



# CYBER HAWK<sup>®</sup>

by RapidFire Tools



## QUICK START GUIDE

3/7/2024 3:10 PM

Cyber Hawk (previously known as  
Detector)

Detecting and Responding to IT Security Policy Violations



+1-678-323-1300



[rapidfiretools.com](https://www.rapidfiretools.com)



[support@rapidfiretools.com](mailto:support@rapidfiretools.com)

# Contents

---

- [Cyber Hawk Overview](#) ..... 4
- Setting Up Cyber Hawk** ..... **5**
- [Initial Cyber Hawk Set Up](#) ..... 5
- Step 1 — Provision Cyber Hawk Appliance ID in Network Detective ..... 5
- Step 2 — Install Cyber Hawk and Create a New Site ..... 6
- Step 3 — Associate Cyber Hawk with a Site and Access Cyber Hawk Settings ..... 7
- [Configure Cyber Hawk Using the Setup Wizard \(Virtual Appliance\)](#) ..... 10
- Step 1 — Configure Scan Settings ..... 11
- Step 2 — Schedule Scans and Alert Notifications ..... 21
- Tips for Scheduling the Level 2 Scan ..... 22
- Step 3 — Configure Tech Email Groups ..... 23
- Step 4 — Configure End User Email Groups ..... 26
- Step 5 — Perform Pre-Scan Analysis ..... 27
- Step 6 — Perform Initial Cyber Hawk Scan ..... 30
- Step 7 — Configure Policies ..... 30
- Step 8 — Configure Notifications ..... 33
- Step 9 — Configure Smart Tags ..... 34
- Step 10 — Set Up RapidFire Tools Portal ..... 36
- RapidFire Tools Portal Set Up** ..... **37**
- [Set Up Portal Branding](#) ..... 37
- Set Custom Portal Theme ..... 38
- Set Custom Portal Subdomain ..... 39
- Set Custom Company Name ..... 40
- Set Custom Company Logo ..... 41
- [Set Up a Custom Subdomain to Access the RapidFire Tools Portal](#) ..... 42
- [Set Up Custom SMTP Server Support](#) ..... 45
- [Set Up and Assign a Ticketing/PSA System Integration to a Site Using Cyber Hawk](#) ..... 48
- Step 1 — Gather Credentials and Set Up your PSA System ..... 48

Step 2 — Set Up a Connection to your Ticketing System/PSA .....49

Step 3 — Map your Cyber Hawk’s Site to a Ticketing System/PSA Connection .....55

**Pre-Scan Network Configuration Checklist .....58**

Checklist for Domain Environments .....58

Checklist for Workgroup Environments ..... 60

## Cyber Hawk Overview

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

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

In the RapidFire Tools Portal you can:

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

```
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.
```

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

Setting up Cyber Hawk consists of two parts:

1. Install Cyber Hawk on the target network and bind it to a Site in the Network Detective Application: ["Initial Cyber Hawk Set Up" below](#)
2. Configure Cyber Hawk scans and how it will enforce security policies on the target network: ["Configure Cyber Hawk Using the Setup Wizard \(Virtual Appliance\)" on page 10](#)

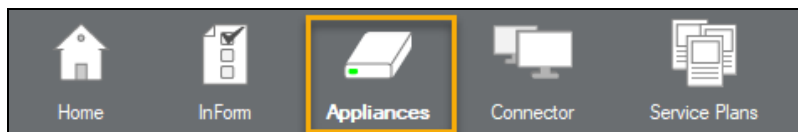
## Initial Cyber Hawk Set Up

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

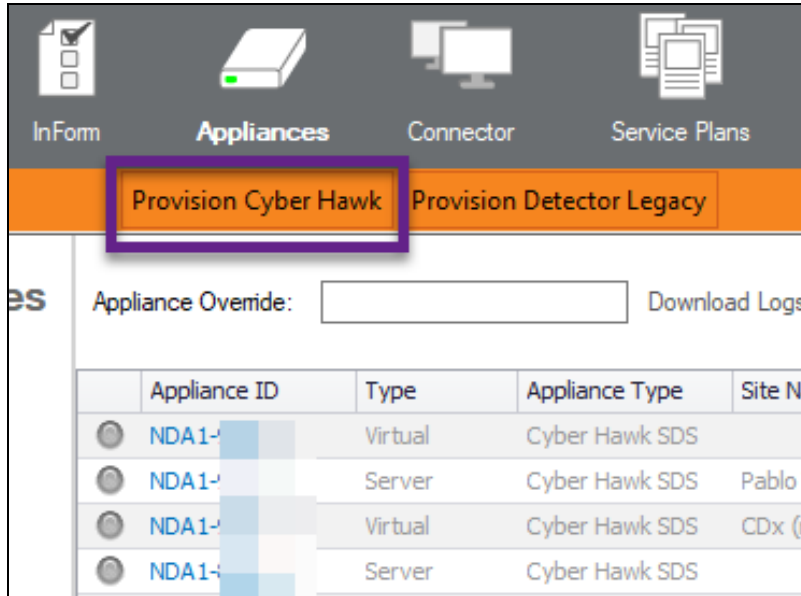
### Step 1 — Provision Cyber Hawk Appliance ID in Network Detective

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

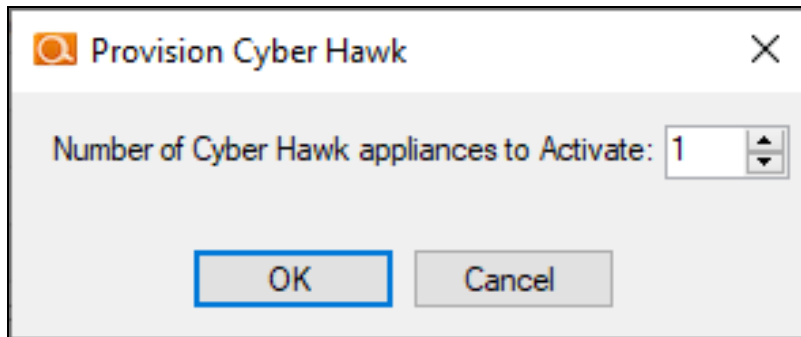
1. Visit <https://www.rapidfiretools.com/nd> to download and install the latest version of the **Network Detective Application**.
2. **Run Network Detective** and **log in** with your credentials.
3. Click **Appliances**.



4. Click **Provision Cyber Hawk**.



5. Select the number of appliances to activate.



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

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

Appliance ID	Type	Appliance Type	Site	Activated	
NDA1-87	Virtual	Cyber Hawk SDS	Site	Activated	-
NDA1-73	Virtual	Cyber Hawk SDS		Not activated	-

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

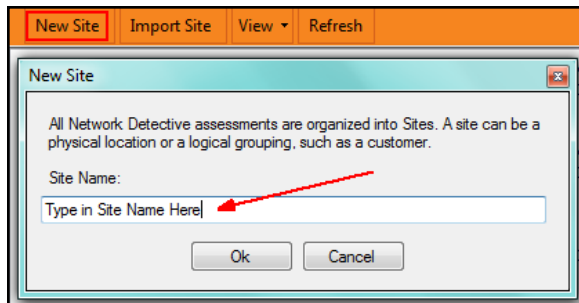
## Step 2 — Install Cyber Hawk and Create a New Site

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

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

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

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



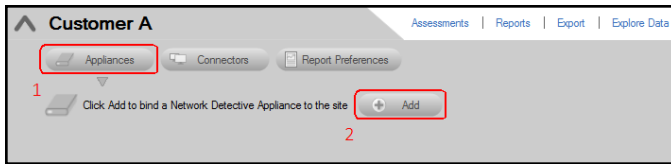
4. Enter the **Site Name** and click **OK**.

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

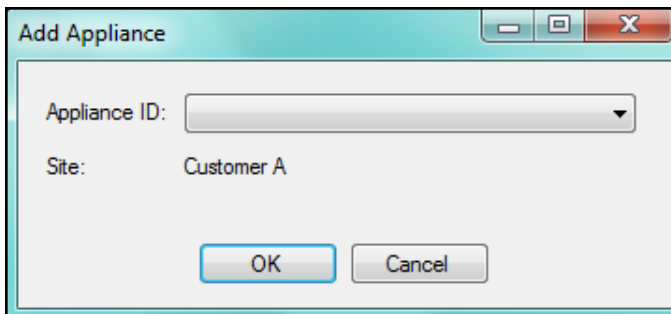
1. From within the Site Window, select the  selector symbol to expand the Site's Preferences in order to Add an Appliance.



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



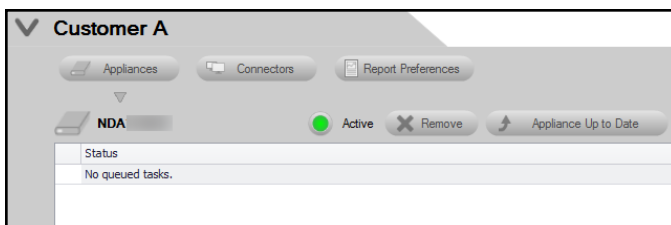
- Select the **Appliance ID** of the **Cyber Hawk** Appliance from the drop down menu.



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

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

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



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



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

The screenshot shows the Cyber Hawk management interface. On the left is a sidebar with a 'SITE' header and several report categories: Active Project, Archived Projects, Generated Reports, and Downloaded Reports. At the bottom of the sidebar is the 'Cyber Hawk' icon, which is highlighted in yellow and has a red arrow pointing to it. The main content area is titled 'Customer' and includes an 'Edit Site' link and 'Configure' and 'Smart Tags' buttons. Below this, there's a status bar for 'NDA1' with 'Host Type: Virtual' and a green 'Active' indicator. The 'Settings' section is expanded, showing 'Policy Configuration' (7 Active Policies), 'Scan Configuration' (Local Scan Merge: Primary Domain, Domains: All Domains, IP Range(s): 10.200.1.0-10.200.1.255), and 'Schedules' (Time Zone: (UTC-05:00), Level 1 Scan (Daily): 1:00 AM, Level 2 Scan (Weekly): 1:00 AM). Below the settings is the 'Notification Rules' section, which includes a table with columns for Policy Name, Action, and Group Name. The table lists several rules under the 'Access Control' group, such as 'Authorize New Devices to be Added to Restricted Networks' and 'Restrict Access to Accounting Owner Computers to Authorized Users', each with a specific action and group name.

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

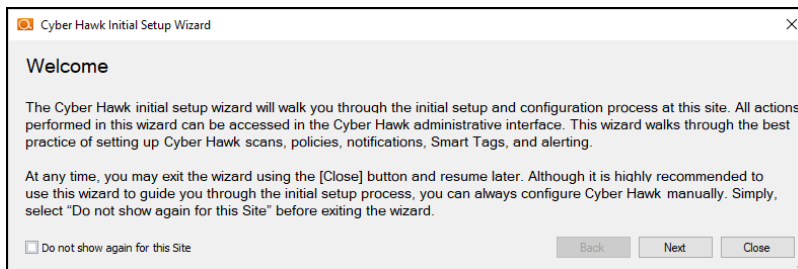
Continue to the next step in setting up Cyber Hawk: ["Configure Cyber Hawk Using the Setup Wizard \(Virtual Appliance\)" on the next page.](#)

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

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



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



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

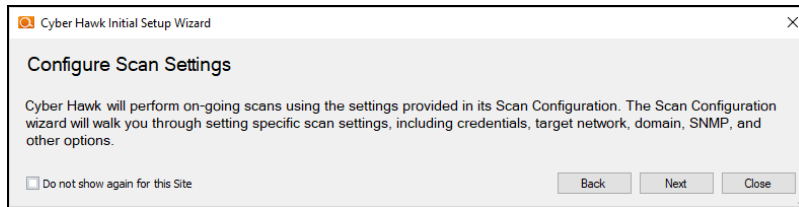
**Note:** This section of the guide walks you through the Initial Setup Wizard. This guide also contains separate topics on configuring Cyber Hawk settings. Refer to these topics if you need to change Cyber Hawk after you have completed the initial set up process using the Wizard.

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

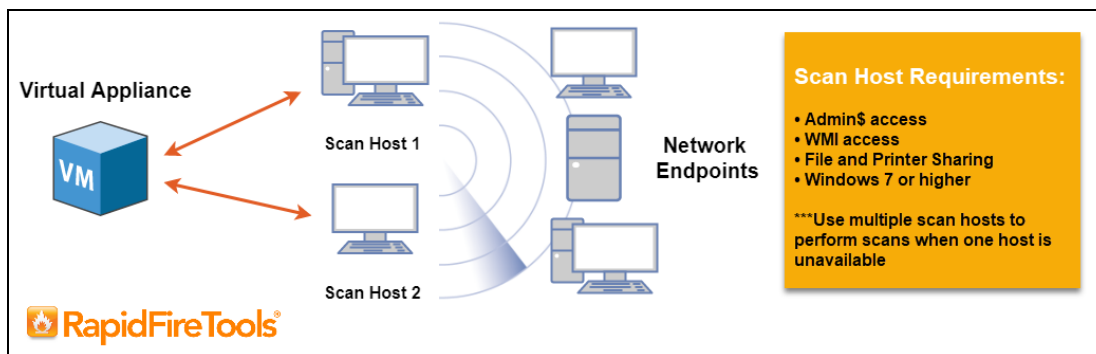
**Important:** For best results, the target network must be configured to allow for successful scans on all network endpoints. See ["Pre-Scan Network Configuration Checklist" on page 58](#) for configuration guidance for both Windows Active Directory and Workgroup environments.

