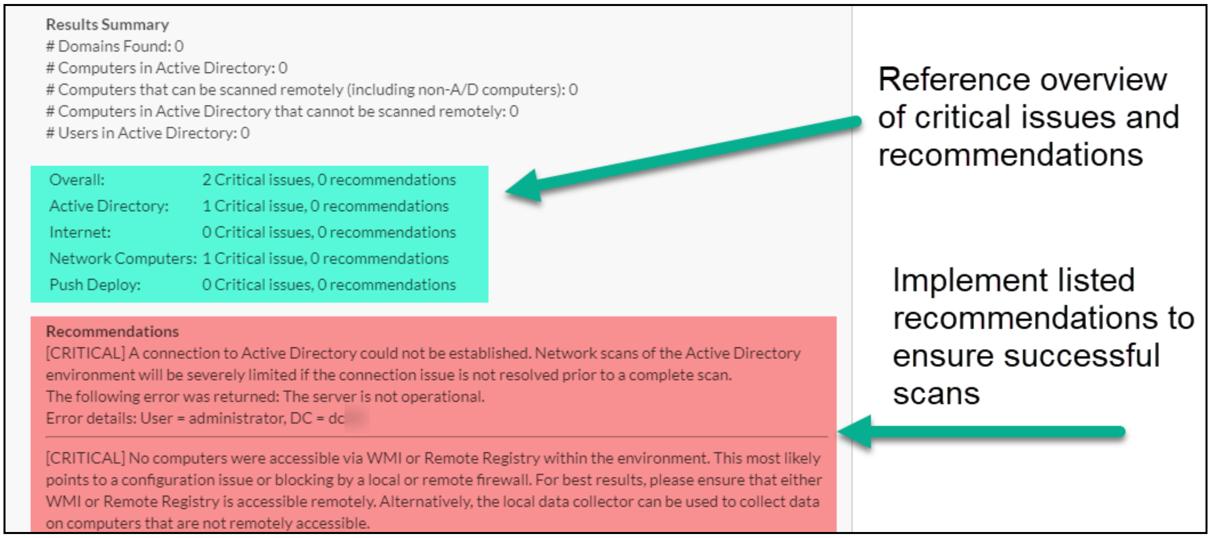
Action	Date	Message
Complete	~~5/16/19, 2:08 PM~~	~~Install Cyber Hawk~~
Complete	~~5/16/19, 2:39 PM~~	~~Configure Scan Settings~~
Complete	~~5/16/19, 3:28 PM~~	~~Configure Schedule Scans and Alert Notifications~~
Complete	~~5/16/19, 3:37 PM~~	~~Set up Email Configurations~~
Complete	~~5/17/19, 12:02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

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

Important: For best results, the target network must be configured to allow for successful scans on all network endpoints. See "Pre-Scan Network Configuration Checklist" on page 50 for configuration guidance for both Windows Active Directory and Workgroup environments.

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

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



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

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

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

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

Reference overview of critical issues and recommendations

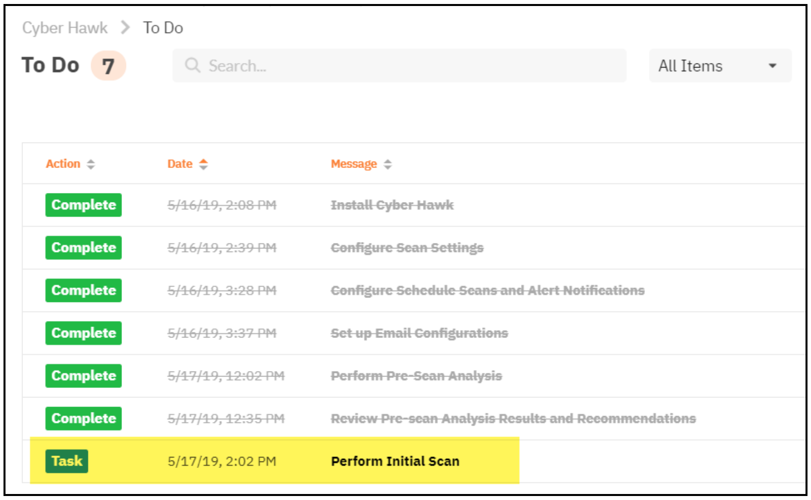
Implement listed recommendations to ensure successful scans

When you have reviewed the pre-scan analysis and are finished making any recommended changes to the target network, click **Mark Complete**.

Task 7 — Perform Initial Cyber Hawk Scan

Before you can continue setting up Cyber Hawk, you need to perform an *initial scan* in order to gather more information about the target network. The initial scan will begin as soon as you click Mark Complete on the previous task, "Review Pre-scan Analysis Results and Recommendations."

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



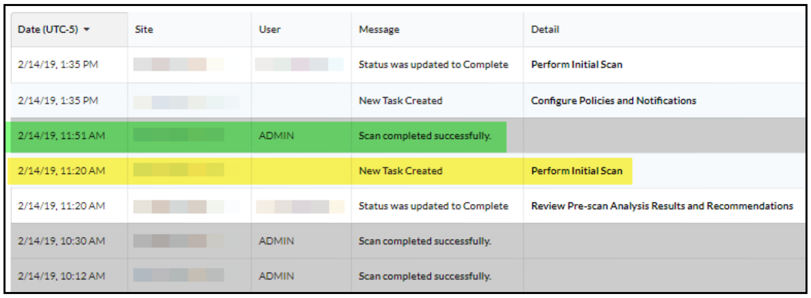
Cyber Hawk > To Do

To Do 7

Search... All Items

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

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

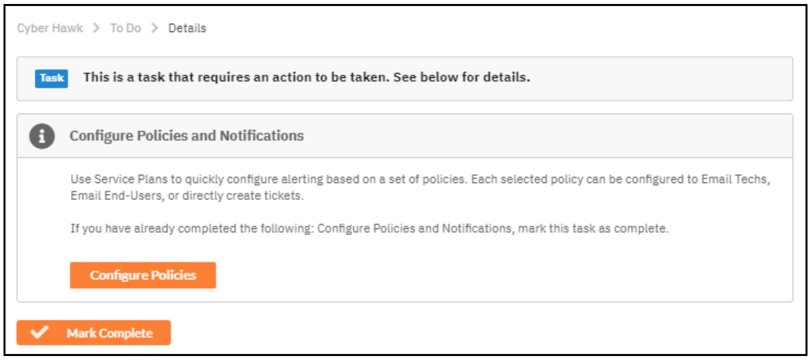


Date (UTC-5)	Site	User	Message	Detail
2/14/19, 1:35 PM	[redacted]	[redacted]	Status was updated to Complete	Perform Initial Scan
2/14/19, 1:35 PM	[redacted]		New Task Created	Configure Policies and Notifications
2/14/19, 11:51 AM	[redacted]	ADMIN	Scan completed successfully.	
2/14/19, 11:20 AM	[redacted]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

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

Task 8 — Configure Policies and Notifications

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



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

Configure Policies and Notifications

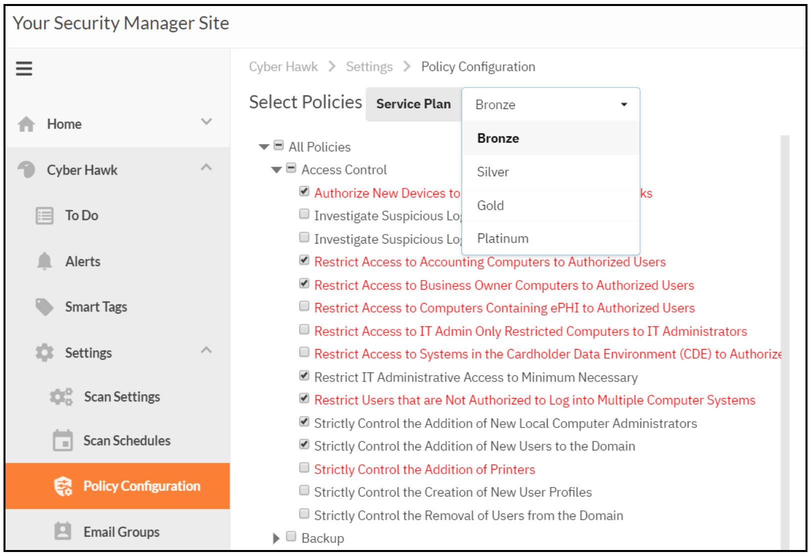
Use Service Plans to quickly configure alerting based on a set of policies. Each selected policy can be configured to Email Techs, Email End-Users, or directly create tickets.

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

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

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

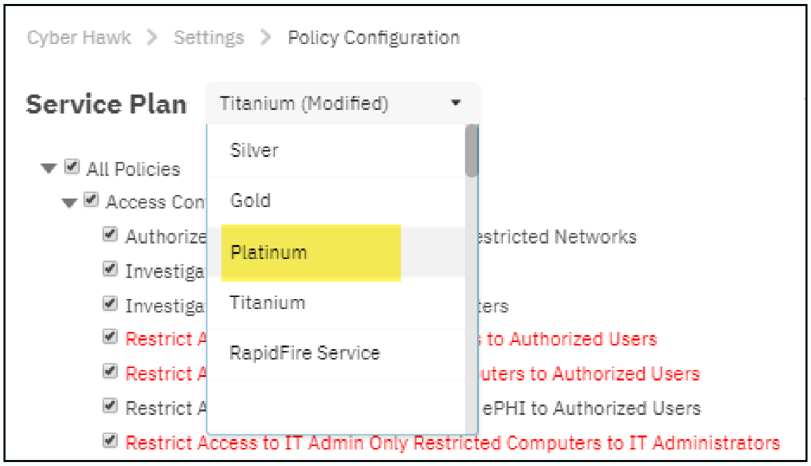
> **Tip:** If you wish to create a "global" Service Plan that you can apply to multiple sites, see "Create Global Service Plans for Cyber Hawk" on page 70, then return to this step and apply your global policy to this site.



Service Plan: Bronze

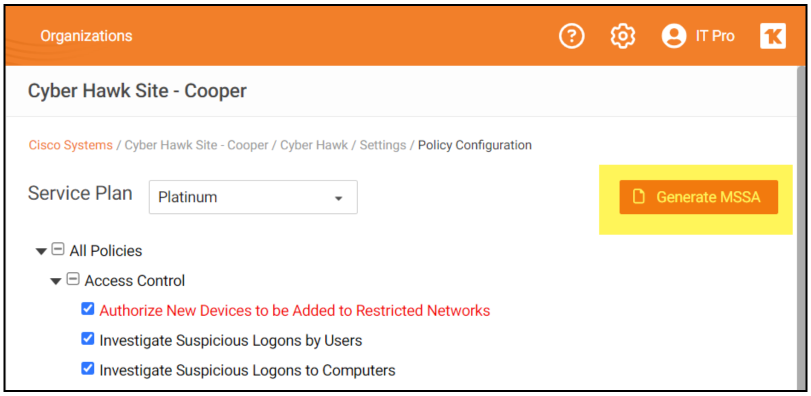
- ☑ All Policies
  - ☑ Access Control
    - ☑ Authorize New Devices to ... ks
    - □ Investigate Suspicious Lo...
    - □ Investigate Suspicious Lo...
    - ☑ Restrict Access to Accounting Computers to Authorized Users
    - ☑ Restrict Access to Business Owner Computers to Authorized Users
    - □ Restrict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

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

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

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

   a. Click **Generate MSSA**.



