

Service Plan Creator

Quick Reference Guide

© 2017 RapidFire Tools, Inc. All rights reserved.

V20170423 - Ver 1I

Contents

Purpose of this Guide2
Service Plan Creator Use Cases
Creating Service Plans and Service Catalogs
Step 1 – Create a New Service Plan
Step 2 – Assign Security Policies to Your Service Plan4
Step 3 – Defining Reports Deliverables to be Included in the Service Plan
Step 4 – Creating a Service Catalog7
Generating a Service Catalog Document9
Generating a Service Plan Matrix Document
Generating a Sample Master Services Agreement for a Service Plan
Managing Service Plans
Modifying a Plan16
Deleting a Plan
Managing Service Catalogs
Modifying a Catalog
Deleting (excluding) Service Plans from a Catalog21
Adding Service Plans to a Catalog22
Removing (deleting) a Service Catalog from the List of Catalogs

Purpose of this Guide

This guide is designed to provide an overview and specific steps required to use the Network Detective **Service Plan Creator**.

Other supplementary Guides to be referenced along with this guide include the Detector Quick Reference Guide and the Network Detective User Guide available at <u>www.rapidfiretools.com/nd</u>.

Service Plan Creator Use Cases

There are four use cases for the **Service Plan Creator**:

- Create Service Plans that are used to offer and deliver one-time Assessment Services
- Create **Service Plans** that leverage the Network Detective Detector to deliver an on-going Security Policy-based Service Offering to your customers using the Detector Appliance
- Create Service Catalogs used to produce a Service Catalog document in Word format. The purpose of the Service Catalog document is to enable you to produce marketing literature, sales proposals, and service agreements. The Service Catalog document presents:
 - a **Service Plan Matrix** of the plans you are proposing to a prospective client or customer
 - o descriptions of the Security Policies and Procedures associated with each Service Plan
 - o a list of reports deliverables for each of the proposed plans
- Generate a stand-alone Service Plan Matrix document in Word format summarizing the Service Plans you created

The next section outlines the steps necessary to create **Service Plans** and **Catalogs**.

Creating Service Plans and Service Catalogs

To create a new Service Plan, follow these steps:

Step 1 – Create a New Service Plan

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



3. Select Create New Service Plan.

		Create New Service P	lan	
Service Pla	ns	Manage Plans	5	
	•	Silver (Silver)		
Manage Plans	=	Sites	Policies	Scheduled Reports
		1 •	12 •	0 🔻
Manage Catalogs	*			

Enter a name for the Service Plan: YourIT Company's Svc Plan

Cancel

OK

x

4. Enter the name for your **Service Plan**.

Select **Ok** to generate the basic **Service Plan** template.

Your **Service Plan** template will be displayed within the **Manage Plans** window.

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

	C	Create New Service P	lan	
Service Plans	s I	Manage Plans	;	
Manage Plans		YourIT Con	npany's Svc	Plan 🖍 🗙
	=	Sites	Policies	Scheduled Reports
I≣ `i Manage Catalogs	•	0 •	0 •	0 •

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

Create New Service Plan

Step 2 – Assign Security Policies to Your Service Plan

 Select the Edit Service Plan option to add the Security Policy assignments to the newly created plan.

