



COMPLIANCE MANAGER™

by RapidFireTools®

USER GUIDE

Compliance Manager for CMMC (Cybersecurity
Maturity Model Certification)

Instructions to Perform a CMMC Assessment

Contents

About Compliance Manager for CMMC	10
Introduction to Compliance Manager for CMMC	11
<u>Compliance Manager for CMMC Assessment Overview</u>	11
Project Roles	11
Notifications for Assessment To Do Tasks	12
What You Will Need	14
Network Prerequisites for Assessment Scans	16
Automated Scans Performed During the CMMC Assessment Process	17
<u>Compliance Manager Online Help</u>	18
<u>Pre-Scan Network Configuration Checklist</u>	20
Checklist for Domain Environments	20
Checklist for Workgroup Environments	22
Setting Up and Starting your CMMC Assessment Project	25
<u>Add Organizations</u>	25
Add an Organization	25
Move a Site to an Organization	28
<u>Create a New Site</u>	30
Assessment Progress Bar	37
View Site Details	37
Task 1: Create additional users and assign to roles	38
Task 2: Set up Report Preferences	43
Task 3: Install Server	46
Task 4: Configure Server Scan Settings	48
Configure Scan Settings for Active Directory Domain	48
Configure Scan Settings for Workgroup	55
Performing a CMMC Assessment	62
<u>Collect Initial CMMC Assessment Data</u>	62
Task 5: Start CMMC Assessment	63

Task 5.1: Running Pre-scan Analysis	64
Task 5.2: Review Pre-scan Analysis Results and Recommendations	65
Task 6: Running Automated Scan of Internal Network	68
Error while running Internal Network Scan	68
Task 7: Running Local Scan of Remote Computers	69
Task 8: Run Local Data Collector	70
Import RMM Connector Scans	72
Task 9: Perform Automated External Vulnerability Scan	73
Error while Running External Vulnerability Scan	73
<u>Collect Secondary CMMC Assessment Data</u>	73
Task 10: Complete External Port Use Worksheet	73
No External Port Found During External Vulnerability Scan	74
Task 11: Complete Anti-virus Verification Worksheet	74
Attach Supporting Documents	76
Select Multiple Fields	77
Copy and Paste Responses	78
Task 12: Complete User Access Review Worksheet	80
Task 13: Complete Asset Inventory Worksheet	81
Task 14: Complete Application Inventory Worksheet	83
Task 15: Complete External Information System Worksheet	83
Task 16: Select Level of CMMC Assessment	84
Which CMMC Level Should I Choose?	86
Change Assessment Level	86
<u>Complete Level 1 CMMC Worksheets</u>	87
Note Regarding Worksheet Cross References to NIST SP 800-171	88
Task 17: Complete CMMC Access Control Worksheet	88
Task 18: Complete CMMC Identification and Authentication Worksheet	89
Task 19: Complete CMMC Media Protection Worksheet	90
Task 20: Complete CMMC Physical Protection Worksheet	91
Task 21: Complete CMMC System and Communications Protection Worksheet	92
Task 22: Complete CMMC System and Information Integrity Worksheet	93
<u>Complete Level 2 CMMC Worksheets</u>	94
Note Regarding Worksheet Cross References to NIST SP 800-171	94

Task 17: Complete CMMC Access Control Worksheet	95
Task 18: Complete CMMC Audit and Accountability Worksheet	96
Task 19: Complete CMMC Awareness and Training Worksheet	97
Task 20: Complete CMMC Configuration Management Worksheet	98
Task 21: Complete CMMC Identification and Authentication Worksheet	99
Task 22: Complete CMMC Incident Response Worksheet	100
Task 23: Complete CMMC Maintenance Worksheet	101
Task 24: Complete CMMC Media Protection Worksheet	102
Task 25: Complete CMMC Personnel Security Worksheet	103
Task 26: Complete CMMC Physical Protection Worksheet	104
Task 27: Complete CMMC Recovery Worksheet	105
Task 28: Complete CMMC Risk Management Worksheet	106
Task 29: Complete CMMC Security Assessment Worksheet	107
Task 30: Complete CMMC System and Communications Protection Worksheet	108
Task 31: Complete CMMC System and Information Integrity Worksheet	109
Task 32: Complete NIST 800-171 Scoring Supplement (Optional)	110
<u>Complete Level 3 CMMC Worksheets</u>	111
Note Regarding Worksheet Cross References to NIST SP 800-171	112
Task 17: Complete CMMC Access Control Worksheet	112
Task 18: Complete Asset Management Worksheet	113
Task 19: Complete CMMC Audit and Accountability Worksheet	114
Task 20: Complete CMMC Awareness and Training Worksheet	115
Task 21: Complete CMMC Configuration Management Worksheet	116
Task 22: Complete CMMC Identification and Authentication Worksheet	117
Task 23: Complete CMMC Incident Response Worksheet	118
Task 24: Complete CMMC Maintenance Worksheet	119
Task 25: Complete CMMC Media Protection Worksheet	120
Task 26: Complete CMMC Personnel Security Worksheet	121
Task 27: Complete CMMC Physical Protection Worksheet	122
Task 28: Complete CMMC Recovery Worksheet	123
Task 29: Complete CMMC Risk Management Worksheet	124
Task 30: Complete CMMC Security Assessment Worksheet	125
Task 31: Complete Situational Awareness Worksheet	126

Task 32: Complete CMMC System and Communications Protection Worksheet	127
Task 33: Complete CMMC System and Information Integrity Worksheet	127
<u>Generate CMMC Reports</u>	129
Complete the Compensating Controls Worksheet	129
Review Final Reports	130
<u>Manage Assessment Issues</u>	131
View Assessment Issues	131
Optional Task: Export Issues to Kaseya BMS	133
Step 1 — Gather Credentials and Set Up Kaseya BMS	133
Step 2 — Set Up a Connection to your Kaseya BMS	133
Step 3 — Map your Compliance Manager's Site to a Kaseya BMS Connection	139
Step 4 — Export Issues to Kaseya BMS	140
<u>Complete and Archive your CMMC Assessment</u>	141
Task 22: CMMC Assessment Complete	142
View an Archived Assessment	143
CMMC Assessment Reports	144
<u>CMMC Compliance Reports</u>	144
<u>Supporting Documentation</u>	147
<u>Worksheets by Assessment Level</u>	148
<u>CMMC Risk Update Assessment Reports</u>	153
<u>Report Date Format (Global Settings)</u>	154
Ongoing CMMC Assessments	155
<u>Start a New CMMC Assessment after Completing a Previous Assessment</u>	155
<u>Generate Risk Update Reports</u>	157
Automatically Generate Risk Update Reports	157
Manually Generate Risk Update Reports	158
Risk Profile Settings	160
List of Risk Update Reports	161
Additional Compliance Manager Assessment Features	163
<u>Restart an Compliance Manager Assessment before it is Complete</u>	163

<u>Completing Assessment Worksheets and Surveys</u>	165
Attach Supporting Documents	168
Select Multiple Fields	169
Copy and Paste Responses	170
<u>Dynamic Guidance for Worksheets and Surveys in the RapidFire Tools Portal</u>	173
Download and Print Assessment Forms	175
<u>Re-use Previous Responses in Questionnaires</u>	176
Simple Form Entries	176
Tables and Checklists	176
Re-Use All Previous Responses	177
<u>Compliance Manager Assessment Files (Document Repository)</u>	178
Delete an Assessment File	179
<u>Invite Subject Matter Experts (SMEs) to Complete Forms</u>	180
Multiple Contributors and Locking Forms	182
Revoke (Un-Invite) SME Invitation	182
Manage SME Invites to Contribute to Questionnaires and Worksheets	183
<u>Project Roles in the CMMC Assessment</u>	186
Manage Portal Users and Access	187
<u>Manage Users (Global Level)</u>	187
Users and Global Access Roles	188
Add User at Global Level	189
Edit User at Global Level	192
<u>Set Up Portal Branding</u>	194
Set Custom Portal Theme	195
Set Custom Portal Subdomain	196
Set Custom Company Name	197
Set Custom Company Logo	198
<u>Set Up a Custom Subdomain to Access the RapidFire Tools Portal</u>	200
<u>Log Out of RapidFire Tools Portal</u>	202
<u>Compliance Manager Resources</u>	203
<u>Recover Forgotten Password</u>	204

<u>Change your Password</u>	206
Scans for Compliance Manager Assessments	207
<u>Compliance Manager Server Firewall Requirements</u>	207
<u>View Assessment Scan Status</u>	208
Important Notes for Scan Status	209
<u>Scan Schedules</u>	210
Scan Start Time	210
Scan Start Time Feature Impact on Compliance Manager Automated Scan Job Performance	211
Scan Start Time Chronology Example	211
Monthly Scans	212
Monthly Scan Requirements	213
<u>Manage Site Data Collectors</u>	214
Data Collector Commands	215
<u>Run CMMC Local Data Collector</u>	218
How to Upload the Local Scan Files	221
<u>Local Computer Scans</u>	222
Local Computer Scanning Dependencies and Recommendations	222
Scanning Process and Scanning Surface Area	222
Computer Resource Related	222
Scan Interference Factors	223
Recommendations to Improve Local Computer Scan Performance	223
Quick Local Computer Scans	223
Deep Local Computer Scans	223
<u>Performing Scans on Mac and Linux Computers</u>	225
<u>Integration with VSA Agents for Local Data Collection (Compliance Manager)</u>	226
Purpose	226
Requirements	226
Step 1: Download ZIP file from Kaseya Automation Exchange	226
Step 2: Upload the Compliance Manager Resources to Files to VSA	227
Step 3: Import Kaseya VSA Procedures for Compliance Manager local scans	229

Step 4: Executing Local Data Procedures	230
Step 5: Verifying successful Collection	232
Import RMM Connector Scans	233
Appendices	235
<u>Configuring Report Preferences</u>	<u>238</u>
Set Reports Text Preferences	240
Set Reports Logo Preferences	241
Set Themes Preferences	242
Access Updated Report Styles	243
Set Reports Cover Images Preferences	244
Set Company Information Preferences	245
Use Network Detective to Add Your MSP Name to Report Headers	245
<u>Upgrade your Site License (MSPs Only)</u>	<u>247</u>
Site License Options	248
Account-wide License Options (MSP and SMB)	248
<u>Enable BMS Contract Updates for Compliance Manager GRC</u>	<u>250</u>
Step 1 — Gather Credentials for Kaseya BMS	250
Step 2 — Set Up a Connection to your Kaseya BMS	251
Step 3 — Map your Compliance Manager's Site to a Kaseya BMS Connection	256
Step 4 — Enable BMS Billing Integration from Site	257
<u>Delete a Site</u>	<u>264</u>
<u>Set Time Zone</u>	<u>265</u>
<u>Admin Alerts (RapidFire Tools Portal)</u>	<u>266</u>
Admin Alerts: Global Settings vs. Site Settings	266
Configure Admin Alerts	266
<u>Audit Log</u>	<u>268</u>
Compliance Manager Audit Log Details	268
Examples of Audit Log Entries	269
Creation of To Do Task Items	269
Automated Scanning Start and Completion Activity	269
Assessment Questionnaire and Worksheet Form Access and Modification Activity	270

<u>CMMC To Do Task Complete List</u>	270
<u>Import Worksheet Attachments from ITGlue</u>	275
<u>Augment Antivirus Verification Worksheets to Detect Antivirus Apps</u>	280
Step 1 — Augment Reports in Network Detective	280
Step 2 — Generate Antivirus Verification Worksheet	282
<u>License Usage (Global Settings)</u>	284

About Compliance Manager for CMMC

The **Cybersecurity Maturity Model Certification** (CMMC) presents a standard for achieving cybersecurity for companies that comprise the defense industrial base (DIB). The United States Department of Defense (DoD) formulated the CMMC to improve the cyber-security posture of the DIB supply-chain.

Compliance Manager for CMMC combines automated data collection with a structured framework for collecting supplemental assessment information not available through automated tools.

It is the first solution to allow for the automatic generation of the key documents that are necessary to demonstrate compliance with the CMMC framework. More than just documents to satisfy a compliance requirement, Compliance Manager provides factual evidence, expert advice, and direction to minimize or eliminate the risk of a data breach.

You can compare Compliance Manager for CMMC to getting a medical exam. Compliance Manager automates the 'lab tests' for the technology environment. It includes interview and survey features to gather information manually. In addition, it provides a recommended treatment plan.

You can learn more about the CMMC model at: <https://www.acq.osd.mil/cmmc/index.html>.

Introduction to Compliance Manager for CMMC

This section covers everything you need to know before getting started with your CMMC Assessment.

Compliance Manager for CMMC Assessment Overview

Compliance Manager for CMMC combines 1) automated data collection with 2) a structured framework for collecting supplemental assessment information through surveys and worksheets. To perform a CMMC Assessment, you will:

- Access and log in to the RapidFire Tools Portal
- Create a site and set up a project
- Install the Compliance Manager server on the target network
- Collect data from the target network using the Portal's guided To Do List
- Generate CMMC Assessment reports and documentation

Project Roles

Compliance Manager helps you complete your assessment by presenting you with a guided To Do list. Tasks within the To Do list are assigned to one of four user **Roles** within the assessment project. Portal users can be assigned several different Site **Roles**. These are:

- **Site Administrator:** Performs initial project setup; creates Users and adds them to the appropriate project Roles; has access to all Site Settings
- **Technician:** Installs the scan server on the target network; configures the scan server with the correct scan settings; initiates automated network scans
- **Internal Auditor:** Performs the compliance assessment using the Portal; completes worksheets and forms to prepare compliance documentation
- **Subject Matter Expert:** (Optional) Contributes to worksheets and surveys. *Can only view and edit forms.*

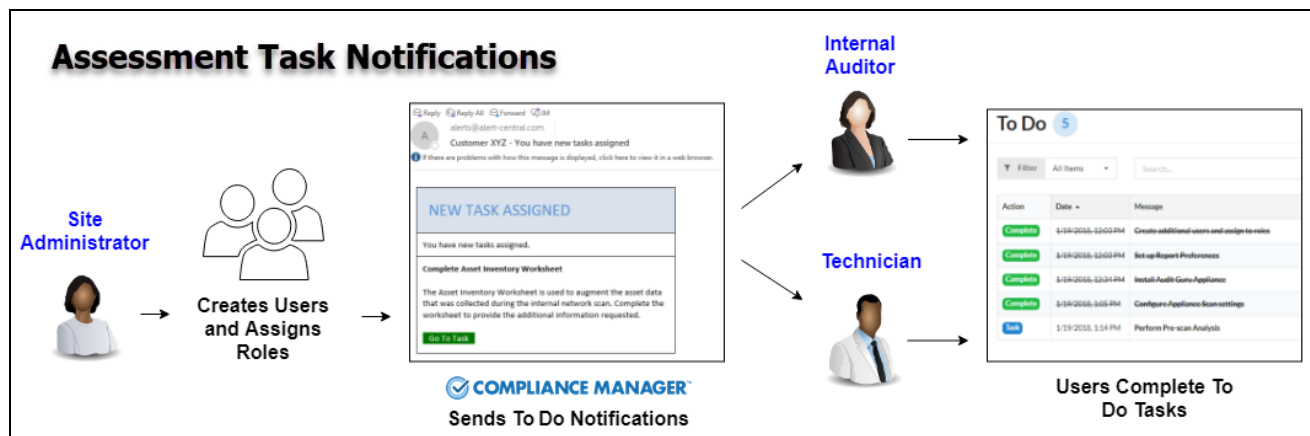
Important: Do not assign the SME role to users with other role assignments. Doing so will limit their access to the portal.

Tip: For a more detailed breakdown of project roles, see ["Project Roles in the CMMC Assessment"](#) on page 186.

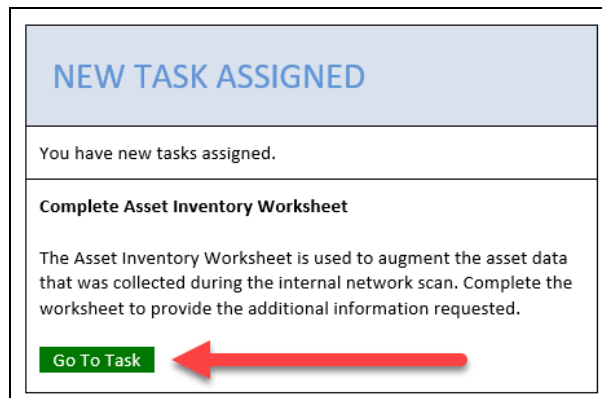
Notifications for Assessment To Do Tasks

Compliance Manager for CMMC sends your team automatic email notifications when new tasks need to be completed to advance the CMMC Assessment.

For example, when Compliance Manager completes an automated scan, the assessment team will receive email notifications for new tasks based on the results of the scan, such as completing worksheets or identifying false positives.



To respond to a task notification, open the email and click **Go to Task**. The RapidFire Tools Portal will open in a browser and you will receive additional instructions. This user guide also provides detailed instructions for completing each assessment task.



Note: In order for your team to receive notifications, you must assign them to Roles within the assessment from the **[Site] > Home > Roles** page. The user will then receive notifications for their assigned role at their email address.

Compliance Manager directs you to add users and assign roles as part of the guided assessment process. But you can visit the **[Site] > Home > Roles** page to configure users and assessment roles at any time. See also [Setting Up and Starting your CMMC Assessment Project](#).

For a list of assessment tasks and their assignees by role, see [CMMC To Do Task Complete List](#).

What You Will Need

In order to perform a CMMC Assessment, you will need the following components:

CMMC Assessment Component	Description
Rapid Fire Tools Portal	<p>The Rapid Fire Tools Portal allows you to create sites to manage your CMMC assessments for specific clients. Use the convenient To Do list to guide you through each task within the assessment.</p> <p>You can access the Rapid Fire Tools Portal at https://www.youritportal.com.</p>
Compliance Manager Server	<p>The technician will install the Compliance Manager server on the target network.</p> <p>You can download the server Installer at this link.</p>
Network Information and Credentials	<p>You will need to have administrative credentials to access network components. In addition, you will need some basic network information, such as internal and external IP addresses and IP addresses for specific machines (such as the Domain Controller in Windows Active Directory environments).</p> <p>See "Network Prerequisites for Assessment Scans" on page 16 for more details.</p>
CMMC Data Collector	<p>The CMMC Data Collector is used on computers that cannot be accessed by the Compliance Manager server. Use the data collector to scan computers locally and upload scan files into the assessment. This is useful for scanning computers that are not connected to the network or domain, for example.</p> <p>You can download the CMMC Data Collector at this link.</p>
Surveys and Worksheets	<p>Surveys and worksheets contain questions that require investigation outside of an automated scan. You create and manage these documents directly from the RapidFire Tools Portal, where you can also invite SMEs</p>

CMMC Assessment Component	Description
	to contribute.



Network Prerequisites for Assessment Scans

For a successful network scan:

1. **ENSURE ALL NETWORK ENDPOINTS ARE TURNED ON THROUGHOUT THE DURATION OF THE SCAN.** This includes PCs and servers. The scan can last several hours.
2. **CONFIGURE THE TARGET NETWORK TO ALLOW FOR SUCCESSFUL SCANS ON ALL NETWORK ENDPOINTS.** See ["Pre-Scan Network Configuration Checklist" on page 20](#) for configuration guidance for both Windows Active Directory and Workgroup environments.
3. **GATHER THE INFORMATION BELOW TO CONFIGURE YOUR SCANS FOR THE CLIENT SITE.** Work with the project Technician and/or your IT admin on site to collect the following:
 - **Admin network credentials** that have rights to use WMI, ADMIN\$, and File and Printer Sharing on the target network.
 - **Internal IP range** information to be used when performing internal scans.

Note: Compliance Manager will automatically suggest an IP range to scan on the network. However, you may wish to override this or exclude certain IP addresses.

- **External IP addresses** for the organisation to be used when setting up External Vulnerability Scans.
- **RapidFire Tools Portal User Credentials**
- For Windows Active Directory environments, you will need admin credentials to connect to the Domain Controller, as well as the name/IP address of the domain controller.
- For Windows Workgroup network environments, a list of the Computers to be included in the Assessment and the Local Admin Credentials for each computer.

