

CYBER HAWK™

by RapidFireTools®



“PLAN B” — SERVICE PLAN SETUP

Teleworker Guide “Plan B”

Detecting and Responding to IT Security Policy Violations

Contents

Cyber Hawk Teleworker Guide Overview	4
<u>Using Cyber Hawk to Watch Over Your Client's Networks</u>	4
Options to Configure Cyber Hawk Service Plans	5
Create the “Plan B” Security Service Plan	6
<u>Step 1 — Log into the RapidFire Tools and access the Cyber Hawk Service Plan Creator</u>	6
<u>Step 2 — Use the Service Plan Creator to create the “Plan B” Service Plan</u>	7
<u>Step 3 — Select the Security Policies for the “Plan B” service plan</u>	7
<u>Step 4 — Save the new plan as the “Plan B” service plan</u>	10
Create Email Group of Recipients to Receive “Plan B” Plan Alerts	11
<u>Step 1 — Access the Email Configuration Feature</u>	11
<u>Step 2 — Create a “Tech” Group of email recipients to receive “Plan B” Alerts</u>	11
<u>Step 3 (Optional) - Create an “End User” Group of email recipients to receive Alerts</u>	12
<u>Step 4 — Select the Cyber Hawk --- > Settings menu option to continue the set up process</u>	13
Assign Plan B to the Cyber Hawk Site and Create Notification Rules	14
<u>Step 1 — Select the Policy Configuration menu option</u>	14
<u>Step 2 — Assign the “Plan B” Plan to the Cyber Hawk Site</u>	14
<u>Step 3 - Set up the Alert Notification Rules</u>	15
<u>Step 4 - Save the Policy Configuration's Notification Rules</u>	16
Assign the “Single Desktop User” Smart Tag to All Network Users	18
<u>Step 1 — Select the Cyber Hawk > Smart Tags menu</u>	18
<u>Step 2 — Select the Users > Configure Tags button located on the Smart Tags</u>	18

page

Step 3 - Select all network users listed on the Users Smart Tags page 19

Step 4 - Select the Configure Tags menu and select the “Single Desktop User” Smart Tag 19

Step 5 - Select the Apply Changes button to save the “User” Smart Tags settings 20

Cyber Hawk Teleworker Guide Overview

We are in unprecedented and changing times. This guide is designed to provide guidance and specific steps required to create a **“Plan B” Service Plan** to:

- use the flexibility of the **Cyber Hawk Service Plan Creator** to build a plan to deliver cyber security services to your clients that is low impact to your company resources, but offers significant value to you and your clients in the new work-from-home environment
- assign the Plan B service plan to a specific Cyber Hawk Site that has been deployed to detect suspicious activity on a specific client’s network

Using Cyber Hawk to Watch Over Your Client’s Networks

As more of your clients' employees work from home on their own less-secure computers, the threat to the corporate network increases. Employee work credentials are more likely to be compromised now, opening the door for cyber criminals to get into your client’s networks.

But there is a quick and easy way to add on an extra layer of insider threat protection for all your clients that will look for indications of compromised credentials of your end users – things like anomalous end-user behaviors, suspicious log-ins to computers on the corporate network, and unauthorized network and local user account changes.

In response to the changing computing landscape where networks are now being accessed by a high number of remote users (many using their home PCs), this guide was written to help you create a quick-to-implement “Plan B” service plan that allows you to get this extra layer of protection set up and deployed to your clients.

Once operational, Cyber Hawk will scan your clients' corporate networks looking for any suspicious or odd end-user behaviors, unauthorized user account changes, and any attempted unauthorized log-ins to computers connected to the corporate network. Please note that Cyber Hawk will not scan the remote/home computers.

The policies suggested in the plan limit the amount of configuration required by you and your team, and typically provide fewer false positives during the first few weeks.

You will get daily Alerts (emails or tickets) of any detected threats, and you can manage all your client sites through a single web based portal available at <https://secure.youritportal.com>.

Options to Configure Cyber Hawk Service Plans

You can choose to configure Cyber Hawk Service Plans using either 1) the RapidFire Tools Portal or 2) the Network Detective app.