YourIT Com	npany's Svc	Plan 📝 🗙
Sites	Policies	Scheduled Reports
0 •	0 •	0 •

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

Modify S	ervice Plan	
Service Plan:	YourIT Company's Svc Plan Save Delete	
Detector Poli	ies Scheduled Reports Usage	
📃 🔽 Ac	cess Control	
	Authorize New Devices to be Added to Restricted Networks	
	Investigate Suspicious Logons by Users	
	Investigate Suspicious Logons to Computers	
v	Only Connect to Authorized Printers	
V	Restrict Access to Accounting Computers to Authorized Users	
V	Restrict Access to Business Owner Computers to Authorized Users	
	Restrict Access to Computers Containing ePHI to Authorized Users	
	Restrict Access to IT Admin Only Restricted Computers to IT Administrators	
	Restrict Access to Systems in the Cardholder Data Environment (CDE) to Authorized Users	
	Restrict IT Administrative Access to Minimum Necessary	
V	Restrict Users that are Not Authorized to Log into Multiple Computer Systems	
V	Strictly Control the Addition of New Local Computer Administrators	
v	Strictly Control the Addition of New Users to the Domain	E
~	Users Should Only Access Authorized Systems	
⊟ ⊻ Co	nputers	
v	Changes on Locked Down Computers Should be Strictly Controlled	
V	Install Critical Patches for DMZ Computers within 30 Days	
	Install Critical Patches on Network Computers within 30 Days	
- 170 1	Restrict Internet Access for Computers that are Not Authorized to Access the Internet Directly	
	Nork Security	
	Detect Network Changes to Internal Networks	
	Detect ivetwork Changes to Internal Wireless Ivetworks	
	Unity Contract to Authorized Witeless Networks	
	Prenediate Medium Seventy Internal Vulnerabilities (CVSS > 7.0)	
	i temetiate metitum sevenity intental vulneraunities (C+35.2.4.0)	-

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

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

Authorize New Devices to be Added to Restricted Networks
Description
The appearance of new devices on "restricted networks" is to be tightly controlled in compliance with strict network change management policies and procedures.
Detector alerts you when changes have been made to the network. Using the RESTRICTED NETWORK tag enables you to designate an IP address range as a "restricted network" to indicate that changes as a result of adding a device to the network are more significant.
Required Tags
RESTRICTED NETWORK applied to an IP range

 After completing the selection of the Policies that you want associated with your Service Plan, select the Save button before you proceed to the next step.

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

Step 3 – Defining Reports Deliverables to be Included in the Service Plan

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

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

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

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

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

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



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

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

- Select from the Network and Security Reports listed in the Schedule Reports Wizard window, and select the Next button.
- Using the Every list control, select the frequency from the choices available (i.e. day, week, month, year, or once). Select the Finish button once your selections are complete.



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

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

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

Modify Service Plan	
Service Plan: YourIT Company's Svc Plan	Save Delete
Detector Policies Scheduled Reports Usage	
Schedule Report	
Reports	Repeats
😢 NetworkAssessment-Client Risk Report	Weekly
😢 NetworkAssessment-Network Management Plan	Weekly
😣 NetworkAssessment-Full Detail Change Report	Monthly
😢 NetworkAssessment-Quarterly Business Review	Monthly

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

- Select the Save button to save your Service Plan Reports selections and configurations.
- Select the Manage Plans options to view a summary of your new Service Plan.

Modify Serv	Modify Service Plan							
Service Plan: You	rlT Company's Svc Plan	Save Delete						
Service Plans	Modify Service Plan							
	Service Plan: YourIT Company's Svc Plan	Save Delete						
Manage Plans	Detector Policies Scheduled Reports Usage							
	Reports	Reneats						
Plan Matrix	NetworkAssessment-Client Risk Report	Weekly						
	😢 NetworkAssessment-Network Management Plan	Weekly						
	😢 NetworkAssessment-Full Detail Change Report	Monthly						
	NetworkAssessment-Quarterly Business Review	Monthly						

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

The details include the number of:

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

Silver		1 ×	Gold		1
Sites	Policies	Scheduled Reports	Sites	Policies	Scheduleo Reports
0 🔻	10 🔻	2 🔻	1 •	18 🔻	1 •
YourIT Co	mpany's Svc	Plan 🖍 🗙	Platinum		1
YourIT Co	mpany's Svc	Plan X Scheduled Reports	Platinum Sites	Policies	Scheduled Reports

Step 4 – Creating a Service Catalog

- 1. Select the Service Plans icon.
- 2. Select the Manage Catalogs Icon.