## Step 1 — Configure Scan Settings

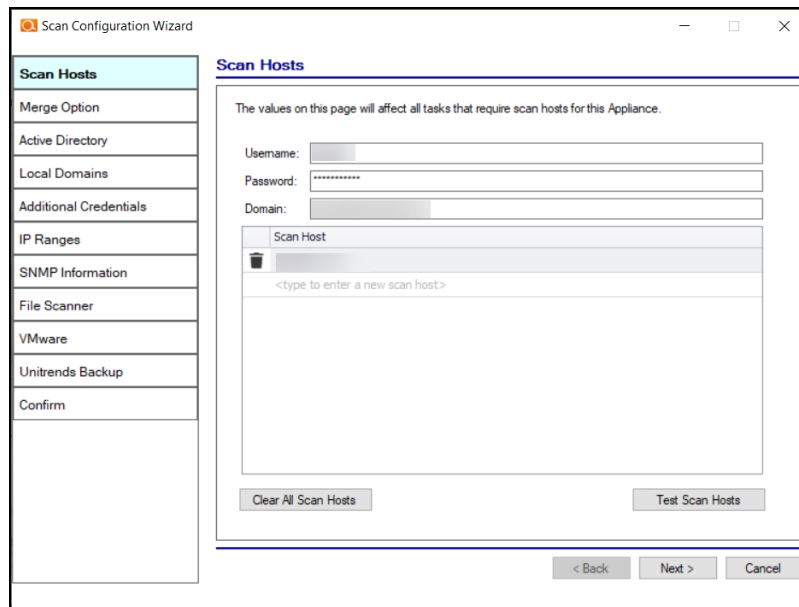
In this step you will configure the Scan Settings for the Cyber Hawk. Click **Next**.



The Cyber Hawk Appliance requires access to at least one separate, additional PC on the client's network. This computer is called the “**Scan Host**.” The Scan Host is used to initiate scans.



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

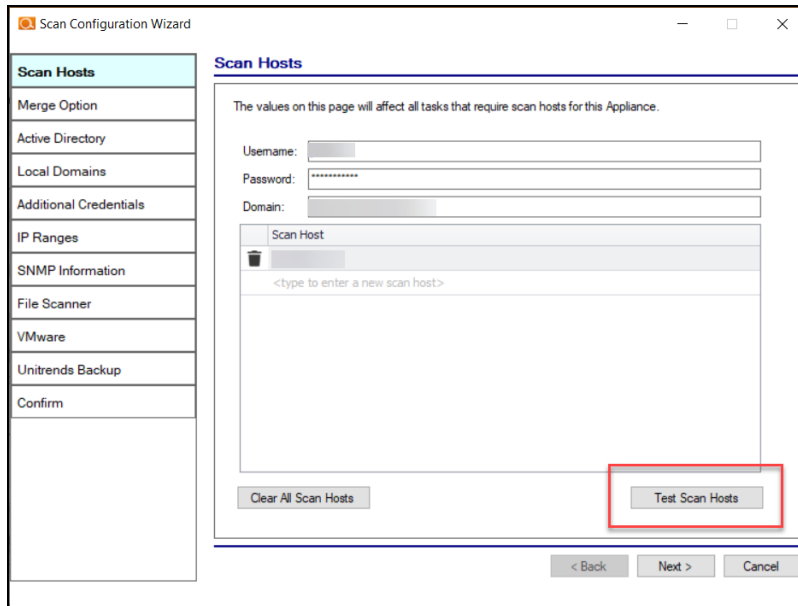
c. **Domain name (NOT the name of the domain controller)**

The screenshot shows the 'Scan Configuration Wizard' window, specifically the 'Scan Hosts' step. On the left is a navigation pane with the following items: Scan Hosts (highlighted), Merge Option, Active Directory, Local Domains, Additional Credentials, IP Ranges, SNMP Information, File Scanner, VMware, Unitrends Backup, and Confirm. The main area is titled 'Scan Hosts' and contains the following elements:

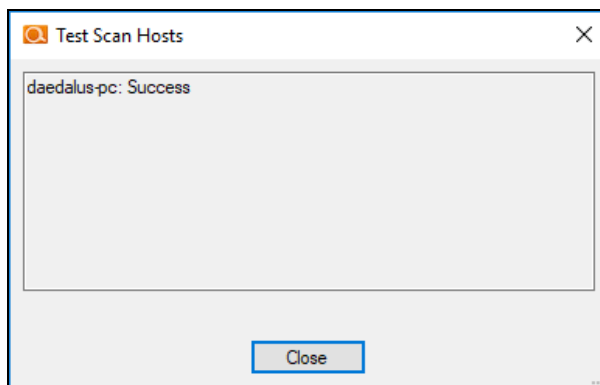
- A note: 'The values on this page will affect all tasks that require scan hosts for this Appliance.'
- Fields for 'Username:', 'Password:', and 'Domain:'.
- A 'Scan Host' table with a trash icon and a placeholder text '<type to enter a new scan host>'. The table is currently empty.
- Buttons for 'Clear All Scan Hosts' and 'Test Scan Hosts'.
- Navigation buttons at the bottom: '< Back', 'Next >', and 'Cancel'.

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

2. Click **Test Scan Hosts**.



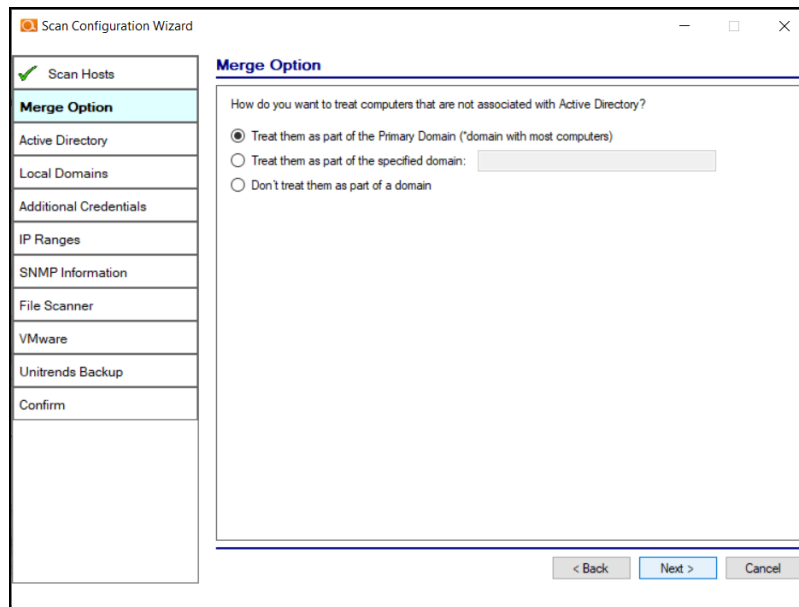
A message will appear indicating whether a connection can be established to each scan host. If the connection cannot be established, be sure the scan host meets the requirements – and that you have entered the correct credentials.



Click **Next**.

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

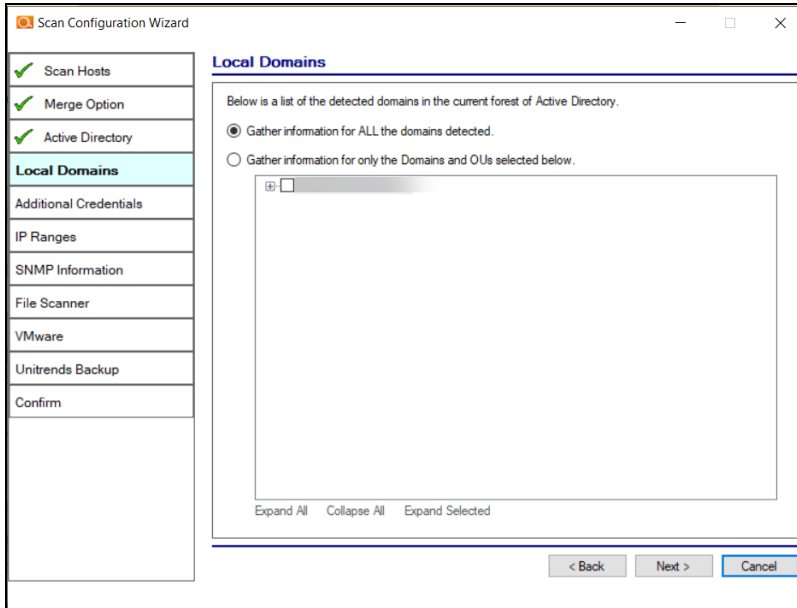
- or choose not to treat them as part of a domain



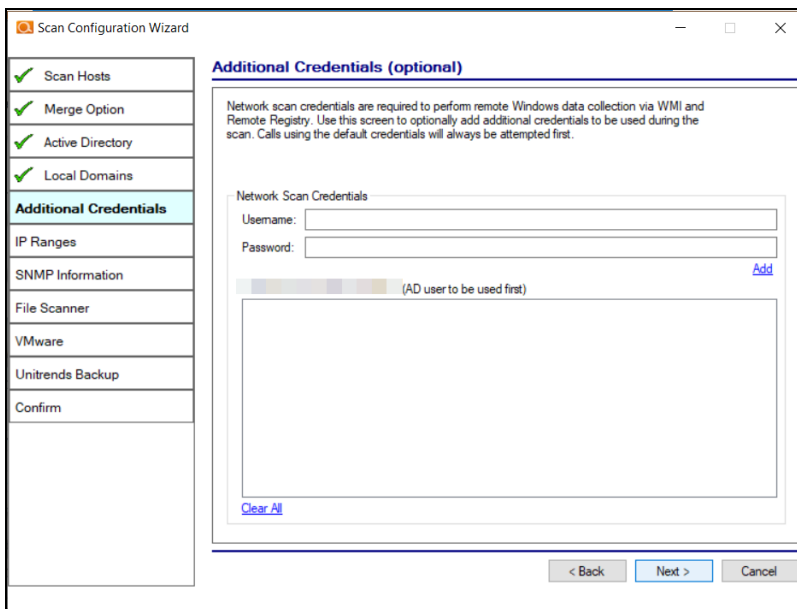
4. Enter credentials *with administrative rights* to connect to a Domain Controller with Active Directory. Click **Next** to test a connection with the Domain Controller and verify your credentials.

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

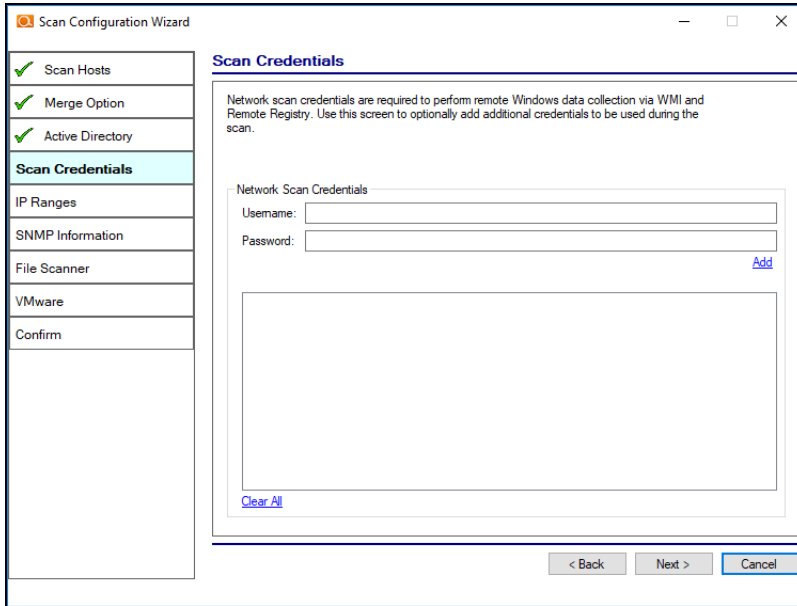
5. If you are scanning a domain, choose whether to scan the entire domain or specific Organizational Units (OUs). Then click **Next**.



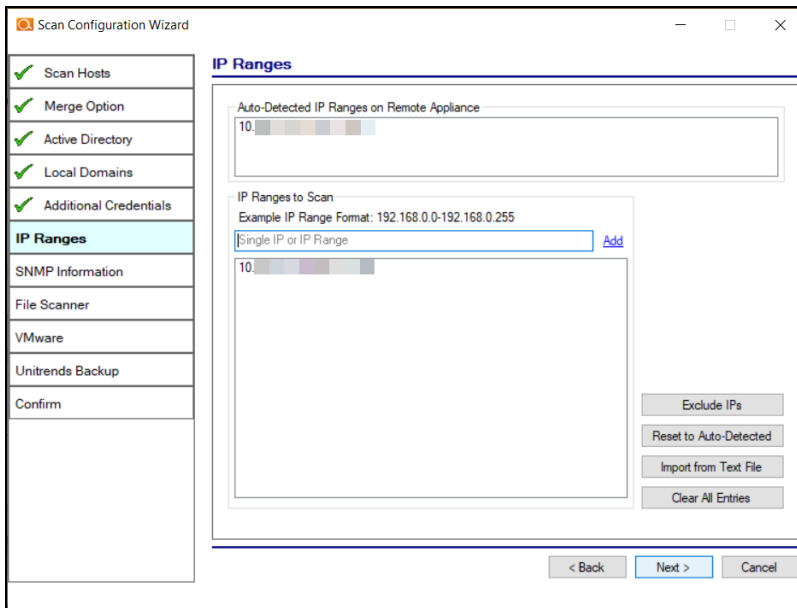
6. If you are scanning a Domain, enter any additional network scan credentials to connect to remote workstations. Then click **Next**.