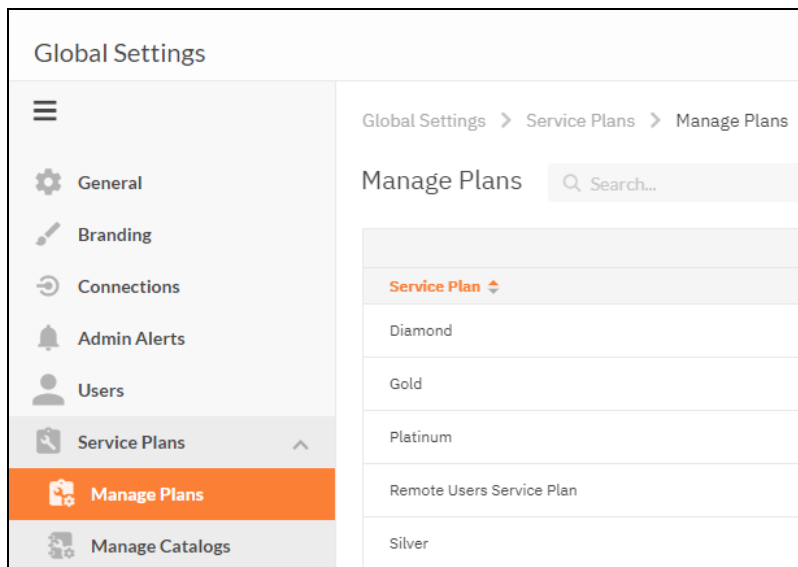
1. **Cyber Hawk 2019 Subscription Users** — Use the instructions that follow this section to set up Plan B using the portal.
2. **Cyber Hawk “Detector SDS” Plan Subscribers (Purchased Cyber Hawk before May 2019)** — If you want to set up Plan B using the Network Detective app, refer to this Guide along with the Cyber Hawk Quick Start Guide available at: https://www.rapidfiretools.com/nd/Cyber_Hawk_Quick_Start.pdf. The **Cyber Hawk Quick Start Guide** illustrates how to use Network Detective to set up **Service Plans** and assign a plan to a Cyber Hawk Site.

Create the “Plan B” Security Service Plan

In this step you will create a “**Plan B**” **Service Plan**. This plan will later be assigned to a Cyber Hawk Site to enable the detection and alerting on suspicious user logins, changes to the network, and potential threats.

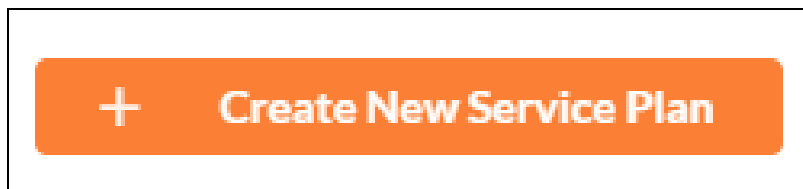
Step 1 — Log into the RapidFire Tools and access the Cyber Hawk Service Plan Creator

1. Access the Portal at <https://secure.youritportal.com> and log in with your user credentials.
2. Select **Global Settings** > **Service Plans** > **Manage Plans** menu option.
3. The **Service Plan** list will be displayed.

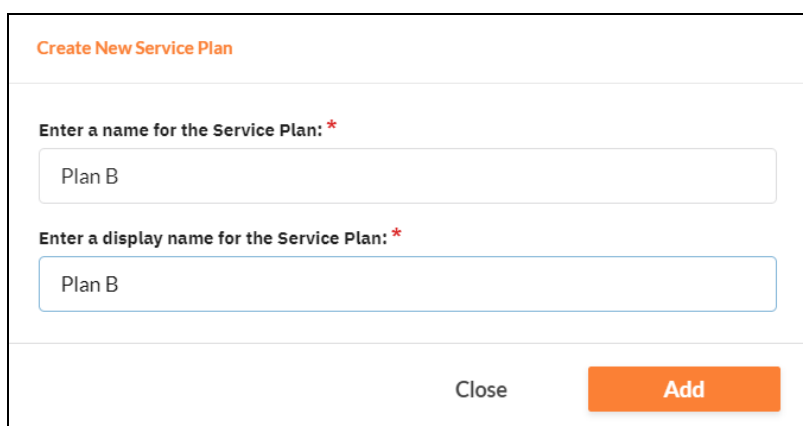


Step 2 — Use the Service Plan Creator to create the “Plan B” Service Plan

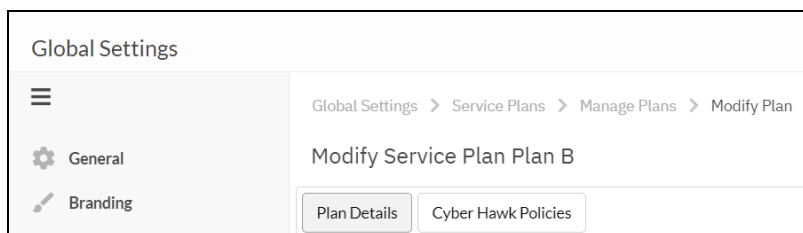
1. Select the **Create New Service Plan** button.