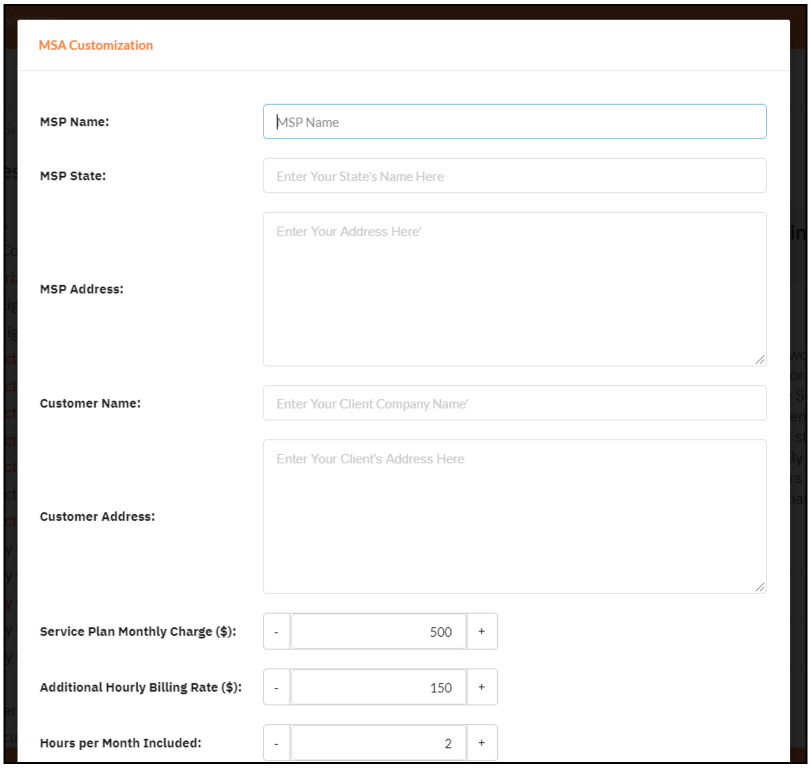
Cyber Hawk Site - Cooper

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

Service Plan: Platinum

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

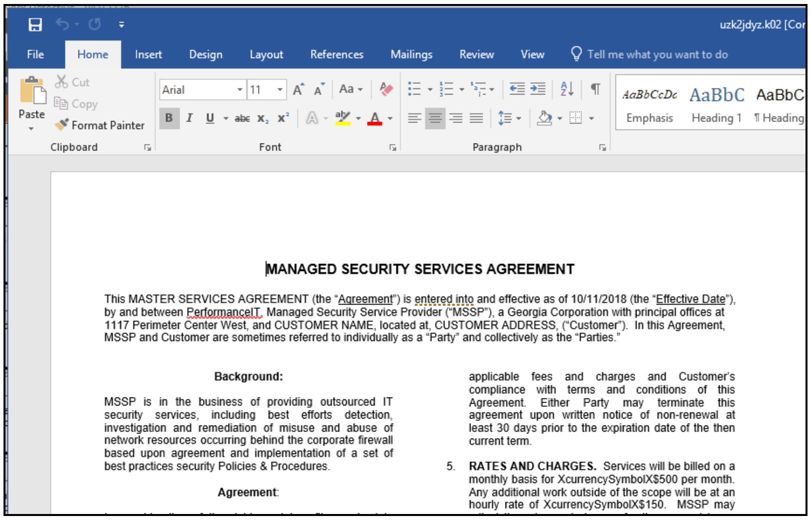
   b. Enter your custom information for the MSSA.



MSA Customization

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

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



MANAGED SECURITY SERVICES AGREEMENT

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

Background:

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

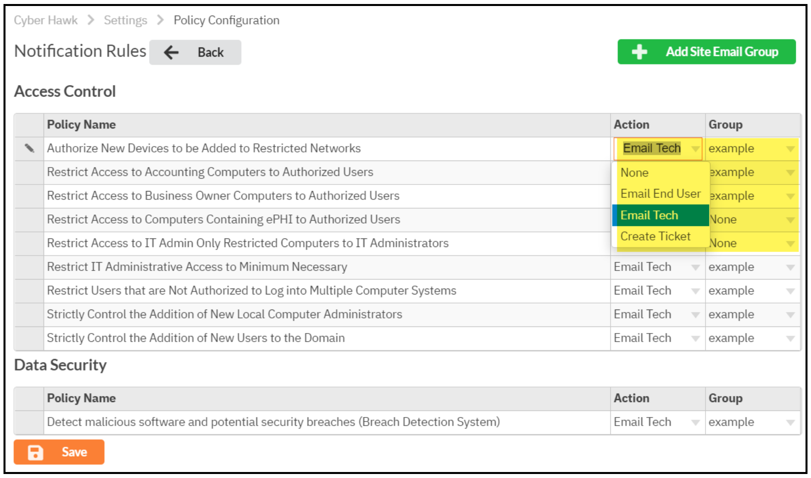
Agreement:

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

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

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

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



Access Control

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

Data Security

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

Actions include:

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

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

6. Select the Email **Group Name** (the email group to whom to send either an End User or Tech email notification).
7. When you have assigned *Actions* and *Groups* to all Security Policies, click **Finish**.

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

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

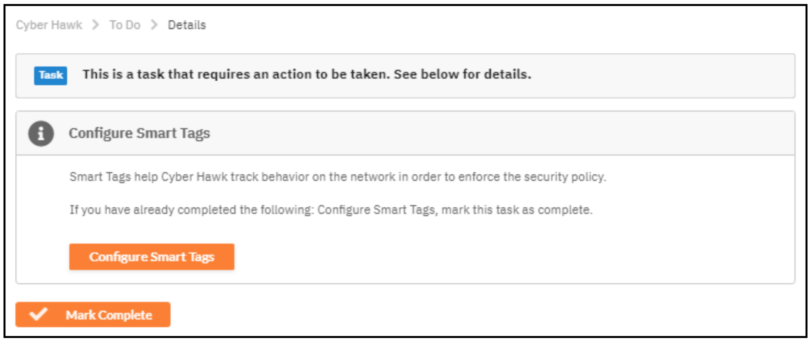
When you complete this To Do item, the **Configure Smart Tags** To Do item will appear.

Task 9 — Configure Smart Tags

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

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

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



Cyber Hawk > To Do > Details

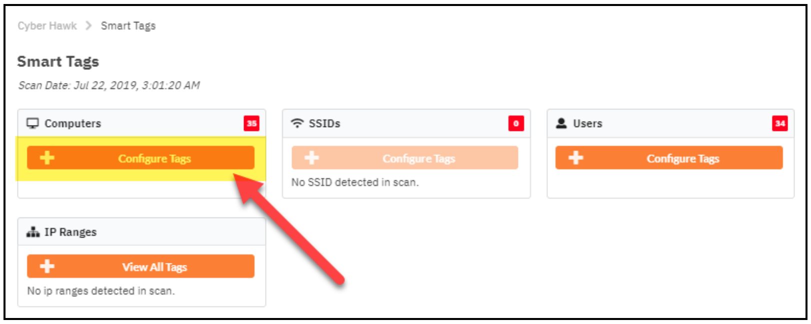
Task This is a task that requires an action to be taken. See below for details.

Configure Smart Tags

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

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

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



Cyber Hawk > Smart Tags

Smart Tags

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

Computers 35

Configure Tags

SSIDs 0

Configure Tags

No SSID detected in scan.

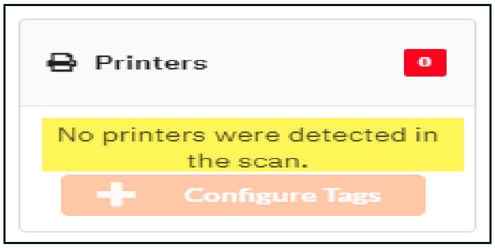
Users 34

Configure Tags

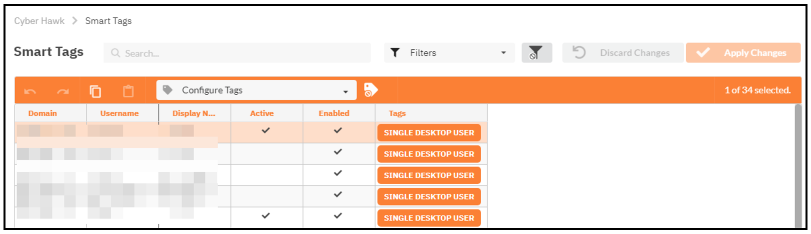
IP Ranges

View All Tags

No ip ranges detected in scan.

> **Note:** If the network scan does not uncover assets, the **Configure Tags** button will not be available.
>
> 
>
> Printers 0
>
> No printers were detected in the scan.
>
> Configure Tags

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



Cyber Hawk > Smart Tags

Smart Tags

Search...

Filters

Discard Changes

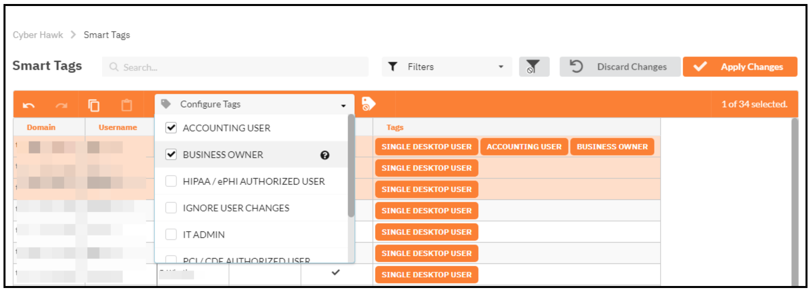
Apply Changes

Configure Tags

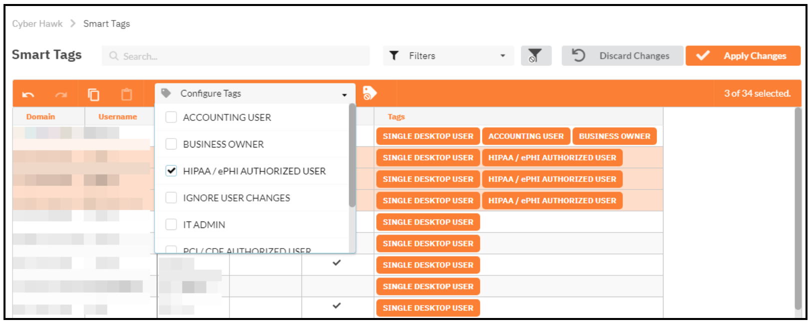
1 of 34 selected.

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

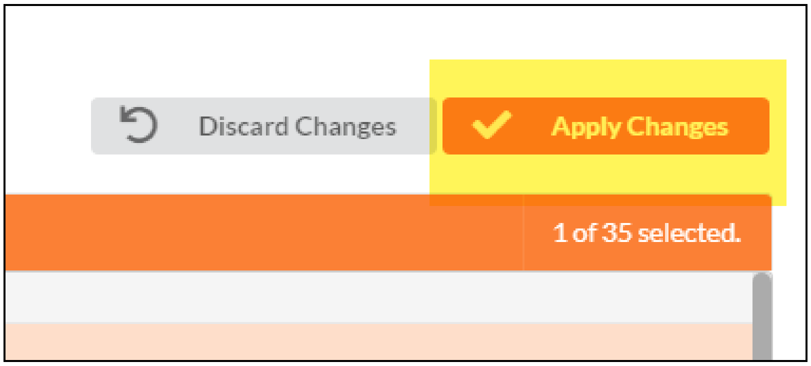
4. With the chosen assets still selected, click on one or more **Smart Tags** at the bottom of the screen.