Automated Scans Performed During the CMMC Assessment Process

The CMMC Assessment consists of the following scans:

- **Internal Network Scan** (*automated*)
- **External Vulnerability Scan** (*automated*)
- **Local Computer Scans** (*optional; performed manually*)

Important: See "[Local Computer Scans](#)" on page 222 for more details, including requirements for a successful local computer scan.


- **Personal Data Scan** (*automated*)

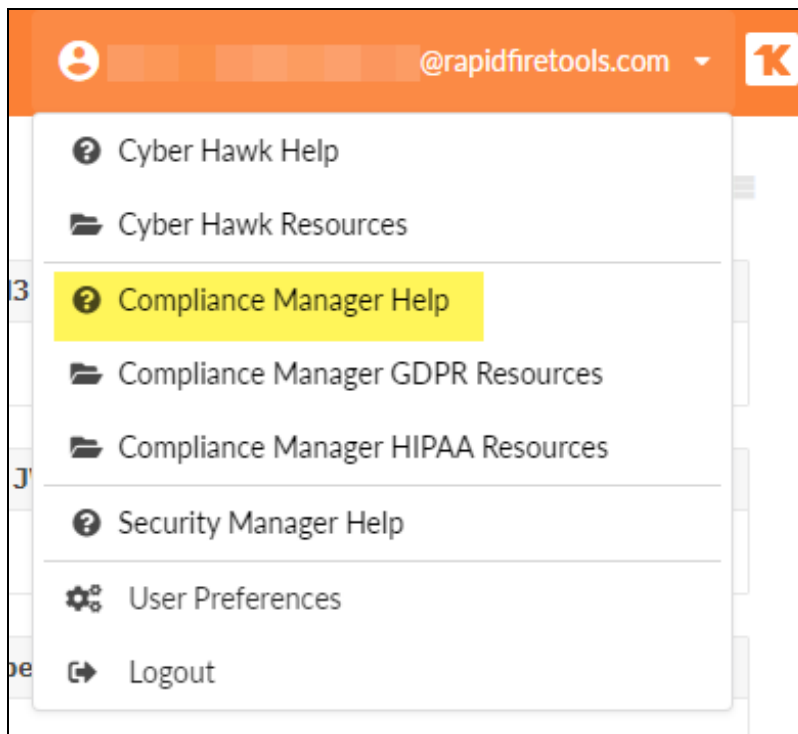
Compliance Manager for CMMC makes use of multiple technologies/approaches for collecting information on the client network, including:

- Network Scan
- Active Directory
- WMI
- Remote Registry
- ICMP
- File System Scanning
- Windows Registry
- Windows Shares and Permissions
- Security Center

Compliance Manager Online Help

The contents of this user guide are also available online, where you can search for specific topics. To access the online help system for Compliance Manager:

1. Log into the RapidFire Tools Portal with your credentials.
2. From the portal, click the user icon  in the top right hand corner of the screen.
3. Click **Compliance Manager Help**.



4. The Compliance Manager Online Help system will appear. Use the search function

to find a particular topic, or browse the table of contents.



Note: You can access the Online Help system directly here: <https://www.rapidfiretools.com/cm/cmonlinehelp>.

Pre-Scan Network Configuration Checklist

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

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

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

Checklist for Domain Environments

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

Complete	Domain Configuration
GPO Configuration for Windows Firewall (Inbound Rules)	
<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"> • Windows Management Instrumentation (ASync-In) • Windows Management Instrumentation (WMI-In) • Windows Management Instrumentation (DCOM-In)
<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"> • File and Printer Sharing (NB-Name-In) • File and Printer Sharing (SMB-In) • File and Printer Sharing (NB-Session-In)
<input type="checkbox"/>	<p>Enable <i>Remote Registry</i> “read only” access on computers targeted for scanning.</p>

Complete	Domain Configuration
	<div data-bbox="427 296 1382 405" style="border: 1px solid #0070C0; padding: 5px;"> Note: Remote Registry access should be restricted for use by the user access account credentials to be used during network and local computer scan. </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"> • operating a Kaseya-RapidFire Tools product network data collector to issue ICMP echo request messages to be sent to Windows computers and network devices • to send ICMP echo reply messages in response to an ICMP echo request <div data-bbox="427 863 1382 972" style="border: 1px solid #0070C0; padding: 5px;"> Note: ICMP requests are used to detect active Windows computers and network devices to scan. </div>
GPO Configuration for Windows Services	
<input type="checkbox"/>	<p><i>Windows Management Instrumentation (WMI)</i></p> <ul style="list-style-type: none"> • Startup Type: Automatic
<input type="checkbox"/>	<p><i>Windows Update Service</i></p> <ul style="list-style-type: none"> • Startup Type: Automatic
<input type="checkbox"/>	<p><i>Remote Registry</i></p> <ul style="list-style-type: none"> • Startup Type: Automatic
<input type="checkbox"/>	<p><i>Remote Procedure Call</i></p> <ul style="list-style-type: none"> • Startup Type: Automatic
Network Shares	
<input type="checkbox"/>	<ul style="list-style-type: none"> • <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)

Complete	Domain Configuration
3rd Party Firewalls	
<input type="checkbox"/>	<ul style="list-style-type: none"> • Ensure that 3rd party Firewalls are configured similarly to Windows Firewall rules described within this checklist. <div> Note: This is a requirement for both Active Directory and Workgroup Networks. </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
	Network Settings
<input type="checkbox"/>	<ul style="list-style-type: none"> • <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
<input type="checkbox"/>	<ul style="list-style-type: none"> • <i>File and printer sharing</i> must be enabled on the computers you wish to scan
<input type="checkbox"/>	<ul style="list-style-type: none"> • <i>Ensure the Windows Services below are running and allowed to communicate through Windows Firewall:</i> <ul style="list-style-type: none"> • Windows Management Instrumentation (WMI) • Windows Update Service • Remote Registry • Remote Desktop • Remote Procedure Call
<input type="checkbox"/>	<ul style="list-style-type: none"> • Workgroup computer administrator user account credentials. <div> <p>Note: Before configuring scan settings for workgroups, prepare a list of the workgroup computer(s) administrator user account credentials for entry into the scan settings wizard.</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">operating a Kaseya-RapidFire Tools product network data collector to issue ICMP echo request messages to be sent to Windows computers and network devicesto send ICMP echo reply messages in response to an ICMP echo request <div data-bbox="443 491 1325 600">Note: ICMP requests are used to detect active Windows computers and network devices to scan.</div>

Setting Up and Starting your CMMC Assessment Project

This topic covers starting a first new CMMC Assessment. Before you begin your CMMC Assessment, you will need to complete a few basic tasks to set up the project. These items will be completed by the Technician and Internal Auditor user roles. See more information on Project Roles, see ["Project Roles in the CMMC Assessment" on page 186](#).

Add Organizations

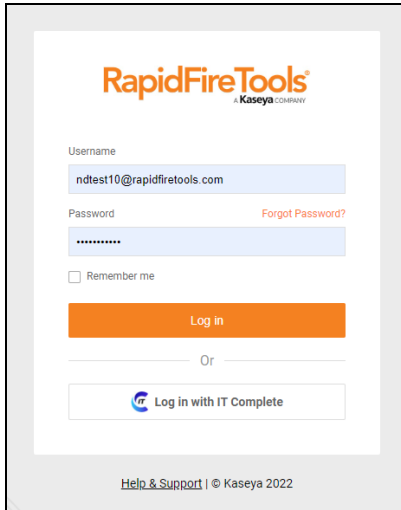
Before you begin your first IT or compliance assessment, you can optionally create an **organization**. Think of an organization as a folder in which you can store assessment projects for a particular client. For example, if a client has multiple sites or distinct networks that you want to assess individually, use an organization to keep these client sites in one neat container.

Tip: Much like folders in Windows Explorer, you can create multiple Organizations and can move your sites between them.

Add an Organization

To add an Organization:

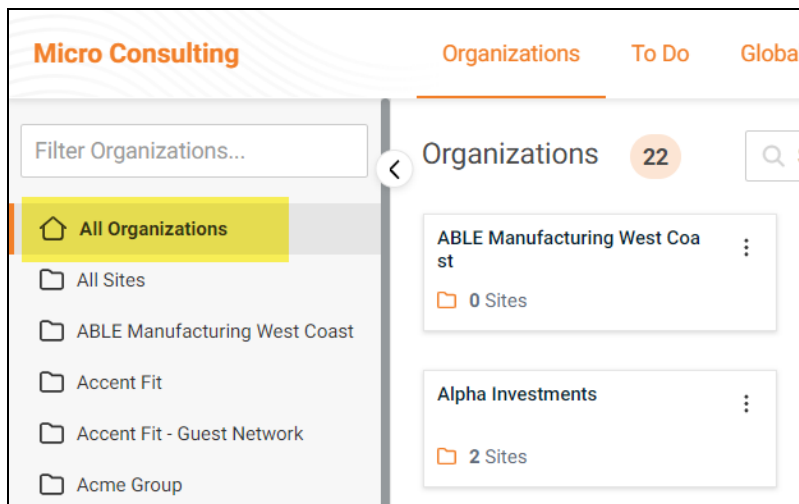
1. Access the RapidFire Tools Portal at <https://www.youritportal.com> and log in with your credentials.



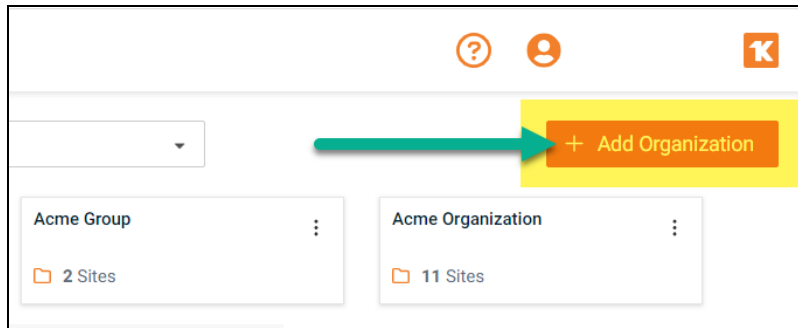
The image shows the login page for RapidFireTools, a Kaseya company. It features a white login form centered on a light gray background. The form includes a 'Username' field with the text 'ndtest10@rapidfiretools.com', a 'Password' field with masked characters, a 'Remember me' checkbox, and a 'Log in' button. Below the 'Log in' button is an 'Or' separator and a 'Log in with IT Complete' button. At the bottom of the form is a link for 'Help & Support' and a copyright notice for Kaseya 2022.

Note: You can also log in with your IT Complete credentials. See [Enable Log In with IT Complete](#).

2. Access the **Organizations** page from the top-menu. Select **All Organizations** from the side menu.

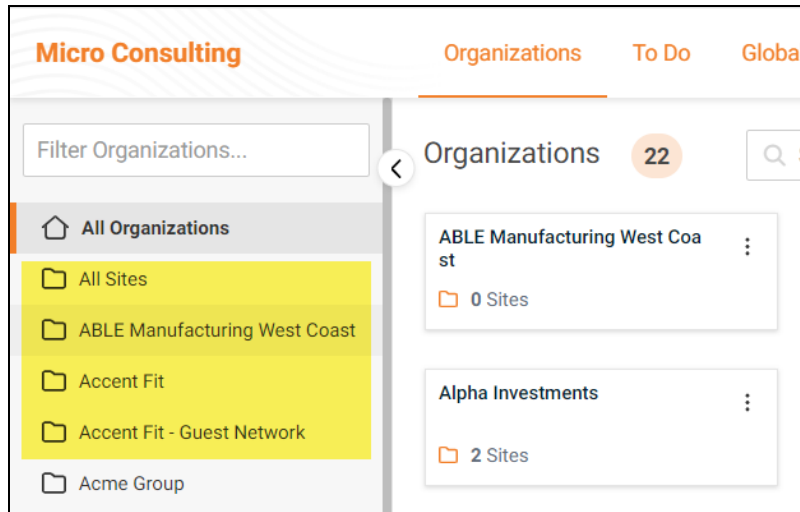



3. Then click **Add Organization**.

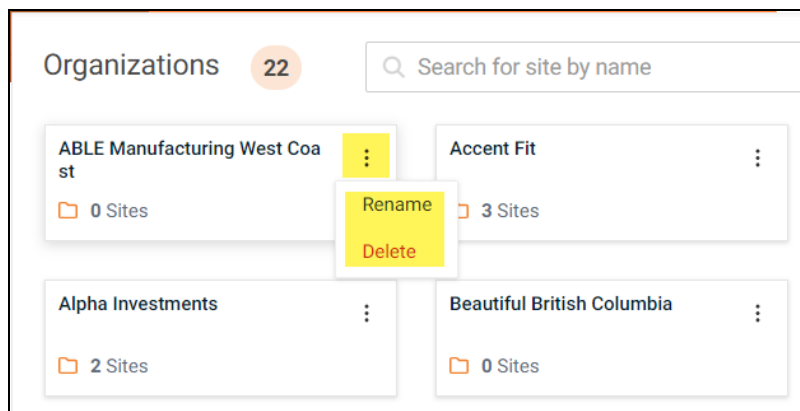


4. Enter an Organization name. For example, this might be the name of a large company for whom you want to create multiple sites and types of IT and compliance assessments. Then click **Confirm**.

5. You can see each organization you've created from the left-side menu.



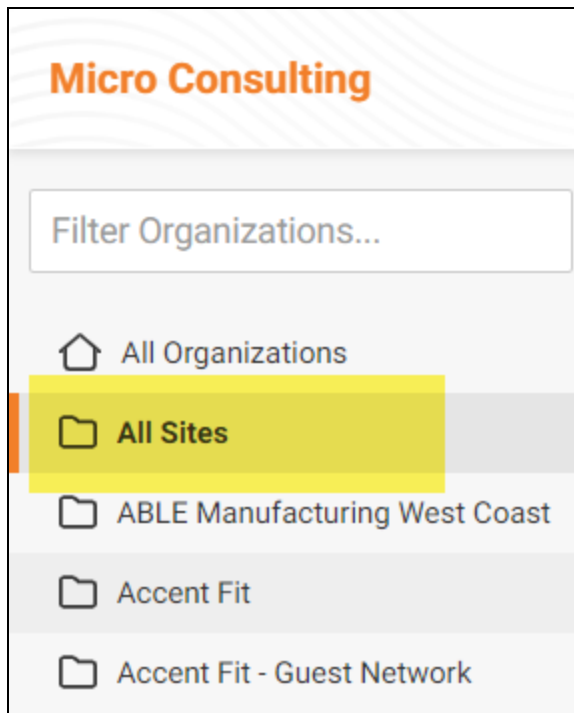
6. From the  button you can rename or delete the Organization. You can also see the number of sites grouped under the Organization.



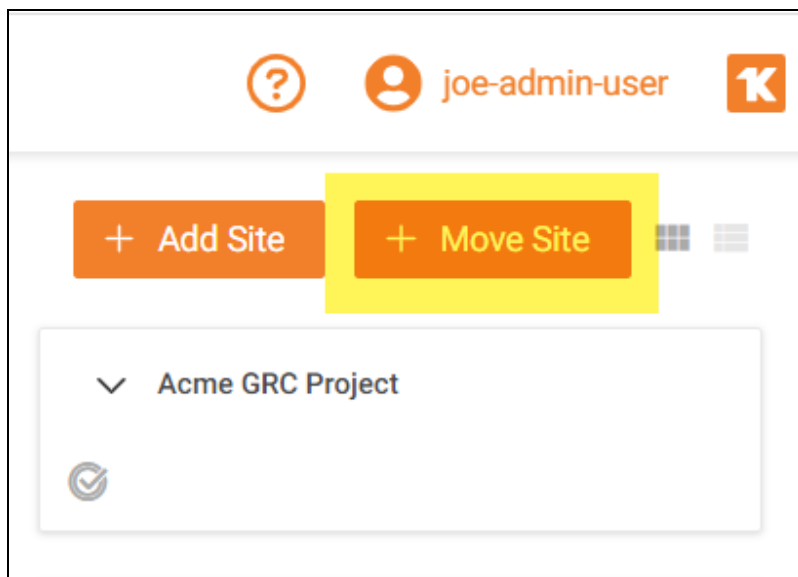
Move a Site to an Organization

To move a site to an organization:

1. From **Organizations**, choose **All Sites** or another specific organization.



2. Click **Move Site**.



- From the Moves Sites menu, select an **Origin Organization** from the drop-down menu. Sites without an organization will be listed under **Unassigned Sites**. Select the sites you want to move. Under **Move to Organization**, select the destination from the drop-down menu. Then click **Move** and confirm your selection.

Move Site(s)

Origin Organization
Select one or more sites under an Organization and move to another Organization from the list on the right.

Accent Fit

- ☐ Example ND Pro Site
- ☒ New Velocity
- ☒ Probable Partners

Move to Organization
Select an Organization from the list to move selected site(s).

Acme Organization

Cancel Move

Move Site(s)

Origin Organization

Accent Fit

- New Velocity
- Probable Partners

Move to Organization

Acme Organization

Back Confirm Move

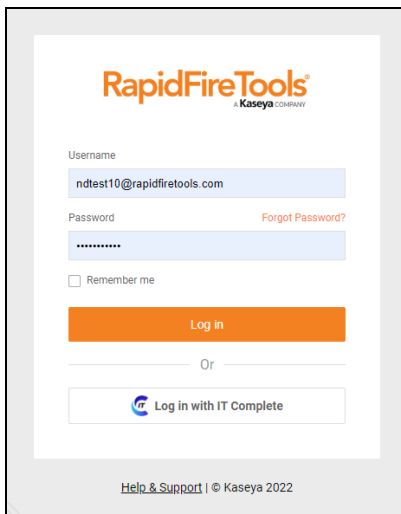
- The selected sites will be moved to the chosen organization.

Create a New Site

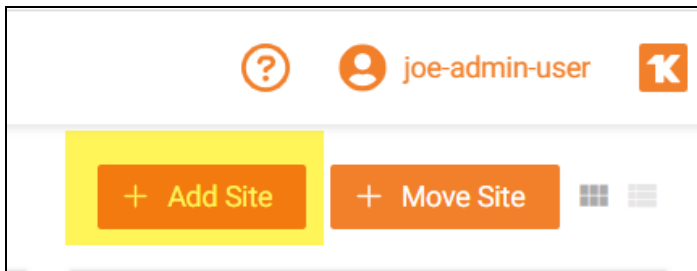
Tip: We recommend you get started by making a "practice site" and running your first assessment in-house. Use this to familiarise yourself with Compliance Manager and the installation and configuration process.

The first step in performing a CMMC Assessment is creating a "Site". Sites help you organise your assessments. This task is performed by the Site Administrator. To create a site:

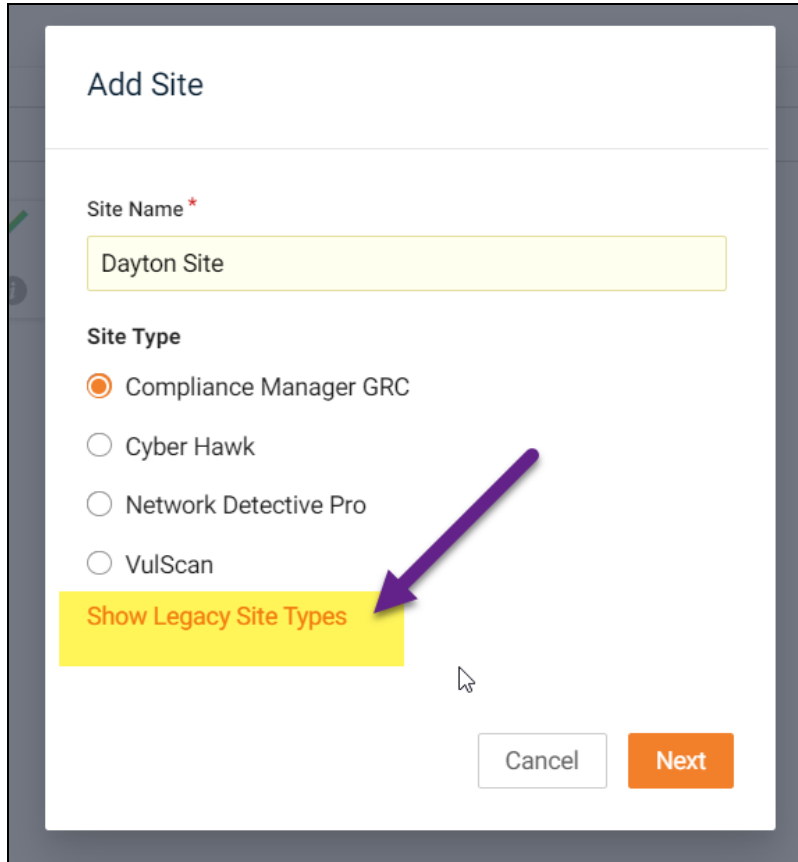
1. Access the RapidFire Tools Portal at <https://www.youritportal.com> and log in with your credentials.