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



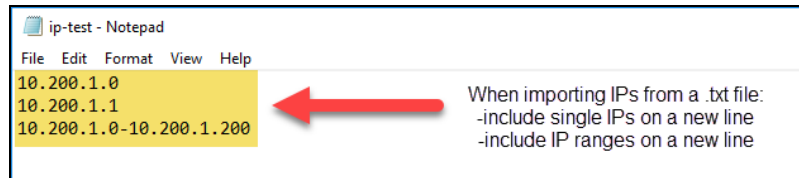
- The Cyber Hawk appliance will automatically suggest an IP range for the scan. If you do not wish to scan the default IP Range, select it and click **Clear All Entries**. Use this screen to enter additional IP Addresses or IP Ranges and click **Add**. Then click **Next**.



From this screen you can also:

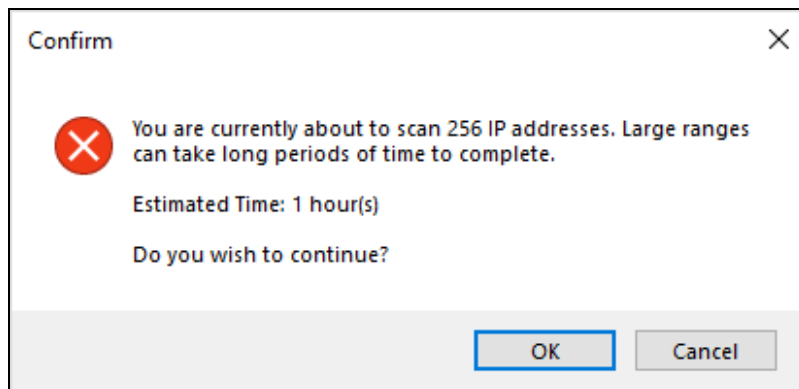


- Click **Exclude IPs** to remove certain IP ranges from the scan.
- Click **Reset to Auto-Detected** to reset the automatically suggested IP Range.
- Click **Import from Text File** to import a predefined list or range of IP addresses.



**Important:** Scans may affect network performance.

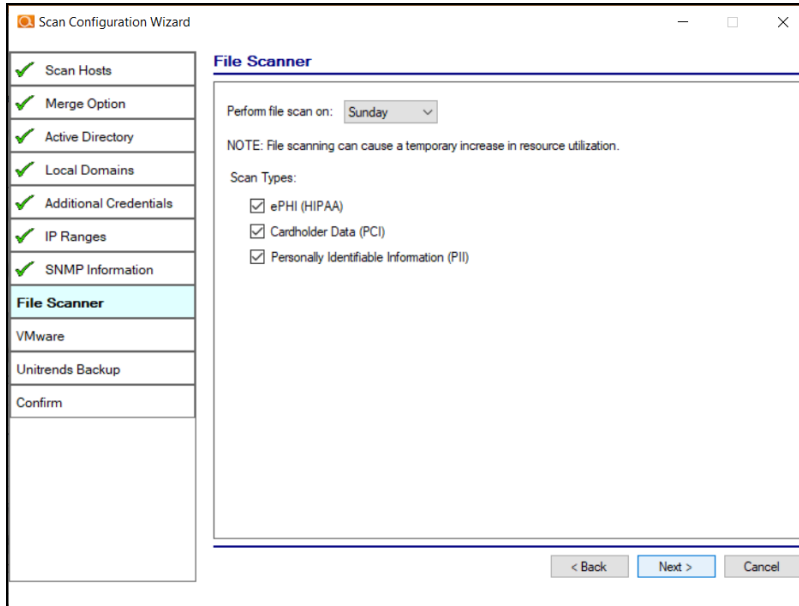
9. A confirmation window will appear estimating the amount of time the scan will take for the designated IP Range. If the scan will take too much time, reduce the size of the IP range. Click **OK**.



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

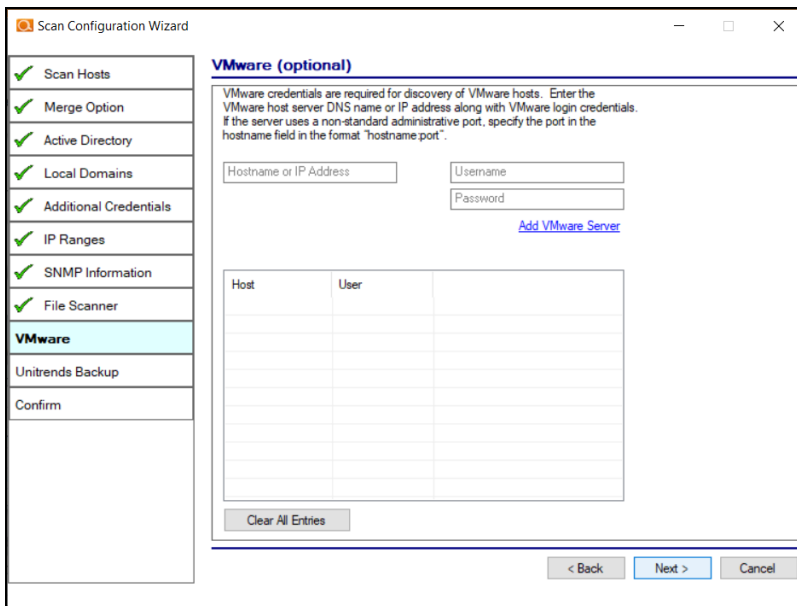
The screenshot shows the 'Scan Configuration Wizard' window. On the left is a sidebar with a list of configuration steps: 'Scan Hosts', 'Merge Option', 'Active Directory', 'Local Domains', 'Additional Credentials', 'IP Ranges', 'SNMP Information' (highlighted in blue), 'File Scanner', 'VMware', 'Unitrends Backup', and 'Confirm'. The main area is titled 'SNMP Information' and contains the following text: '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.' Below this is a text input field with 'public' entered and an 'Add' button. There are three buttons: 'Reset to Default', 'Import from Text File', and 'Clear All Entries'. Underneath is a section for 'Advanced SNMP Options' with a text input for 'SNMP Timeout (seconds):' set to '10' and a 'Use Default' link. A checkbox is checked with the label 'Attempt SNMP against non-pingable devices (slower but more accurate)'. At the bottom right are three buttons: '< Back', 'Next >', and 'Cancel'.

11. Choose what day of the week to perform the file scan. Select a day of the week from the drop-down menu. Next, select the Scan Types that will be performed:
  - **ePHI** (HIPPA) will scan for Electronic Protected Health Information
  - **Cardholder Data** (PCI) will scan for payment card numbers and other related information
  - **Personally Identifiable Information** (PII) will scan for information such as a person's name or social security number



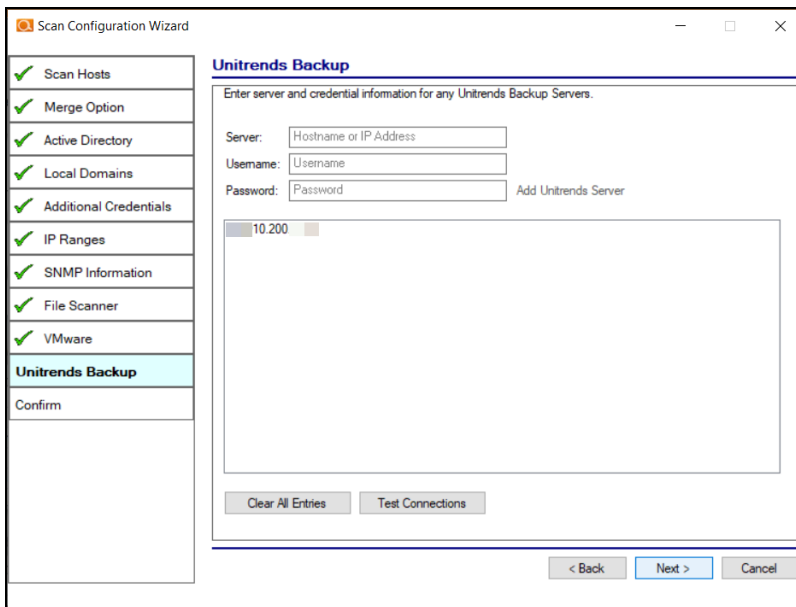
Then click **Next**.

- 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**.



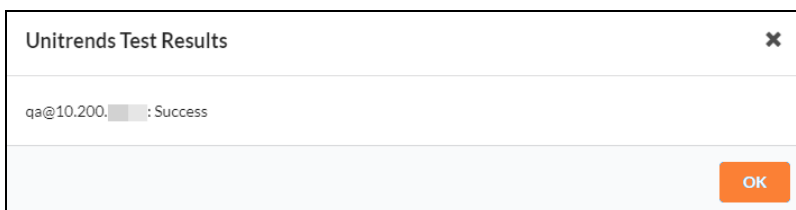
- The **Unitrends Backup** screen will appear. Enter the Unitrends Backup server name and login credentials.

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



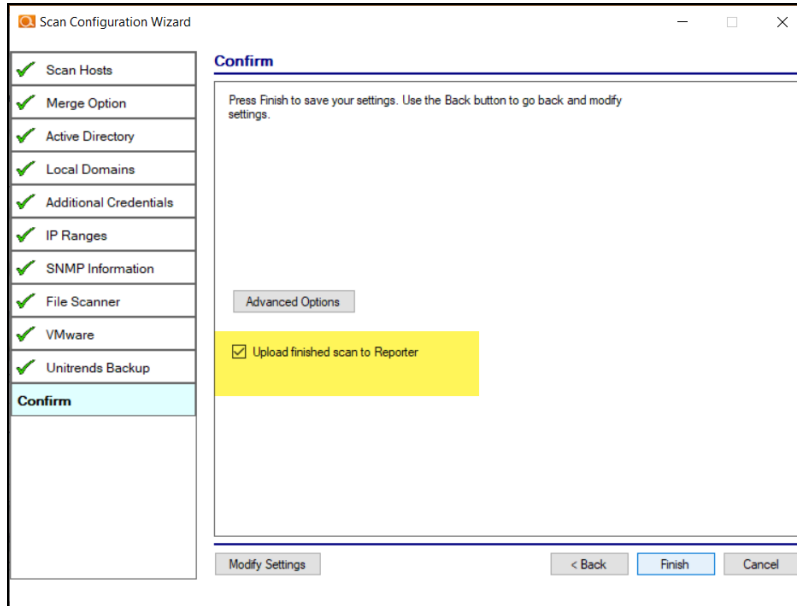
The screenshot shows the 'Scan Configuration Wizard' window. On the left is a sidebar with a list of configuration options, each with a green checkmark: Scan Hosts, Merge Option, Active Directory, Local Domains, Additional Credentials, IP Ranges, SNMP Information, File Scanner, VMware, Unitrends Backup (highlighted in blue), and Confirm. The main area is titled 'Unitrends Backup' and contains the instruction 'Enter server and credential information for any Unitrends Backup Servers.' Below this are three input fields: 'Server:' (with placeholder 'Hostname or IP Address'), 'Username:' (with placeholder 'Username'), and 'Password:' (with placeholder 'Password'). To the right of the Password field is a link that says 'Add Unitrends Server'. Below the input fields is a large text area containing the IP address '10.200'. At the bottom of the main area are two buttons: 'Clear All Entries' and 'Test Connections'. At the very bottom of the window are three navigation buttons: '< Back', 'Next >', and 'Cancel'.

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



The screenshot shows a dialog box titled 'Unitrends Test Results' with a close button (X) in the top right corner. The main area of the dialog contains the text 'qa@10.200. : Success'. At the bottom right of the dialog is an orange button labeled 'OK'.

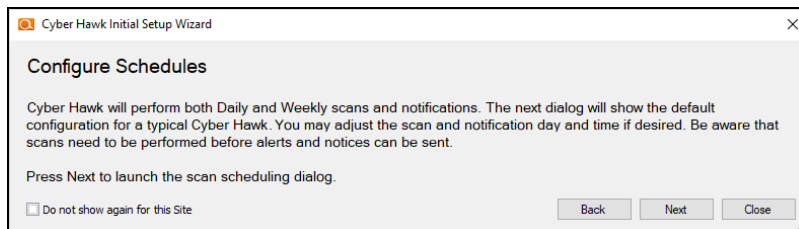
- Click **Finish** to save your scan settings.
  - If you are using a **Reporter** appliance, you can also choose whether to upload the finished scans to the Reporter.
  - You can also select **Skip devices with all ports filtered**. Some devices use IPS (Intrusion Prevention Systems) that may prevent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



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

## Step 2 — Schedule Scans and Alert Notifications

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



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

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

**Important:** See ["Tips for Scheduling the Level 2 Scan"](#) below for tips on scheduling the scan at the best time to avoid affecting network performance.