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

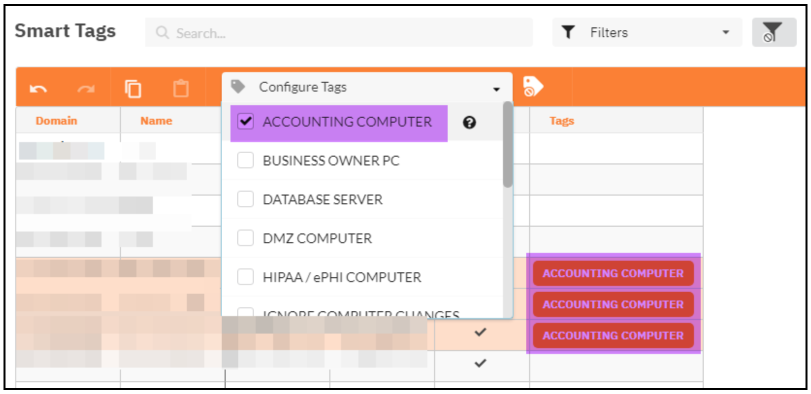


5. Click **Apply Changes** to save your **Smart Tag** configuration.

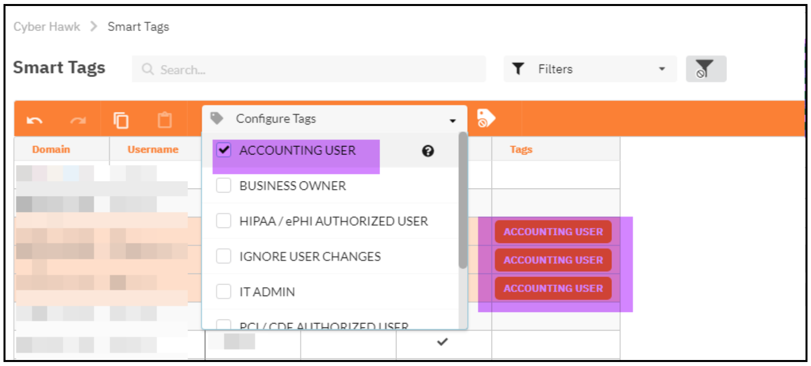


6. Return to **[Your Site]** > **Cyber Hawk** > **Smart Tags**. Continue tagging network assets (*Computers*, *Users*, *Printers*, etc.) until you have assigned all Smart Tags necessary to enforce your chosen Security Policies.

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



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



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

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

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

Pre-Scan Network Configuration Checklist

RapidFire Tools products can gather a great deal of information from the target network with little advance preparation – and with very little footprint! However, if you are having trouble with scans, or you have the ability to configure the target network in advance, we recommend the settings below.

These checklists detail the recommended network configurations for both Windows **Domain** and **Workgroup** environments.

> **Note:** You must have the .NET 4.6.2 framework installed on machines in order to use all data collector and server/appliance tools.

Checklist for Domain Environments

Share this checklist with your IT Administrator and ask them to configure your network's Domain Controller as follows:

Complete	Domain Configuration
	GPO Configuration for Windows Firewall (Inbound Rules)
□	Allow *Windows Management Instrumentation (WMI)* service to operate through Windows Firewall This includes the following rules: • Windows Management Instrumentation (ASync-In) • Windows Management Instrumentation (WMI-In) • Windows Management Instrumentation (DCOM-In)
□	Allow *File and printer sharing* to operate through Windows Firewall This includes the following rules: • File and Printer Sharing (NB-Name-In) • File and Printer Sharing (SMB-In) • File and Printer Sharing (NB-Session-In)
□	Enable *Remote Registry* “read only” access on computers targeted for scanning.

Complete	Domain Configuration
	Note: Remote Registry access should be restricted for use by the user access account credentials to be used during network and local computer scan.
□	Enable the *Internet Control Message Protocol (ICMP)* to allow authorized ICMP echo request messages and ICMP echo reply messages to be sent and received by Windows computers and network devices. Windows firewall rules on Windows computers may need to be created/enabled to allow a computer: • operating a Kaseya-RapidFire Tools product network data collector to issue ICMP echo request messages to be sent to Windows computers and network devices • to send ICMP echo reply messages in response to an ICMP echo request **Note:** ICMP requests are used to detect active Windows computers and network devices to scan.
	GPO Configuration for Windows Services
□	*Windows Management Instrumentation (WMI)* • Startup Type: Automatic
□	*Windows Update Service* • Startup Type: Automatic
□	*Remote Registry* • Startup Type: Automatic
□	*Remote Procedure Call* • Startup Type: Automatic
	Network Shares
□	• *Admin$* must be present and accessible using supplied credentials (usually a local admin or user in the local Computer's Administrative Security group)

Complete	Domain Configuration
	3rd Party Firewalls
□	• Ensure that 3rd party Firewalls are configured similarly to Windows Firewall rules described within this checklist. **Note:** This is a requirment for both Active Directory and Workgroup Networks.

Checklist for Workgroup Environments

Before you perform a workgroup assessment, run the following PowerShell commands on the target network and the machine that will perform the scan. These three configurations should help you avoid most issues in a workgroup environment. Each command is followed by an explanation and link to Microsoft documentation.

1.
   ```
   reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system /v LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f
   ```

   By default, UAC only allows remote administration tasks to be performed by the Built-in Administrator account. To work around this, this command sets the LocalAccountTokenFilterPolicy registry key to 1. This allows any local admin to perform remote administrative tasks (i.e. access to system shares C$, Admin$, etc.).

   https://support.microsoft.com/en-us/help/951016/description-of-user-account-control-and-remote-restrictions-in-windows

2.
   ```
   netsh advfirewall firewall set rule group="windows management instrumentation (wmi)" new enable=yes
   ```

   This command creates an Inbound firewall rule to allow access to the WMI service and namespaces.

   https://docs.microsoft.com/en-us/windows/win32/wmisdk/connecting-to-wmi-remotely-starting-with-vista

3.
   ```
   netsh advfirewall firewall set rule group="File and Printer Sharing" new enable=Yes
   ```

This command creates an Inbound firewall rule which enables File and Printer Sharing on the machine. File and printer sharing is required in order to access the Admin$ share on remote machines.

https://answers.microsoft.com/en-us/windows/forum/all/turning-on-file-and-printer-sharing-windows-10/bb3066eb-f589-4021-8f71-617e70854354

You can also share this checklist with your IT Administrator and ask them to configure each computer in your workgroup as follows:

Complete?	Workgroup Configuration
	Network Settings
□	• *Admin$* must be present on the computers you wish to scan, and be accessible with the login credentials you provide for the scan
□	• *File and printer sharing* must be enabled on the computers you wish to scan
□	• *Ensure the Windows Services below are running and allowed to communicate through Windows Firewall*: • Windows Management Instrumentation (WMI) • Windows Update Service • Remote Registry • Remote Desktop • Remote Procedure Call
□	• Workgroup computer administrator user account credentials. **Note:** Before configuring scan settings for workgroups, prepare a list of the workgroup computer(s) adminstrator user account credentials for entry into the scan settings wizard.
□	Enable the *Internet Control Message Protocol (ICMP)* to allow authorized ICMP echo request messages and ICMP echo reply messages to be sent and received by Windows computers and network devices. Windows firewall rules on Windows computers may need to be created/enabled to allow a computer:

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

RapidFire Tools Portal Set Up

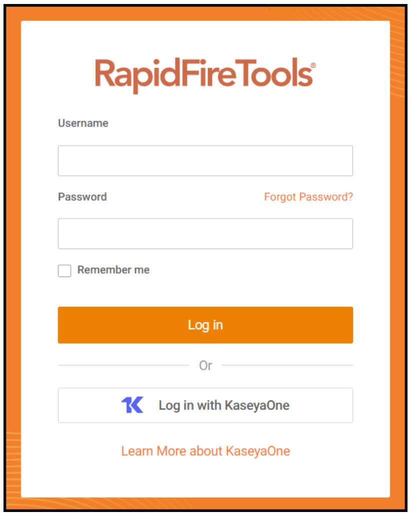
See the topics below for additional Cyber Hawk set up and help topics.

Set Up Portal Branding

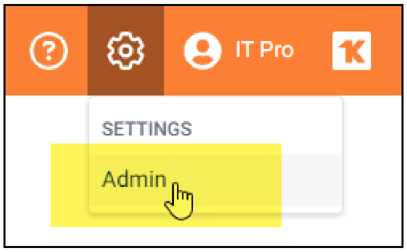
The RapidFire Tools Portal allows you to customize many elements to fit with your organization's brand and identity. This topic covers how you can modify the Portal's look and feel.

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

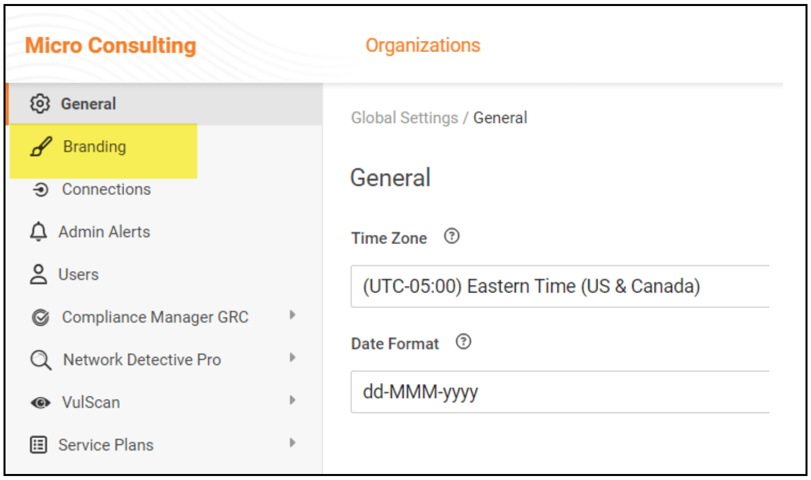
> **Note:** In order to configure the settings in the Portal, the login credentials you use to access the Portal will require the Master User rights.



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



3. Click **Branding**.



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

Date Format: dd-MMM-yyyy

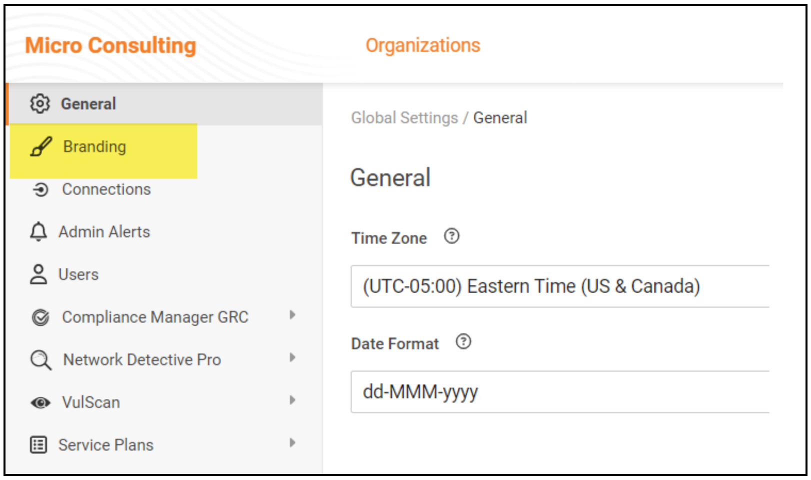
From this page, you can then:

- "Set Custom Portal Theme" below
- "Set Custom Portal Subdomain" on the facing page
- "Set Custom Company Name" on page 58
- "Set Custom Company Logo" on page 59

Set Custom Portal Theme

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

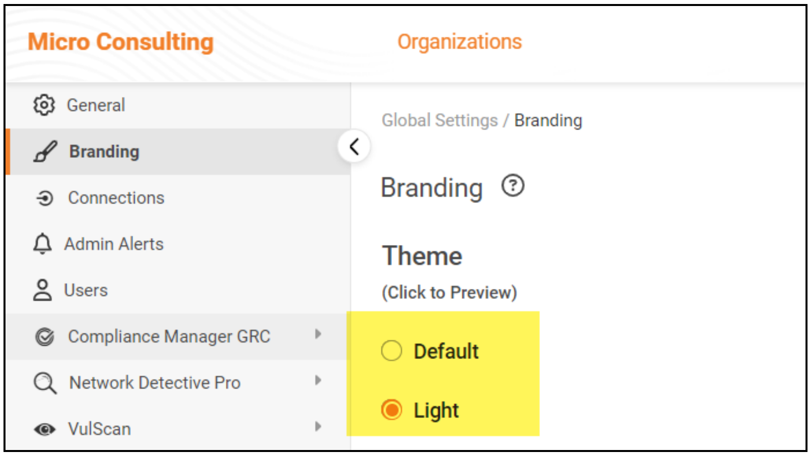
1. From global **Settings (Admin)** > **Branding**, select the *Default* or *Light* under theme.