The image shows the login page for RapidFireTools, a Kaseya company. The page has a white background with a light gray border. At the top, the "RapidFireTools" logo is displayed in orange, with "a Kaseya COMPANY" in smaller text below it. Below the logo, there are two input fields: "Username" with the text "ndtest10@rapidfiretools.com" and "Password" with masked characters "*****". A "Forgot Password?" link is to the right of the password field. Below the password field is a checkbox labeled "Remember me". A large orange "Log in" button is centered below the inputs. Below the button is a horizontal line with the word "Or" in the center. Underneath is a button with the "IT Complete" logo and the text "Log in with IT Complete". At the bottom, there is a link for "Help & Support" and a copyright notice "© Kaseya 2022".

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



3. Enter a **Site Name**. This can be the name of the client for whom the assessment is being performed, for example.
4. Under **Site Type**, select **Show Legacy Site Types**.



Add Site

Site Name *

Dayton Site

Site Type

☒ Compliance Manager GRC

☐ Cyber Hawk

☐ Network Detective Pro

☐ VulScan

Show Legacy Site Types

Cancel Next

5. Select **Compliance Manager (Legacy)** and then select your assessment type.
 - If you wish to perform a EU GDPR assessment, select **EU GDPR**.
 - If you wish to perform a UK GDPR assessment, select **UK GDPR**.
 - If you wish to perform a HIPAA assessment, select **HIPAA**.
 - If you wish to perform a Cyber Insurance assessment, select **Cyber Insurance**.
 - If you wish to perform a NIST CSF assessment, select **NIST**.
 - If you wish to perform a CMMC/NIST 800-171 assessment, select **CMMC/NIST 800-171**.

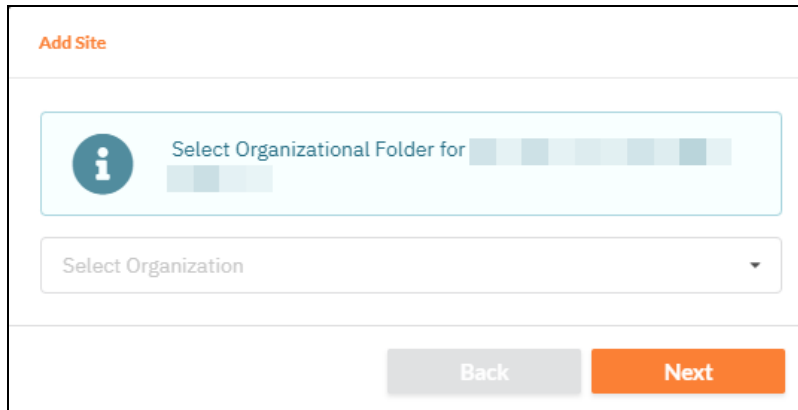
Add Site

Site Type

- ☐ Compliance Manager GRC
- ☐ Cyber Hawk
- ☐ Network Detective Pro
- ☐ VulScan
- ☒ Compliance Manager (Legacy)

- ☐ EU GDPR
- ☐ UK GDPR
- ☐ HIPAA
- ☐ Cyber Insurance
- ☐ NIST CSF
- ☐ CMMC / NIST 800-171

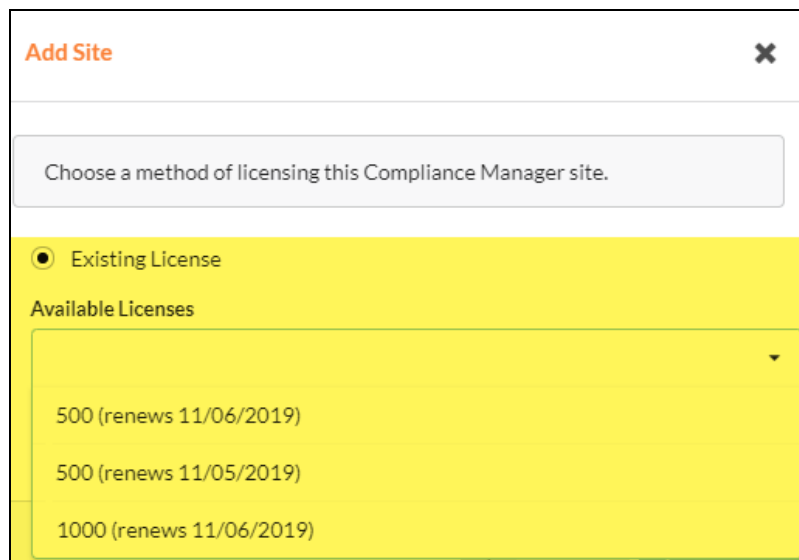
6. Click **Next**. Select an **Organization Folder** for the new site.



The screenshot shows a web form titled "Add Site". It contains a light blue box with an information icon and the text "Select Organizational Folder for" followed by a series of colored squares. Below this is a dropdown menu labeled "Select Organization". At the bottom are "Back" and "Next" buttons.

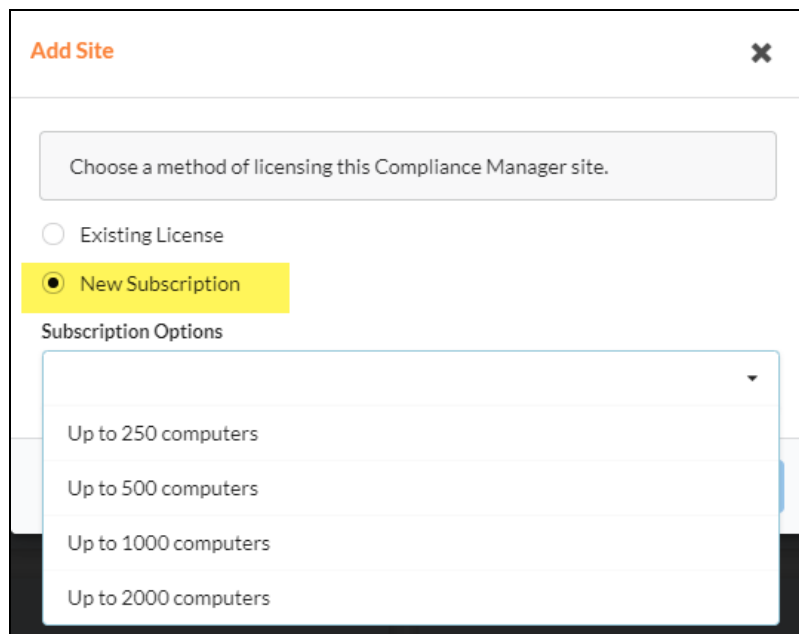
7. Select a subscription option (MSP only). You can choose to:

- a. Use an **Existing License** you have purchased previously. Select the existing license from the drop-down menu and click **Next**.



The screenshot shows the "Add Site" form with a close button (X) in the top right. A message box says "Choose a method of licensing this Compliance Manager site." Below this, the "Existing License" option is selected with a radio button. Under "Available Licenses", a dropdown menu is open showing three options: "500 (renews 11/06/2019)", "500 (renews 11/05/2019)", and "1000 (renews 11/06/2019)".

- b. Create a **New Subscription**. Select the subscription option from the drop-down menu and click **Next**.



Add Site [X]

Choose a method of licensing this Compliance Manager site.

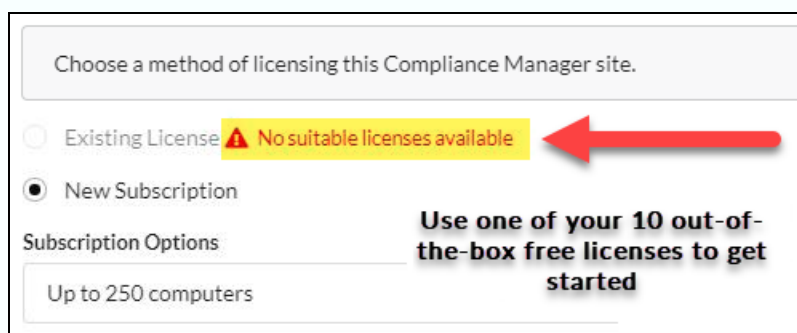
☐ Existing License

☒ **New Subscription**

Subscription Options

- Up to 250 computers
- Up to 500 computers
- Up to 1000 computers
- Up to 2000 computers

Note: You have **10 FREE** Site licenses as part of your initial Compliance Manager subscription. Each of these licenses can cover a site with up to 250 computers. *Select one of these free licenses for use with your first 10 new Sites.* We suggest that you use 1 of the 10 licenses for your own internal use, such as familiarizing yourself with the product and assessment processes.



Choose a method of licensing this Compliance Manager site.

☐ Existing License **⚠ No suitable licenses available**

☒ New Subscription

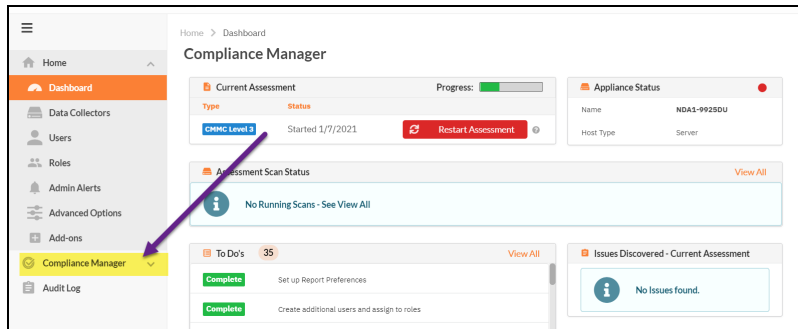
Subscription Options

- Up to 250 computers

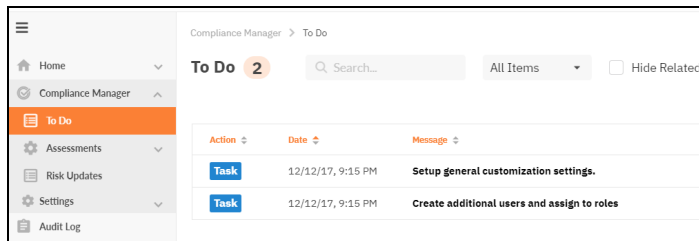
Use one of your 10 out-of-the-box free licenses to get started

If you wish to purchase additional licenses or upgrade to a higher license (500 and above), you will be billed extra. Contact your Sales Representative for more details.

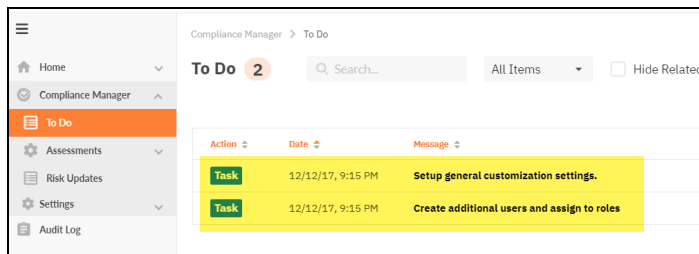
8. The Site Home page will appear. Click the **Compliance Manager** tab.



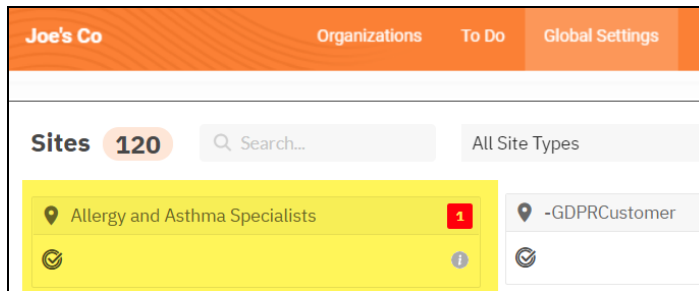
The Site To Do page will appear.



Two new **To Do** items will also appear in the Site's To Do list.

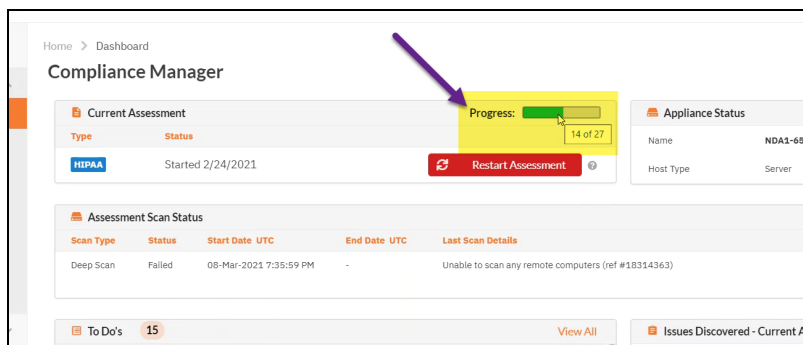


The new site will be added to the Sites home page in the RapidFire Tools Portal.



Assessment Progress Bar

From the Site Dashboard, you can view a progress bar for your assessment. This progress bar is advanced when you complete assessment tasks.

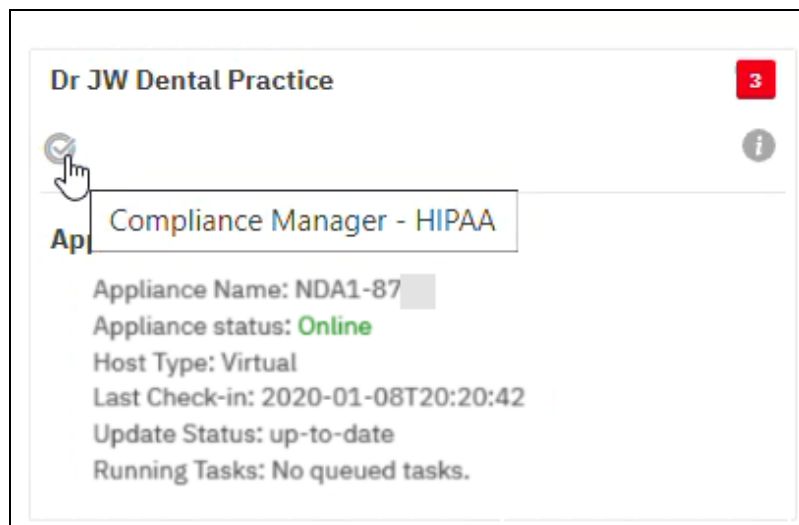


If you hover over the progress, you can see the number of To Do items remaining in the assessment. This number is based on the total steps in the assessment, rather than the current To Do list. Once all To Do items are completed, the Progress Bar will be removed from the Current Assessment panel in the Compliance Manager Dashboard.

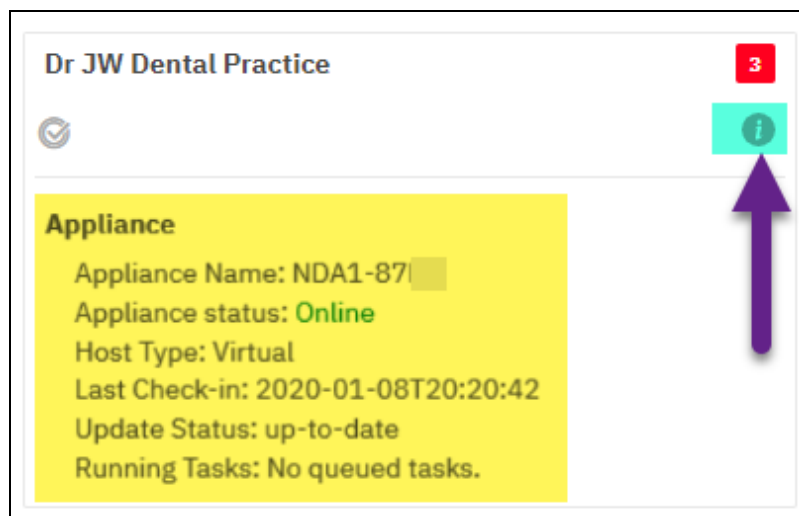
View Site Details

From the Sites page, you can quickly view the details for any Site. To do this:

1. To see which assessment is active at the Site, **hover over the Compliance Manager icon**:



2. Likewise, you can click the "i" icon to review the status of the Site's appliance:



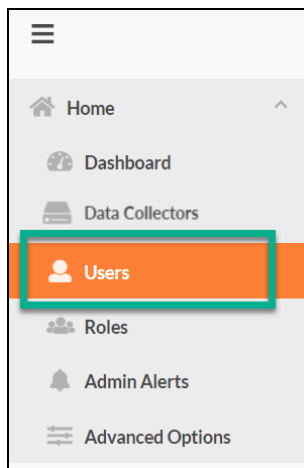
Task 1: Create additional users and assign to roles

Your CMMC Assessment has several roles: these include **Site Administrator**, **Technician**, **Internal Auditor**, and (optional) **Subject Matter Expert (SME)**. Each role performs different tasks within the assessment.

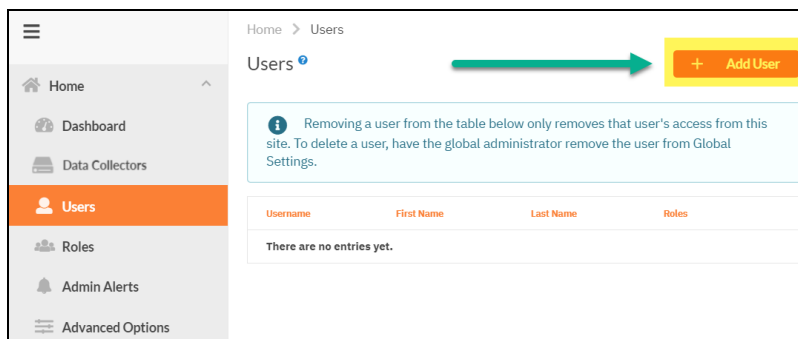
Tip: Before you begin the assessment, you will need to assign users to each role except the optional SME role. This allows users to be assigned assessment tasks within their To Do list and email notifications.

This task is performed by the Site Administrator. To assign users to project roles:

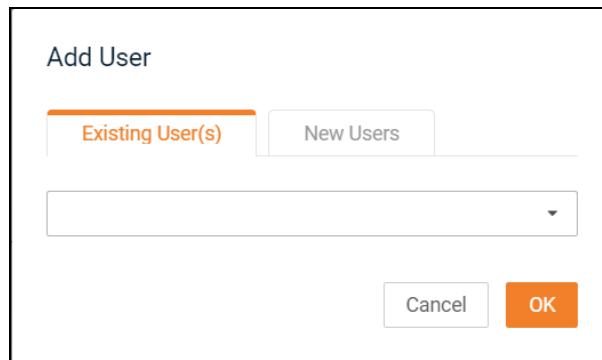
1. From the Home page for your Site, click **Users**.



2. Click **Add User**.



- i. Add **Existing Users(s)** by searching for their user name within the drop-down menu.

A dialog box titled "Add User" with two tabs: "Existing User(s)" (selected) and "New Users". Below the tabs is a text input field with a dropdown arrow. At the bottom are "Cancel" and "OK" buttons.

Add User

Existing User(s) New Users

Cancel OK

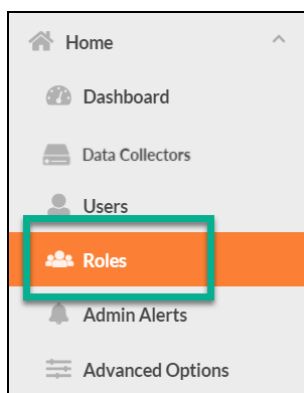
- ii. Alternatively, you can create a **New User** account to provide individuals access to the Portal and assessment process. You will need to enter an email address, first and last name, and password for each user. The email address you enter is where the user will receive To Do Notifications from Compliance Manager.