	Create New Service F	Plan				
Service Plans	Manage Plans	6				
Manage Plans	Silver (Silve	ər)	/ ×	Gold (Gold)	/ ×
	Sites 1 ▼	Policies	Scheduled Reports 0 ▼	Sites 2 🔻	Policies	Scheduled Reports 0 ▼
	Platinum (F	Platinum)	/ ×	Titanium (1	Titanium)	/ ×
	Sites 2 ▼	Policies 23	Scheduled Reports 1 V	Sites	Policies	Scheduled Reports 22 ▼

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

- Service Plans Manage Catalogs Generate Catalog Name Clone Remove Include All Pla U Plans Silver Gold Platinum Jatalog 1 Jew Variant Catalog Security Services Catalog MB Service Catalog IIPAA Services Jike SMB Manage Plans Descripti Manage Catalogs old ariant 1 anaged Services Offerings per Small SMBs 1 Service Catalog Authorize stricted Networks ent Company Service Plan Install Critic ers within 30 Days
- To create a new Service Catalog, select the default Catalog named "All Plans" and select the Clone button.

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

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

Enter a New Catalog Name		
Your IT Company Catalog		
OK Cancel		

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

Service Plans	Manage Catalogs Generate				
	Catalog Name: Your IT Company	iy Catalog 🗸	Clone Remov	e Include All P	lans
Manage Plans	Description	Silver (Silver) Exclude	YourIT Company's Svc Plan (YourIT Company's Svc Plan) Exclude	Gold (Gold) Exclude	Platinum (Platinum) Exclude

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

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

Service Plans	Manage Catalogs Generate			
	Catalog Name: Your IT Company Catalog V Clone Rem	ove Include All Pl	ans	
Manage Plans	Description	YourlT Company's Svc Plan (YourlT Company's Svc Plan) Exclude	Gold (Gold) Exclude	Platinum (Platinum) Exclude
	Authorize New Devices to be Added to Restricted Networks	*	*	*

Generating a Service Catalog Document

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

The Service Catalog document will contain a list of the Security Plans you have assigned to your Service Catalog(s) along with an overview of the Service Plan Security Policies and Procedures, and a list of Reports deliverables.

Service Plans

Manage Plans

To generate the **Service Catalog** document, follow these steps:

1. Select the Service Plans icon.



Clone Remove Inc

Gold

(Gold)

.

Platinum

(Platinum)

.

Titanium

1

(Titani

Silver

(Silver)

.

Manage Catalogs Generate

Catalog Name: All Plans

Authorize New Devices to be

Added to Restricted Ne

Description

2. Select the Manage Catalogs Icon.

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

- Service Plans Manage Catalogs Generate Catalog Nar Remove In Clone anage Plans Gold Platinun Titanium Descr (Gold) Authorize Manage Catalogs Added to I Install Cr Network C Davs
- To generate the Service Catalog document, select the name of the Catalog from the Catalog Name list.
- Service Plans
 Manage Catalogs
 Generate

 Image Plans
 Catalog Name:
 Silver Gold Platinum
- Select the Generate and then select the Service Plan Catalog menu option to generate the Service Catalog document.



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



Generating a Service Plan Matrix Document

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

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

Service Plans

Manage Plans

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

1. Select the Service Plans icon.



v 0

Platinum

1

Titanium

1

(Titar

Silver

(Silver

1

(Gold)

Manage Catalogs Generate

Catalog Name: All Plans

Authorize New Devices to be

Added to Restricted Netw

Description

2. Select the Manage Catalogs Icon.

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

Service Plans	Manage C	atalogs Generate				
	Catalog Name:	All Plans	Clone	Remove	nclude All Plans	
manage mans	Descriptio	Silver Gold Platinum Catalog 1 New Variant Catalog	ar 1)	Gold (Gold)	Platinum (Platinum)	Titanium (Titanium)
Manage Catalogs	Authorize N Added to R	SHA Service Stating SHA Service Stating HIPAA Services Silver Gold Variant 1 Managed Services Offerings Super Small SMBs PCI Service Catalog Audition Common Service Rinn		*	*	1
	Install Critic Network Co Days			*	~	~
	Only Conne	Small Office Solution				

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

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

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

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

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

The **Security Policies** associated with the **Plan** are in the document.