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

Date Format: dd-MMM-yyyy

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



Theme
(Click to Preview)

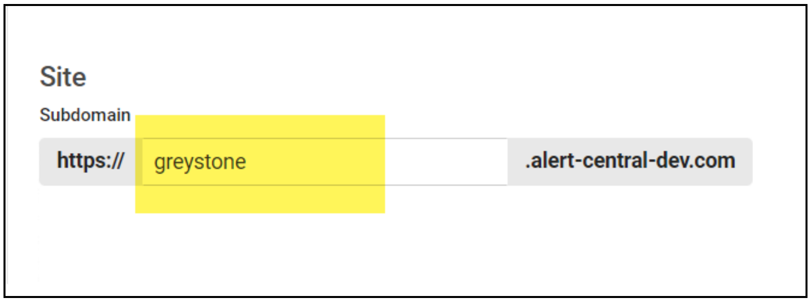
○ Default
● Light

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

Set Custom Portal Subdomain

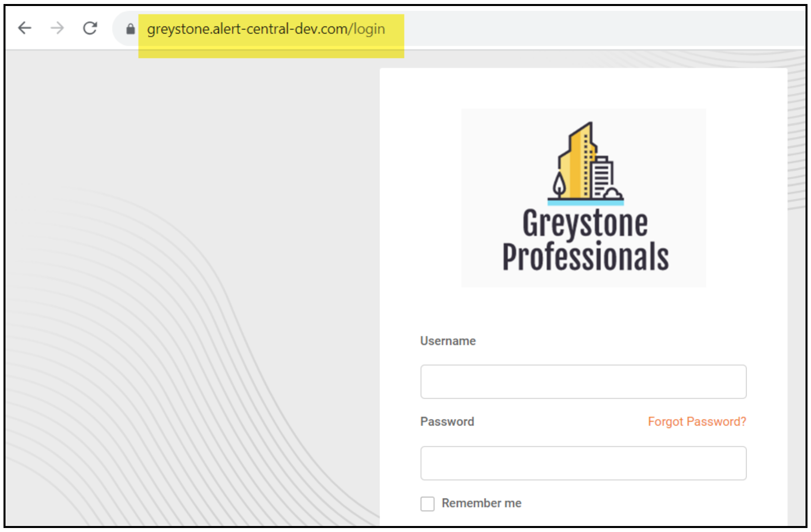
You can enter a custom subdomain to communicate your company name/brand to users when they access the URL for the portal. To do this:

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



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

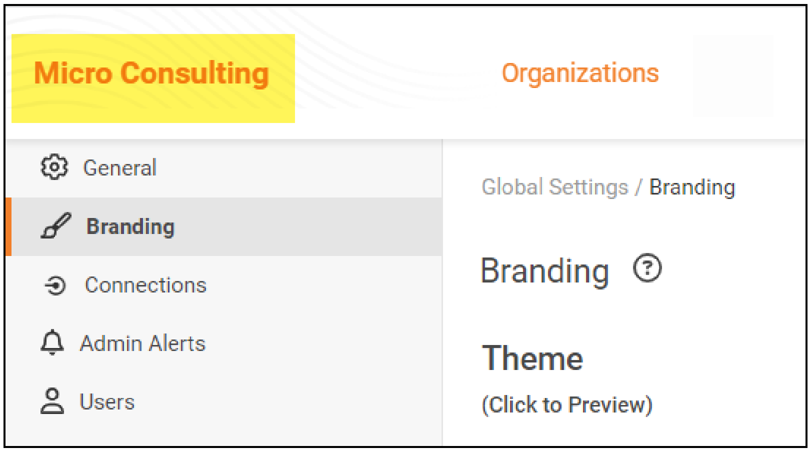
2. Click **Save**.
3. Log out of the RapidFire Tools Portal.
4. Next, access the RapidFire Tools Portal by using the URL for the new Subdomain you configured to access the Portal's login screen.



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

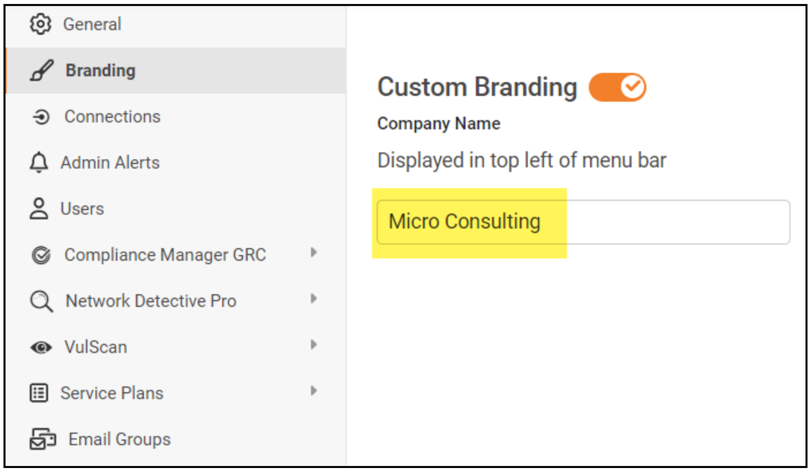
Set Custom Company Name

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



To do this:

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



Custom Branding

Company Name

Displayed in top left of menu bar

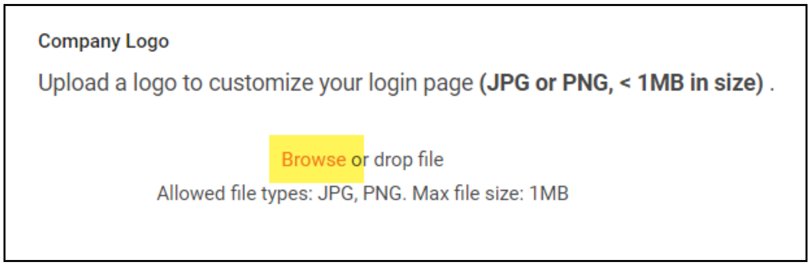
Micro Consulting

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

Set Custom Company Logo

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

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



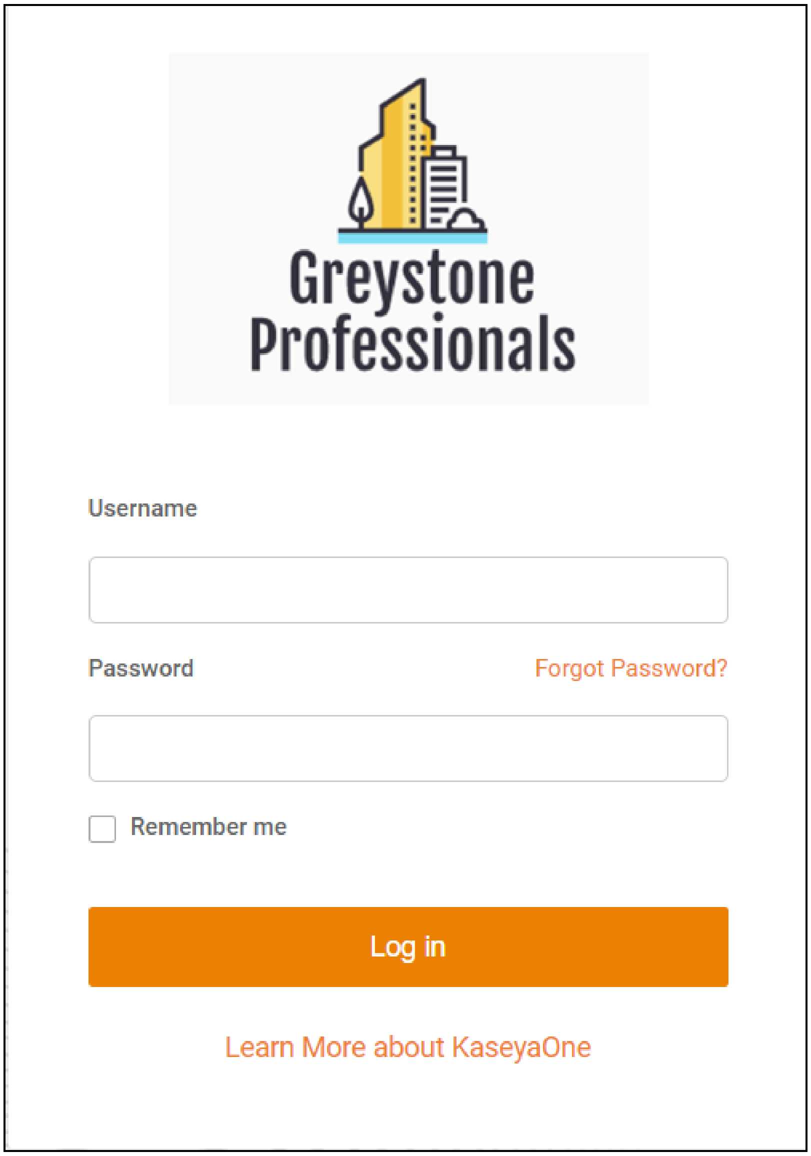
Company Logo

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

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

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

login screen.



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

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

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

Step 1 — Gather Credentials and Set Up your PSA System

Before you begin, you will need:

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

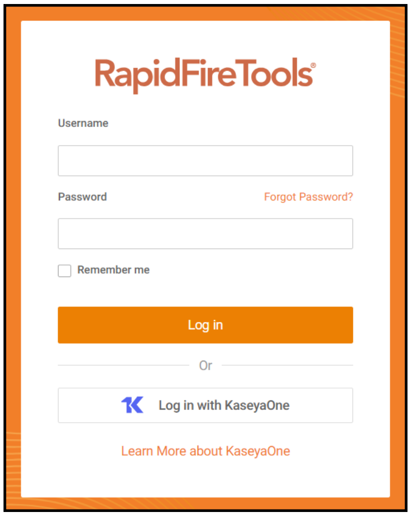
PSA System	PSA Prerequisites
Autotask®	The Autotask SOAP integration has been deprecated (see below). To use the new integration, all you need is a username and password for a non-API user. **Important:** The new Autotask integration is not supported by Network Detective or Network Detective on the web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

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

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

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

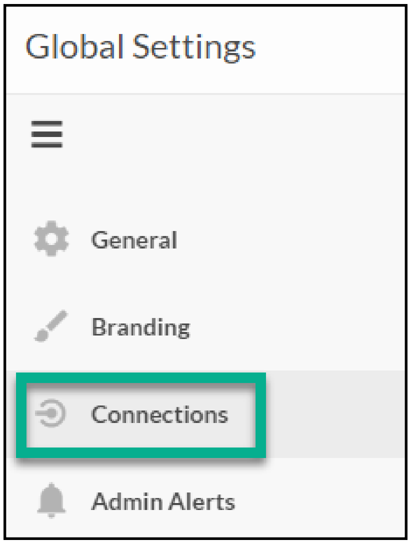
1. Visit https://www.youritportal.com and log into the RapidFire Tools Portal.