Important: Send new users their login credentials after you add them to the site.

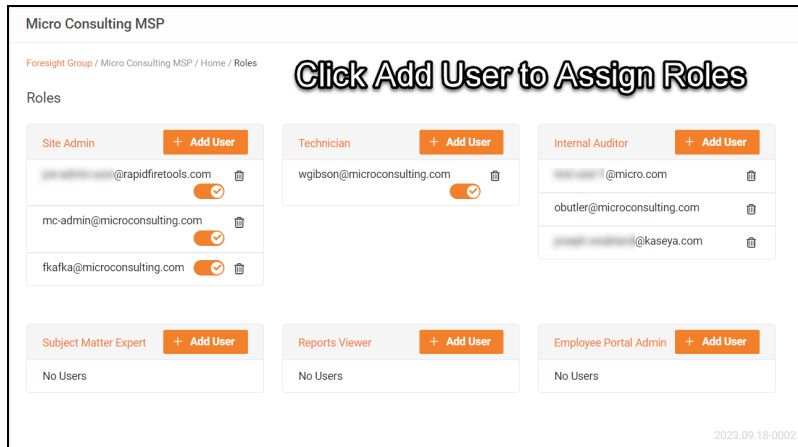
- iii. Click **Add** to add the user to the site.

Next you will associate these new users with your CMMC Assessment Site. To do this:

3. From the Home tab side menu, click **Roles**.

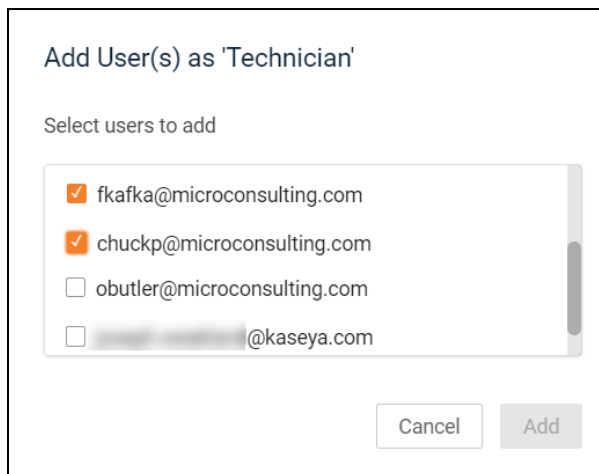


4. Next to each role, click **Add User** to assign users to the **Technician**, **Internal Auditor**, and (optional) **Subject Matter Expert (SME)** roles. The users assigned to these roles will receive assessment task notifications for that role.



5. Select each user you wish to assign to the role. Then click **Add**.

Note: Before you can assign a user a Role, you must first create that user and/or associate them with your Site.



Important: Do not assign the SME role to users with other role assignments. Doing so will limit their access to the portal.

6. When you have finished adding users to your site and assigning roles, click **Mark Complete** on the task To Do page.

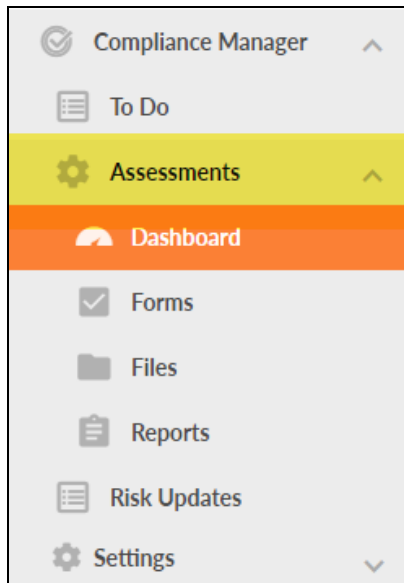


Important: Be sure to send the users their login credentials in order to access the RapidFire Tools Portal and begin working on assessment tasks.

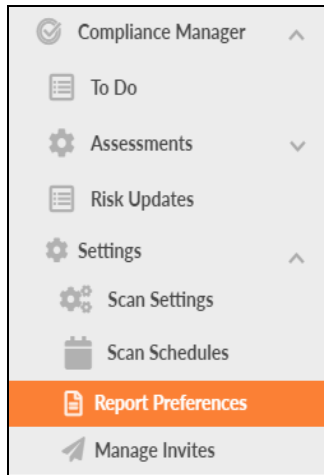
Task 2: Set up Report Preferences

Before you perform your first assessment using Compliance Manager for CMMC, you should configure the report generation tool to use your company's logos, color themes, and other details. This ensures your CMMC Assessment reports conform to your company's corporate branding and image standards.

1. From your Site Home Page, go to **Compliance Manager > Settings**.



Next, click **Report Preferences** to access the customization settings. This includes company information, images, and design elements for this site's reports.



2. Customize your reports. This includes company information, images, and design elements for this site's reports.

A screenshot of the 'Report Preferences' configuration page. The breadcrumb trail at the top reads 'Compliance Manager GRC / Settings / Report Preferences'. The page title is 'Report Preferences'. Below the title are four tabs: 'Text' (selected and underlined in orange), 'My Logo', 'Theme', and 'Cover Image'. The 'Text' tab contains a form with the following fields:

- 'Report Prepared For:' with the value 'Advent Technologies'.
- 'Report Prepared By:' with the value 'Micro Consulting'.
- 'Footer:' with the value 'PROPRIETARY & CONFIDENTIAL'.
- 'Cover Page Disclaimer:' with a text area containing the text: 'CONFIDENTIALITY NOTE: The information contained in this report d of the client specified above and may contain confidential, privileged information. If the recipient of this report is not the client or address prohibited from reading, photocopying, distributing or otherwise usir any way.'

You can also Select Target Language for Assessment Reports. **LANGUAGES OTHER THAN ENGLISH ARE ONLY AVAILABLE FOR COMPLIANCE MANAGER FOR EU GDPR.**

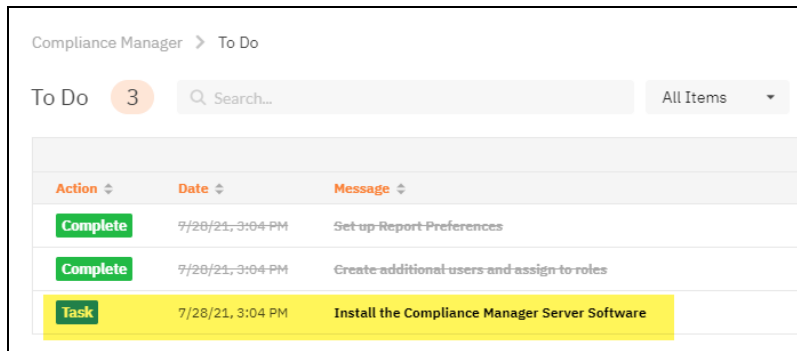
3. Once you finish configuring Report Preferences, return to the item in the To Do list and click **Mark Complete**. Do this each time you complete a task in the To Do list.



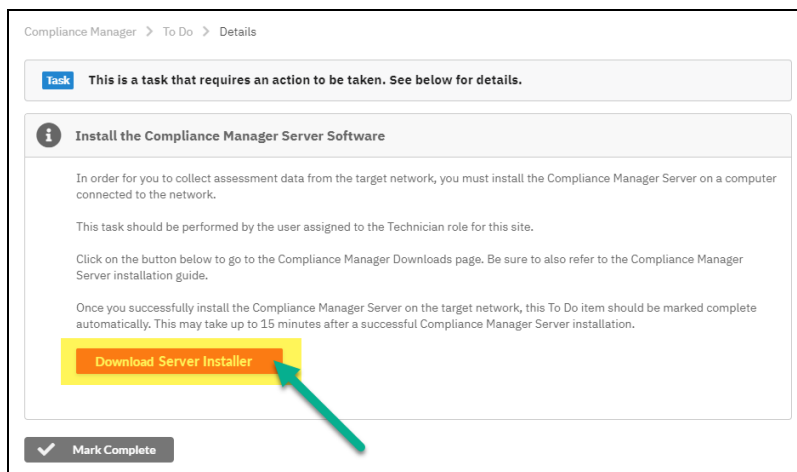
Note: For more details and instructions on how you can customize your reports, see ["Configuring Report Preferences" on page 238](#).

Task 3: Install Server

Install the **Compliance Manager Server** on the target network. *This task is performed by the Technician.* The Server collects data and performs automated scans within the assessment environment.



Click **Download Server Installer** to visit <https://www.rapidfiretools.com/cm>. Refer to the separate **Compliance Manager Server Installation Guide** for more detailed instructions.

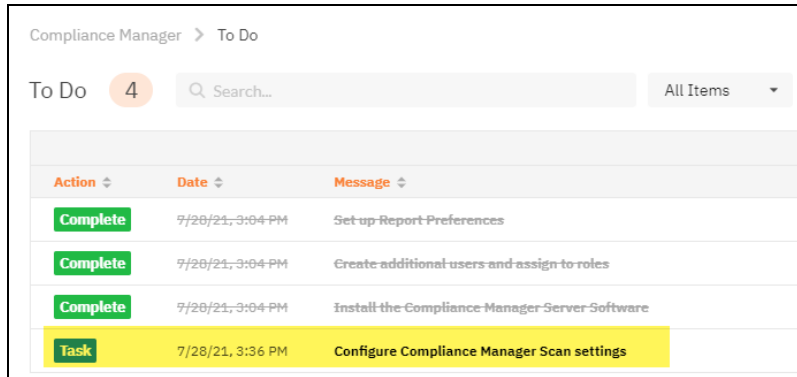


Important: You can only install **one** RapidFire Tools server/appliance on a PC or endpoint at a time. If you need to install multiple server(s)/appliance(s), install each one on a separate endpoint on the network.

Note: Once you install the Server, this To Do item will automatically be marked complete. **This may take several minutes.**

Task 4: Configure Server Scan Settings

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

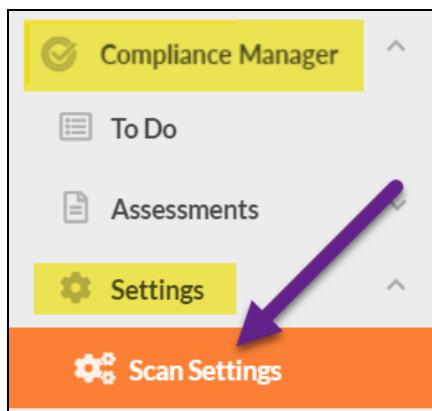


Compliance Manager > To Do		
To Do	4	Search...
All Items		
Action	Date	Message
Complete	7/28/21, 3:04 PM	Set up Report Preferences
Complete	7/28/21, 3:04 PM	Create additional users and assign to roles
Complete	7/28/21, 3:04 PM	Install the Compliance Manager Server Software
Task	7/28/21, 3:36 PM	Configure Compliance Manager Scan settings

- Look here to ["Configure Scan Settings for Active Directory Domain" below](#)
- Look here to ["Configure Scan Settings for Workgroup" on page 55](#)

Configure Scan Settings for Active Directory Domain

Set the **Scan Settings** from the [Your Site] > **Compliance Manager** > **Settings** > **Scan Settings** page. Complete all required prompts. This task is performed by the Technician.



Follow the steps below to configure the Scan Settings for the Compliance Manager Server:

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

Scan Type

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

☒ Active Directory domain

☐ Workgroup

→ Next Page

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

Merge Option

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

☒ Treat them as part of the primary domain

☐ Treat them as part of the specified workgroup

← Previous Page → Next Page

- a. Treat them as part of the primary domain
- b. Treat them as part of a specific workgroup by entering a workgroup name

Tip: Use this feature to tell Compliance Manager how to handle computers that are not connected to the domain. This will help those computers appear where you want them when you generate reports at the end of the assessment.

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

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

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

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

Scan Credentials

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

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

Username (domain\user):

Password:

Domain Controller:

[< Previous Page](#) [Next Page >](#)

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

Local Domains

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

☒ Gather Information for ALL the domains detected.

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

☐ test.performanceit.com

☐ Builtin

☐ Computers

☐ Domain Controllers

☐ ForeignSecurityPrincipals

☐ Keys

☐ Managed Service Accounts

☐ Program Data

☐ Microsoft

☐ System

☐ TEST

☐ Users

[< Previous Page](#) [Next Page >](#)

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

The screenshot shows the 'Additional Credentials' screen. At the top, there is a title 'Additional Credentials'. Below it, a grey box contains the text: 'Network scan credentials are required to perform remote Windows data collection via WMI and Remote Registry. Use this screen to optionally add additional credentials to be used during the scan. Calls using the default credentials will always be attempted first.' Below this, the section 'Network Scan Credentials' contains two input fields: 'Username:' with a placeholder 'username' and 'Password:' with a placeholder 'password'. Below these fields are two buttons: an orange '+ Add' button and a grey 'Remove Selected Entry' button. Below the buttons, there is a list of credentials, with the first one being 'test.performanceit.com\jwadmin (AD user to be used first)'. At the bottom of the screen, there are two navigation buttons: a grey '← Previous Page' button and an orange '→ Next Page' button.

7. The **IP Ranges** screen will then appear. The Compliance Manager server 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**.

YOU MUST ENTER AN IP RANGE TO PERFORM THE SCAN.

IP Ranges ?

Auto-Detected IP Ranges on Remote Appliance

10.

IP Ranges to Scan

Example IP Range Format: 192.168.0.0-192.168.0.255

Single IP or IP Range + Add

10.

Exclude IPs

Reset to Auto-Detected

Remove Selected Entry

Clear All Entries

← Previous Page → Next Page

From this screen you can also:

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

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

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

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

SNMP Information

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

+ add

public

Reset to Default Clear All Entries

Advanced SNMP Options

SNMP Timeout (seconds): Use Default

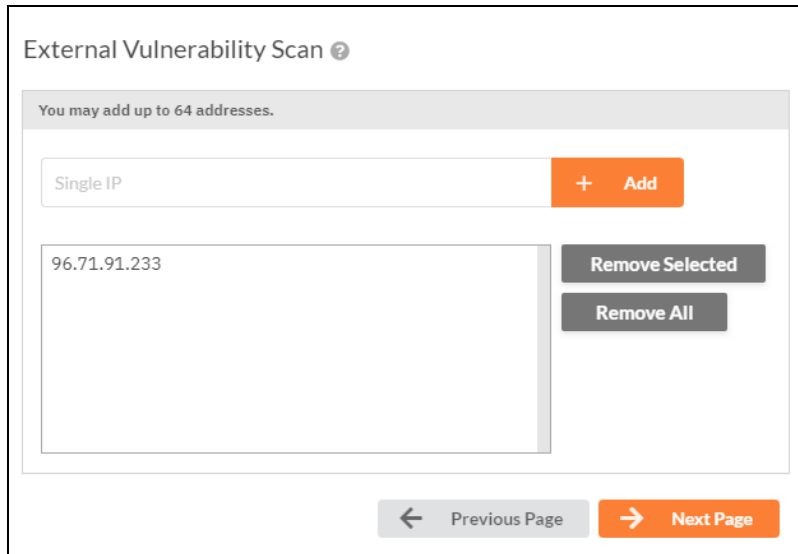
☐ Attempt SNMP against non-pingable devices (slower but more accurate)

← Previous Page Next Page →

9. Enter the IP addresses for the external vulnerability scan. Click **Next Page**.

Important: You must ensure that no other Network Detective or Compliance Manager products are being used to perform an External Vulnerability Scan on the same external IP Address range at the same time. Allow at least several hours between repeat external vulnerability scans. Scheduling external scans at the same time will result in reports with missing or incomplete data.

Note: IP ranges for the external vulnerability scan are not supported at this time. Please enter individual IPs for the external scan.



External Vulnerability Scan ?

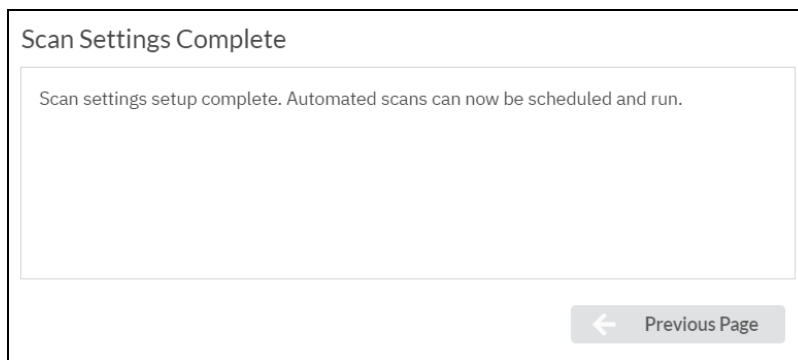
You may add up to 64 addresses.

Single IP + Add

96.71.91.233 Remove Selected
Remove All

← Previous Page Next Page →

10. Your scan settings will then be complete. Return to the To Do list and continue assessment tasks.



Scan Settings Complete

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

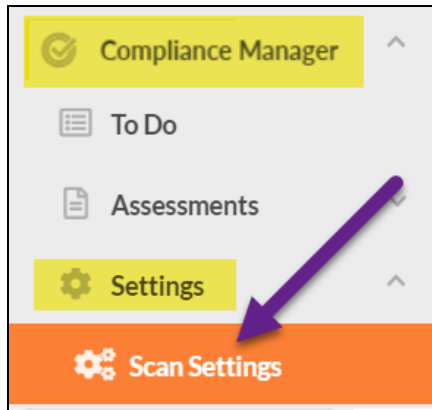
← Previous Page

Note: Stepping through the prompts creates the Scan Settings. Once the settings are saved, the Start CMMC Assessment To Do item is what is used to trigger the scans.

When you have finished entering the scan settings, return to the To Do item and click **Mark Complete**.

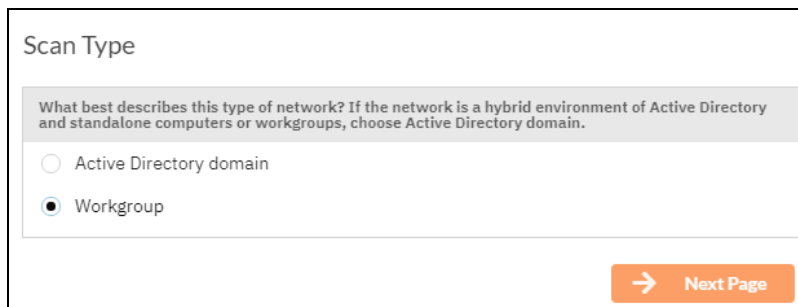
Configure Scan Settings for Workgroup

Set the **Scan Settings** from the **[Your Site] > Compliance Manager > Settings > Scan Settings** page. Complete all required prompts. This task is performed by the Technician.



Follow the steps below to configure the Scan Settings for the Compliance Manager Server:

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



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

The screenshot shows a window titled "Merge Option". Inside, there is a grey header bar with the text "How do you want to treat computers that are not associated with active directory?". Below this, there are two radio button options. The first option, "Treat them as part of the primary domain", is selected with a black dot. The second option, "Treat them as part of the specified workgroup", is unselected and has a text input field labeled "Workgroup" next to it. At the bottom of the window, there are two buttons: "Previous Page" with a left arrow and "Next Page" with a right arrow.

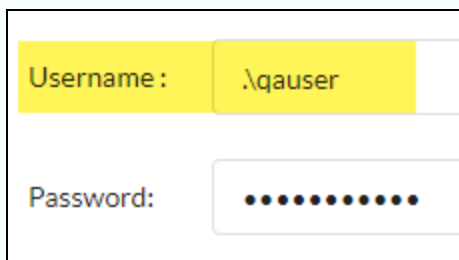
- a. Treat them as part of the primary domain
- b. Treat them as part of a specific workgroup by entering a workgroup name

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

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

The screenshot shows a window titled "Scan Credentials". Inside, there is a grey header bar with the text "Please enter a username and password with administrative rights to connect to the local computers. Additional users and passwords can be added in the Additional Credentials screen." Below this, there are two input fields. The first is labeled "Username :" and contains the text ".\quser". The second is labeled "Password:" and contains a series of dots. At the bottom of the window, there are two buttons: "Previous Page" with a left arrow and "Next Page" with a right arrow.