2. Enter “**Plan B**” as the name of the **Service Plan** and the plan’s **Display Name**.

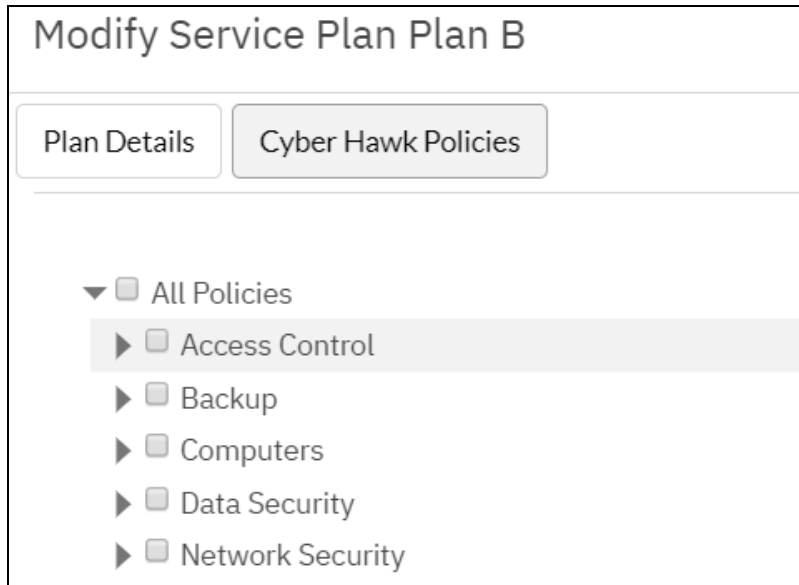
A screenshot of a web form titled "Create New Service Plan" in orange text. Below the title are two text input fields. The first field is labeled "Enter a name for the Service Plan: *" and contains the text "Plan B". The second field is labeled "Enter a display name for the Service Plan: *" and also contains the text "Plan B". At the bottom right of the form are two buttons: a grey "Close" button and an orange "Add" button.

3. Select the **Add** button to create the plan.
4. The **Modify Service Plan** page will be displayed.

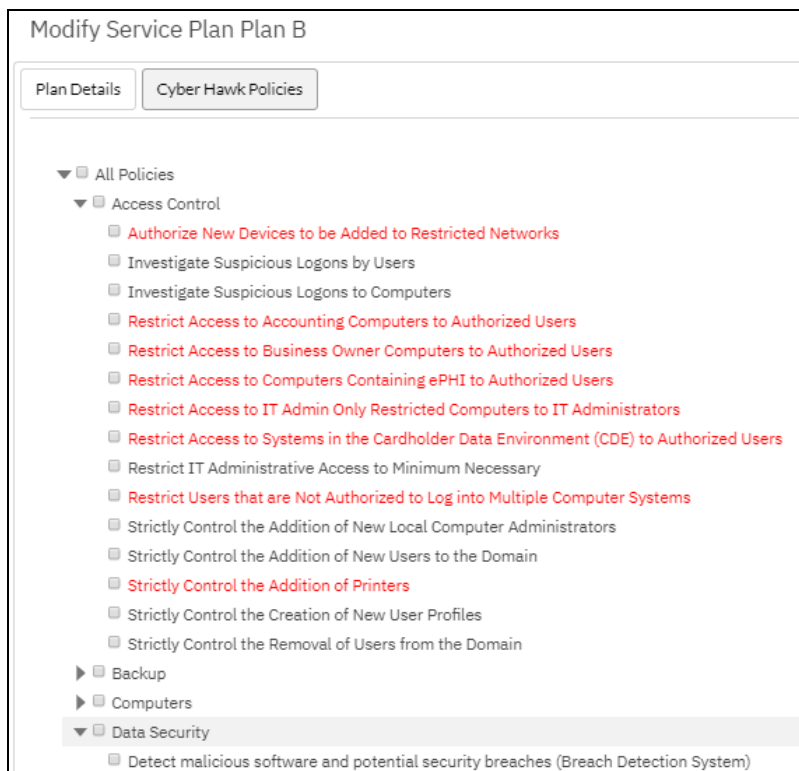


Step 3 — Select the Security Policies for the “Plan B” service plan

1. Select the **Cyber Hawk Policies** tab in the **Modify Service Plan** window.
2. The default **Security Policies** will be listed for the **Plan B Plan**.