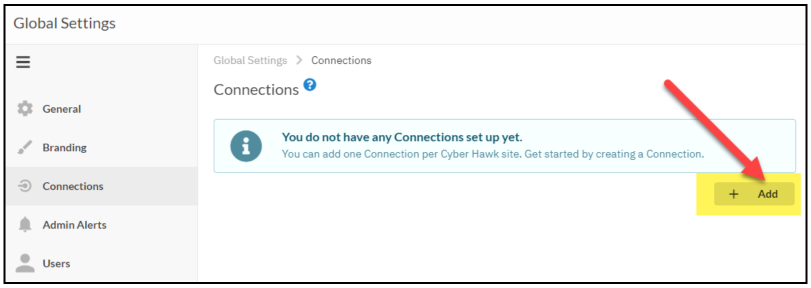
2. Click global **Settings (Admin)** ⚙.

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

3. Click **Connections**.

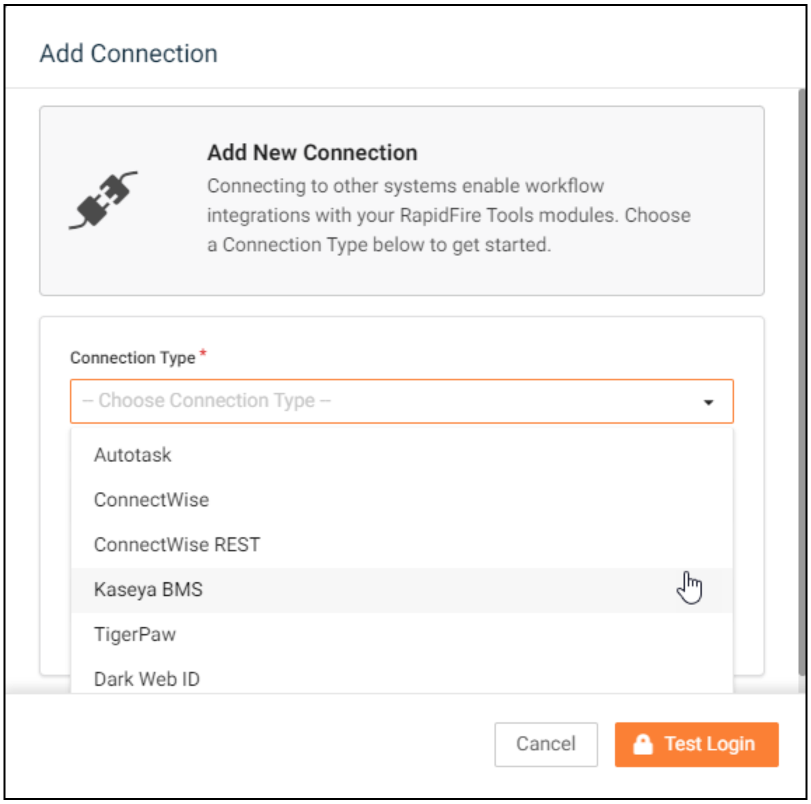


4. Click **Add** to create a new Ticketing System/PSA Connection.



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

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



Add Connection

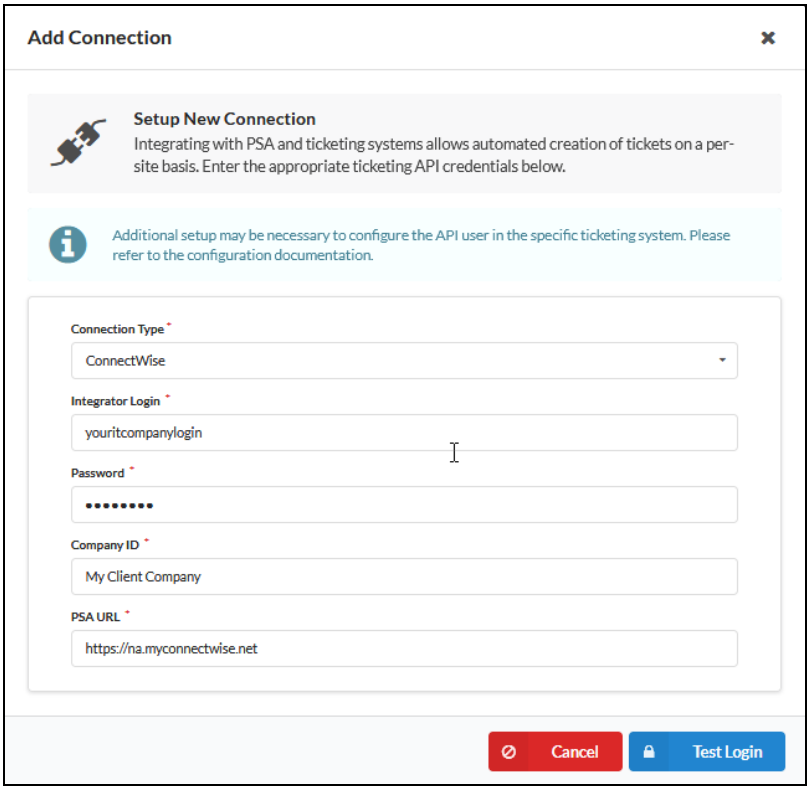
Add New Connection

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

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

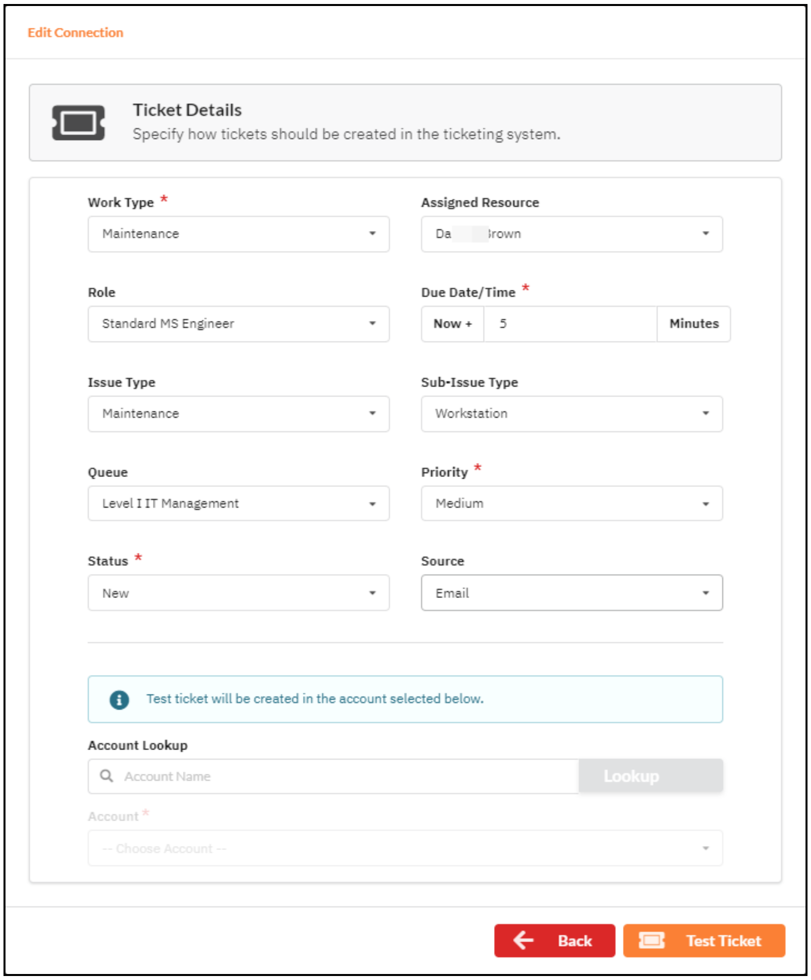
Integrator Login *: youritcompanylogin

Password *: ••••••••

Company ID *: My Client Company

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

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


Edit Connection

Ticket Details
Specify how tickets should be created in the ticketing system.

Work Type * : Maintenance

Assigned Resource: Da[redacted]rown

Role: Standard MS Engineer

Due Date/Time * : Now + 5 Minutes

Issue Type: Maintenance

Sub-Issue Type: Workstation

Queue: Level I IT Management

Priority * : Medium

Status * : New

Source: Email

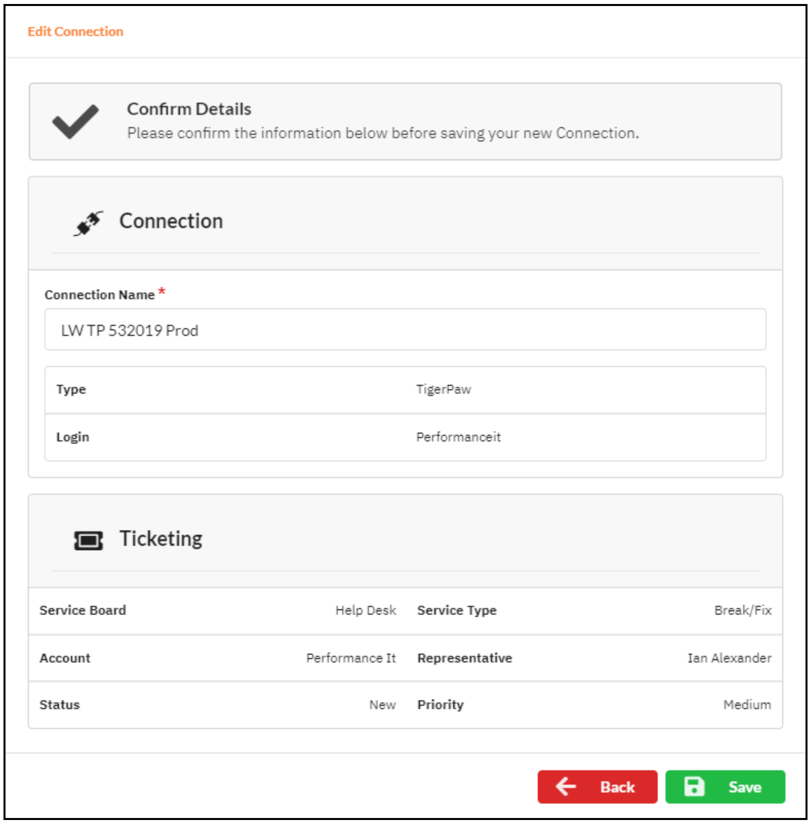
Test ticket will be created in the account selected below.

Account Lookup: Account Name

Account * : -- Choose Account --

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

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



Edit Connection

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

Connection

Connection Name *

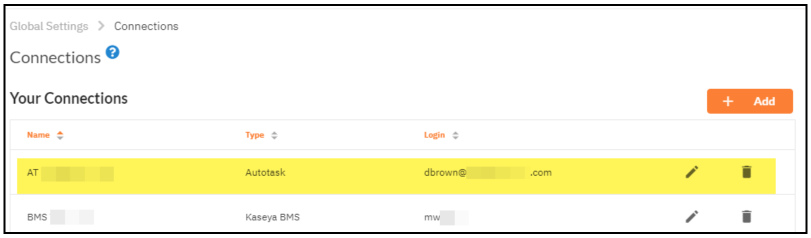
LW TP 532019 Prod

Type	TigerPaw
Login	Performanceit

Ticketing

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

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



Global Settings > Connections

Connections

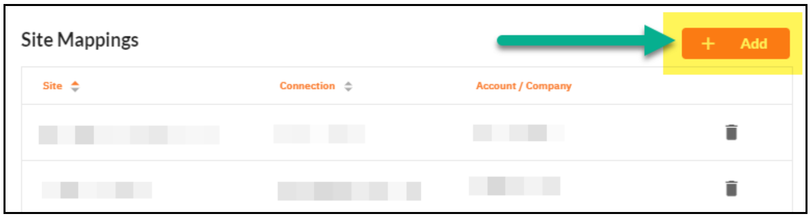
Your Connections

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

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

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

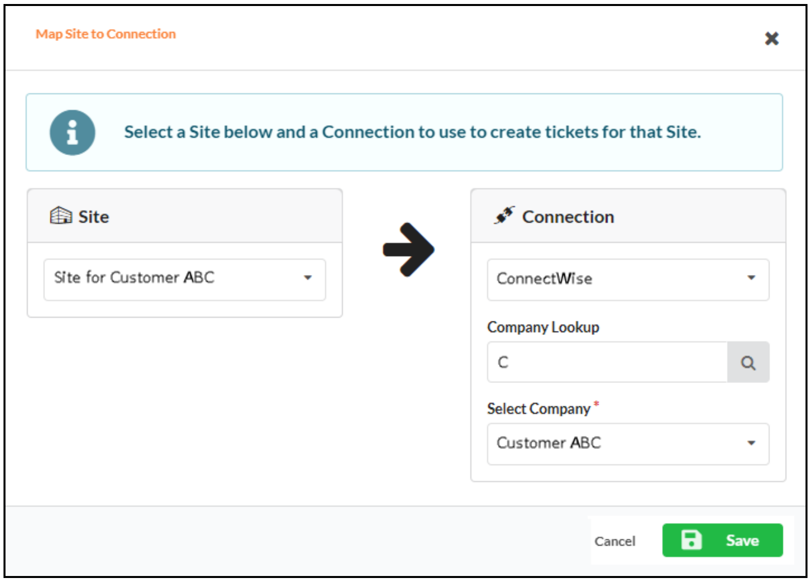
1. In the Integrations window, click **Add** under Site Mappings. The Map Site to Connection window will be displayed.