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

The screenshot shows a 'Schedule' dialog box with the following configuration:

- Time Zone:** (UTC-05:00) Eastern Time (US & Canada)
- Level 1 Scan (Daily):** 01:00 AM,  Enabled
- Level 2 Scan (Weekly):** 01:00 AM, Saturday,  Enabled
- Daily Alert:** 08:00 AM,  Mon,  Tue,  Wed,  Thu,  Fri,  Sat,  Sun
- Weekly Notice:** 08:00 AM, Monday

Buttons: Save, Discard

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

### Tips for Scheduling the Level 2 Scan

Cyber Hawk's Level 2 Scan (Weekly) functionality relies on the use of an Internal Network Vulnerability scanner process to perform this scan. Internal Network Vulnerability scans are intentionally designed to be aggressive and comprehensive in nature. At Internal Network Vulnerability scan run time, there are instances where these scans can impact network performance and access to computer endpoints by network users during the time a scheduled Internal Network Vulnerability scan is being performed.

It is recommended that:

- Level 2 scans are scheduled and performed at times when the network is not in use by network users, back-up processes, or any other system or process that requirements unimpeded network access.
- any routers, switches, computers, industrial devices connected to the network, security devices, and other network devices that should not be interfered with in any way during day to day network operation or must be operational and accessible to network systems and users on a 24x7x365 basis, that these IP addresses of the aforementioned devices should be excluded from the Cyber Hawk's IP Range settings contained within the Cyber Hawk's Scan Settings.

### Step 3 — Configure Tech Email Groups

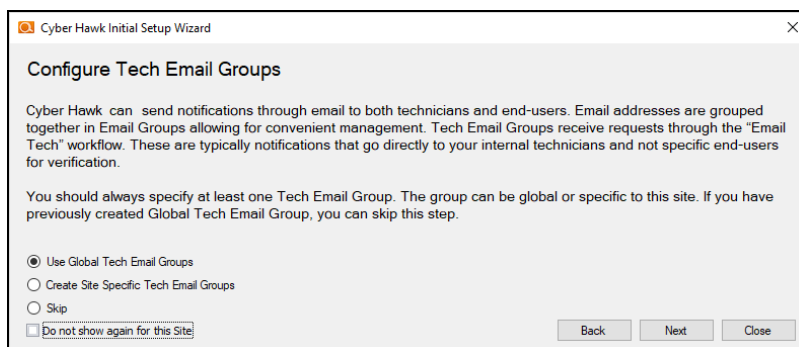
In this step you will configure the email addresses and groups of users for your Technician Group. This is the group that will respond to security alerts sent by Cyber Hawk.

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

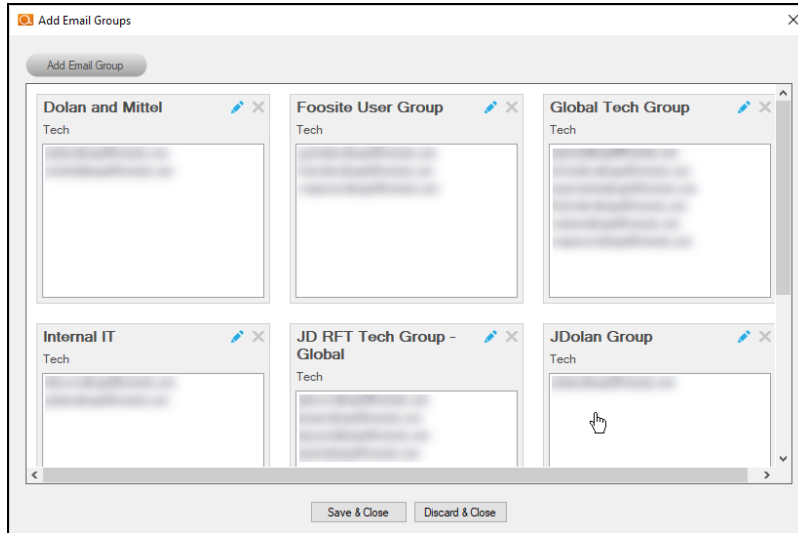
**Note:** If you choose to use a Global Email Group, you can select from among your pre-existing Global Email Groups or create a new one.

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

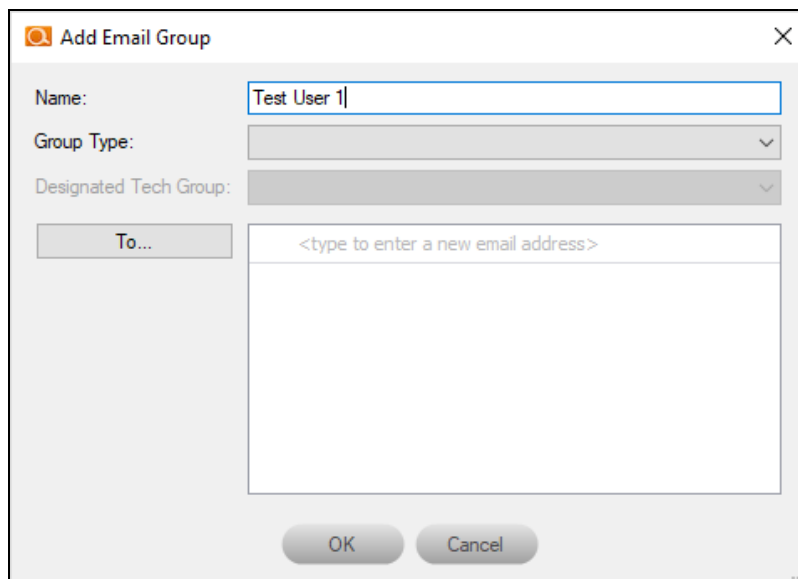
Later, you can continue to create and edit Global Email Groups from **Preferences > Email Groups** at any time. You can also later create and edit site-specific email groups from the Cyber Hawk **Email Configuration** button at your specific Site.



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



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



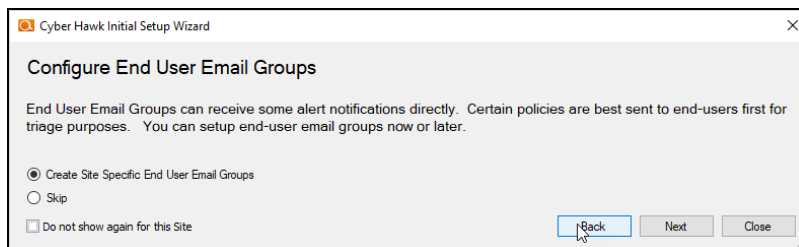


5. When you are finished, click **OK**.

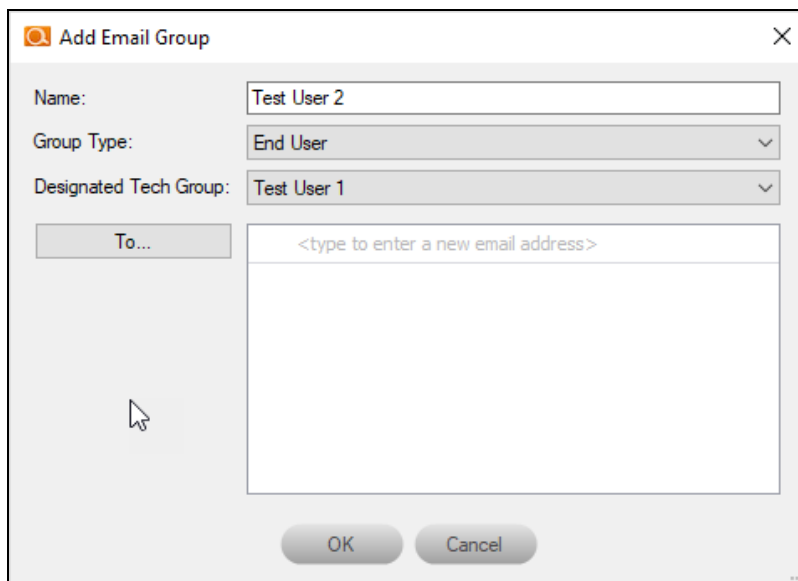
## Step 4 — Configure End User Email Groups

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

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



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



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

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

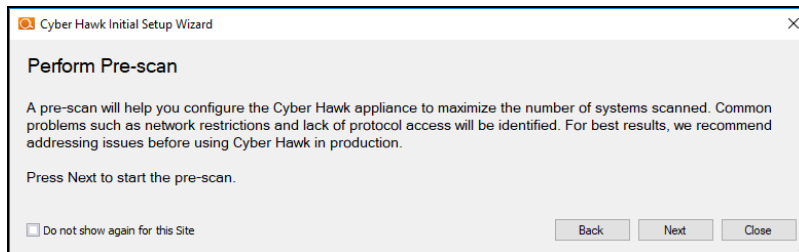
The screenshot shows the 'Administrative Emails' configuration window. It includes a 'To...' field with a red 'X' icon and a placeholder '@rapidfiretools.com'. Below this is a large text area for entering email addresses. There is a 'Subject Prefix' field with the value '%SITE%'. Three checkboxes are checked: 'Scan Failed (subject: <prefix> - Scan Failed)', 'Notification Error (subject: <prefix> - Notification Error)', and 'Scan Complete (subject: <prefix> - Scan Complete)'. At the bottom, there is a checkbox for 'Do not show again for this Site' and 'Back', 'Next', and 'Close' buttons.

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

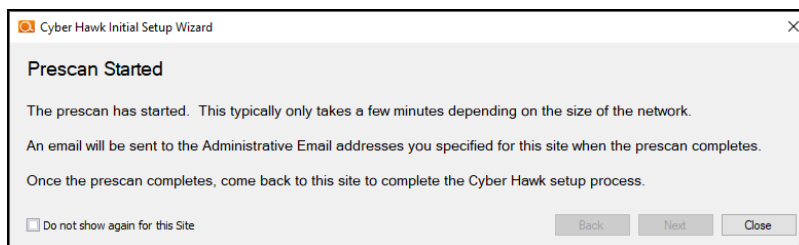
The screenshot shows the 'Email Server' configuration window. It has two radio buttons: 'Use Default SMTP Server' (selected) and 'Use Custom SMTP Server'. Below are three rows of fields for 'Alert From', 'Report From', and 'Admin Notice From', each with a 'Display Name' field. A yellow note states: 'Note: SMTP Server must support TLS 1.2 or above.' Under 'Custom SMTP Settings', there are fields for 'SMTP Server Address', 'Port' (set to 465), 'Security' (set to None), 'Username', and 'Password'. A 'Send Test Emails' button is located at the bottom right. At the bottom left, there is a checkbox for 'Do not show again for this Site' and 'Back', 'Next', and 'Close' buttons.

## Step 5 — Perform Pre-Scan Analysis

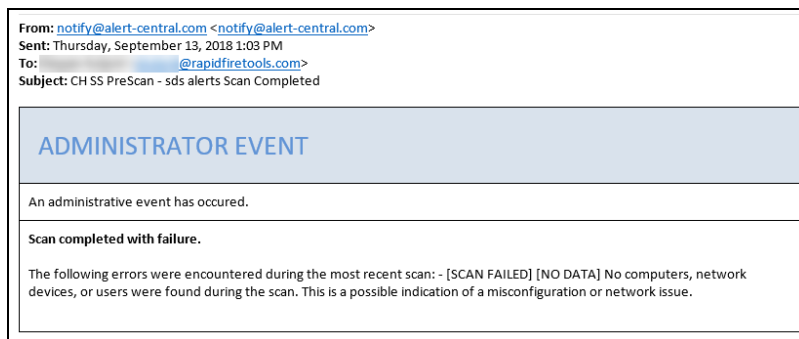
Next you will **Perform a Pre-Scan Analysis** on the target network. This will show you any issues with your scan configuration. Click **Next**.

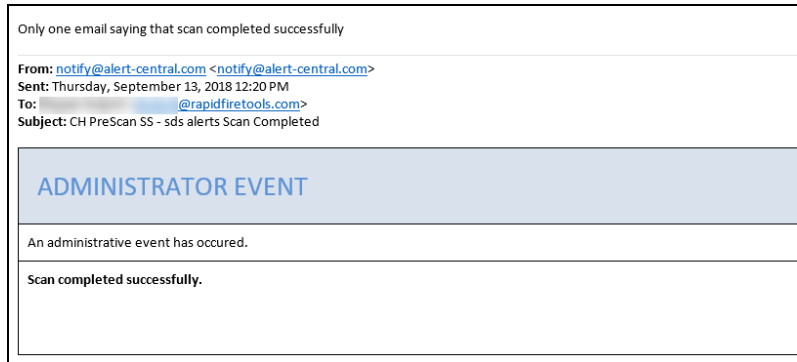


The Pre-Scan Analysis will begin.



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



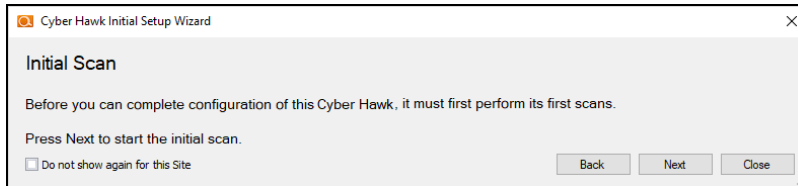


If the Pre-Scan Analysis identifies issues with your Cyber Hawk scan configuration, click Modify next to Scan Configuration and make the recommended changes.