3. Expand the security policies list to view all of the available **Access Control**, **Computers**, **Data Security**, and **Network Security Policies**.



4. Select the following **Security Policies** to create the **Plan B**:

Plan B Service Plan	
Investigate Suspicious Logons by Users	✓
Investigate Suspicious Logons to Computers	✓
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	✓
Detect malicious software and potential security breaches (Breach Detection System)	✓
Strictly Control the Creation of New User Profiles	✓
Strictly Control the Clearing of System and Audit Logs	✓
Strictly Control the Removal of Users from the Domain	✓
Strictly control changes to Group Policy	✓
Strictly control changes to the Default Domain Policy	✓

5. After completing the selection and assignment of the **Security Policies** to the **Plan B Plan**, select the **Configure Notifications** button.



6. Assign the default **Notification Rules** for **Plan B** by:
7. Assigning the **Action** of “None” to each **Security Policy**.
8. Verifying that the **Email Group** set to none for each **Security Policy**.

Modify Service Plan Plan B

Plan Details Cyber Hawk Policies + Add Global Email Group

Access Control

Policy Name	Action	Group
Investigate Suspicious Logons by Users	None	None
Investigate Suspicious Logons to Computers	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 Creation of New User Profiles	None	None
Strictly Control the Removal of Users from the Domain	None	None

Computers

Policy Name	Action	Group
Strictly Control the Clearing of System and Audit Logs	None	None

Data Security

Policy Name	Action	Group
Detect malicious software and potential security breaches (Breach Detection System)	None	None

Network Security

Policy Name	Action	Group
Strictly control changes to Group Policy	None	None
Strictly control changes to the Default Domain Policy	None	None

✕ Cancel Save

Step 4 — Save the new plan as the “Plan B” service plan

The saving of the **“Plan B” Service Plan** will be confirmed. The user will be redirected back to the **Policy Configuration** page.

Create Email Group of Recipients to Receive “Plan B” Plan Alerts

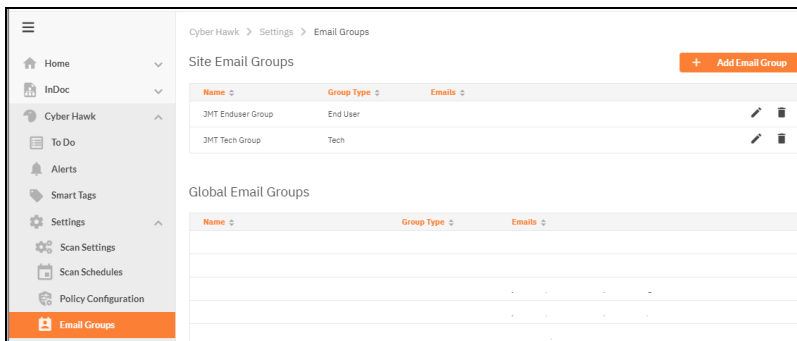
In this step you will configure “Email Groups” containing the email addresses for:

- **Tech Groups** – Members of your company’s Technician Team that manages your clients’ networks and responds to suspected IT security incidents.
- **End User Groups** (optional) – Members of your client company’s Senior Management team which may include the CEO, Accounting Manager, HR Manager, and other management team members that should be made aware of when suspicious IT security events are detected.

Members of these groups will be sent Cyber Hawk **Alert Notifications** with a request to respond to suspected **Security Policy** violations.

Step 1 — Access the Email Configuration Feature

1. From within the Cyber Hawk Site select the **Cyber Hawk > Settings > Email Groups** menu.
2. The **Email Groups** user interface will be displayed.



Step 2 — Create a “Tech” Group of email recipients to receive “Plan B” Alerts

1. Select the **Add Email Group** button.



The **Add Email Group** window will be displayed.

2. In the **Add Email Group** window presented, enter in the **Group Name**, select the **“Tech” Group Type**, and enter the email addresses in the **Email Recipients** field for individuals in your company that are to receive Cyber Hawk Alerts.



3. Select the **Add** button to save the new **Tech Email Group**.

Step 3 (Optional) - Create an “End User” Group of email recipients to receive Alerts

1. Select the **Add Email Group** button.



The **Add Email Group** window will be displayed.

2. In the **Add Email Group** window presented, enter in the **Group Name**, select the **End User Group Type**, and enter the email addresses in the **Email Recipients** field for members of your **client’s management team** that are to receive Cyber Hawk Alerts.