Site Mappings

Site	Connection	Account / Company
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

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



Map Site to Connection

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

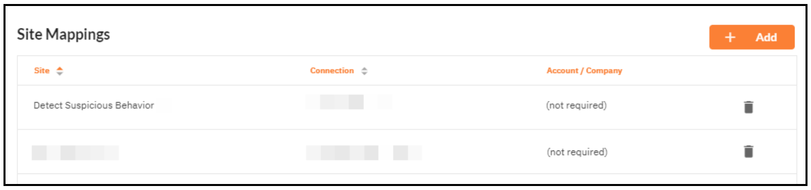
Site: Site for Customer ABC

Connection: ConnectWise

Company Lookup: C

Select Company *: Customer ABC

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



Site Mappings

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

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

Create Global Service Plans for Cyber Hawk

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

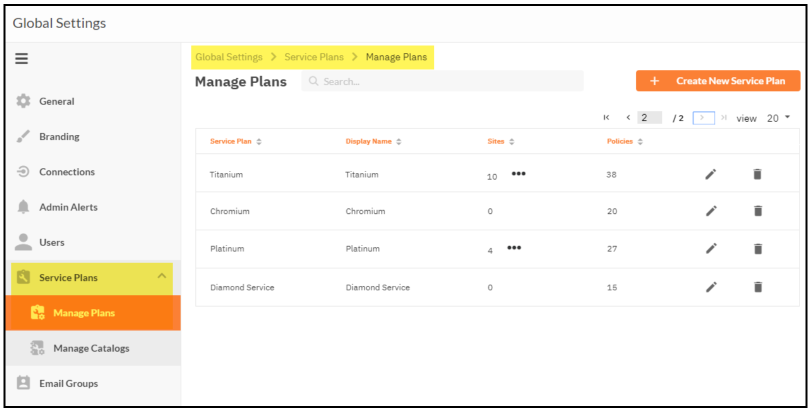
> **Note:** You can think of Service Plans as the "tiers" of Security Services you can offer your clients depending on their needs (think Bronze, Silver, Gold, etc.). You can even create *Service Catalogs* to show clients your service offerings in an easy-to-read chart (see "Create Service Catalogs" on page 75).

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

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

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

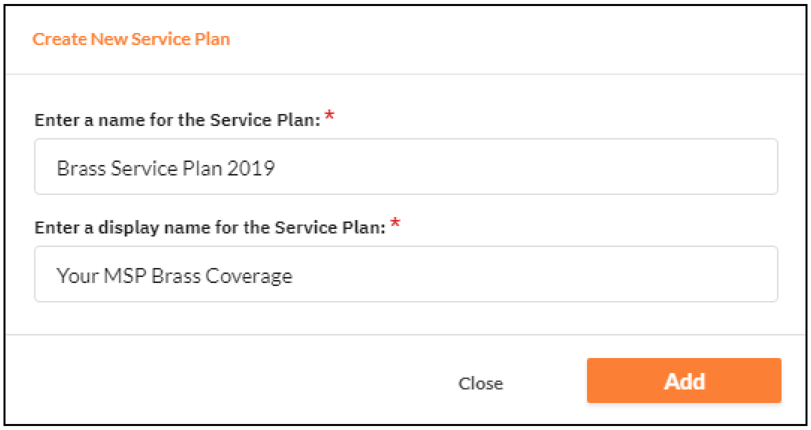
1. First, in the RapidFire Tools Portal, go to global **Settings (Admin)** ⚙ > **Service Plans** > **Manage Plans**.



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

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

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

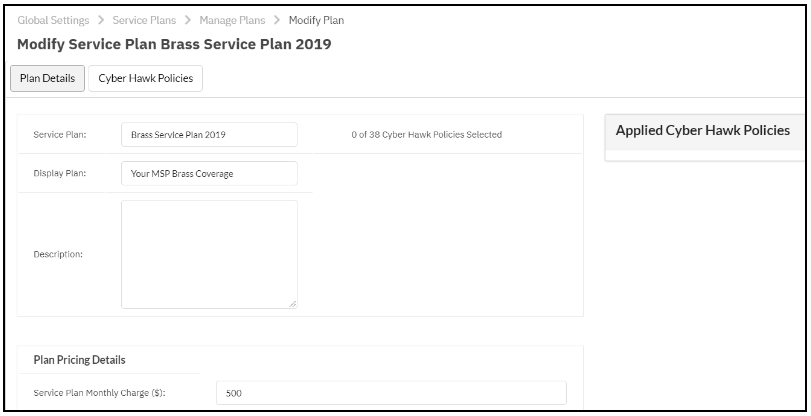


Create New Service Plan

Enter a name for the Service Plan: *
Brass Service Plan 2019

Enter a display name for the Service Plan: *
Your MSP Brass Coverage

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



Global Settings > Service Plans > Manage Plans > Modify Plan

Modify Service Plan Brass Service Plan 2019

Plan Details
Cyber Hawk Policies
Applied Cyber Hawk Policies

Service Plan: Brass Service Plan 2019

0 of 38 Cyber Hawk Policies Selected

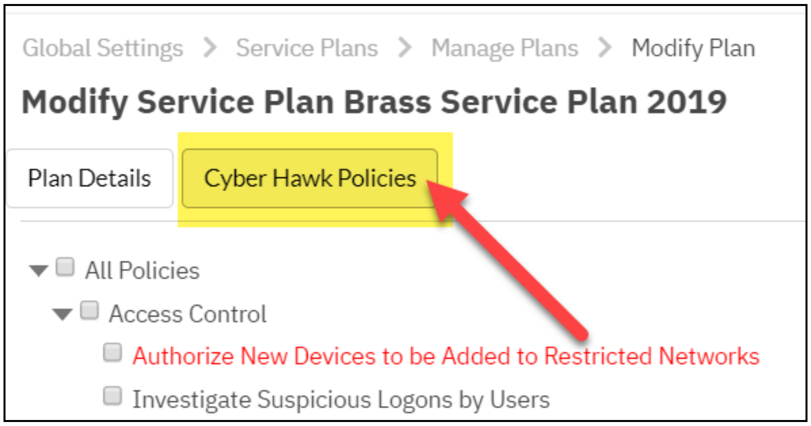
Display Plan: Your MSP Brass Coverage

Description:

Plan Pricing Details

Service Plan Monthly Charge ($): 500

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



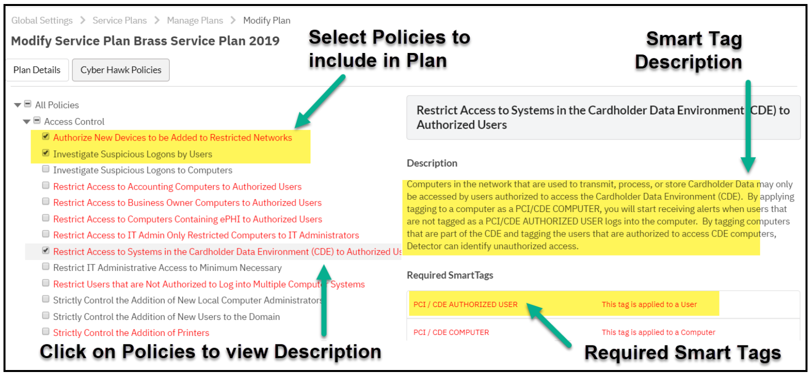
Global Settings > Service Plans > Manage Plans > Modify Plan

Modify Service Plan Brass Service Plan 2019

Plan Details
Cyber Hawk Policies

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

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



Global Settings > Service Plans > Manage Plans > Modify Plan

Modify Service Plan Brass Service Plan 2019

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

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

Description

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

Required SmartTags

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

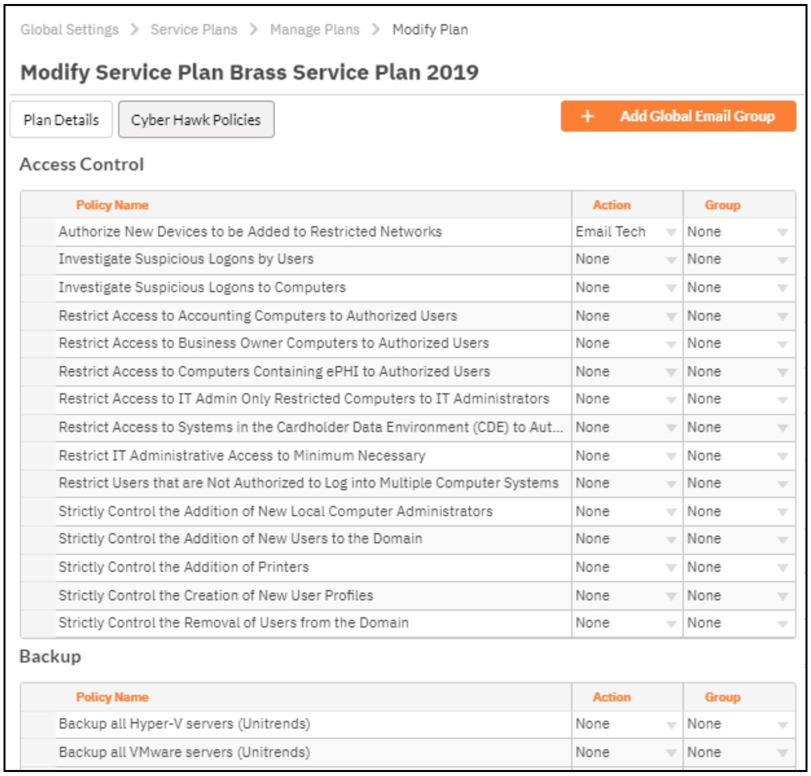
Select Policies to include in Plan

Smart Tag Description

Click on Policies to view Description

Required Smart Tags

6. Check the box next to each Security Policy to include in the plan. Click ▶ to expand the category of available options.
7. Click on a Policy to read a Description of that Policy, as well as to see any **Required Smart Tags**. You will need to deploy these Smart Tags on the appropriate network assets (such as Users or Computers) in order for Cyber Hawk to enforce these policies. See also "Task 9 — Configure Smart Tags" on page 46.
8. When you have selected the Security Policies you want to include in the Service Plan, click **Configure Notifications**.
9. Next, assign **Actions** and **Email Groups** for each Security Policy's Notification Rule. This is where you tell Cyber Hawk what to do when it discovers a potential security policy violation.