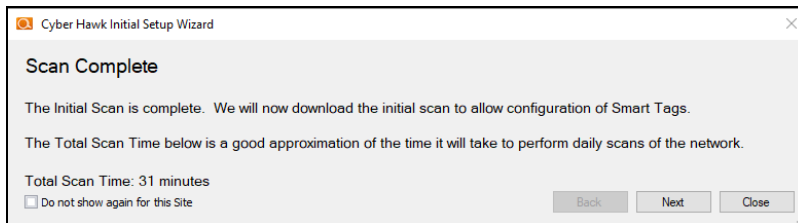
**Important:** For best results, the target network must be configured to allow for successful scans on all network endpoints. See "[Pre-Scan Network Configuration Checklist](#)" on page 58 for configuration guidance for both Windows Active Directory and Workgroup environments.

## Step 6 — Perform Initial Cyber Hawk Scan

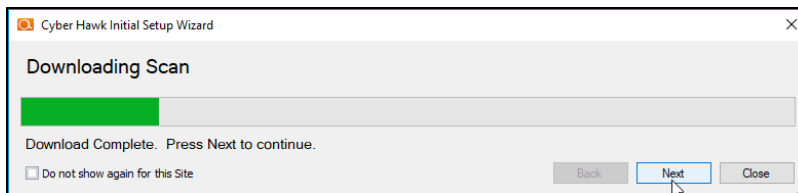
Before you can continue setting up Cyber Hawk, you need to perform an initial scan in order to gather more information about the target network. To initiate the first scan, click **Next**.



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



The scan will be downloaded automatically.



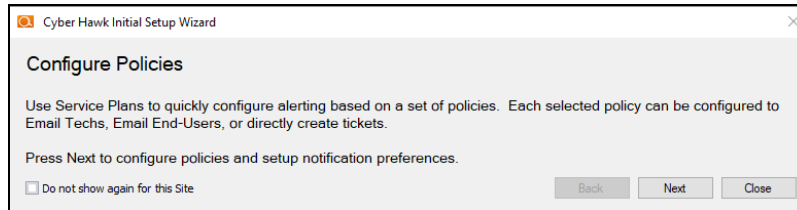
Click **Next** when the download is complete.

## Step 7 — Configure Policies

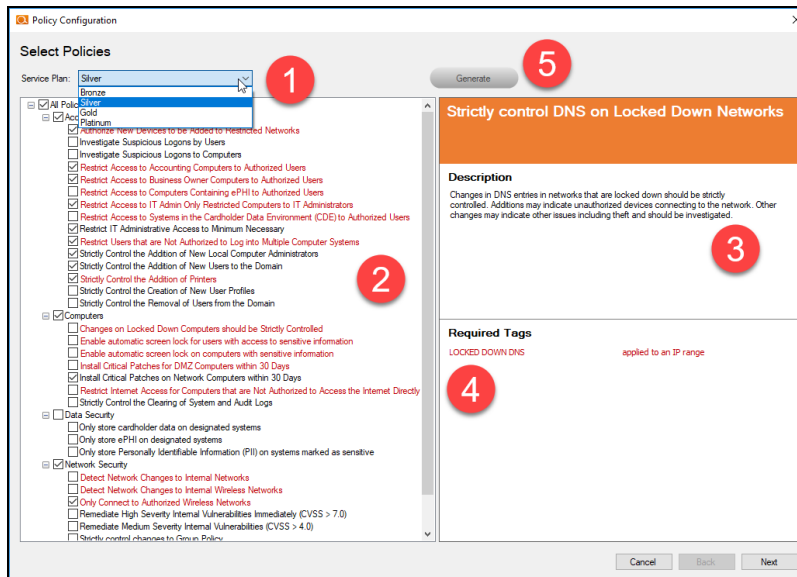
You will then Configure Policies. In short, this is where you create the "Service Plan" that your MSP will offer to the client.

**Tip:** In the Wizard, you will select from one of several pre-defined service plans. However, you can modify or create your own custom service plan at any time.

When you are ready to configure policies, click **Next**.



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

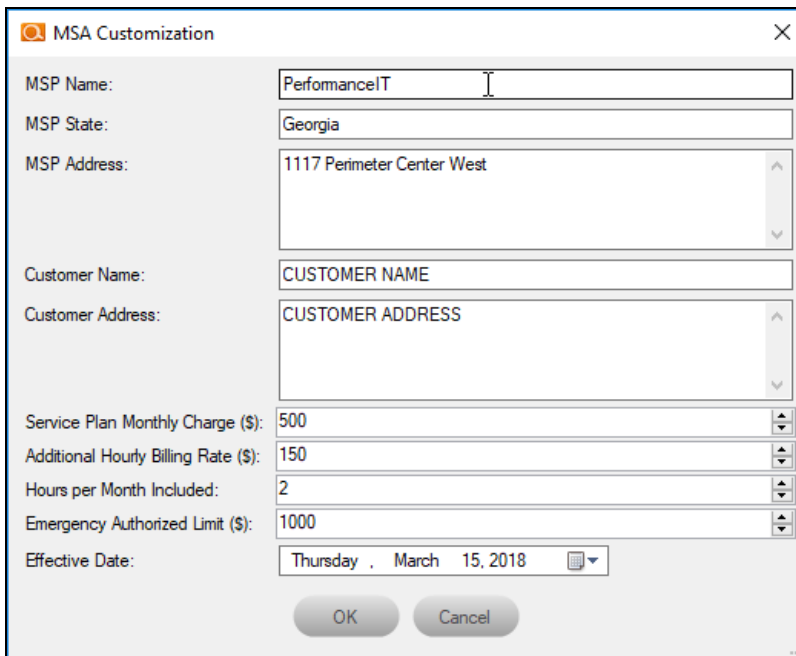


1. **Select from a range of pre-defined service plans: *Bronze, Silver, Gold, or Platinum*.** The higher the service level, the more Security Policies will be enforced.
2. **Review and select individual security policies from the list of available policies.** Use the check box to select or deselect a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

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



- Enter your custom information for the MSSA.

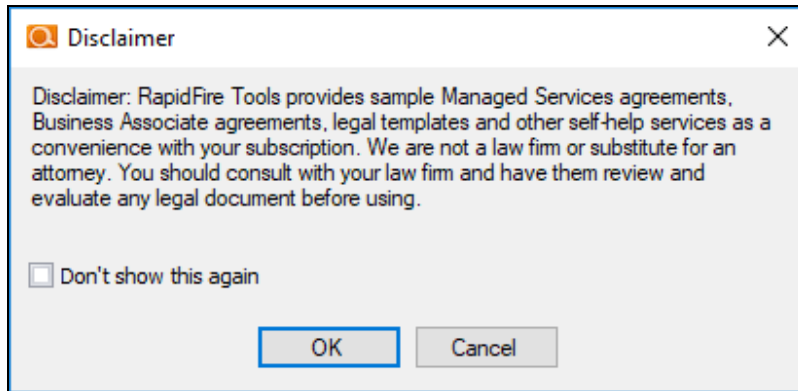
A screenshot of a dialog box titled 'MSA Customization'. The dialog contains several input fields and controls:

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

At the bottom of the dialog are 'OK' and 'Cancel' buttons.

- Review the legal disclaimer.



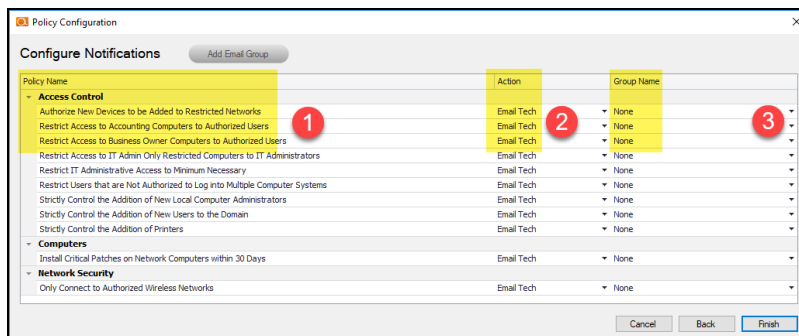


- When you have generated and reviewed your MSSA, click **Next**.

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

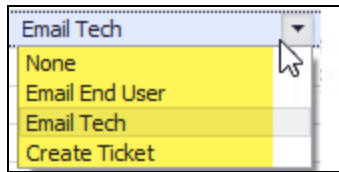
## Step 8 — Configure Notifications

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



- Review the specific **Policy** item.
- Assign an **Action** to the policy item. This can include:
  - None:** Take no action.
  - Email End User:** Send an email to an end user group. The end user will then make a decision about whether to request further investigation from the Tech Team.
  - Email Tech:** Send an email to the Tech Team to investigate the issue.

- **Create a Ticket:** Automatically Create a Ticket in your favorite PSA/ticketing system

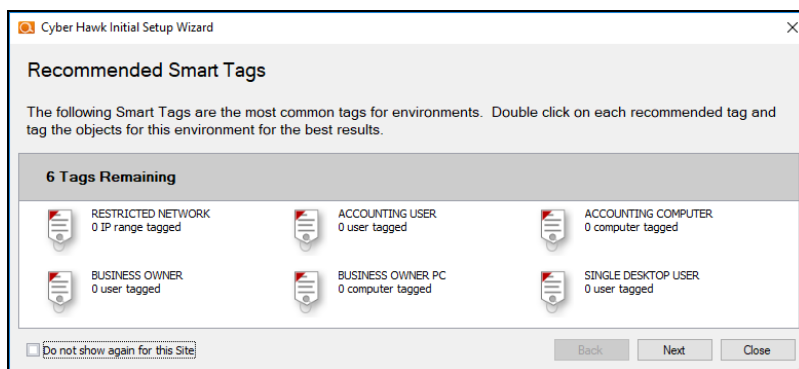


3. Select the Email **Group Name** (the email group to whom to send either an End User or Tech email notification).

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

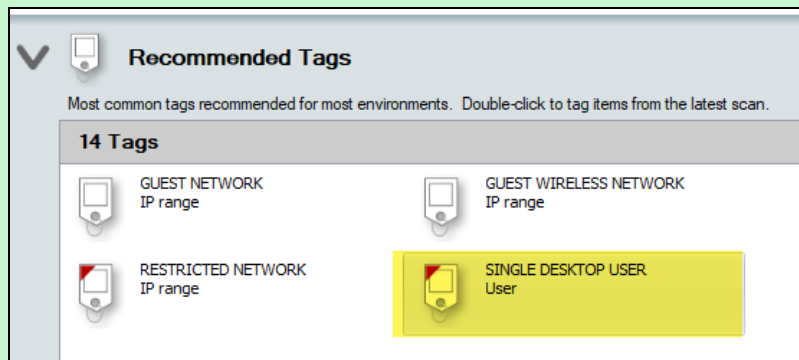
## Step 9 — Configure Smart Tags

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

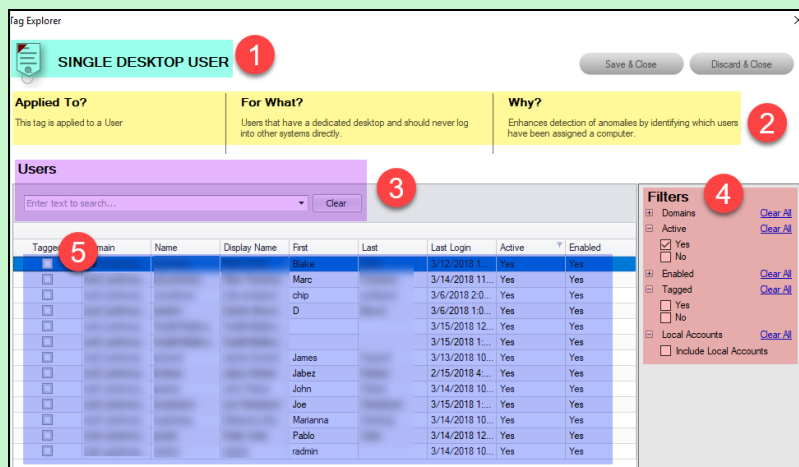


### EXAMPLE:

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



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



On the Smart Tag configuration screen you can find:

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

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

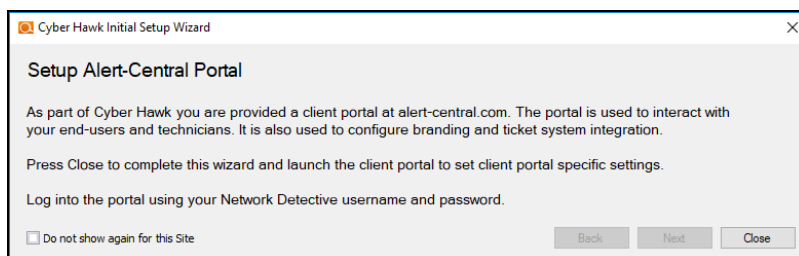
When you have assigned all recommended smart tags to network components, click **Next**.

## Step 10 — Set Up RapidFire Tools Portal

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

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

Click **Close** to dismiss the Cyber Hawk Initial Setup Wizard.