Add Email Group

Group Name

Group Type

Designated Tech Group

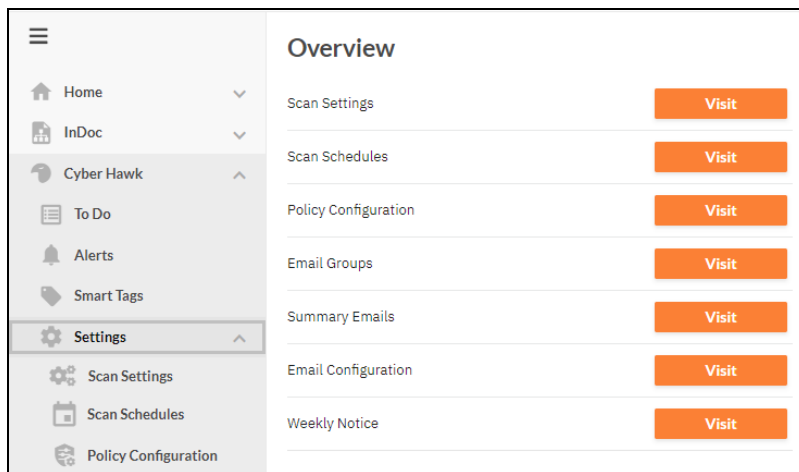
Email Recipients

Separate multiple addresses with a comma (",")

Cancel

3. Select the **Add** button to save the new **End User Email Group**.

Step 4 – Select the Cyber Hawk --- > Settings menu option to continue the set up process



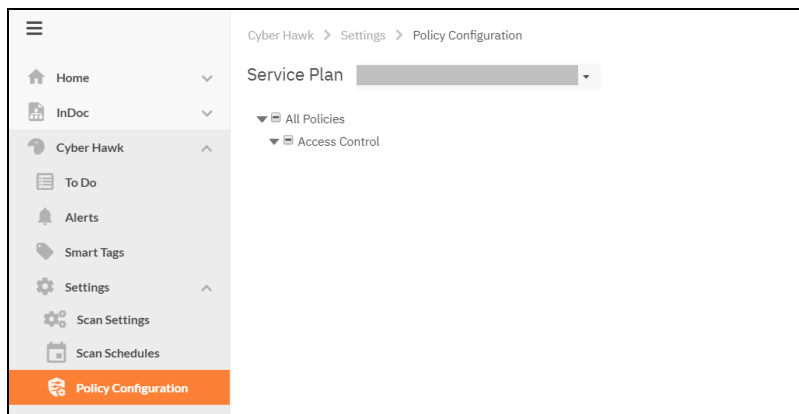
The screenshot shows the Cyber Hawk application interface. On the left is a navigation sidebar with a hamburger menu icon at the top. The sidebar items are: Home, InDoc, Cyber Hawk (highlighted), To Do, Alerts, Smart Tags, Settings (highlighted), Scan Settings, Scan Schedules, and Policy Configuration. The main content area is titled "Overview" and contains a list of settings items, each with an orange "Visit" button to its right:

Setting	Action
Scan Settings	Visit
Scan Schedules	Visit
Policy Configuration	Visit
Email Groups	Visit
Summary Emails	Visit
Email Configuration	Visit
Weekly Notice	Visit

Assign Plan B to the Cyber Hawk Site and Create Notification Rules

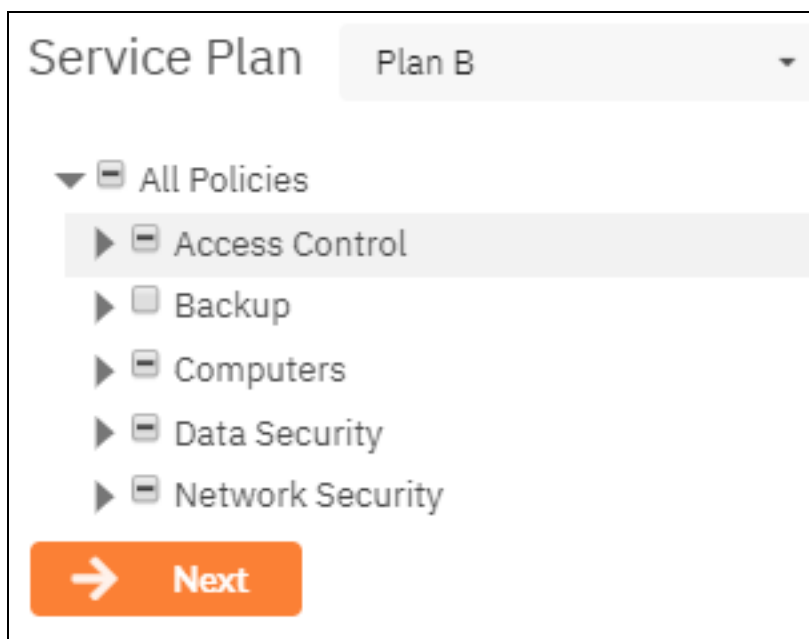
In this step you will assign the “**Plan B**” to a Cyber Hawk Site and configure a series of **Notification Rules** associated with the **Security Policies** contained within the **Plan B Plan**.