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

Modify Service Plan Brass Service Plan 2019

Access Control

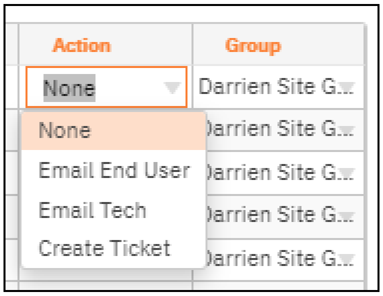
Policy Name	Action	Group
Authorize New Devices to be Added to Restricted Networks	Email Tech	None
Investigate Suspicious Logons by Users	None	None
Investigate Suspicious Logons to Computers	None	None
Restrict Access to Accounting Computers to Authorized Users	None	None
Restrict Access to Business Owner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

Backup

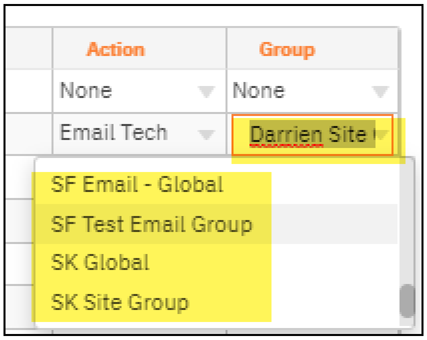
Policy Name	Action	Group
Backup all Hyper-V servers (Unitrends)	None	None
Backup all VMware servers (Unitrends)	None	None

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

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



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



Action	Group
None	None
Email Tech	Darrien Site (

12. When you have assigned *Actions* and *Groups* to all Security Policies, click **Save**. You can then apply this Service Plan to your existing or new Cyber Hawk Sites. See also "Task 8 — Configure Policies and Notifications" on page 41.

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

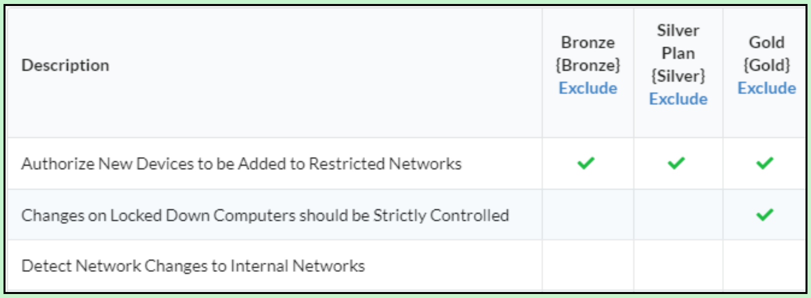
Create Service Catalogs

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

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

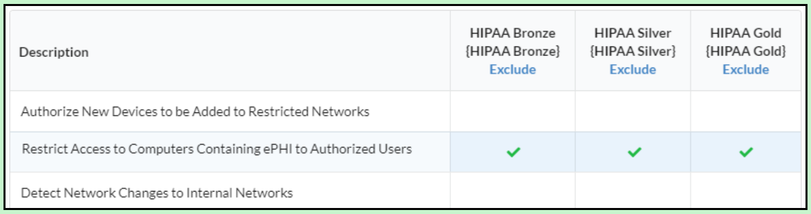
- A Service Catalog contains an easy-to-read matrix of each "tier" of security service you want to offer, such as "Bronze," "Silver," "Gold," or your own custom plans.
- You can generate catalogs as Word documents in order to market your services.
- Cyber Hawk also allows you to create multiple catalogs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

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



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

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

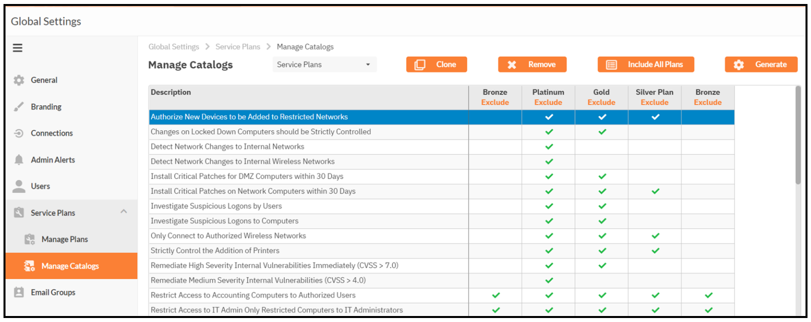


Description	HIPAA Bronze {HIPAA Bronze} Exclude	HIPAA Silver {HIPAA Silver} Exclude	HIPAA Gold {HIPAA Gold} Exclude
Authorize New Devices to be Added to Restricted Networks			
Restrict Access to Computers Containing ePHI to Authorized Users	✓	✓	✓
Detect Network Changes to Internal Networks			

To create and generate a Service Catalog:

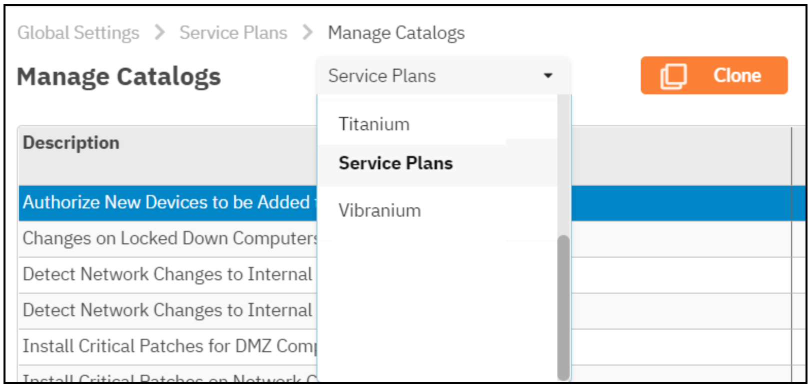
Important: Before you can create a catalog, be sure that you have already created each individual plan that you wish to include in the Catalog. See also "Create Global Service Plans for Cyber Hawk" on page 70.

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



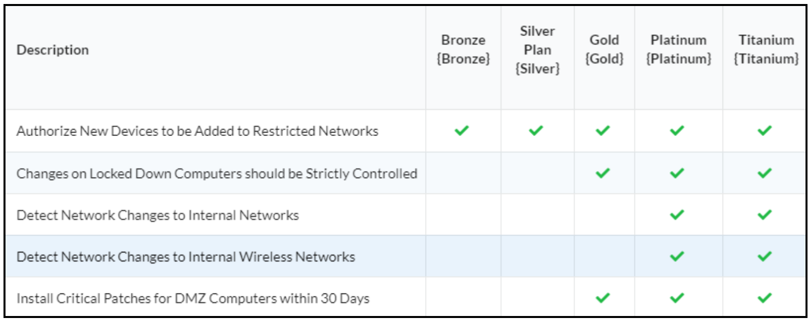
Description	Bronze Exclude	Platinum Exclude	Gold Exclude	Silver Plan Exclude	Bronze Exclude
Authorize New Devices to be Added to Restricted Networks		✓	✓	✓	
Changes on Locked Down Computers should be Strictly Controlled		✓	✓		
Detect Network Changes to Internal Networks		✓			
Detect Network Changes to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

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



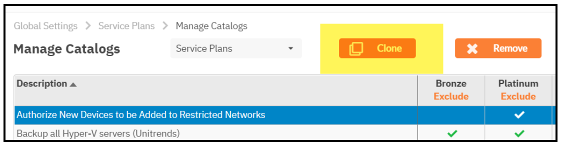
Description
Authorize New Devices to be Added t
Changes on Locked Down Computers
Detect Network Changes to Internal
Detect Network Changes to Internal
Install Critical Patches for DMZ Com
Install Critical Patches on Network C

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



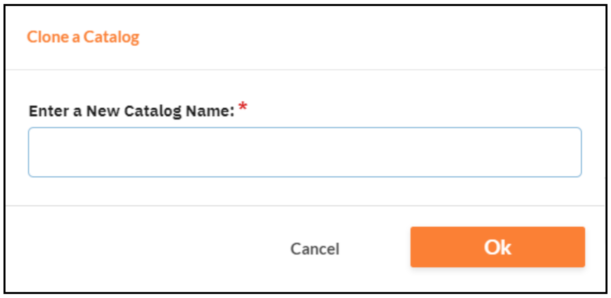
Description	Bronze {Bronze}	Silver Plan {Silver}	Gold {Gold}	Platinum {Platinum}	Titanium {Titanium}
Authorize New Devices to be Added to Restricted Networks	✓	✓	✓	✓	✓
Changes on Locked Down Computers should be Strictly Controlled			✓	✓	✓
Detect Network Changes to Internal Networks				✓	✓
Detect Network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

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

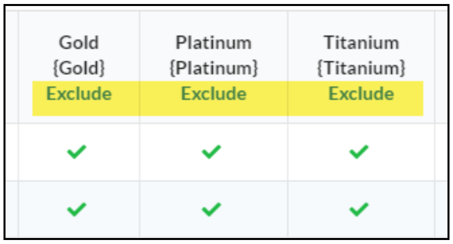


Description ▲	Bronze Exclude	Platinum Exclude
Authorize New Devices to be Added to Restricted Networks		✓
Backup all Hyper-V servers (Unitrends)	✓	✓

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

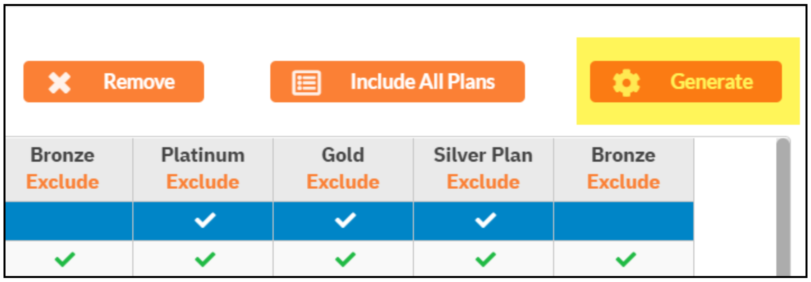


6. To create your custom catalog, click **Exclude** underneath each plan that you wish to REMOVE from the catalog. Continue removing plans until the catalog contains only the plans you want.



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

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



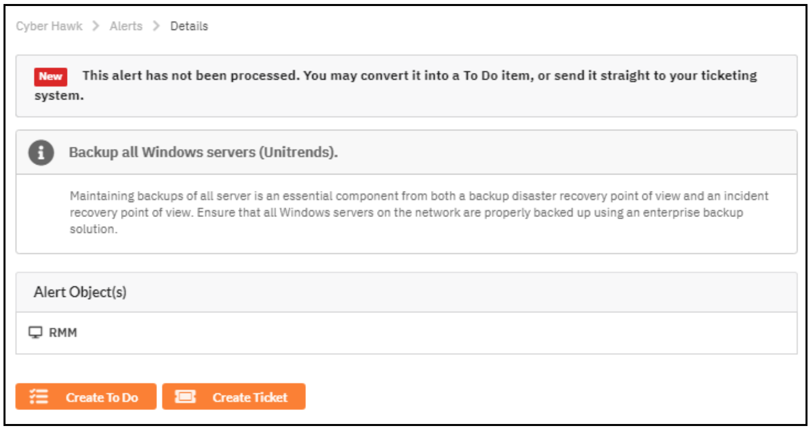
Bronze Exclude	Platinum Exclude	Gold Exclude	Silver Plan Exclude	Bronze Exclude
	✓	✓	✓	
✓	✓	✓	✓	✓

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

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.