Note: For Workgroups, you have two options for how to enter the username. First, you can enter the characters ".\" (without quotation marks) immediately before the username, as in the image below.



A screenshot of a login form. The 'Username:' field contains the text '.\quser'. The 'Password:' field is masked with a series of dots.

Second, you can optionally use the following format:
"computername\localuseraccountname." For example, "WGWINX\user."



A screenshot of a login form. The 'Username:' field contains the text 'QWERTY\quser'. The 'Password:' field is masked with a series of dots.

If you have trouble connecting when using one username format, use the other format presented here.

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

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

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

Additional Credentials

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

Network Scan Credentials

Username:

Password:

+ Add Remove Selected Entry

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

← Previous Page Next Page →

5. The **IP Ranges** screen will then appear. The Compliance Manager server 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**.

YOU MUST ENTER AN IP RANGE TO PERFORM THE SCAN.

IP Ranges ?

Auto-Detected IP Ranges on Remote Appliance

10.

IP Ranges to Scan

Example IP Range Format: 192.168.0.0-192.168.0.255

Single IP or IP Range + Add

10.

Exclude IPs

Reset to Auto-Detected

Remove Selected Entry

Clear All Entries

← Previous Page → Next Page

From this screen you can also:

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

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

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

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

SNMP Information

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

+ add

public

Reset to Default Clear All Entries

Advanced SNMP Options

SNMP Timeout (seconds): Use Default

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

← Previous Page Next Page →

7. Enter the IP addresses for the external vulnerability scan. Click **Next Page**.

Important: You must ensure that no other Network Detective or Compliance Manager products are being used to perform an External Vulnerability Scan on the same external IP Address range at the same time. Allow at least several hours between repeat external vulnerability scans. Scheduling external scans at the same time will result in reports with missing or incomplete data.

Note: IP ranges for the external vulnerability scan are not supported at this time. Please enter individual IPs for the external scan.

External Vulnerability Scan ?

You may add up to 64 addresses.

Single IP + Add

96.71.91.233 Remove Selected
Remove All

← Previous Page Next Page →

8. Your scan settings will then be complete. Return to the To Do list and continue assessment tasks.

Scan Settings Complete

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

← Previous Page

Note: Stepping through the prompts creates the Scan Settings. Once the settings are saved, the Start CMMC Assessment To Do item is what is used to trigger the scans.

When you have finished entering the scan settings, return to the To Do item and click **Mark Complete**.

When you complete these steps, you are ready to begin ["Task 5: Start CMMC Assessment" on page 63](#).

Performing a CMMC Assessment

To perform a CMMC Assessment, complete the steps detailed in this guide.

Collect Initial CMMC Assessment Data

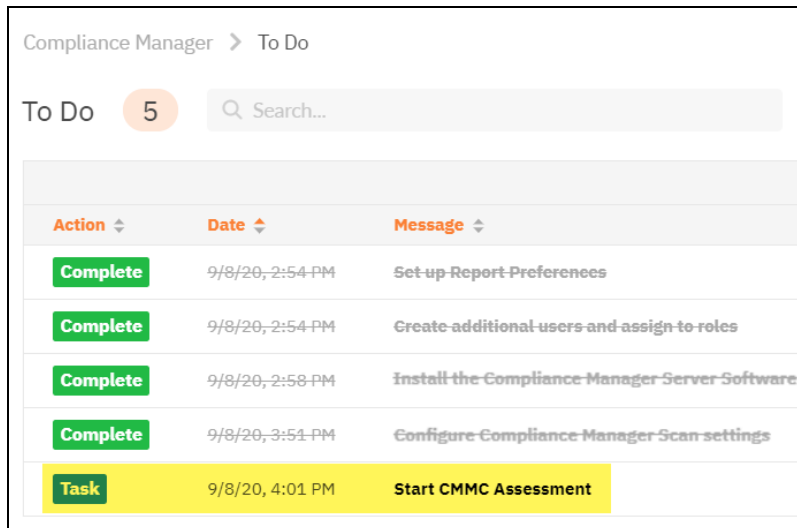
After the project has been set up, the **Internal Auditor** begins the CMMC Assessment. This is the on-site user who can answer compliance questions based on the data collected. The user in the Internal Auditor project role begins the assessment by completing several worksheets. At the same time, the Compliance Manager server performs automated scans on the target network.

Before you can start your CMMC assessment, you first need to follow the steps in ["Setting Up and Starting your CMMC Assessment Project" on page 25](#).

Note: Note that the tasks listed here may appear in a different order depending on which tasks you choose to complete first, or when automated scans are completed. It is OK to complete tasks in a different order than what you see here. Compliance Manager will make sure your CMMC Assessment stays on track!

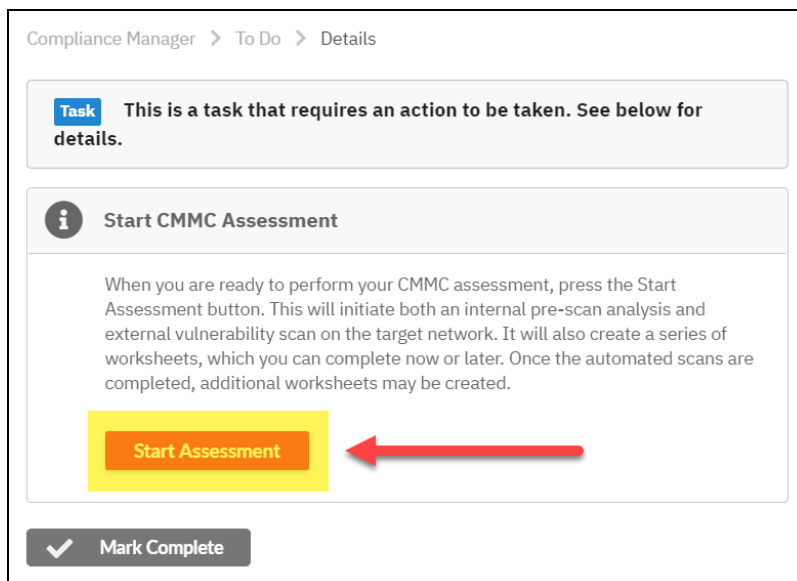
Task 5: Start CMMC Assessment

To begin performing the CMMC Assessment, click on the **Start CMMC Assessment** task from the To Do list:



Compliance Manager > To Do		
To Do	5	Search...
Action	Date	Message
Complete	9/8/20, 2:54 PM	Set up Report Preferences
Complete	9/8/20, 2:54 PM	Create additional users and assign to roles
Complete	9/8/20, 2:58 PM	Install the Compliance Manager Server Software
Complete	9/8/20, 3:51 PM	Configure Compliance Manager Scan settings
Task	9/8/20, 4:01 PM	Start CMMC Assessment

When you are ready to perform your first initial CMMC Assessment, click **Start Assessment**.



Compliance Manager > To Do > Details

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

i Start CMMC Assessment

When you are ready to perform your CMMC assessment, press the Start Assessment button. This will initiate both an internal pre-scan analysis and external vulnerability scan on the target network. It will also create a series of worksheets, which you can complete now or later. Once the automated scans are completed, additional worksheets may be created.

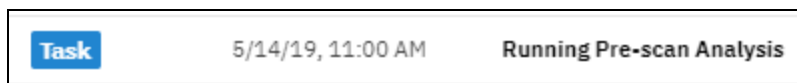
Start Assessment

✓ Mark Complete

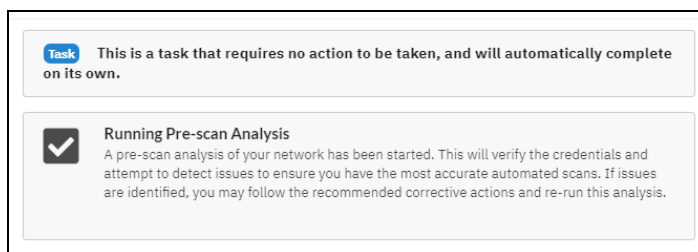
Note: Completing this task will create several new assessment tasks in the To Do list. The task **Type of CMMC Assessment** will be added, where you can choose whether to add additional worksheets for an expanded CMMC assessment. Two scans that will begin automatically: the **Pre-Scan** and the **External Vulnerability Scan**. The scans will be marked complete automatically when they finish.

Task 5.1: Running Pre-scan Analysis

In this task, the Compliance Manager server will begin an automated pre-scan analysis of the target network.



This will verify the credentials and attempt to detect issues to ensure you have the most accurate automated scans.



When the automated scan is completed, and any issues are identified, you may follow the recommended corrective actions and re-run this analysis.

Before proceeding with an assessment of your network, it is vital to ensure the scan is as accurate as possible. In some cases, 100% coverage is never possible due to network restrictions. You will be given the option during the assessment process to manually run local computer scans in those cases and upload them directly to this assessment.

Task 5.2: Review Pre-scan Analysis Results and Recommendations

Use the **Pre-Scan Analysis Results and Recommendations** to address any identified network configuration issues before continuing the assessment.

Task 5/14/19, 11:08 AM Review Pre-scan Analysis Results and Recommendations

The results from the pre-scan analysis will appear on the task details page.

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 20](#) for configuration guidance for both Windows Active Directory and Workgroup environments.

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

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

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

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

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

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

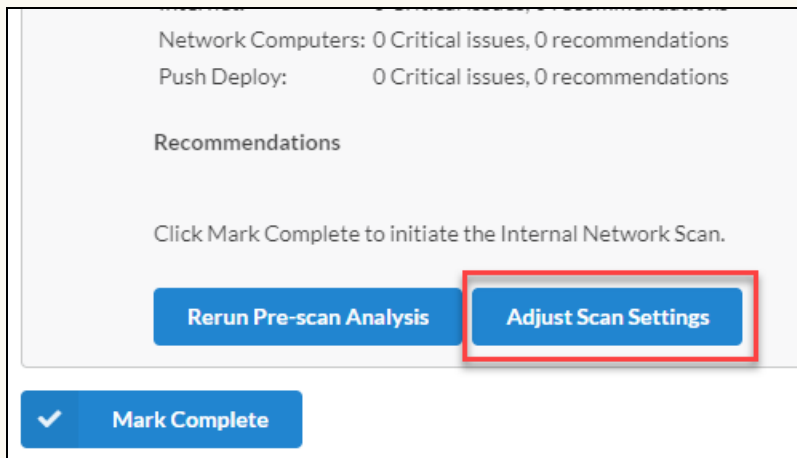
Reference overview of critical issues and recommendations

Implement listed recommendations to ensure successful scans

Tip: If the Analysis reveals CRITICAL issues:

- a) Review recommendations and address any identified network restriction issues, and
- b) Resolve identified issues before proceeding with marking the Review Pre-scan Analysis Results and Recommendations task complete.

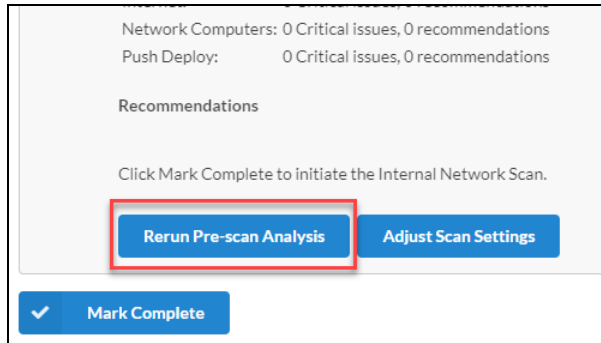
You can also click **Adjust Scan Settings** and check your scan settings.



Specifically:

- Also be sure that the Compliance Manager server successfully connected to the **Domain Controller**.
- If you still have issues, work with your Technician to be sure the target network meets the ["Pre-Scan Network Configuration Checklist" on page 20](#).

Once you finish making any changes, click **Rerun Pre-scan Analysis** to check for any remaining issues.



When you have reviewed the pre-scan analysis and are finished making any recommended changes to the target network, click **Mark Complete**. The **Internal Scan** will then begin automatically (or at the time specified in **Scan Schedules**; see ["Scan Schedules" on page 210](#)).


See also: ["Pre-Scan Network Configuration Checklist" on page 20](#).

Task 6: Running Automated Scan of Internal Network

The Compliance Manager server performs the **Internal Network Scan** on the target network. The Internal Scan begins automatically once you complete the pre-scan analysis and review the results.

Complete	5/10/19, 2:10 PM	Review Pre-scan Analysis Results and Recommendations
Complete	5/13/19, 10:27 AM	Complete External Port Use Worksheet
Task	5/13/19, 1:00 PM	Running Automated Scan of the Internal Network

Once the scan is complete, this To Do item will automatically be marked as complete.

**Running Automated Scan of the Internal Network**

A scan of your network has been started as part of the assessment process. Once the scan is complete, this To Do item will automatically be marked as complete.

Important: At least 1 computer must be successfully scanned in order for this To Do item to be automatically marked complete.

Error while running Internal Network Scan

If there is an error while running the Internal Network Scan, you will receive a separate To Do task. Click **Go to Scan Settings** to change your scan configuration. Return to the To Do task and click **Initiate Rescan** once you fix any issues and wish to restart the scan.

The most common problems are communication and permission issues. Ensure all scan settings are correct and all systems required to be up during the Network Scan are available including the server and domain controllers. Please correct the errors and re-initiate a rescan of the network.

Possible errors that might appear include:

- Unable to communicate with Domain Controller (in an A/D network)
- Invalid Active Directory username and password (in an A/D network)


- No users found
- No computers found

Task 7: Running Local Scan of Remote Computers

Once the Internal Network Scan is successfully completed, a scan of remote computers on the target network will automatically begin.

Complete	5/10/19, 2:19 PM	Review Pre-scan Analysis Results and Recommendations
Complete	5/13/19, 10:27 AM	Complete External Port Use Worksheet
Complete	5/13/19, 1:00 PM	Running Automated Scan of the Internal Network
Task	5/13/19, 1:26 PM	Running Local Scan of Remote Computers

This scan gathers more detailed data from individual endpoints on the target network.

**Running Local Scan of Remote Computers**

A scan of remote computers has been started as part of the assessment process. Once the scan is complete, this To Do item will automatically be marked as complete.

Important: At least 1 computer must be successfully scanned in order for this To Do item to be automatically marked complete.

Note: If the network is an Active Directory domain and consists of many computers, it is highly encouraged to correct issues that may prevent scanning of computers remotely. Ensure all scan settings are correct, including additional credentials, and re-initiate the scan below. This will only re-initiate the Local Scan of Remote Computers.

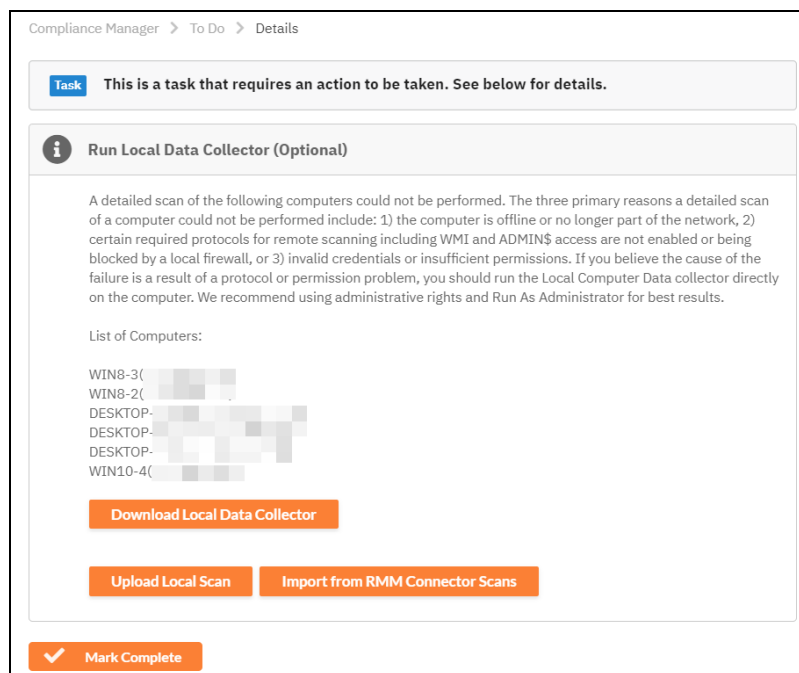
- You will receive a separate To Do item if there is an error during the local scan of Remote Computers.
- You can then click **Go to Scan Settings** to change your scan configuration.
- You can also click **Initiate Rescan** once you fix any issues and wish to restart the scan.

Task 8: Run Local Data Collector

In this task, you can perform manual scans on computers that could not be scanned automatically. You will also receive a list of known computers on the target network that could not be scanned. From this to do item, you can:

- A. Upload scans for computers that are connected to the network but cannot be scanned
- B. Upload scans for computers that are not available on the network being scanned, but that should be accounted for in the assessment process

Tip: You will also be notified if all computers are scanned successfully. You can then just click **Mark Complete** and move on with your assessment.



Primary reasons a detailed scan of a computer could not be performed include:

- The computer is offline or no longer part of the network,
- Certain required protocols for remote scanning including WMI and ADMIN\$ access are not enabled or are being blocked by a local firewall, or
- Invalid credentials or insufficient permissions.

To perform the scan manually, first download the **Local Computer Data Collector** from <https://www.rapidfiretools.com/cm>. To do this:

1. Click **Download Local Data Collector**.

Important: Be sure to select the data collector for the module you are using (GDPR, Cyber Insurance, HIPAA, etc.).

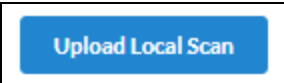
A blue rectangular button with rounded corners and a thin black border. The text "Download Local Data Collector" is centered in white.

2. Run the Local Data Collector on the target machine(s) selecting **Quick Scan**.

See for specific instructions.

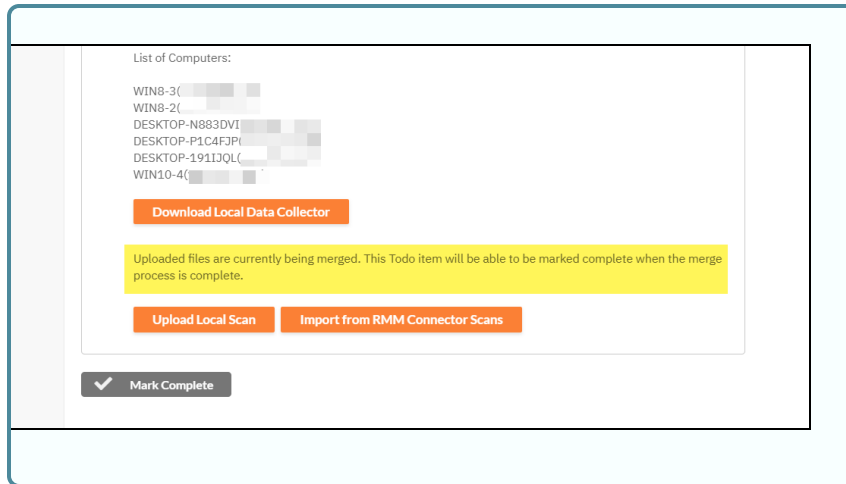
Note: If you need to scan Linux or Mac workstations, use the Mac and Linux data collectors on those machines during this step. Upload the Local Scan files on this page as instructed below. See ["Performing Scans on Mac and Linux Computers" on page 225](#) for more details.

3. Click **Upload Local Scan** to upload each scan file into the assessment. You can upload the .zip files containing the scans, too.

A blue rectangular button with rounded corners and a thin black border. The text "Upload Local Scan" is centered in white.