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

And a list of **Reports deliverables** associated with the plan are referenced the **Report Tasks** section of the **Service Plan's Matrix**.

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

Generating a Sample Master Services Agreement for a Service Plan

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

The sample **MSA** document will include an example of terms and conditions for an **MSA** and reference an Exhibit that will present a list of the **Security Policies and Procedures** that reflect the **Service Plan** that will be selected when setting up the Detector for your customer.

To generate the Sample MSA document, follow these steps:

Step 1 – Opening Existing Network Detective Site that is Associated with your Detector

- 1. Start the Network Detective application.
- 2. Select the **Site** that that is **Associated** with your **Detector Appliance**.
- 3. To open the **Site**, double-click on the **Site** name.



Step 2 – Access the Detector Settings

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



Step 3 – Select the Policy Configuration Option

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

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

In the **Detector Settings** window, select the **Policy Configuration Modify** button to access the **Policy Configuration** options window.



The **Policy Configuration** window will be displayed.

envice Plan: Gold 🔹	Generate
Bit Advance Sectors	Authorize New Devices to be Added to Restricted Networks Description The spasmor produces on "tastistic study," is to is type; product and compare any environment and any environment and any environment compare any environment and any environment and any environment method environment and any environment any environment method environment and any environment any environment method environment and any environment any environment environment and any environment and any environment environment and any environment any environment environment and any environment any environment environment any environment and any environment environment and any environment any environment environment any environment any environment any environment any environment environment any environment any environment any environment any environment environment any environment any environment any environment environment any environment an
Service of the control of the service of the servi	Required Tegn ISSTRUCTO ACTIVIDE applied to an Drange

Step 4 – Generate Master Service Agreement Option

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

Next, select the Master Service Agreement Option.

g Policy Connguration	
Service Plan: Gold	Generate
EVAnce Concerning Concer	Author in Concern Approved (MAI) Restricted Methods and a second and and a second and association are second are seco
Einstal Geor Transit for DCC Company with 20 Geo Shard Geor Transit, Company with 20 Geor Shard Geor Transit, Company with 20 Geor Total Constraints, Company with 20 Geor Dest Elsawd, Chongins Ward Medication Science In Head Option Stand, Science In Head Mendication Science In Head	Required Tags ASTRUCTO / ETVICAS: epided to an IP range
Save & Close D	scard & Close

The MSA Customization window will be displayed

MSA Customization	X
MSP Name:	YourIT Company From Company Info Tab
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
Emergency Authorized Limit (\$):	1000
Effective Date:	Thursday , April 20, 2017
	OK Cancel

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

In the MSA Configuration window, enter the MSP Name, State, and Address along with the Customer Name and Address.

Next, enter the Service Plan Monthly Charge, Additional Hourly Billing Rate, Hours per Month Included, Emergency Authorized Limit, and the Effective Date to be referenced in the sample MSA.

After entering the **MSA Configuration** information, select the **OK** button.

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

O. Disclaimer ∑
Disclaimer: RapidFire Tools provides sample Managed Services agreements, Business Associate agreements, legal templates and other self-help services as a convenience with your subscription. We are not a law firm or substitute for an attorney. You should consult with your law firm and have them review and evaluate any legal document before using.
Don't show this again
OK Cancel