Alert Object(s)

RMM

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:

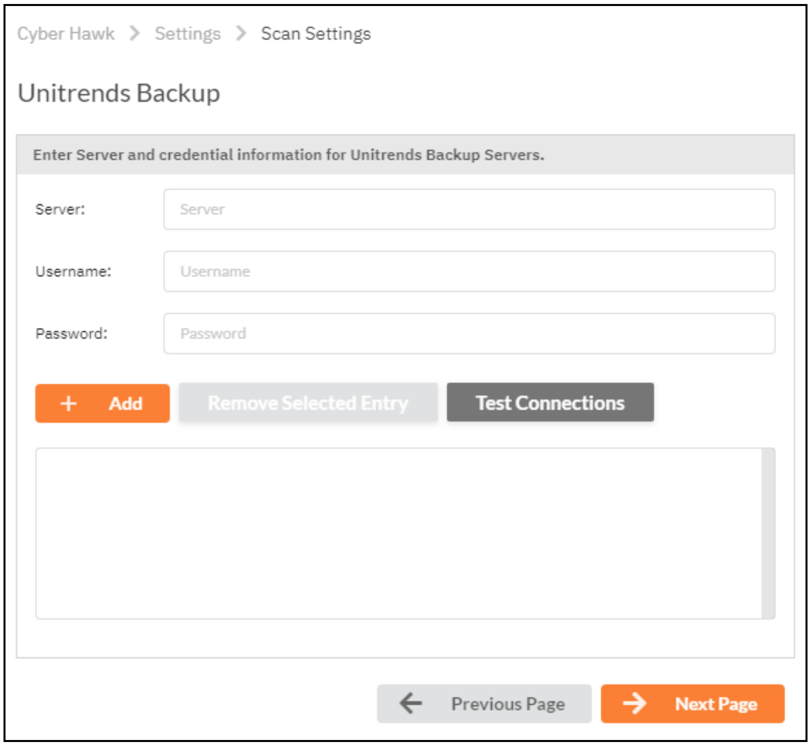
- Deploy and configure Unitrends Backup on the target network (see Unitrends Backup documentation)
    - You will need Unitrends Backup **login credentials** to set up Backup Alerts

- 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

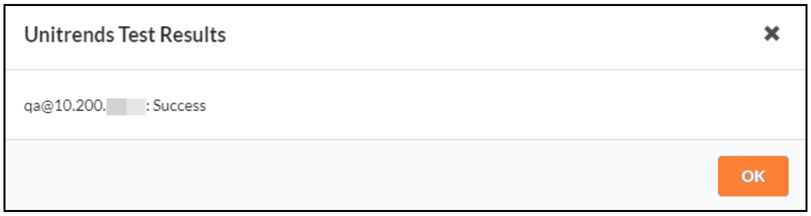
Enter Server and credential information for Unitrends Backup Servers.

Server: Server

Username: Username

Password: Password

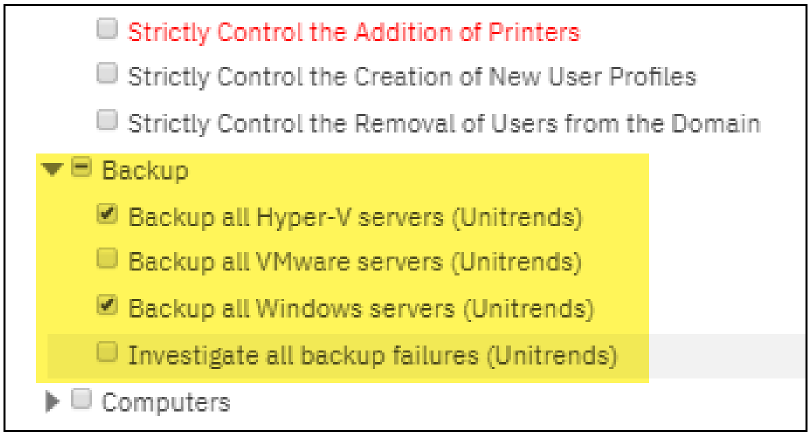
4. Enter the Unitrends Backup server name and login credentials. Click **Test Connection** to verify your configuration.



Unitrends Test Results

qa@10.200.[redacted]: Success

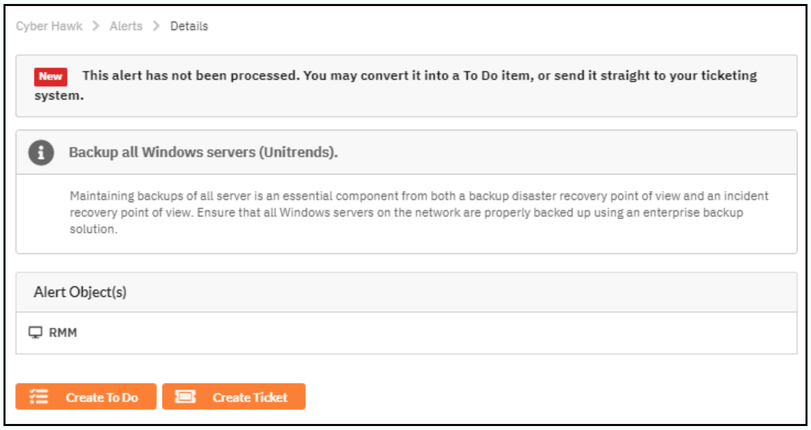
5. Save the Scan Settings.
6. Next, enable Unitrends Backup Alerts in the Cyber Hawk Policy Configuration.



- □ 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)
- ▶ □ Computers

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.



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).

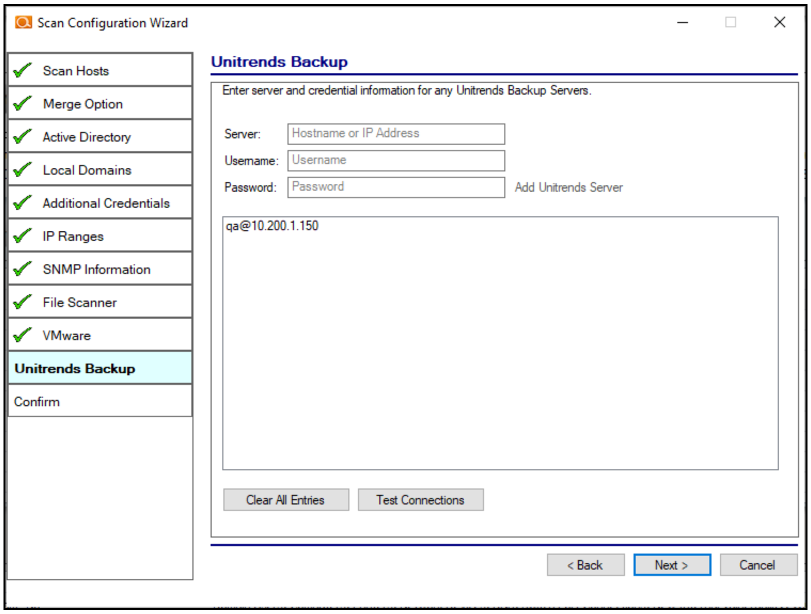
Maintaining backups of all server is an essential component from both a backup disaster recovery point of view and an incident recovery point of view. Ensure that all Windows servers on the network are properly backed up using an enterprise backup solution.

Alert Object(s)

RMM

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**.



Unitrends Backup

Enter server and credential information for any Unitrends Backup Servers.

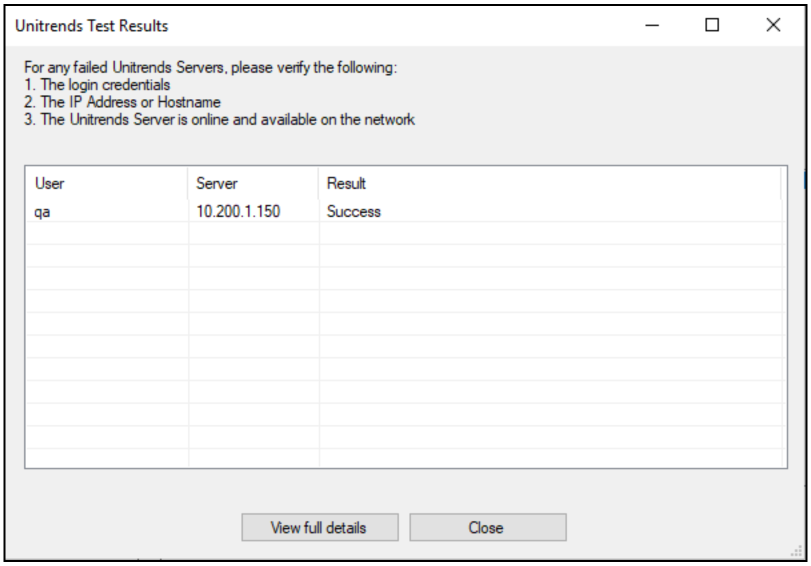
Server: Hostname or IP Address

Username: Username

Password: Password

qa@10.200.1.150

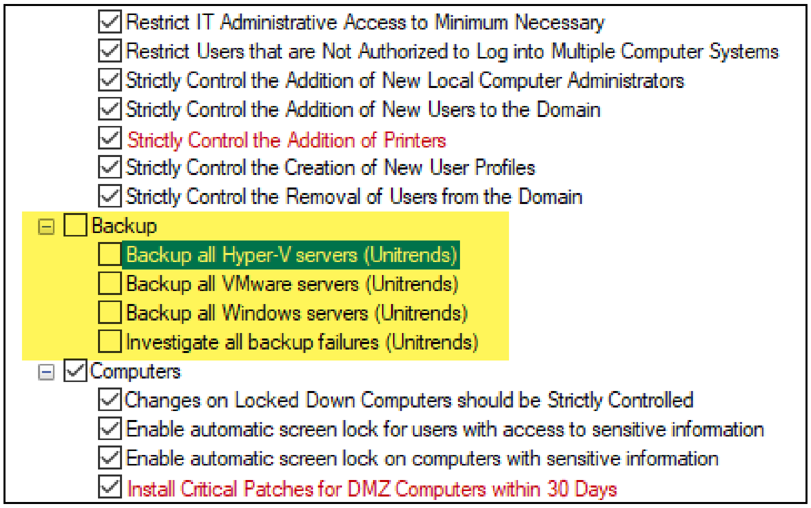
4. Enter the Unitrends Backup server name and login credentials. Click **Test Connection** to verify your configuration.



For any failed Unitrends Servers, please verify the following:
1. The login credentials
2. The IP Address or Hostname
3. The Unitrends Server is online and available on the network

User	Server	Result
qa	10.200.1.150	Success

5. Save the Scan Settings.
6. Next, enable Unitrends Backup Alerts in the Cyber Hawk Policy Configuration.



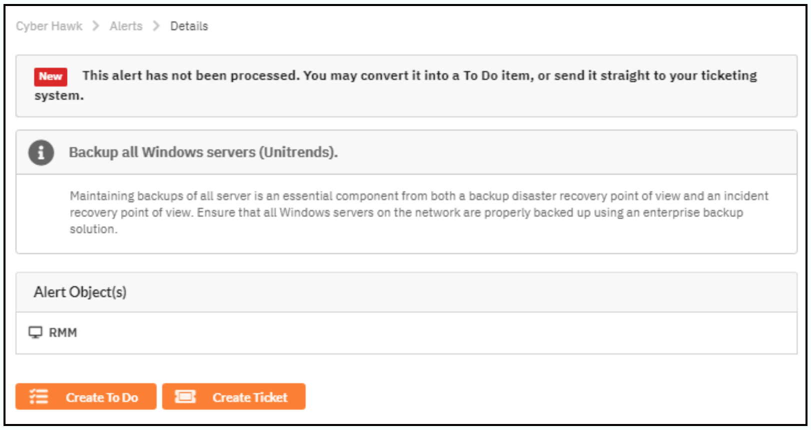
- ☑ Restrict IT Administrative Access to Minimum Necessary
- ☑ Restrict Users that are Not Authorized to Log into Multiple Computer Systems
- ☑ Strictly Control the Addition of New Local Computer Administrators
- ☑ Strictly Control the Addition of New Users to the Domain
- ☑ Strictly Control the Addition 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)

⊟ ☑ Computers
- ☑ 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.



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)

RMM

Security Policy Details

The table below documents each Security Policy, including the Smart Tags 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

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

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

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