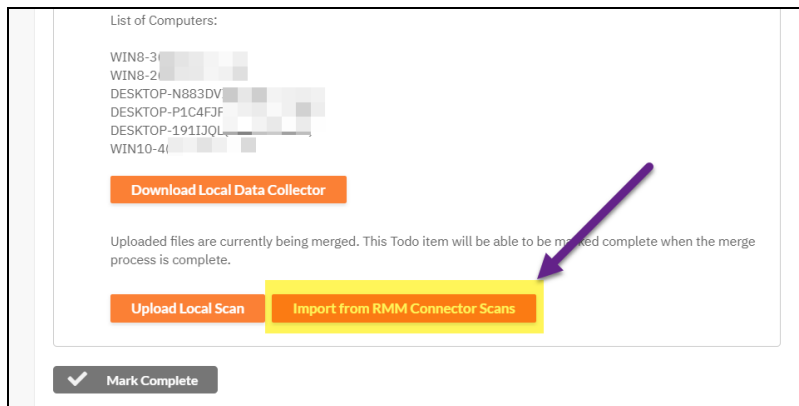
4. When you have finished uploading all local scans, click **Mark Complete** on the task To Do page.

Note: If you upload local scans, the Mark Complete button will be disabled until all local scans that you uploaded have been merged into the assessment project. You can then click Mark Complete once the merge is completed.



Import RMM Connector Scans

You also have the option to import RMM Connector scans from Kaseya VSA.

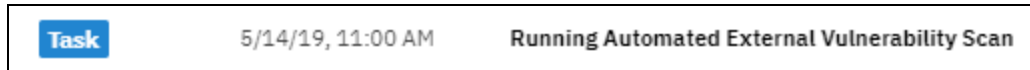


See ["Import RMM Connector Scans" on page 233](#) for a complete walkthrough.

Note: You must **Mark Complete** this To Do task before you can proceed.

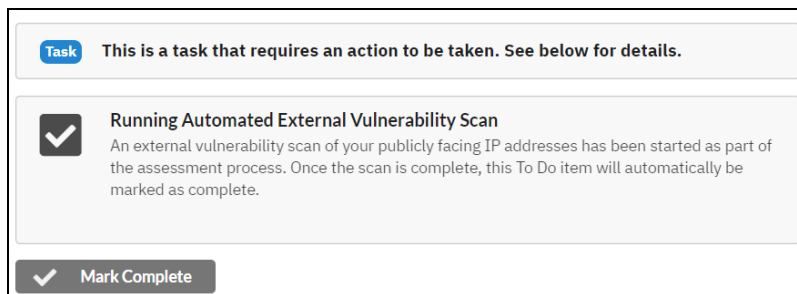
Task 9: Perform Automated External Vulnerability Scan

The assessment includes an external vulnerability scan of your publicly facing IP addresses.



Once the scan is complete, this To Do item will automatically be marked as complete.

The RapidFire Tools Cloud performs the External Vulnerability Scan. It begins automatically once you complete the initial To Do items.



Note: New worksheets will appear once the External Vulnerability scan completes.

Error while Running External Vulnerability Scan

Errors were encountered while running the External Vulnerability Scan. The most common problems are failure to initiate the scan or prolonged scan times causing a timeout. Timeouts most often happen when IPS (an Intrusion Prevention System) is turned on. You may need to [add the external scan range](#) as an IPS exclusion. Verify the IP range and click **Initiate Rescan**.

Collect Secondary CMMC Assessment Data

When the automated Internal Network and External Vulnerability Scans complete, new tasks appear in the To Do list.

Task 10: Complete External Port Use Worksheet

Note: The **External Port Use Worksheet** will become available 1) once the **External Vulnerability Scan** is complete, and 2) one or more external ports are found to be open.

An attacker can exploit unnecessary open ports to gain access to the network. This worksheet details ports that were found to be open during the external vulnerability scan. Use this worksheet to document the business justification for each open port. Also indicate whether the port uses a secure protocol.

Port	Business Justification	Protocol Secure	Security Feature Documented
80/TCP		No	No
443/TCP		No	No

When you are finished entering your responses, click **Save**. You can also click **Save and Return** to return to the To Do task details page. If you do not wish to save changes, click **Return**.

Worksheet English (US) Select Assessment Current Assessment

Save Save and Return

Click **Mark Complete** on the task To Do page when you are ready to finalize the worksheet and continue the assessment.

No External Port Found During External Vulnerability Scan

If no external listening ports were discovered during the external vulnerability scan, you will receive a separate To Do notification and will be prompted to continue.

Task 11: Complete Anti-virus Verification Worksheet

Tip: For helpful, time-saving tips for completing worksheets and surveys, see ["Completing Assessment Worksheets and Surveys" on page 165](#).

Compliance Manager will automatically detect any anti-virus software installed on PCs on the target network. Use the **Anti-virus Verification Worksheet** to quickly determine if each endpoint on the network has anti-virus software installed.

To use the worksheet:

1. From the To Do list, click the **Go To Form** button to open the worksheet.

Computer	IP Address	AV Detected	Detected Antivirus	Assessment
APV101	10.80.1.1	Yes	Windows Defender	Verified Present
BACKUP	10.80.1.2	Yes	Windows Defender	Verified Present
DC	10.80.1.3	Yes	Windows Defender	Verified Present
DC01	10.80.1.4	Yes	Windows Defender	Verified Present
DESKTOP-	10.80.1.5	Yes	Windows Defender	Verified Present
DESKTOP-	10.80.1.6	Yes	Windows Defender	Verified Present
DESKTOP-	10.80.1.7	Yes	Windows Defender	Verified Present
DESKTOP-	10.80.1.8	Yes	Windows Defender	Verified Present
DESKTOP-	10.80.1.9	Yes	Windows Defender	Verified Present
DESKTOP-	10.80.1.10	Yes	Windows Defender	Verified Present
DESKTOP-	10.80.1.11	Yes	Windows Defender	Verified Present
DESKTOP-	10.80.1.12	Yes	Windows Defender	Verified Present
DESKTOP-	10.80.1.13	Yes	Windows Defender	Verified Present
DESKTOP-	10.80.1.14	Yes	Windows Defender	Verified Present
DESKTOP-	10.80.1.15	Yes	Windows Defender	Verified Present

2. The results of the scan for anti-virus software will appear in the worksheet for all PCs detected. Review the results:
 - PCs detected with anti-virus will automatically be marked **Verified Present**.
 - PCs detected without anti-virus will automatically be marked **Not Detected**.

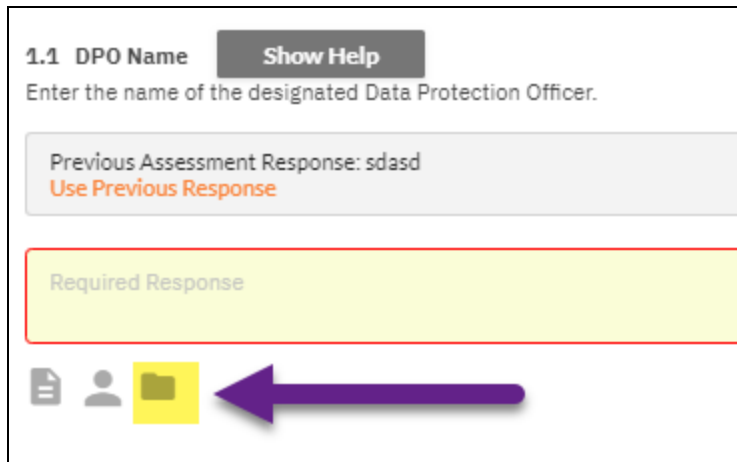
Note: You can also manually change each response if needed. For example, you can mark a PC as **Verified Present** if you know the PC has anti-virus, but Compliance Manager did not detect it. Alternatively, you can mark the entry **Verified Not Present** if you know the PC does not have anti-virus installed.

3. When finished, **Save**, return to the To Do item and click **Mark Complete**.

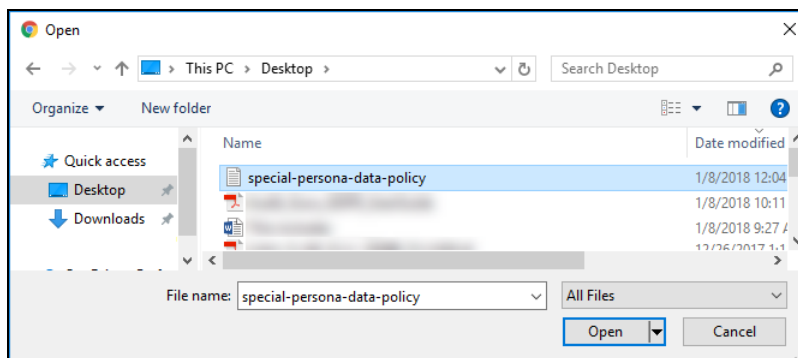
Attach Supporting Documents

As evidence of compliance, you can add supporting documents that will be included as attachments when you generate assessment and compliance reports with Compliance Manager. To attach a supporting document:

1. Click on the folder icon underneath the appropriate questionnaire field.



2. Choose whether to Add Attachment from **Previously Uploaded** or from your **Local Computer**.
3. Select the file you wish to upload and click Open. The selected file(s) will appear in the attachments queue.



- The file will be added to the assessment document as an attachment.

1.1 DPO Name [Show Help](#)
Enter the name of the designated Data Protection Officer.

Previous Assessment Response: sdasd
[Use Previous Response](#)

Required Response

Attachments:

File Name
additional-assessment-evidence-example.txt

Add Attachment From Previously Uploaded From Local Computer

Close

Note: The attachment will appear in your supporting documents and reports that are generated at the end of the assessment process.

Select Multiple Fields

In worksheets that have tables with multiple fields, you can select several or all fields at once in order to enter responses more quickly. To select multiple fields:

- Click the left mouse button and hold on the first field you would like to include in the selection.

1 ISSUE CHECKLIST

1.1 Issue Checklist
As you walk through the site environment, check to see if any of the following security issues are present. Check the box next to any issues that you find. Check the box next to any issues that you find security controls necessary to achieve the ISO 27001 standard.

Previous Assessment Response: Multiple Responses
[View Previous Responses](#)

<input type="checkbox"/>	Removable media not secure. Left on desks in unsecured office or cubicles or in public areas. (8.3.1)
<input type="checkbox"/>	Hard drives or defunct systems with media left in unsecured offices or cubicles or in public areas. (8.3.2)
<input type="checkbox"/>	Servers or devices containing sensitive information reside in an insecure area (11.1.1a)
<input type="checkbox"/>	Perimeter of building or site is not physically sound allowing easy break-in (11.1.1b)
<input type="checkbox"/>	Lack of physical access control either manned or unmanned (11.1.1c)
<input type="checkbox"/>	Fire doors on security perimeter found that are not alarmed or monitored (11.1.1e)
<input type="checkbox"/>	Lack of physical intrusion detection system (11.1.1f)
<input type="checkbox"/>	Processing facilities maintained by external parties co-located with the organisation's information processing facilities (11.1.1g)
<input type="checkbox"/>	Visitors allowed entry to secured areas without recording date and time (11.1.2a)
<input type="checkbox"/>	Visitors allowed to move unsupervised through secured areas (11.1.2a)

- While holding the left mouse button, drag and select your desired fields.

1 ISSUE CHECKLIST

1.1 Issue Checklist
As you walk through the site environment, check to see if any of the following security issues are present. Check the box next to any issues that you find. Check the box next to any issues that you find. Check the box next to any issues that you find.

Previous Assessment Response: Multiple Responses
[View Previous Responses](#)

<input type="checkbox"/>	Removable media not secure. Left on desks in unsecured office or cubicles or in public areas. (8.3.1)
<input type="checkbox"/>	Hard drives or defunct systems with media left in unsecured offices or cubicles or in public areas. (8.3.2)
<input type="checkbox"/>	Servers or devices containing sensitive information reside in an insecure area (11.1.1a)
<input type="checkbox"/>	Perimeter of building or site is not physically sound allowing easy break-in (11.1.1b)
<input type="checkbox"/>	Lack of physical access control either manned or unmanned (11.1.1c)
<input type="checkbox"/>	Fire doors on security perimeter found that are not alarmed or monitored (11.1.1e)
<input type="checkbox"/>	Lack of physical intrusion detection system (11.1.1f)
<input type="checkbox"/>	Processing facilities maintained by external parties co-located with the organisation's information processing facilities (11.1.1g)
<input type="checkbox"/>	Visitors allowed entry to secured areas without recording date and time (11.1.2a)
<input type="checkbox"/>	Visitors allowed to move unsupervised through secured areas (11.1.2a)
<input type="checkbox"/>	Lack of authentication mechanism to secure areas (11.1.2b)
<input type="checkbox"/>	Lack of physical or electronic audit trail for all access to secure areas (11.1.2c)
<input type="checkbox"/>	Employees, contractors, or external parties in secure area without visible identification (11.1.2d)

3. You can use this feature to copy and paste multiple responses at once. See ["Copy and Paste Responses"](#) below.

Copy and Paste Responses

Some worksheets allow you to copy and paste the responses you entered, much like a spreadsheet. This saves you time by allowing you to enter many responses at once. To do this:

1. First answer one or more questions that require a response. Enter your response within the field.

Note: You can copy and paste both free-form and multiple choice entries.

(such as privileges) with the covered entity. For active employees and vendors, indicate if the user is

Last Login	ePHI Access
4/3/2018 4:16:37 AM	Employee - ePHI authorization
9/12/2018 6:25:29 AM	Employee - ePHI authorization
10/8/2018 9:14:33 AM	Employee - no ePHI authorization
1/16/2019 12:43:04 PM	Vendor - ePHI authorization
10/8/2018 9:29:47 AM	Vendor - no ePHI authorization
12/3/2018 9:20:19 AM	Former Employee
4/9/2018 4:17:06 AM	Employee - ePHI authorization

2. Use your mouse to drag and select multiple rows that contain the responses you wish to copy.

	ePHI Access
	Employee - ePHI authorization
	Employee - ePHI authorization
	Employee - ePHI authorization
	Employee - ePHI authorization
	Vendor - ePHI authorization
	Vendor - ePHI authorization
	Vendor - ePHI authorization
	Vendor - ePHI authorization
	Vendor - ePHI authorization
	Vendor - ePHI authorization
	Vendor - ePHI authorization

3. On your keyboard, press **CTRL+C**.
4. Use your mouse to drag and select the rows you wish to paste the responses into.
5. On your keyboard, click **CTRL+V**. Your pasted responses will appear in the worksheet.

ty. For active employees and vendors, indicate if the user is

	ePHI Access
	Employee - ePHI authorization
	Employee - ePHI authorization
	Employee - ePHI authorization
	Employee - ePHI authorization
	Employee - ePHI authorization
	Employee - ePHI authorization
	Employee - ePHI authorization
	Employee - ePHI authorization
	Employee - ePHI authorization
	Vendor - ePHI authorization
	Vendor - ePHI authorization
	Vendor - ePHI authorization

Use this feature to save time completing worksheet responses that can be answered with the same answer.

Task 12: Complete User Access Review Worksheet

Tip: For helpful, time-saving tips for completing worksheets and surveys, see ["Completing Assessment Worksheets and Surveys" on page 165](#).

The **User Access Review Worksheet** enables you to identify each user and to document their status: Employee, Third Party, Former Employee, Former Third Party, Service Account. You can also indicate whether each user has **Remote Access**.

Note: In addition to other scan procedures that identify Windows admin accounts, a user will also be marked as a "Privileged (Administrator) Account" if they are associated with any group or organizational unit that contains the word "admin."

To use the worksheet:

1. Click the **Go To Form** button to open the worksheet.

Compliance Manager > Assessments > InForm

Select Assessment: Current Assessment

User Access Review Worksheet

Search Topics [Search]

Hide # | Expand All | Collapse All | Download | Invite Others | Save | Save and Return | Return

1 TEST, .COM

1.1 User Access Review
The table below lists the users discovered on the network. For each user, specify the status. Then indicate whether the account has remote access.

Previous Assessment Response: Multiple Responses
[View Previous Responses](#)

User Name	Display Name	Privileged (Administrator) Account	Last Login	Status	Has Remote Access?
[Redacted]	[Redacted]	No	04-Jun-2019 3:47:12 PM	Former Employee	Yes
[Redacted]	[Redacted]	No		Employee	Yes
[Redacted]	[Redacted]	No		Employee	Yes
[Redacted]	[Redacted]	Yes	29-May-2019 2:07:45 PM	Employee	Yes
[Redacted]	[Redacted]	Yes	04-Jun-2019 10:19:51 AM	Employee	Yes

2. Assign each identified user the correct **Status**.
3. Indicate whether each user has **Remote Access**.
4. When are finished, **Save**, return to the To Do item and click **Mark Complete**.

Task 13: Complete Asset Inventory Worksheet

Tip: For helpful, time-saving tips for completing worksheets and surveys, see ["Completing Assessment Worksheets and Surveys" on page 165](#).

Note: The Asset Inventory Worksheet will become available once the Internal Network Scan is complete.

The **Asset Inventory Worksheet** details the computer assets discovered on the network. Complete all of the required fields in the worksheet.

See the table below for an explanation of each field.

Asset Inventory Worksheet Field	Description and Instructions
Asset Owner	Enter the name of the person who is responsible for the information security of this asset. The owner does not need to be the actual user of the system.
Acceptable Use	Enter a short description of the primary acceptable use for this system (i.e., "user workstation").
Environment	Indicate whether the device is part of the Development, Test, and/or Operations environment(s).
Backup Agent Status	Answer "Yes" or "No" to indicate whether the device has a backup agent.
Device	Indicate whether the device is authorized or not authorized.
CUI (Controlled Unclassified Information) Access	Specify whether the asset: <ul style="list-style-type: none"> • Has CUI: Does the Computer Asset have CUI stored on the computer? • No CUI: Does the Computer Asset have NO CUI stored on the computer? • Access Gateway to CUI: Is the computer used to access CUI within the network being assessed or outside of the network through access to an External Application (such as a cloud based system)?

Task 14: Complete Application Inventory Worksheet

This worksheet details the applications discovered on the network. For each application, specify the criticality, i.e. the level of importance the app has for operations as per the NIST framework.

The purpose of this worksheet is to inventory applications in use so as to allow the organization to manage the risk posed by using multiple apps. Specifically, you establish the business priority (criticality) of each app.

Note: The apps in this worksheet are discovered during the network scan - and you might find that certain apps are redundant or not authorized by the organization. In this case, they can be removed from the network.

This worksheet is designed to be shared with others in the organization who can contribute the necessary information. See ["Invite Subject Matter Experts \(SMEs\) to Complete Forms" on page 180](#) for details.

Application	Number of Computers	List of Computers	Criticality
Active Directory Authentication Library for SQL Server	1	SQL02	Medium
Audit Guru Server	2	DESKTOP-BDJFFUG,DESKTOP-FACKERQ	Medium
Browser for SQL Server 2016	1	SQL02	Medium
Google Chrome	1	DESKTOP-FACKERQ	Medium
Microsoft Help Viewer 1.1	1	SQL02	Medium
Microsoft Help Viewer 2.3	1	SQL02	Medium

Tip: Do you want to attach supporting documents or copy and paste multiple responses to save time? See ["Completing Assessment Worksheets and Surveys" on page 165](#) for helpful tips that can improve the efficiency and effectiveness of your responses.

Task 15: Complete External Information System Worksheet

This worksheet is used to document external information systems used by your organization. Add entries for each external information system along with a description, purpose for using the system, name of the business owner of the system, along with its criticality. Examples of external information systems include Salesforce, QuickBooks Online, and Office 365.

The purpose of this worksheet is to inventory systems in use at the organization, but that are largely outside of (external to) that organization's control and/or ownership. This can allow the organization to manage the risk posed by using external systems. Specifically, you must:

- Identity each external info system
- Determine the business owner and business purpose of that system
- Establish the business priority (criticality) of that system

The screenshot shows the 'External Information System Worksheet' interface. At the top, there's a breadcrumb trail: 'Compliance Manager > Assessments > Inform'. Below this, the title 'External Information System Worksheet' is displayed. A search bar with a magnifying glass icon and a 'Search' button is present. To the right, there's a language dropdown set to 'English (US)' and a 'Select Assessment' dropdown set to 'Current Assessment'. Below the search bar, there are buttons for 'Hide # | Expand All | Collapse All', 'Download', 'Invite Others', 'Save', 'Save and Return', and 'Return'. The main content area is titled '1 EXTERNAL INFORMATION SYSTEMS'. Underneath, there's a section '1.1 External Information Systems' with a descriptive paragraph. Below the text is a table with five columns: 'Name', 'Description', 'Purpose', 'Business Owner', and 'Criticality'. The table is currently empty. At the bottom right of the table area, there are buttons for 'Save', 'Save and Return', and 'Return'. A 'Jump To Top' link is at the bottom left.