Step 6 – Confirm Acceptance of the Disclaimer and Generate the Sample MSA

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

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

👿 🛃 🌱 🕶 🙆 🚽 🖘 Sam	nple MSA.docx [Com	patibility Mode] - Micros	oft Word 📃	
File Home Insert	Page Layout R	eferences Mailings	Review	/iew 🗠 🕜
Print Full Screen Dottine Layout Document Views	ut Show Zoom	New Window	Switch Windows +	Macros Macros
MANAGED SECURITY SERVICES AGREEMENT This MATER SERVICES AGREEMENT (In: "Aggenerat") is the set of too and effective as of 4200017 (In: "Effective Date), by and behaves "Justic Company Info Tau Manage Security Service Provider (MSSP), a Security Company Info Tau Corporation High proced and the 111 Provider Of the Welc Company Info Tau Corporation High Tau Control High Tau Con				
Exagrand: Exagrand: Series Term(1), espect to ordinary systemet of series are seen or prombing valuescess or the series are series and to contend or a series series are series of the series are serie				
Page: 1 of 7 Words: 5,000 🤇	English (U.S.)	🔲 🛱 🖓 🗃 🔳 64	I% ——U-	+ + .;

Managing Service Plans

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

Modifying a Plan

To edit a Service Plan, follow these steps:

1. Select the **Service Plans** icon.



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

Manage Plans	5			
Silver		 × 		
Sites	Policies	Scheduled Reports		
0 •	10 •	2 •		
YourIT Company's Svc Plan 💉 🗙				
Sites	Policies	Scheduled Reports		
0 •	19 🔻	4 v		

The **Modify Service Plan** window will be displayed.

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

Modify Service Plan	
Service Plan: YourIT Company's Svc Plan Save Delete	
Detector Policies Scheduled Reports Usage	
Access Control	^
Authorize New Devices to be Added to Restricted Networks	
✓ Investigate Suspicious Logons by Users	
Investigate Suspicious Logons to Computers	
Only Connect to Authorized Printers	
Restrict Access to Accounting Computers to Authorized Users	
Restrict Access to Business Owner Computers to Authorized Users	
Restrict Access to Computers Containing ePHI to Authorized Users	
Restrict Access to IT Admin Only Restricted Computers to IT Administrators	
Restrict Access to Systems in the Cardholder Data Environment (CDE) to Authorized Users	
Hestrict II Administrative Access to Minimum Necessary	
Hestnet 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	
Users Should Uniy Access Authorized Systems	
Changes on Locked Down Computers Should be Strictly Controlled	
Install Critical Patches on Maturals Computers within 30 Days	
Install Childai Patches on Network Computers within 50 Days	
Network Security	
Detect Network Changes to Internal Networks	
Detect ive:work changes to internal Weilage Naturales	
Concerner work of anges to internal wireless Networks	
Panadista kich Savarity Internal Vylnarshiltias Immedistaly (CVSS > 7.0)	
Panedista Medium Savarity Internal Vylnarshilitias (CVSS > / 0)	
Promounaire meanain Sevency incential valitet dollates (CVSS > 4.0)	~

Impact of Service Plan Changes upon Deployed Detector Service Policy Settings - IMPORTANT

In cases where a **Service Plan** has been previously assigned to one or more Detector Appliances that are deployed, and the **Service Plan** has been updated, this revised **Service Plan** and its new **Detector Policy Settings** must be manually applied to each Detector that will continue to use the plan.

For more information about how to apply the **Security Policies** contained within a **Service Plan** to a Detector Appliance, please refer to the **Detector Quick Start Guide** available at <u>www.rapidfiretools.com/nd</u>.

Deleting a Plan

To **Delete** a **Service Plan**, follow these steps:

- 1. Select the Service Plans icon.
- 2. Select the **Edit** × icon on the **Service Plan** that you would like to **Delete**.





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



Manage Plans	5	
Silver		/ ×
Sites	Policies	Scheduled Reports
0 🔻	10 •	2 *

Impact of Deleting a Service Plan Previously Used to Configure Security Policy Settings - IMPORTANT

In cases where a **Service Plan** has been previously assigned to one or more Detector Appliances that are deployed, and the **Service Plan** has been deleted, a new **Service Plan** and its new **Detector Policy Settings** will need to be associated with these Detectors.