Step 1 — Select the Policy Configuration menu option



Step 2 — Assign the “Plan B” Plan to the Cyber Hawk Site

1. Select the “**Plan B**” **Service Plan**.



2. Select the “Next” button.

The **Notification Rules** user interface will be displayed.

Notification Rules ← Back Add Site Email Group

Access Control

Policy Name	Action	Group
Investigate Suspicious Logons by Users	None	None
Investigate Suspicious Logons to Computers	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 Creation of New User Profiles	None	None
Strictly Control the Removal of Users from the Domain	None	None

Computers

Policy Name	Action	Group
Strictly Control the Clearing of System and Audit Logs	None	None

Data Security

Policy Name	Action	Group
Detect malicious software and potential security breaches (Advanced Breach Detection System)	None	None

Network Security

Policy Name	Action	Group
Strictly control changes to Group Policy	None	None
Strictly control changes to the Default Domain Policy	None	None

Save

Step 3 - Set up the Alert Notification Rules

1. For each **Security Policy** in the **Policy Name** list, select and assign the **Action** to be “**Email Tech**” or “**Email End User**”*

Access Control

Policy Name	Action	Group
Investigate Suspicious Logons by Users	Email Tech	None
Investigate Suspicious Logons to Computers	None	None
Restrict IT Administrative Access to Minimum Necessary	Email End User	None
Restrict Users that are Not Authorized to Log into Multiple Computer Systems	Email Tech	None
Strictly Control the Addition of New Local Computer Administrators	Create Ticket	None
Strictly Control the Addition of New Users to the Domain	None	None
Strictly Control the Creation of New User Profiles	None	None
Strictly Control the Removal of Users from the Domain	None	None

***End User Notification Action Assignments** (optional) – When configuring the **Notification Rules** for the following three policies, consider having **Alerts** sent to your client’s management team members assigned to the “**End User**” **Email Group**:

- Investigate Suspicious Logons by Users
- Investigate Suspicious Logons to Computers
- Restrict Users that are Not Authorized to Log into Multiple Computer Systems

- For each **Security Policy** in the **Policy Name** list, select and assign the **Group** to be the **“Tech” Email Group**, or **“End User” Email Group** created in the create **Email Group** configuration step previously performed.

REFER TO THE SCREEN SHOT ON THE NEXT PAGE

Policy Name	Action	Group
Investigate Suspicious Logons by Users	Email Tech	JMT Tech
Investigate Suspicious Logons to Computers		JMT Tech Group
Restrict IT Administrative Access to Minimum Necessary		JS Global Tech
Restrict Users that are Not Authorized to Log into Multiple Computer Systems		jw-test
Strictly Control the Addition of New Local Computer Administrators		KL Test
Strictly Control the Addition of New Users to the Domain	None	None
Strictly Control the Creation of New User Profiles	None	None
Strictly Control the Removal of Users from the Domain	None	None

Step 4 - Save the Policy Configuration’s Notification Rules

- After all **Actions** and **Groups** have been assigned, select the **“Save”** button located below the **“Notification Rules”** table.

Policy Name	Action	Group
Investigate Suspicious Logons by Users	Email Tech	JMT Tech G...
Investigate Suspicious Logons to Computers	Email Tech	JMT Tech G...
Restrict IT Administrative Access to Minimum Necessary	Email Tech	JMT Tech G...
Restrict Users that are Not Authorized to Log into Multiple Computer Systems	Email Tech	JMT Tech G...
Strictly Control the Addition of New Local Computer Administrators	Email Tech	JMT Tech G...
Strictly Control the Addition of New Users to the Domain	Email Tech	JMT Tech G...
Strictly Control the Creation of New User Profiles	Email Tech	JMT Tech G...
Strictly Control the Removal of Users from the Domain	Email Tech	JMT Tech G...