See these topics to set up the RapidFire Tools Portal:

- ["Set Up and Assign a Ticketing/PSA System Integration to a Site Using Cyber Hawk" on page 48](#)
- ["Set Up Portal Branding" on the facing page](#)
- ["Set Up a Custom Subdomain to Access the RapidFire Tools Portal" on page 42](#)
- ["Set Up Custom SMTP Server Support" on page 45](#)

# RapidFire Tools Portal Set Up

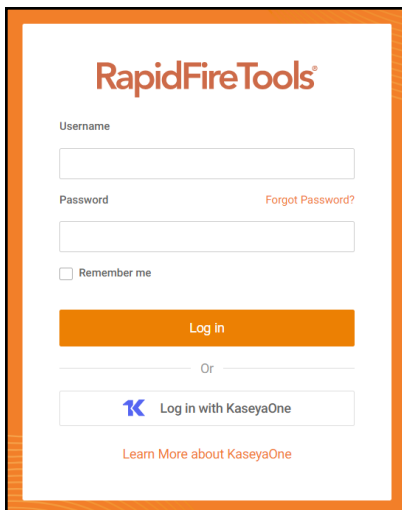
See the topics below for additional Cyber Hawk set up and help topics.

## Set Up Portal Branding

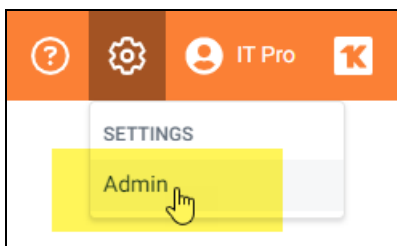
The RapidFire Tools Portal allows you to customize many elements to fit with your organization's brand and identity. This topic covers how you can modify the Portal's look and feel.

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

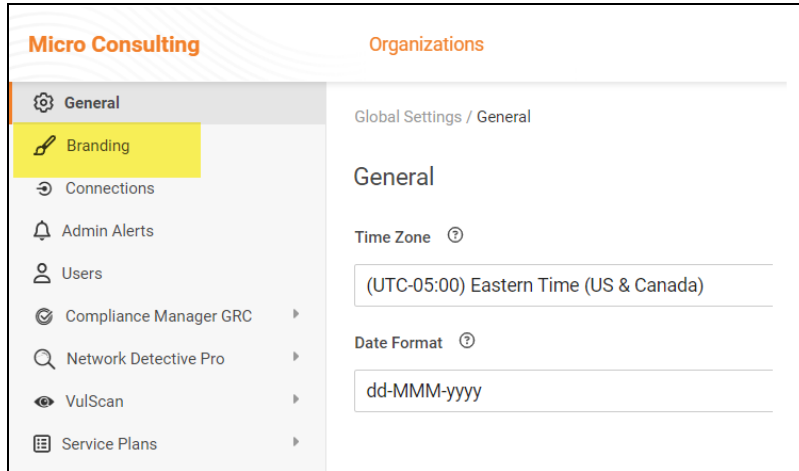
**Note:** In order to configure the settings in the Portal, the login credentials you use to access the Portal will require the Master User rights.



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



3. Click **Branding**.



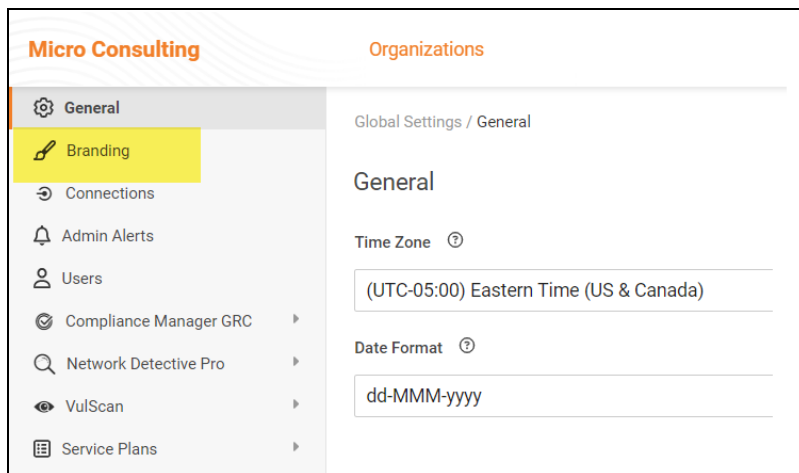
From this page, you can then:

- ["Set Custom Portal Theme" below](#)
- ["Set Custom Portal Subdomain" on the facing page](#)
- ["Set Custom Company Name" on page 40](#)
- ["Set Custom Company Logo" on page 41](#)

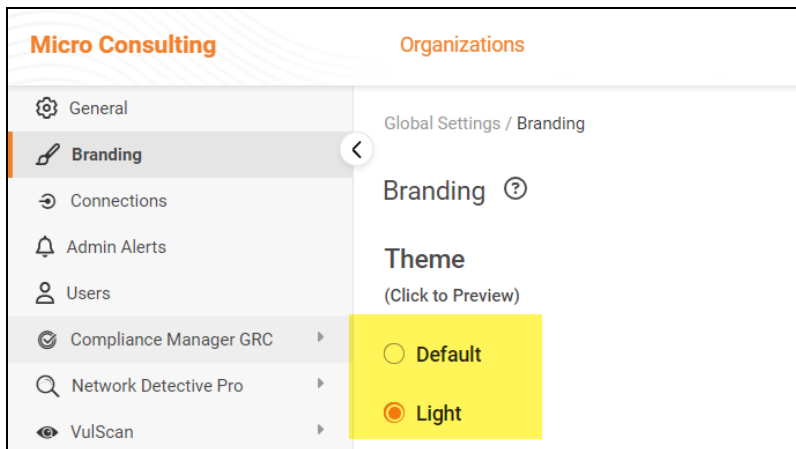
## Set Custom Portal Theme


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

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



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

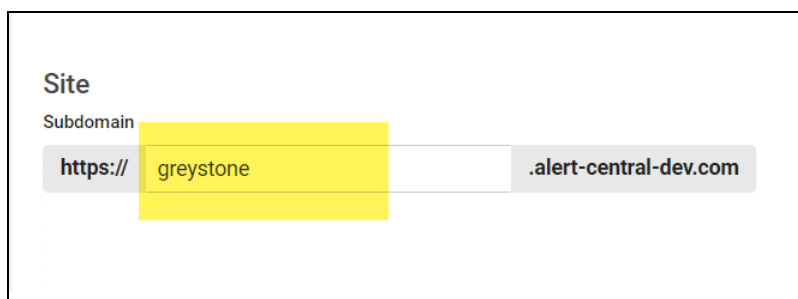


3. When you select the theme, you can click around the Portal and preview it. You must click **Save** from global **Settings (Admin)**  > **Branding** to apply your changes. This change will apply to all users.

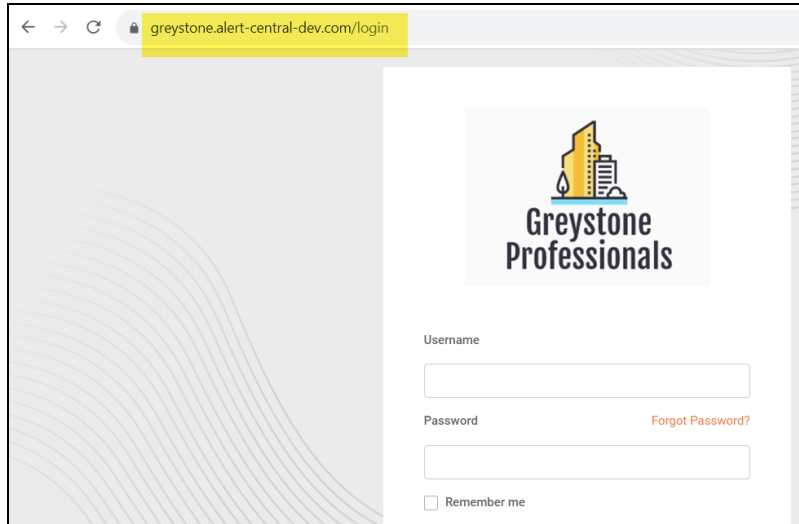
## Set Custom Portal Subdomain

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

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



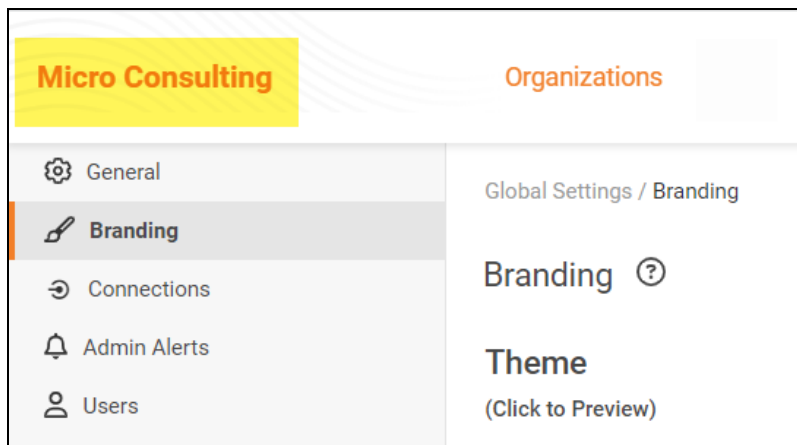
2. Click **Save**.
3. Log out of the RapidFire Tools Portal.
4. Next, access the RapidFire Tools Portal by using the URL for the new Subdomain you configured to access the Portal's login screen.



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

## Set Custom Company Name

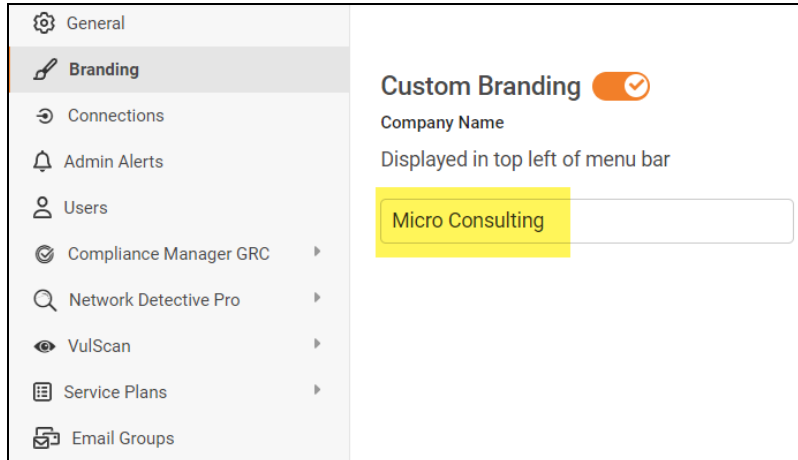
You can set a custom company name that will appear in the top left-hand corner of the Portal.



To do this:

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



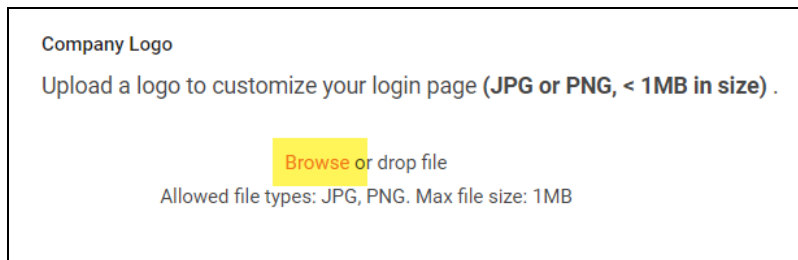


2. Click **Save**. Your custom name will then appear in the top-left corner of the portal for all users to see.

## Set Custom Company Logo

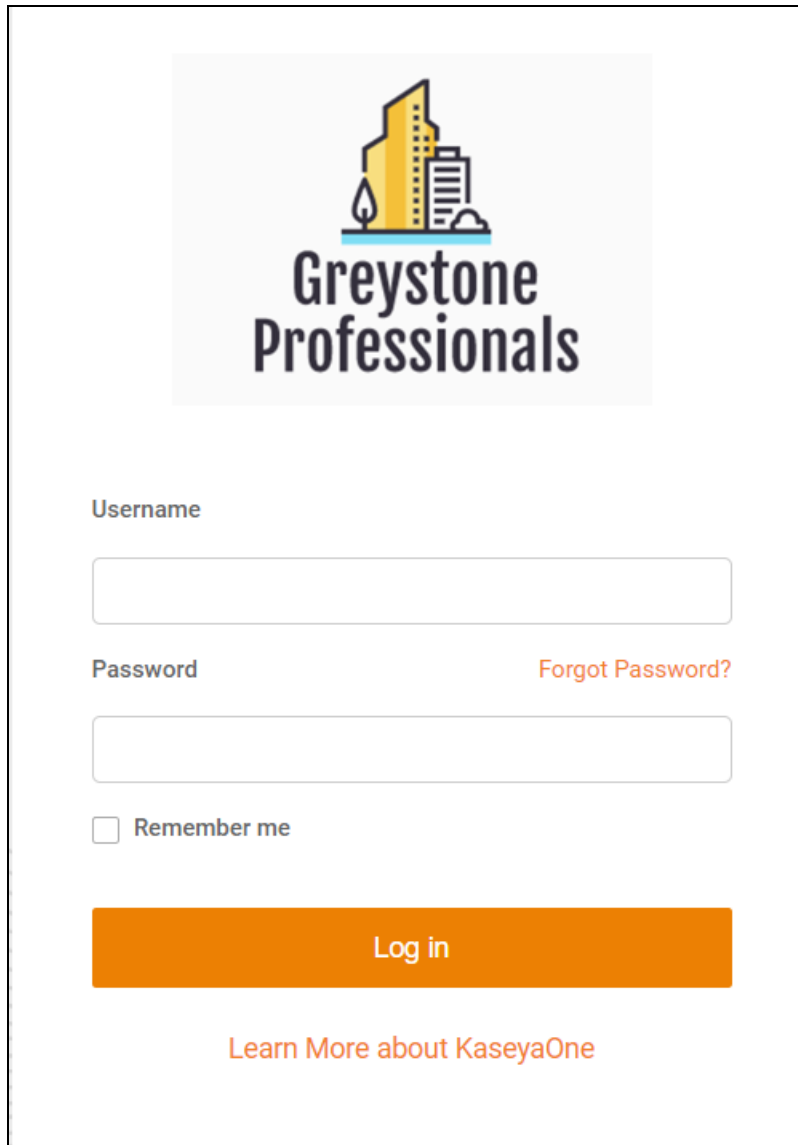
You can set a custom company logo on the Portal login screen to communicate your brand to users. To do this:

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



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

login screen.