Enter each information system one line at a time. Complete all relevant fields for each entry.

This is a close-up of the table from the previous screenshot. The table has five columns: 'Name', 'Description', 'Purpose', 'Business Owner', and 'Criticality'. The first row is populated with the following data: 'Name' is 'Gmail', 'Description' is 'Email system', and 'Purpose' is 'Office communication'. The 'Business Owner' and 'Criticality' columns are empty. There is a small star icon in the first column of the second row.

Task 16: Select Level of CMMC Assessment

In this step, choose whether you wish to perform a **Level 1**, **Level 2**, or **Level 3** CMMC Assessment.

Compliance Manager > To Do > Details

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

Select Level of CMMC Assessment

Select Level of the CMMC Assessment that you want to perform.

The Cybersecurity Maturity Model (CMM) and its control domains have “Levels” of IT security controls that can be implemented to secure an information system and access to CUI.

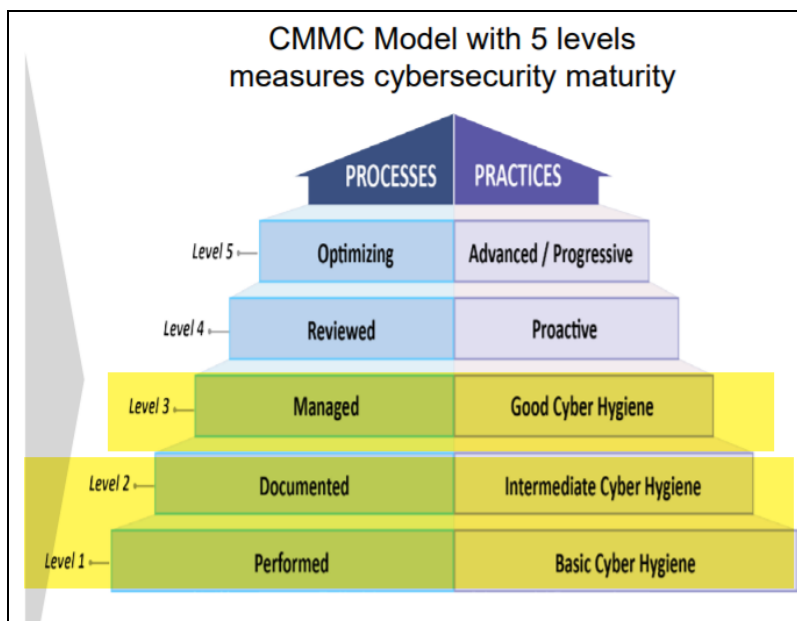
Compliance Manager enables an assessor to perform a CMMC assessment based on CMMC control levels 1, 2 and 3.

Select the level of the CMMC Assessment you want to perform.

Level 1 **Level 2** **Level 3**

✓ Mark Complete

CMMC has multiple “Levels” of IT security controls that can be implemented to secure the IT environment. **Level 1**, **Level 2**, **Level 3** represent the first two levels of the CMMC assessment.



Note: To learn more about the CMMC model and its associated levels, visit <https://www.acq.osd.mil/cmmc/>.

Which CMMC Level Should I Choose?

- The **Level 1** assessment presents fewer worksheets for the auditor to complete. In addition, the CMMC worksheets will be simplified and contain fewer questions. Use this level if you want to perform a relatively quick "Basic Cyber Hygiene" check as per the CMMC framework.

Continue to ["Complete Level 1 CMMC Worksheets " on the next page](#) for step-by-step instructions.

- The **Level 2** assessment presents several additional worksheets to complete. Likewise, the CMMC worksheets will contain added sections and questions. Use this level if you want to perform an "Intermediate Cyber Hygiene" check as per the CMMC framework. Once you complete a Level 2 assessment, you will have a wealth of documentation to support your Level 2 compliance.

Continue to ["Complete Level 2 CMMC Worksheets " on page 94](#) for step-by-step instructions.

The **Level 3** allows you to perform a "Good Cyber Hygiene" check as per the CMMC framework. Once you complete a Level 3 assessment, you will have a wealth of documentation to support your Level 3 compliance.

- Continue to ["Complete Level 3 CMMC Worksheets " on page 111](#) for step-by-step instructions.

Change Assessment Level

During your assessment, you may decide to change CMMC assessment levels. To do this:

1. Return to the **Select CMMC Level** to do item.
2. Click Re-run and select your desired assessment level. Confirm that you wish to regenerate the worksheet To Do items.

Compliance Manager > To Do > Details

Complete This issue/task has been marked complete.

i Select Level of CMMC Assessment

Select Level of the CMMC Assessment that you want to perform.

The Cybersecurity Maturity Model (CMM) and its control domains have “Levels” of IT security controls that can be implemented to secure an information system and access to CUI.

Compliance Manager enables an assessor to perform a CMMC assessment based on CMMC control levels 1, 2 and 3.

Select the level of the CMMC Assessment you want to perform.

Level 1 Level 2 Level 3

✓ Completed Re-run

Your To Do list will be updated with the worksheets for the selected level.

Note: Your saved responses will be available to re-use in the regenerated worksheets.

Complete Level 1 CMMC Worksheets

Once you choose the Level 1 CMMC assessment, new worksheets will appear in your to do list.

CMMC Demo Site 2			
Complete	9/21/20, 10:19 AM	Review Pre-scan Analysis Results and Recommendations	
Complete	9/21/20, 12:41 PM	Running Automated Scan of the Internal Network	
Complete	9/21/20, 3:01 PM	Running Local Scan of Remote Computers	
Complete	9/22/20, 10:29 AM	Run Local Data Collector (Optional)	
Complete	9/22/20, 10:30 AM	Complete Antivirus Verification Worksheet	
Complete	9/22/20, 10:30 AM	Complete User Access Review Worksheet	
Complete	9/22/20, 10:39 AM	Complete Asset Inventory Worksheet	
Complete	9/22/20, 10:39 AM	Complete Application Inventory Worksheet	
Complete	9/22/20, 10:39 AM	Complete External Information System Worksheet	
Complete	9/22/20, 10:39 AM	Select Level of CMMC Assessment	
Task	9/22/20, 11:17 AM	Complete CMMC – Access Control Worksheet	
Task	9/22/20, 11:17 AM	Complete CMMC – Identification and Authentication Worksheet	
Task	9/22/20, 11:17 AM	Complete CMMC – Media Protection Worksheet	
Task	9/22/20, 11:17 AM	Complete CMMC – Physical Protection Worksheet	
Task	9/22/20, 11:17 AM	Complete CMMC – System and Communications Protection Worksheet	
Task	9/22/20, 11:17 AM	Complete CMMC – System and Information Integrity Worksheet	

Note Regarding Worksheet Cross References to NIST SP 800-171

Many CMMC worksheets include cross references to items within the NIST SP 800-171 rev1 framework. However, note that CMMC contains additional security requirements, and thus not every CMMC provision references a NIST requirement.

1.2 Protect CUI Backups - CMMC Ctrl: RE.2.138 - Protect the confidentiality of backup CUI at storage locations. (NIST 800-171 Rev. 2 Ctrl Ref: 3.8.9)

Is the confidentiality and integrity of backup CUI protected at the storage location?

Previous Assessment Response: No
[Use Previous Response](#)

No >

Icons: Document, User, Folder

Task 17: Complete CMMC Access Control Worksheet

Complete the **CMMC Access Control Worksheet**. This worksheet should be completed by an Internal Auditor.

Compliance Manager > To Do > Details

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

i Complete CMMC – Access Control Worksheet

Complete the worksheet to assess compliance with the Access Control control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.

[Go to Form: CMMC - Access Control Worksheet](#)

✓ Mark Complete

Specifically, this worksheet asks you to examine:

- Restrictions on internal system access
- Restrictions on access to external information systems
- Restrictions on information posted to public-facing data systems
- Utilization of the principle of least privilege for user accounts and their access to sensitive data

The screenshot shows the 'Acme CMMC Project' interface. On the left is a navigation menu with options: Home, Compliance Manager, To Do, Assessments, Dashboard, Forms (selected), Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The main content area is titled 'Compliance Manager > Assessments > Inform' and 'CMMC Access Control Worksheet'. It includes a search bar, a 'Download' button, and buttons for 'Invite Others', 'Save', 'Save and Return', and 'Return'. The worksheet content includes a header '1.001 - ESTABLISH SYSTEM ACCESS REQUIREMENTS (REQUIRED REMAINING)' and a sub-header '1.1 Limit system access - CMMC Ctrl: AC.1.001 - Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). (NIST 800-171 Rev. 2 Ctrl Ref: 3.3.1)'. Below this is a text input field with a yellow background and a red border. Another section '1.2 Privacy and Security Notices - CMMC Ctrl: AC.2.006 - Provide privacy and security notices consistent with applicable CUI rules. (NIST 800-171 Rev. 2 Ctrl Ref: 3.3.9)' is visible, followed by another text input field. At the bottom, a status bar indicates '22 required remaining' and buttons for 'Save', 'Save and Return', and 'Return'.

Task 18: Complete CMMC Identification and Authentication Worksheet

Complete the **CMMC Identification and Authentication Worksheet**. This worksheet should be completed by an Internal Auditor.

The screenshot shows the 'Compliance Manager > To Do > Details' view. It features a 'Task' section with the text 'This is a task that requires an action to be taken. See below for details.' Below this is an information icon and the title 'Complete CMMC - Identification and Authentication Worksheet'. The description states: 'Complete the worksheet to assess compliance with the Identification and Authentication control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' At the bottom of the task card is an orange button labeled 'Go to Form: CMMC - Identification and Authentication Worksheet'. Below the task card is a 'Mark Complete' button with a checkmark icon.

Specifically, this worksheet asks you to examine:

- User identification procedures and practices
- Password policy, management, and enforcement

The screenshot displays the 'Acme CMMC Project' interface. On the left is a navigation sidebar with options: Home, Compliance Manager, To Do, Assessments, Forms (selected), Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The main content area is titled 'Compliance Manager > Assessments > Inform' and shows the 'CMMC Identification and Authentication Worksheet'. It includes a search bar, a 'Download' button, and buttons for 'Invite Others', 'Save', 'Save and Return', and 'Return'. The worksheet content includes a header '1 C015 - GRANT ACCESS TO AUTHENTICATED ENTITIES (11 REQUIRED REMAINING)' and two sections for user accounts and password complexity, each with a 'Show Guidance' link and a yellow input field. At the bottom, it indicates '11 required remaining' and has 'Save', 'Save and Return', and 'Return' buttons.

Tip: For helpful, time-saving tips for completing worksheets and surveys, see ["Completing Assessment Worksheets and Surveys" on page 165](#).

Task 19: Complete CMMC Media Protection Worksheet

Complete the **CMMC Media Protection Worksheet**. This worksheet should be completed by an Internal Auditor.

The screenshot shows the 'Compliance Manager > To Do > Details' view. It features a 'Task' section with the text: 'This is a task that requires an action to be taken. See below for details.' Below this is a task card titled 'Complete CMMC – Media Protection Worksheet' with an information icon. The card text reads: 'Complete the worksheet to assess compliance with the Media Protection control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' An orange button labeled 'Go to Form: CMMC - Media Protection Worksheet' is at the bottom of the card. At the very bottom of the details view is a 'Mark Complete' button with a checkmark icon.

Specifically, this worksheet asks you to examine:

- Procedures in place to protect CUI (Controlled Unclassified Information) present on both analog and digital media within the organization
- Procedures to destroy or sanitize media devices no longer in use that might contain sensitive data

The screenshot shows the 'Acme CMMC Project' interface. On the left is a navigation menu with options: Home, Compliance Manager, To Do, Assessments, Dashboard, Forms (selected), Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The main content area is titled 'CMMC Media Protection Worksheet'. It includes a search bar, a 'Download' button, and buttons for 'Invite Others', 'Save', 'Save and Return', and 'Return'. A note states: 'Complete the following worksheet regarding the compliance with the CMMC – Media Protection (MP) control domain. This worksheet should be completed by an Internal Auditor'. The worksheet contains three sections, each with a title, a description, and a 'Show Guidance' link. Section 1.1 is titled '1.1 Protect and Control - CMMC Ctrl: MP.2.120 - Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital, (NIST 800-57 Rev. 2 Ctrl Ref: 3.8.5)' and asks 'Does the company protect system media containing CUI, both paper form and to digital form?'. Section 1.2 is titled '1.2 Protect and Control - CMMC Ctrl: MP.2.120 - Limit access to CUI on system media to authorized users, (NIST 800-57 Rev. 2 Ctrl Ref: 3.8.6)' and asks 'Does the company limit access to CUI on system media to authorized users?'. Section 1.3 is titled '1.3 Protect and Control - CMMC Ctrl: MP.2.122 - Control the use of removable media on system components, (NIST 800-57 Rev. 2 Ctrl Ref: 3.8.7)' and asks 'Does the company control the use of removable media on system components?'. At the bottom, there is a '0 required remaining' status and buttons for 'Save', 'Save and Return', and 'Return'.

Tip: For helpful, time-saving tips for completing worksheets and surveys, see ["Completing Assessment Worksheets and Surveys" on page 165](#).

Task 20: Complete CMMC Physical Protection Worksheet

Complete the **CMMC Physical Protection Worksheet**. This worksheet should be completed by an Internal Auditor.

The screenshot shows the 'Task' details for 'Complete CMMC - Physical Protection Worksheet'. The breadcrumb trail is 'Compliance Manager > To Do > Details'. A 'Task' box states: 'This is a task that requires an action to be taken. See below for details.' Below this is a section titled 'Complete CMMC - Physical Protection Worksheet' with an information icon. The text reads: 'Complete the worksheet to assess compliance with the Physical Protection control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' Below the text is an orange button labeled 'Go to Form: CMMC - Physical Protection Worksheet'. At the bottom, there is a 'Mark Complete' button with a checkmark icon.

Specifically, this worksheet asks you to examine:

- Measures to control physical access to site and its resources
- Visitor access control
- Visitor access audit logs
- Physical access control devices and their management

The screenshot shows the 'CMMC Physical Protection Worksheet' in the Compliance Manager application. The left sidebar contains navigation links: Home, Compliance Manager, To Do, Assessments, Dashboard, Forms (selected), Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The main content area displays the worksheet title, a search bar, and buttons for 'Search', 'Add Others', 'Save', 'Save and Return', and 'Return'. Below this, a section titled '1 C208-LIMIT PHYSICAL ACCESS (6 REQUIRED REMAINING)' contains two sub-sections: '1.1 Control Physical Access - CMMC Ctrl: PE.1.131 - Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals. (NIST 800-171 Rev. 2 Ctrl Ref: 3.10.3)' and '1.2 Visitor Access Monitoring - CMMC Ctrl: PE.1.532 - Escort visitors and monitor visitor activity. (NIST 800-171 Rev. 2 Ctrl Ref: 3.10.3)'. Each sub-section has a 'Show Guidance' link and a large yellow input field. At the bottom, a section for '1.3 Access Audit Logs - CMMC Ctrl: PE.1.133 - Maintain audit logs of physical access. (NIST 800-171 Rev. 2 Ctrl Ref: 3.10.4)' is partially visible, showing '6 required remaining' and buttons for 'Save', 'Save and Return', and 'Return'.

Tip: For helpful, time-saving tips for completing worksheets and surveys, see ["Completing Assessment Worksheets and Surveys" on page 165](#).

Task 21: Complete CMMC System and Communications Protection Worksheet

Complete the **CMMC System and Communications Protection Worksheet**. This worksheet should be completed by an Internal Auditor.

The screenshot shows the 'To Do' task details in the Compliance Manager application. The breadcrumb trail is 'Compliance Manager > To Do > Details'. A 'Task' box contains the text: 'This is a task that requires an action to be taken. See below for details.' Below this is an information box with an 'i' icon, titled 'Complete CMMC – System and Communications Protection Worksheet'. The text inside states: 'Complete the worksheet to assess compliance with the Systems and Communication Protection control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' At the bottom of the information box is an orange button labeled 'Go to Form: CMMC - Systems and Communication Protection Worksheet'. At the very bottom of the task details is a grey button with a checkmark icon labeled 'Mark Complete'.

Specifically, this worksheet asks you to examine:

- Collaborative computing devices
- Session encryption
- Communication boundary definition and protection

The screenshot shows the 'Acme CMMC Project' interface. On the left is a navigation menu with options: Home, Compliance Manager, To Do, Assessments, Dashboard, Forms (selected), Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The main content area is titled 'CMMC System and Communications Protection Worksheet'. It includes a search bar, a 'Select Assessment' dropdown, and buttons for 'Hide #', 'Expand All', 'Collapse All', 'Download', 'Invite Others', 'Save', 'Save and Return', and 'Return'. The worksheet content includes a header '1. COSS8 - DEFINE SECURITY REQUIREMENTS FOR SYSTEMS AND COMMUNICATIONS (15 REQUIRED REMAINING)' and two sections: '1.1 Collaborative Computing Devices - CMMC Ctrl: SC.2.378 - Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device. (NIST 800-171 Rev. 2 Ctrl Ref: 3.15.12)' and '1.2 Session Encryption - CMMC Ctrl: SC.2.379 - Use encrypted sessions for the management of network devices. Does the company employ mechanisms to encrypt sessions during the management of network devices?'. Each section has a yellow input field and a '(Show Guidance)' link. At the bottom, it says '19 required remaining' and has 'Save', 'Save and Return', and 'Return' buttons.

Task 22: Complete CMMC System and Information Integrity Worksheet

Complete the **CMMC System and Information Integrity Worksheet**. This worksheet should be completed by an Internal Auditor.

The screenshot shows the 'Compliance Manager > To Do > Details' view. It features a 'Task' box with the text 'This is a task that requires an action to be taken. See below for details.' Below this is a task card titled 'Complete CMMC – System and Information Integrity Worksheet' with an information icon. The card contains the text: 'Complete the worksheet to assess compliance with the System and Information Integrity control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' Below the text is an orange button labeled 'Go to Form: CMMC - System and Information Integrity Worksheet'. At the bottom of the card is a grey button with a checkmark icon labeled 'Mark Complete'.

Specifically, this worksheet asks you to:

- Catalog information systems in use and their responsible parties
- Identify and manage information system flaws
- Identify malicious content
- Perform network and system monitoring

Note: For additional guidance in answering worksheet questions 1 through 1.3, please refer to the publication "NIST SP800-18, Guide for Developing Security Plans

for Federal Information Systems," page 19, section 3, "Plan Development." This document is currently available at:

<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-18r1.pdf>

CMMC Demo Site 2

Compliance Manager > Assessments > Inform

CMMC System and Information Integrity Worksheet

Select Assessment: Current Assessment

Search Topics

Hide # | Expand All | Collapse All | Download

Invite Others | Save | Save and Return | Return

Complete the following worksheet to document the organization's system identification details and compliance with the controls contained within the CMMC – System and Information Integrity (SI) control domain. This worksheet should be completed by an Internal Auditor.

1 INFORMATION SYSTEM NAME AND TITLE (REQUIRED REMAINING)

1.1 System Name
State the name of the system in the field below. Spell out acronyms.

Required Response

1.2 System Categorization
Enter the System Categorization in the field below.

Required Response

13 required remaining

Save | Save and Return | Return

Complete Level 2 CMMC Worksheets

Once you choose the Level 2 CMMC assessment, new worksheets will appear in your to do list.