Policy Name	Action	Group
Strictly Control the Clearing of System and Audit Logs	Email Tech	JMT Tech G...

Policy Name	Action	Group
Detect malicious software and potential security breaches (Advanced Breach Detection System)	Email Tech	JMT Tech G...

Policy Name	Action	Group
Strictly control changes to Group Policy	Email Tech	JMT Tech G...
Strictly control changes to the Default Domain Policy	Email Tech	JMT Tech G...

Save

- After the **Notification Rules** has been saved, the user will return to the **Service Plan Policy Configuration** page.

Service Plan Plan B ▼

- ▼ All Policies
 - ▶ Access Control
 - ▶ Backup
 - ▶ Computers
 - ▶ Data Security
 - ▶ Network Security

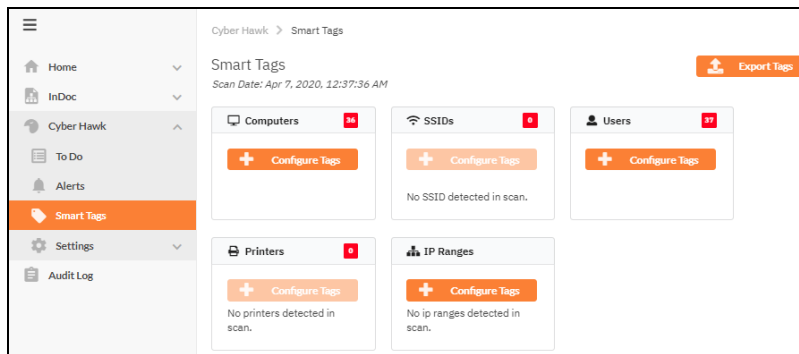
[→ Next](#)

Assign the “Single Desktop User” Smart Tag to All Network Users

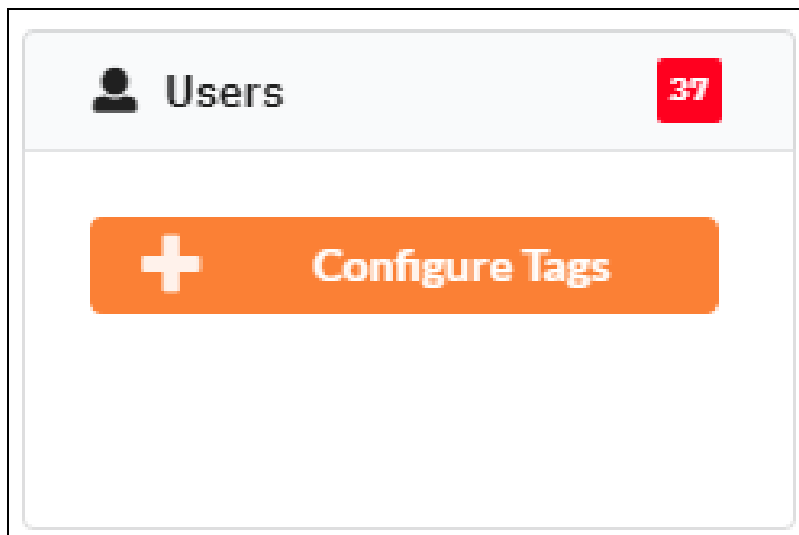
In this step you will assign a Smart Tag to all network users of your client’s network that are not authorized to access more than one computer on the network.*

Note: IT Administrators of the network may be excluded from being Smart Tagged as a “Single Desktop User”.

Step 1 — Select the Cyber Hawk > Smart Tags menu



Step 2 — Select the Users > Configure Tags button located on the Smart Tags page



Step 3 - Select all network users listed on the *Users Smart Tags* page

Use the multiple row selection feature to select all network users listed on the *Users Smart Tags* page.

Domain	Usenam...	Display N...	Active	Enabled	Tags
performanc...	abadmin	A Brown			
performanc...	ajadmin	A Jones		✓	
performanc...	arogers	Aaron Rogers		✓	
performanc...	Administrator	Administrator		✓	
performanc...	backslash	back slash		✓	
performanc...	dadmin	D Brown	✓	✓	
performanc...	dkadmin	D Kabzinski	✓	✓	
performanc...	dwadmin	D Whatley		✓	
performanc...	DefaultAccount	DefaultAccount			
performanc...	ebland	Eric Bland		✓	