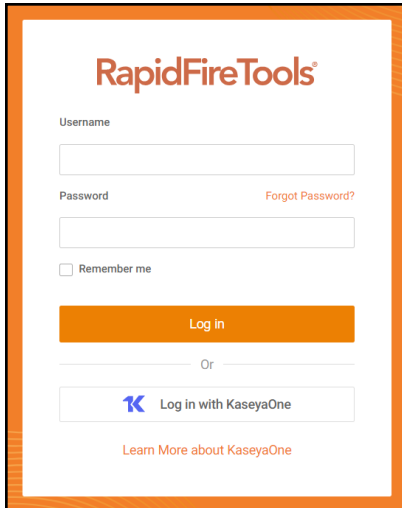


The image shows a login screen for Greystone Professionals. At the top center is the Greystone Professionals logo, which features a stylized yellow and blue building icon above the text "Greystone Professionals". Below the logo are two input fields: "Username" and "Password". To the right of the "Password" field is a link that says "Forgot Password?". Below the "Password" field is a checkbox labeled "Remember me". At the bottom of the form is a large orange button labeled "Log in". Below the button is a link that says "Learn More about KaseyaOne".

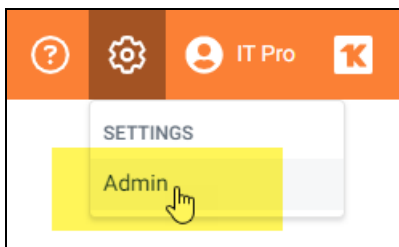
## Set Up a Custom Subdomain to Access the RapidFire Tools Portal

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

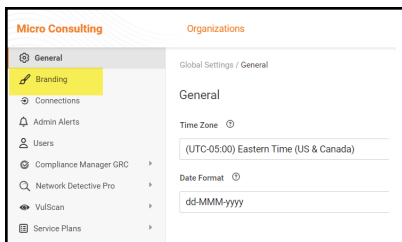
**Note:** In order to configure the settings in the Portal, the login credentials you use to access the Portal will require the Master User rights.



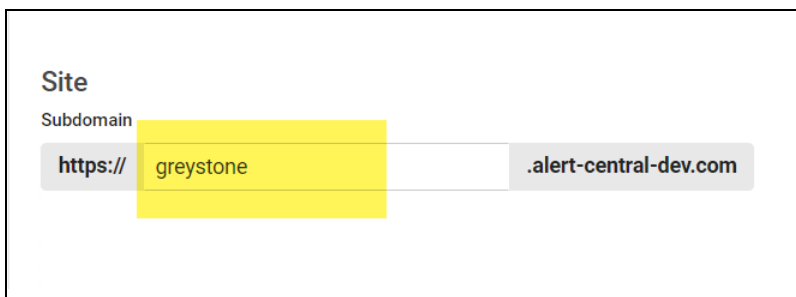
2. Click global **Settings (Admin)** .



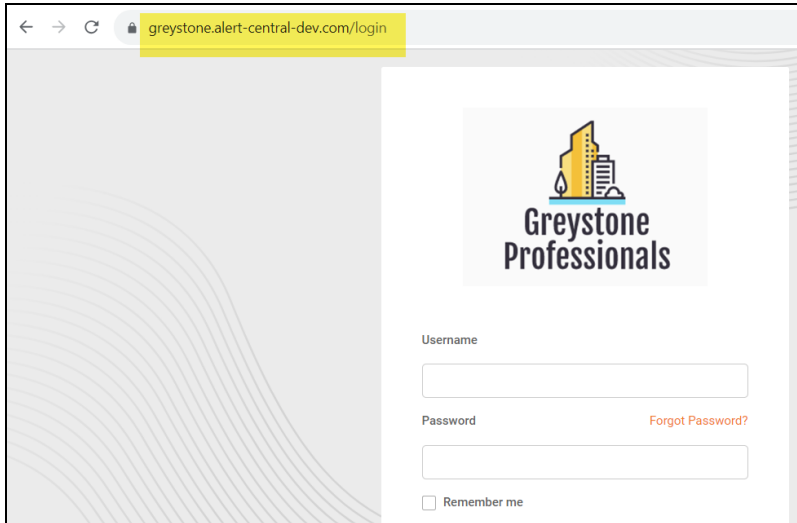
3. Click **Branding**.



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



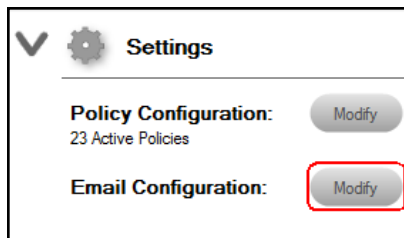
5. Click **Save**.
6. Log out of the RapidFire Tools Portal.
7. Next, access the RapidFire Tools Portal by using the URL for the new Subdomain you configured to access the Portal's login screen.



## Set Up Custom SMTP Server Support

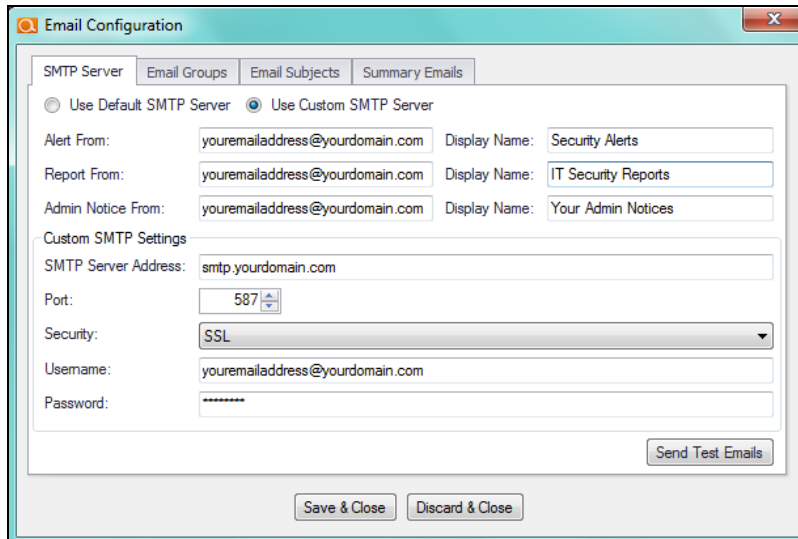
Follow these steps to set up the use of your own SMTP server to send Alerts and Notices from Cyber Hawk.

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



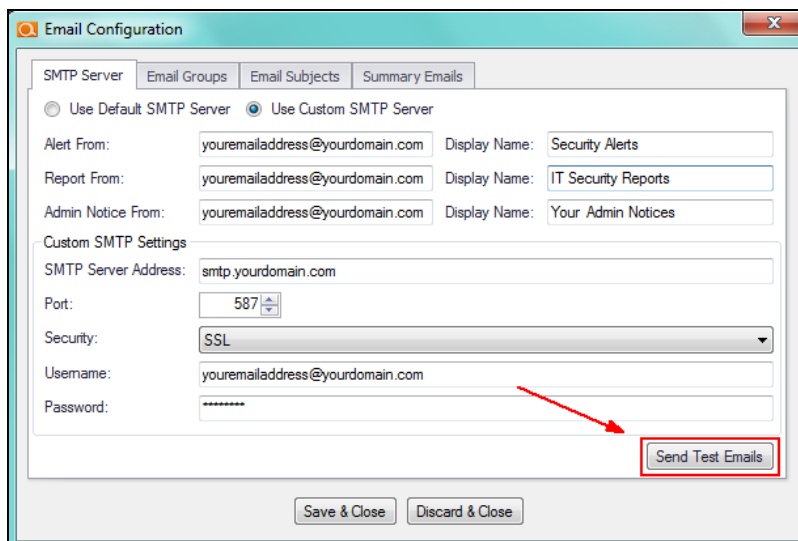
The Email Configuration window will be displayed.

2. Select the **SMTP Server** tab within the Email Configuration window to access the Custom SMTP Server settings.
3. Configure the following to set up your Customer SMTP Server to send Cyber Hawk Alerts and Notices:
  - Alert From email address and display name
  - Report From email address and display name
  - SMTP Server Address
  - Port Number
  - Security Method
  - SMTP Server Username and Password



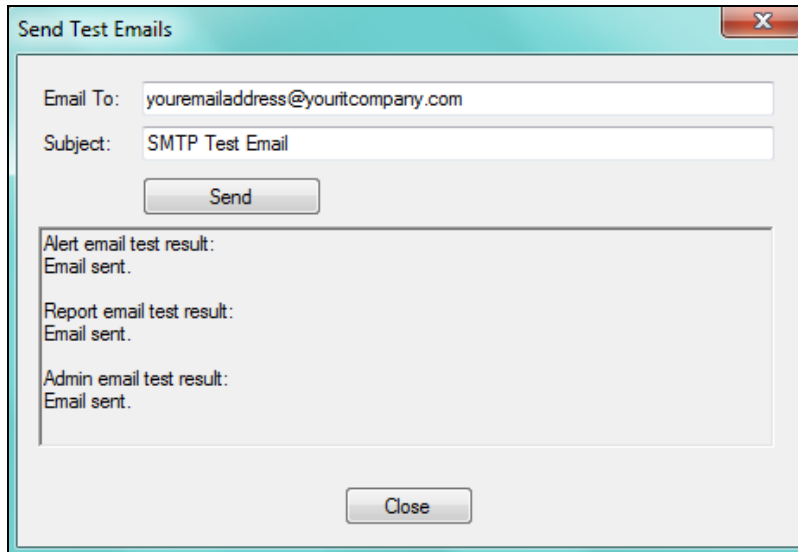
The screenshot shows the 'Email Configuration' window with the 'SMTP Server' tab selected. The 'Use Custom SMTP Server' radio button is chosen. The 'Alert From' field is 'youremailaddress@yourdomain.com' with a 'Display Name' of 'Security Alerts'. The 'Report From' field is 'youremailaddress@yourdomain.com' with a 'Display Name' of 'IT Security Reports'. The 'Admin Notice From' field is 'youremailaddress@yourdomain.com' with a 'Display Name' of 'Your Admin Notices'. Under 'Custom SMTP Settings', the 'SMTP Server Address' is 'smtp.yourdomain.com', the 'Port' is '587', the 'Security' is set to 'SSL', the 'Username' is 'youremailaddress@yourdomain.com', and the 'Password' is masked with asterisks. A 'Send Test Emails' button is located at the bottom right of the configuration area. At the very bottom of the window are 'Save & Close' and 'Discard & Close' buttons.

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



This screenshot is identical to the previous one, but a red arrow points from the 'Send Test Emails' button to a red rectangular box that highlights the button. The rest of the configuration is the same as in the previous image.

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



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

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

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

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


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

### Step 1 — Gather Credentials and Set Up your PSA System





Before you begin, you will need:

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

**Tip:** If you're having trouble, see the **Appendices** section in the [Network Detective User Guide](#) for more detailed information on how to configure your PSA to integrate with RapidFire Tools products.

PSA System	PSA Prerequisites
	<p>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.</p> <ul style="list-style-type: none"> <li>• Autotask Username</li> <li>• Autotask Password</li> </ul>

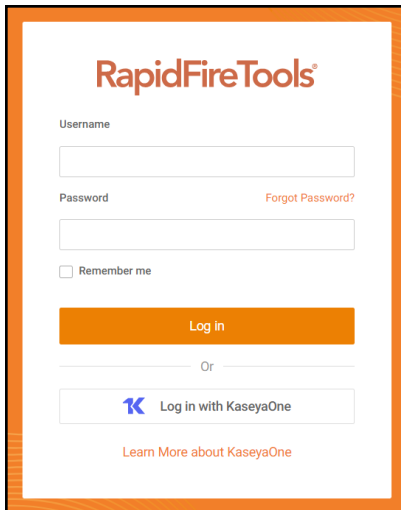


PSA System	PSA Prerequisites
 <p>SOAP (Deprecated)</p>	<ul style="list-style-type: none"> <li>• Autotask API Username</li> <li>• Autotask API Password</li> </ul>
	<ul style="list-style-type: none"> <li>• ConnectWise REST Public Key</li> <li>• ConnectWise REST Private Key</li> <li>• ConnectWise Company ID</li> <li>• ConnectWise PSA URL</li> </ul>
	<ul style="list-style-type: none"> <li>• ConnectWise Username</li> <li>• ConnectWise Password</li> <li>• ConnectWise Company ID</li> <li>• ConnectWise PSA URL</li> </ul>
	<ul style="list-style-type: none"> <li>• Tigerpaw Username</li> <li>• Tigerpaw Password</li> <li>• Tigerpaw API URL</li> </ul>

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

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

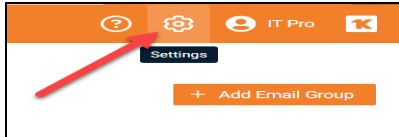
1. Visit <https://www.youritportal.com> and log into the RapidFire Tools Portal.