For more information about how to apply the **Security Policies** contained within a **Service Plan** to a Detector Appliance, please refer to the **Detector Quick Start Guide** available at <u>www.rapidfiretools.com/nd</u>.

Managing Service Catalogs

The instructions below detail the processes used to **Modify** and **Remove** (i.e. delete) **Service Catalogs**.

Modifying a Catalog

To edit a Service Catalog, follow these steps:

- 1. Select the Service Plans icon.
- 2. Select the Manage Catalogs icon.



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

Service Plans	Manage Catalogs Generate
Manage Plans	Catalog Name: Silver Gold Platinum Cione Remove
Manage Catalogs	Description Similar One Source State of

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

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

At this point in the process, you may:

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

Deleting (excluding) Service Plans from a Catalog

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

- 1. Select the Service Plans icon.
- 2. Select the Manage Catalogs icon.



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

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

Service Plans	Manage Catalogs Generate
	Catalog Name: Sliver Gold Platinum
Manage Plans	All Platts Silver Gold Platinum Small Office Solution To Your IT Company Catalog Titanium
Manage Catalogs	Authorize New Devices to be Added to Restricted Networks

Clone Remove Include All Plans

Manage Catalogs Generate

Authorize New Devices to be Added to Restricted Networks

Descripti

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

 Just below the name of each Service Plan is a link labeled <u>Exclude</u>. The selection of the <u>Exclude Link</u> removes the Service Plan from the Catalog.

Select the <u>Exclude Link</u> to remove the specific Service Plan selected from the Service Catalog.

Catalog Name: Vour IT Company Catalog	Class			*
Description	YourlT Company's Svc Plan (YourlT Company's Svc Plan) Exclude	Gold (Gold) Exclude	Platinum (Platinum) Exclude	III
Authorize New Devices to be Added to Restricted Networks	*	~	*	

The **Excluded Service Plan** will no longer be listed within the **Service Catalog** user interface unless re-added in the future.

Adding Service Plans to a Catalog

To Add a Service Plan to a Service Catalog, follow these steps:

- 1. Select the Service Plans icon.
- 2. Select the Manage Catalogs icon.



Service Plans Manage Plans			
	Silver (Silve	er)	✓ ×
Manage Plans	Sites	Scheduled Reports	
	3 🔻	12 🔻	0 •
Manage Catalogs			

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

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

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

Select the Include All Plans button.

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

 Just below the name of each Service Plan is a link labeled <u>Exclude</u>. The selection of the <u>Exclude Link</u> removes the Service Plan from the Catalog.

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

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



Catalog Name: Silver Gold Platinum	Clone Rem	ove Include All Plan	s		
Description	Silver (Silver) Exclude	Yourl T Company's Svc Plan (Yourl T Company's Svc Plan) Exclude	Gold (Gold) Exclude	Platinum (Platinum) Exclude	Titanium (Titanium) Exclude
Authorize New Devices to be Added to Restricted Networks	*	~	*	*	1
Install Critical Patches on Network Computers within 30 Days	1	*	1	1	1

Removing (deleting) a Service Catalog from the List of Catalogs

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

- 1. Select the Service Plans icon.
- 2. Select the Manage Catalogs icon.



Service Plans	5 Manage Plans				
	Silver (Silve	/ ×			
Manage Plans	Sites	Policies	Scheduled Reports		
	3 •	12 •	0 •		
Manage Catalogs					

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

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

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

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

Manage Catalogs Generate

- 4. Select **Remove** button to delete the **Catalog** from the **Service Plan Creator**.
- 5. The **Catalog** that you **Removed** will no longer be present in the **Catalog Name** list.

Catalog Name:	Your IT Company Catalog	Clone	Remove	Include All Plans
Description	n			
Authorize N	lew Devices to be Added to Re	estricted N	letworks	

Catalog Name: Your IT Company Catalog V Clone Remove Include All Plans