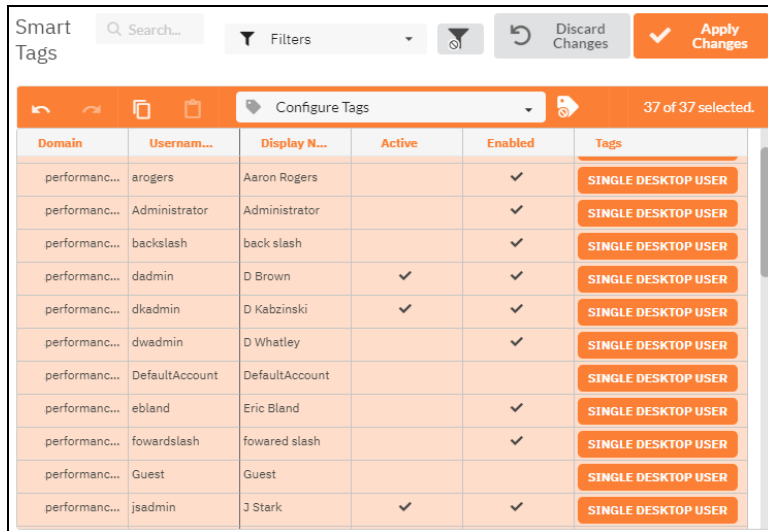
When using the multiple row selection feature, the network user list will be highlighted in *orange*.

Step 4 - Select the *Configure Tags* menu and select the “*Single Desktop User*” Smart Tag

Domain	Usenam...	Display N...	Active	Enabled	Tags
performanc...	abadmin	A Brown			SINGLE DESKTOP USER
performanc...	ajadmin	A Jones		✓	SINGLE DESKTOP USER
performanc...	arogers	Aaron Rogers		✓	SINGLE DESKTOP USER
performanc...	Administrator	Administrator		✓	SINGLE DESKTOP USER
performanc...	backslash	back slash		✓	SINGLE DESKTOP USER
performanc...	dadmin	D Brown	✓	✓	SINGLE DESKTOP USER
performanc...	dkadmin	D Kabzinski	✓	✓	SINGLE DESKTOP USER
performanc...	dwadmin	D Whatley		✓	SINGLE DESKTOP USER
performanc...	DefaultAccount	DefaultAccount			SINGLE DESKTOP USER
performanc...	ebland	Eric Bland		✓	SINGLE DESKTOP USER
performanc...	fowardslash	fowared slash		✓	SINGLE DESKTOP USER
performanc...	Guest	Guest			SINGLE DESKTOP USER
performanc...	jsadmin	J Stark	✓	✓	SINGLE DESKTOP USER
performanc...	jwadmin	J Weakland		✓	SINGLE DESKTOP USER

The Single Desktop User Smart Tag will be assigned to the selected network users.

Step 5 - Select the *Apply Changes* button to save the “User” Smart Tags settings



The screenshot shows the 'Smart Tags' configuration page. At the top, there is a search bar, a 'Filters' dropdown, and buttons for 'Discard Changes' and 'Apply Changes'. Below this is a toolbar with icons for back, forward, refresh, and a 'Configure Tags' dropdown menu. A status bar indicates '37 of 37 selected'. The main table has columns for 'Domain', 'Usernam...', 'Display N...', 'Active', 'Enabled', and 'Tags'. Each row represents a user, and the 'Tags' column contains an orange button labeled 'SINGLE DESKTOP USER'.

Domain	Usernam...	Display N...	Active	Enabled	Tags
performanc...	arogers	Aaron Rogers		✓	SINGLE DESKTOP USER
performanc...	Administrator	Administrator		✓	SINGLE DESKTOP USER
performanc...	backslash	back slash		✓	SINGLE DESKTOP USER
performanc...	dadmin	D Brown	✓	✓	SINGLE DESKTOP USER
performanc...	dkadmin	D Kabzinski	✓	✓	SINGLE DESKTOP USER
performanc...	dwadmin	D Whatley		✓	SINGLE DESKTOP USER
performanc...	DefaultAccount	DefaultAccount			SINGLE DESKTOP USER
performanc...	ebland	Eric Bland		✓	SINGLE DESKTOP USER
performanc...	fowarded slash	fowared slash		✓	SINGLE DESKTOP USER
performanc...	Guest	Guest			SINGLE DESKTOP USER
performanc...	jsadmin	J Stark	✓	✓	SINGLE DESKTOP USER

After the changes to Smart Tags are applied, a “Tags Saved” confirmation message will be presented. The **Plan B** setup process is now complete.