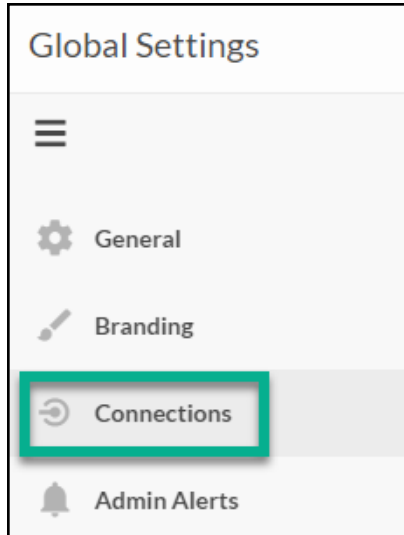
The image shows the login page for RapidFireTools. It features the logo at the top, followed by input fields for Username and Password. A 'Forgot Password?' link is next to the password field. There is a 'Remember me' checkbox and a 'Log in' button. Below this, there is an 'Or' separator and a 'Log in with KaseyaOne' button. At the bottom, there is a link to 'Learn More about KaseyaOne'.

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

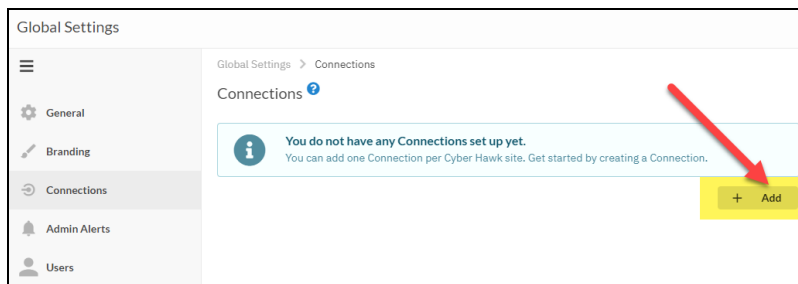
2. Click global **Settings (Admin)** .



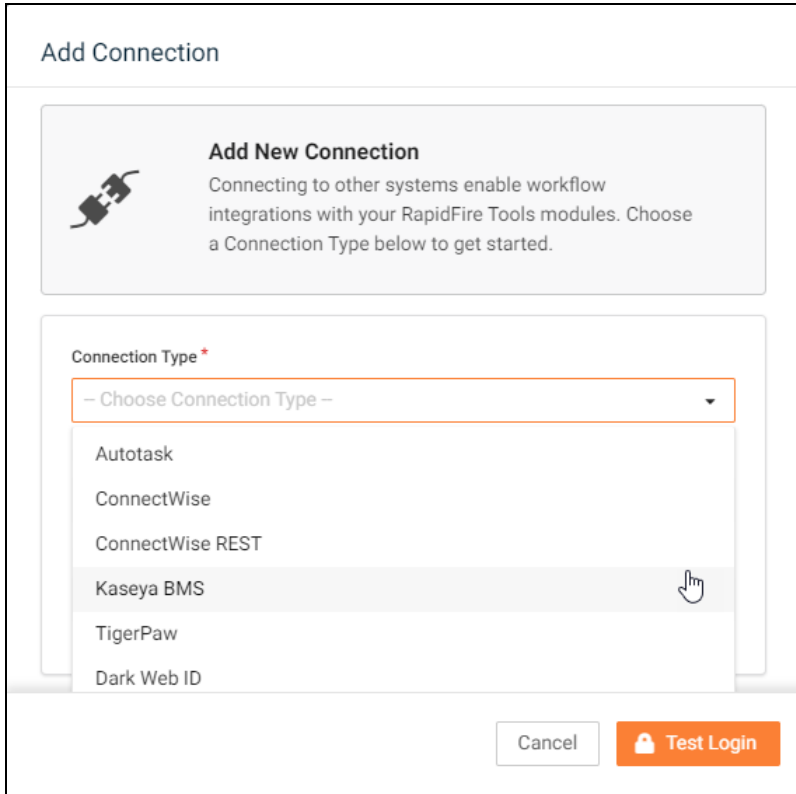
3. Click **Connections**.



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



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

Connection Type \*

– Choose Connection Type –

- Autotask
- ConnectWise
- ConnectWise REST
- Kaseya BMS**
- TigerPaw
- Dark Web ID


Cancel Test Login

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

⏪ Cancel 🔑 Test Login

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.

<b>Work Type *</b> Maintenance	<b>Assigned Resource</b> Darl Brown
<b>Role</b> Standard MS Engineer	<b>Due Date/Time *</b> Now + 5 Minutes
<b>Issue Type</b> Maintenance	<b>Sub-Issue Type</b> Workstation
<b>Queue</b> Level I IT Management	<b>Priority *</b> Medium
<b>Status *</b> New	<b>Source</b> Email

**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.

- In the Add Connection Confirm Settings window presented, enter a **Connection Name**.
- 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**

---

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

← Back
Save

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

Global Settings > Connections

Connections ?

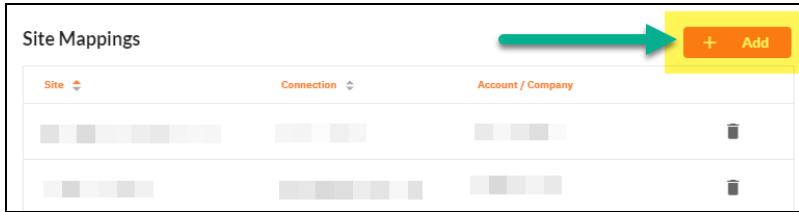
Your Connections + Add

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

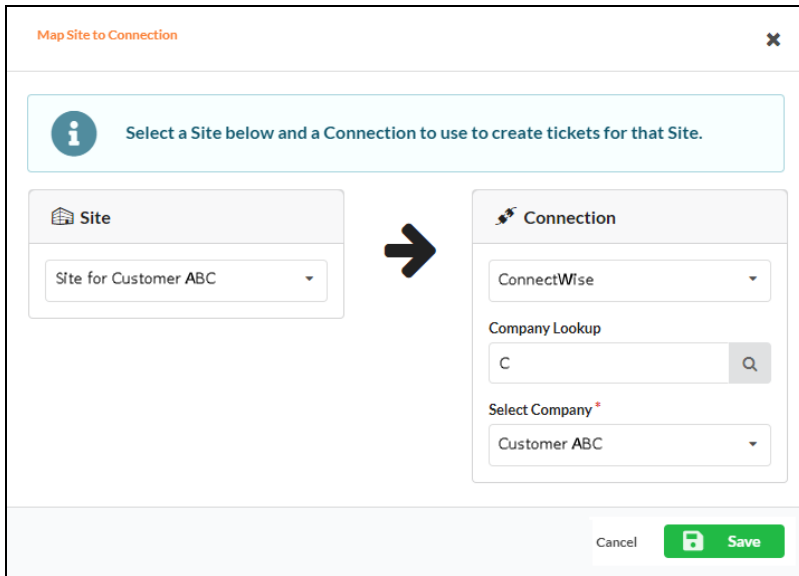
### Step 3 — Map your Cyber Hawk’s Site to a Ticketing System/PSA Connection

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

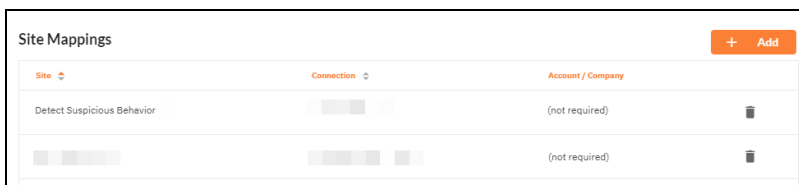
1. In the Integrations window, click **Add** under Site Mappings. The Map Site to Connection window will be displayed.



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



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





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

## 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
<b>GPO Configuration for Windows Firewall (Inbound Rules)</b>	
<input type="checkbox"/>	<p>Allow <i>Windows Management Instrumentation (WMI)</i> service to operate through Windows Firewall</p> <p>This includes the following rules:</p> <ul style="list-style-type: none"> <li>Windows Management Instrumentation (ASync-In)</li> <li>Windows Management Instrumentation (WMI-In)</li> <li>Windows Management Instrumentation (DCOM-In)</li> </ul>
<input type="checkbox"/>	<p>Allow <i>File and printer sharing</i> to operate through Windows Firewall</p> <p>This includes the following rules:</p> <ul style="list-style-type: none"> <li>File and Printer Sharing (NB-Name-In)</li> <li>File and Printer Sharing (SMB-In)</li> <li>File and Printer Sharing (NB-Session-In)</li> </ul>
<input type="checkbox"/>	<p>Enable <i>Remote Registry</i> “read only” access on computers targeted for scanning.</p>

Complete	Domain Configuration
	<div style="border: 1px solid #00a0c0; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p><b>Note:</b> Remote Registry access should be restricted for use by the user access account credentials to be used during network and local computer scan.</p> </div>
<input type="checkbox"/>	<p>Enable the <i>Internet Control Message Protocol (ICMP)</i> to allow authorized ICMP echo request messages and ICMP echo reply messages to be sent and received by Windows computers and network devices.</p> <p>Windows firewall rules on Windows computers may need to be created/enabled to allow a computer:</p> <ul style="list-style-type: none"> <li>• operating a Kaseya-RapidFire Tools product network data collector to issue ICMP echo request messages to be sent to Windows computers and network devices</li> <li>• to send ICMP echo reply messages in response to an ICMP echo request</li> </ul> <div style="border: 1px solid #00a0c0; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p><b>Note:</b> ICMP requests are used to detect active Windows computers and network devices to scan.</p> </div>
<p><b>GPO Configuration for Windows Services</b></p>	
<input type="checkbox"/>	<p><i>Windows Management Instrumentation (WMI)</i></p> <ul style="list-style-type: none"> <li>• Startup Type: Automatic</li> </ul>
<input type="checkbox"/>	<p><i>Windows Update Service</i></p> <ul style="list-style-type: none"> <li>• Startup Type: Automatic</li> </ul>
<input type="checkbox"/>	<p><i>Remote Registry</i></p> <ul style="list-style-type: none"> <li>• Startup Type: Automatic</li> </ul>
<input type="checkbox"/>	<p><i>Remote Procedure Call</i></p> <ul style="list-style-type: none"> <li>• Startup Type: Automatic</li> </ul>
<p><b>Network Shares</b></p>	
<input type="checkbox"/>	<ul style="list-style-type: none"> <li>• <i>Admin\$</i> must be present and accessible using supplied credentials (usually a local admin or user in the local Computer's Administrative Security group)</li> </ul>

Complete	Domain Configuration
<b>3rd Party Firewalls</b>	
<input type="checkbox"/>	<ul style="list-style-type: none"> <li>• Ensure that 3rd party Firewalls are configured similarly to Windows Firewall rules described within this checklist.</li> </ul> <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 5px; margin-top: 10px;"> <p><b>Note:</b> This is a requirement for both Active Directory and Workgroup Networks.</p> </div>

## 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
	<b>Network Settings</b>
<input type="checkbox"/>	<ul style="list-style-type: none"> <li>• <i>Admin\$</i> must be present on the computers you wish to scan, and be accessible with the login credentials you provide for the scan</li> </ul>
<input type="checkbox"/>	<ul style="list-style-type: none"> <li>• <i>File and printer sharing</i> must be enabled on the computers you wish to scan</li> </ul>
<input type="checkbox"/>	<ul style="list-style-type: none"> <li>• <i>Ensure the Windows Services below are running and allowed to communicate through Windows Firewall:</i></li> <li>• Windows Management Instrumentation (WMI)</li> <li>• Windows Update Service</li> <li>• Remote Registry</li> <li>• Remote Desktop</li> <li>• Remote Procedure Call</li> </ul>
<input type="checkbox"/>	<ul style="list-style-type: none"> <li>• Workgroup computer administrator user account credentials.</li> </ul> <div style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;"> <p><b>Note:</b> Before configuring scan settings for workgroups, prepare a list of the workgroup computer(s) administrator user account credentials for entry into the scan settings wizard.</p> </div>
<input type="checkbox"/>	<p>Enable the <i>Internet Control Message Protocol (ICMP)</i> to allow authorized ICMP echo request messages and ICMP echo reply messages to be sent and received by Windows computers and network devices.</p> <p>Windows firewall rules on Windows computers may need to be created/enabled to allow a computer:</p>

Complete?	Workgroup Configuration
	<ul style="list-style-type: none"><li>operating a Kaseya-RapidFire Tools product network data collector to issue ICMP echo request messages to be sent to Windows computers and network devices</li><li>to send ICMP echo reply messages in response to an ICMP echo request</li></ul> <div data-bbox="443 491 1325 604" style="border: 1px solid #0070C0; padding: 5px;"><p><b>Note:</b> ICMP requests are used to detect active Windows computers and network devices to scan.</p></div>