CMMC Demo Site 2

Complete	9/21/20, 3:01 PM	Running Local Scan of Remote Computers
Complete	9/22/20, 10:29 AM	Run Local Data Collector (Optional)
Complete	9/22/20, 10:30 AM	Complete Antivirus Verification Worksheet
Complete	9/22/20, 10:30 AM	Complete User Access Review Worksheet
Complete	9/22/20, 10:39 AM	Complete Asset Inventory Worksheet
Complete	9/22/20, 10:39 AM	Complete Application Inventory Worksheet
Complete	9/22/20, 10:39 AM	Complete External Information System Worksheet
Complete	9/22/20, 1:46 PM	Select Level of CMMC Assessment
Task	9/22/20, 1:46 PM	Complete CMMC – Access Control Worksheet
Task	9/22/20, 1:46 PM	Complete CMMC – Audit and Accountability Worksheet
Task	9/22/20, 1:46 PM	Complete CMMC – Awareness and Training Worksheet
Task	9/22/20, 1:46 PM	Complete CMMC – Configuration Management Worksheet
Task	9/22/20, 1:46 PM	Complete CMMC – Identification and Authentication Worksheet
Task	9/22/20, 1:46 PM	Complete CMMC – Incident Response Worksheet
Task	9/22/20, 1:46 PM	Complete CMMC – Maintenance Worksheet
Task	9/22/20, 1:46 PM	Complete CMMC – Media Protection Worksheet




Note Regarding Worksheet Cross References to NIST SP 800-171

Many CMMC worksheets include cross references to items within the NIST SP 800-171 rev1 framework. However, note that CMMC contains additional security requirements, and thus not every CMMC provision references a NIST requirement.

1.2 Protect CUI Backups - CMMC Ctrl: RE.2.138 - Protect the confidentiality of backup CUI at storage locations. (NIST 800-171 Rev. 2 Ctrl Ref: 3.8.9)
Is the confidentiality and integrity of backup CUI protected at the storage location?

Previous Assessment Response: No
[Use Previous Response](#)

No >

Task 17: Complete CMMC Access Control Worksheet

Complete the **CMMC Access Control Worksheet**. This worksheet should be completed by an Internal Auditor.

Compliance Manager > To Do > Details

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

i Complete CMMC – Access Control Worksheet

Complete the worksheet to assess compliance with the Access Control control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.

[Go to Form: CMMC - Access Control Worksheet](#)

✓ Mark Complete

Specifically, this worksheet asks you to examine:

- Restrictions on internal system access
- Restrictions on access to external information systems
- Restrictions on information posted to public-facing data systems
- Utilization of the principle of least privilege for user accounts and their access to sensitive data

The screenshot shows the 'CMMC Access Control Worksheet' in the Compliance Manager interface. The left sidebar contains navigation links: Home, Compliance Manager, To Do, Assessments, Dashboard, Forms (selected), Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The main content area displays the worksheet title, a search bar, and buttons for 'Search', 'Download', 'Invite Others', 'Save', 'Save and Return', and 'Return'. Below this, a section titled '1 C001 - ESTABLISH SYSTEM ACCESS REQUIREMENTS (REQUIRED REMAINING)' contains three items: 1.1 Limit system access - CMMC Ctrl: AC.1.001, 1.2 Privacy and Security Notices - CMMC Ctrl: AC.2.008, and 1.3 Limit Portable Storage Device Use - CMMC Ctrl: AC.2.006. Each item has a description and a 'Show Guidance' link. The bottom of the page indicates '22 required remaining' and includes 'Save', 'Save and Return', and 'Return' buttons.

Task 18: Complete CMMC Audit and Accountability Worksheet

Complete the **CMMC Audit and Accountability Worksheet**. This worksheet should be completed by an Internal Auditor.

The screenshot shows the 'Task' details for 'Complete CMMC - Audit and Accountability Worksheet'. The breadcrumb trail is 'Compliance Manager > To Do > Details'. A 'Task' box contains the text: 'This is a task that requires an action to be taken. See below for details.' Below this, an information icon is followed by the task title. The description states: 'Complete the worksheet to assess compliance with the Audit and Accountability control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' A prominent orange button reads 'Go to Form: CMMC - Audit and Accountability Worksheet'. At the bottom, there is a 'Mark Complete' button with a checkmark icon.

Specifically, this worksheet asks you to examine:

- Event logging of individual system users and their actions
- Audit log retention
- Audit log review

The screenshot shows the 'CMMC Audit and Accountability Worksheet' in the Compliance Manager interface. The left sidebar contains a navigation menu with options: Home, Compliance Manager, To Do, Assessments, Dashboard, Forms (selected), Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The main content area displays the worksheet title and a search bar. Below the search bar, there are buttons for 'Hide #', 'Expand All', 'Collapse All', and 'Download'. A 'Select Assessment' dropdown menu is set to 'Current Assessment'. The worksheet content includes a section for '1 CO07 - DEFINE AUDIT REQUIREMENTS (3 REQUIRED REMAINING)' and two specific tasks: '1.1 Event Logging - CMMC Ctrl: AU.2.041' and '1.2 Review and Update Logged Events - CMMC Ctrl: AU.3.045'. Each task has a description and a 'Show Guidance' link. At the bottom, there are buttons for 'Save', 'Save and Return', and 'Return'.

Tip: For helpful, time-saving tips for completing worksheets and surveys, see ["Completing Assessment Worksheets and Surveys" on page 165](#).

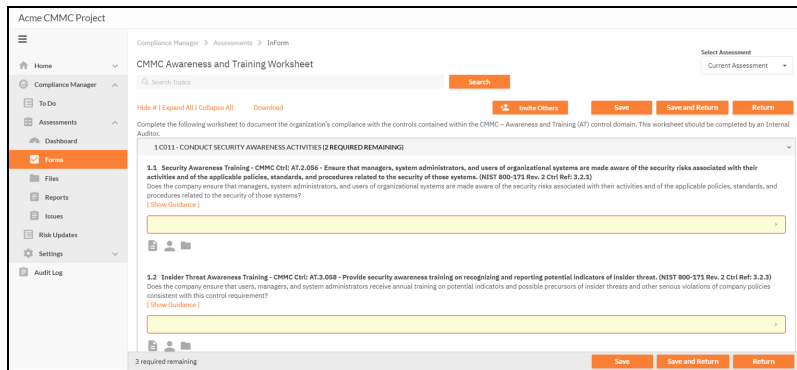
Task 19: Complete CMMC Awareness and Training Worksheet

Complete the **CMMC Awareness and Training Worksheet**. This worksheet should be completed by an Internal Auditor.

The screenshot shows a task card titled 'Complete CMMC - Awareness and Training Worksheet'. The card is part of a 'To Do' list in the 'Compliance Manager' interface. The card contains a task description: 'Complete the worksheet to assess compliance with the Awareness and Training control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' Below the description is a button labeled 'Go to Form: CMMC - Awareness and Training Worksheet'. At the bottom of the card is a button labeled 'Mark Complete'.

Specifically, this worksheet asks you to examine:

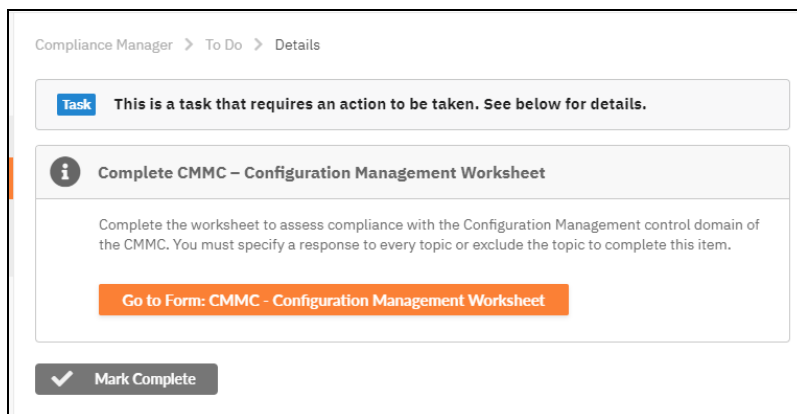
- The status of security awareness training at the organization
- The status of role-based security awareness training at the organization



Tip: For helpful, time-saving tips for completing worksheets and surveys, see ["Completing Assessment Worksheets and Surveys" on page 165](#).

Task 20: Complete CMMC Configuration Management Worksheet

Complete the **CMMC Configuration Management Worksheet**. This worksheet should be completed by an Internal Auditor.



Specifically, this worksheet asks you to examine:

- Establish configuration baselines: Ensure principle of least functionality is employed; restrictions on user-installed software.
- Configuration change management: Ensure organization analyzes security configuration changes and establishes and enforces baseline security settings.

The screenshot shows the 'Acme CMMC Project' interface. On the left is a navigation menu with options: Home, Compliance Manager, To Do, Assessments, Dashboard, Forms (selected), Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The main content area is titled 'CMMC Configuration Management Worksheet' and includes a search bar, a 'Download' button, and buttons for 'Invite Others', 'Save', 'Save and Return', and 'Return'. The worksheet content includes instructions to complete the worksheet for organizational compliance with CMMC Configuration Management (CM) controls. It lists two sections: '1.013- ESTABLISH CONFIGURATION BASELINES (REQUIRED REMAINING)' and '1.1 Baseline Configuration - CMMC CM: CM.2.061 - Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. (NIST 800-171 Rev. 2 CM Ref: 3.4.3)'. Below these sections are input fields for responses. At the bottom, it indicates '9 required remaining' and has 'Save', 'Save and Return', and 'Return' buttons.

Tip: For helpful, time-saving tips for completing worksheets and surveys, see ["Completing Assessment Worksheets and Surveys" on page 165](#).

Task 21: Complete CMMC Identification and Authentication Worksheet

Complete the **CMMC Identification and Authentication Worksheet**. This worksheet should be completed by an Internal Auditor.

The screenshot shows a task card in the 'Compliance Manager > To Do > Details' view. The card has a blue 'Task' icon and text: 'This is a task that requires an action to be taken. See below for details.' Below this is an information icon and the title 'Complete CMMC - Identification and Authentication Worksheet'. The description reads: 'Complete the worksheet to assess compliance with the Identification and Authentication control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' At the bottom of the card is an orange button that says 'Go to Form: CMMC - Identification and Authentication Worksheet'. Below the task card is a grey button with a checkmark icon and the text 'Mark Complete'.

Specifically, this worksheet asks you to examine:

- User identification procedures and practices
- Password policy, management, and enforcement

The screenshot shows the 'Acme CMMC Project' interface. On the left is a navigation sidebar with options: Home, Compliance Manager, To Do, Assessments, Forms (selected), Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The main content area is titled 'Compliance Manager > Assessments > Inform' and 'CMMC Identification and Authentication Worksheet'. It includes a search bar, a 'Search' button, and a 'Select Assessment' dropdown set to 'Current Assessment'. Below this, there are buttons for 'Download', 'Invite Others', 'Save', 'Save and Return', and 'Return'. A message states: 'Complete the following worksheet regarding the compliance with the CMMC – Identification and Authentication (IA) control domain. This worksheet should be completed by an Internal Auditor'. A progress bar shows '1 CD15 - GRANT ACCESS TO AUTHENTICATED ENTITIES (11 REQUIRED REMAINING)'. The first item is '1.1 User Accounts - CMMC Ctrl 1A.1.076 - Identify information system users, processes acting on behalf of users, or devices. (NIST 800-57 Rev. 2 Ctrl Ref: 3.5.3)'. It asks 'Does the company have a mechanism in place to identify information system users, processes acting on behalf of users, or devices?' and has a 'Show Guidance' link. Below this is a yellow input field. The second item is '1.2 Identify Users - CMMC Ctrl 1A.1.077 - Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems. (NIST 800-57 Rev. 2 Ctrl Ref: 3.6.2)'. It asks 'Does the company employ mechanisms to authenticate or verify identities of users, processes, or devices, as a prerequisite to allowing access to the information system?' and has a 'Show Guidance' link. Below this is another yellow input field. The third item is '1.3 Password Complexity - CMMC Ctrl 1A.2.078 - Enforce a minimum password complexity and change of characters when new passwords are created. (NIST 800-57 Rev. 2 Ctrl Ref: 3.6.7)'. It has a 'Show Guidance' link. At the bottom, it says '11 required remaining' and has 'Save', 'Save and Return', and 'Return' buttons.

Task 22: Complete CMMC Incident Response Worksheet

Complete the **CMMC Incident Response Worksheet**. This worksheet should be completed by an Internal Auditor.

The screenshot shows the 'Compliance Manager > To Do > Details' view. It features a 'Task' box with the text 'This is a task that requires an action to be taken. See below for details.' Below this is an information icon and the title 'Complete CMMC – Incident Response Worksheet'. The description reads: 'Complete the worksheet to assess compliance with the Incident Response control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' There is a yellow button labeled 'Go to Form: CMMC - Incident Response Worksheet'. At the bottom, there is a 'Mark Complete' button with a checkmark icon.

Specifically, this worksheet asks you to examine:

- Detail the organization's plan for handling a security incident, including planning, responding, reporting, analyzing, and testing.

The screenshot shows the 'Acme CMMC Project' interface. On the left is a navigation menu with options: Home, Compliance Manager, To Do, Assessments, Dashboard, **Form** (selected), Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The main content area is titled 'Compliance Manager > Assessments > Inform' and 'CMMC Incident Response Worksheet'. It includes a search bar, a 'Select Assessment' dropdown set to 'Current Assessment', and buttons for 'Hide #', 'Expand All', 'Collapse All', 'Download', 'Invite Others', 'Save', 'Save and Return', and 'Return'. The worksheet content includes a header stating 'Complete the following worksheet regarding the compliance with the CMMC – Incident Response (IR) control domain. This worksheet should be completed by an Internal Auditor'. It lists two sections: '1 CS16- INCIDENT PLAN RESPONSE (1 REQUIRED-REMAINING)' and '2 CS17- DETECT AND REPORT EVENTS (2 REQUIRED-REMAINING)'. Each section contains a numbered task (1.1 and 2.1) with a description and a 'Show Guidance' link. Below each task is a large yellow text input field. At the bottom, it says '2 Required remaining' and has 'Save', 'Save and Return', and 'Return' buttons.

Task 23: Complete CMMC Maintenance Worksheet

Complete the **CMMC Maintenance Worksheet**. This worksheet should be completed by an Internal Auditor.

The screenshot shows the 'Compliance Manager > To Do > Details' view. It features a 'Task' box with the text 'This is a task that requires an action to be taken. See below for details.' Below this is an information box with an 'i' icon, titled 'Complete CMMC – Maintenance Worksheet'. The text inside says 'Complete the worksheet to assess compliance with the Maintenance control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' Below the text is an orange button labeled 'Go to Form: CMMC - Maintenance Worksheet'. At the bottom is a grey button with a checkmark icon and the text 'Mark Complete'.

Specifically, this worksheet asks you to examine:

- Management of IT maintenance tools and management of IT personnel
- Multifactor authentication for remote access maintenance tools

The screenshot shows the 'CMMC Maintenance Worksheet' in the Compliance Manager application. The left sidebar contains navigation links: Home, Compliance Manager, To Do, Assessments, Dashboard, Forms (selected), Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The main content area displays the worksheet title, a search bar, and buttons for 'Initiate Others', 'Save', 'Save and Return', and 'Return'. Below this, a summary states: 'Complete the following worksheet to document the organization's compliance with the controls contained within the CMMC - Maintenance (MA) control domain. This worksheet should be completed by an Internal Auditor.' The worksheet content includes three sections: 1.001 - MAINTAINANCE MAINTENANCE (REQUIRED REMAINING), 1.1 Maintenance Tools - CMMC Ctrl: MA.2.111 - Perform maintenance on organizational systems, and 1.2 Controlled Maintenance - CMMC Ctrl: MA.2.112 - Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance. Each section has a yellow progress bar and a 'Show Guidance' link. At the bottom, a status bar indicates '0 required remaining' and includes 'Save', 'Save and Return', and 'Return' buttons.

Task 24: Complete CMMC Media Protection Worksheet

Complete the **CMMC Media Protection Worksheet**. This worksheet should be completed by an Internal Auditor.

The screenshot shows a 'Task' card in the Compliance Manager application. The card title is 'Complete CMMC - Media Protection Worksheet'. The card content includes a description: 'Complete the worksheet to assess compliance with the Media Protection control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' Below the description is a button labeled 'Go to Form: CMMC - Media Protection Worksheet'. At the bottom of the card is a button labeled 'Mark Complete'.

Specifically, this worksheet asks you to examine:

- Procedures in place to protect CUI (Controlled Unclassified Information) present on both analog and digital media within the organization
- Procedures to destroy or sanitize media devices no longer in use that might contain sensitive data

The screenshot shows the 'Acme CMMC Project' interface. On the left is a navigation menu with options: Home, Compliance Manager, To Do, Assessments, Dashboard, Forms (selected), Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The main content area is titled 'CMMC Media Protection Worksheet' and includes a search bar, a 'Download' button, and buttons for 'Invite Others', 'Save', 'Save and Return', and 'Return'. The worksheet content includes a header '1.0023 - PROTECT AND CONTROL MEDIA (3 REQUIRED REMAINING)' and three sections: 1.1 'Protect and Control - CMMC Ctrl: MP.2.119 - Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. (NIST 800-57 Rev. 2 Ctrl Ref: 3.8.5)' with a 'Show Guidance' link and a yellow input field; 1.2 'Protect and Control - CMMC Ctrl: MP.2.120 - Limit access to CUI on system media to authorized users. (NIST 800-57 Rev. 2 Ctrl Ref: 3.8.2)' with a 'Show Guidance' link and a yellow input field; and 1.3 'Protect and Control - CMMC Ctrl: MP.2.122 - Control the use of removable media on system components. (NIST 800-57 Rev. 2 Ctrl Ref: 3.8.7)' with a 'Show Guidance' link and a yellow input field. At the bottom, it says '3 required remaining' and has 'Save', 'Save and Return', and 'Return' buttons.

Task 25: Complete CMMC Personnel Security Worksheet

Complete the **CMMC Personnel Security Worksheet**. This worksheet should be completed by an Internal Auditor.

The screenshot shows the 'Compliance Manager > To Do > Details' view. It features a 'Task' box with the text 'This is a task that requires an action to be taken. See below for details.' Below this is an information box with an 'i' icon, titled 'Complete CMMC – Personnel Security Worksheet'. The text inside says 'Complete the worksheet to assess compliance with the Personnel Security control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' Below the text is an orange button labeled 'Go to Form: CMMC - Personnel Security Worksheet'. At the bottom is a grey button with a checkmark icon labeled 'Mark Complete'.

Specifically, this worksheet asks you to examine:

- Procedures to screen individuals before employment and access to sensitive data
- Procedures to restrict employee data access after they leave the organization

The screenshot shows the 'Acme CMMC Project' interface. On the left is a navigation menu with options: Home, Compliance Manager, To Do, Assessments, Dashboard, Forms (selected), Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The main content area is titled 'CMMC Personnel Security Worksheet' and includes a search bar, a 'Download' button, and buttons for 'Invite Others', 'Save', 'Save and Return', and 'Return'. Below the header, there is a section for '1 CO26 - SCREEN PERSONNEL (1 REQUIRED REMAINING)' with a sub-section '1.1 Personnel Screening - CMMC CnF: PS.2.327 - Screen individuals prior to authorizing access to organizational systems containing CUI. (NIST 800-171 Rev. 2 CUI Ref. 3.9.3)'. This section contains a text input field and a 'Show Guidance' link. Below that is a section for '2 CO27 - PROTECT CUI DURING PERSONNEL ACTIONS (1 REQUIRED REMAINING)' with a sub-section '2.1 Personnel Termination and Transfer - CMMC CnF: PS.2.328 - Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers. (NIST 800-171 Rev. 2 CUI Ref. 3.9.3)'. This section also contains a text input field and a 'Show Guidance' link. At the bottom, it indicates '2 required remaining' and has 'Save', 'Save and Return', and 'Return' buttons.

Task 26: Complete CMMC Physical Protection Worksheet

Complete the **CMMC Physical Protection Worksheet**. This worksheet should be completed by an Internal Auditor.

The screenshot shows the 'Task' details page in the Compliance Manager interface. The breadcrumb trail is 'Compliance Manager > To Do > Details'. A blue 'Task' label is followed by the text 'This is a task that requires an action to be taken. See below for details.' Below this is a section titled 'Complete CMMC - Physical Protection Worksheet' with an information icon. The text in this section reads: 'Complete the worksheet to assess compliance with the Physical Protection control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' Below the text is an orange button labeled 'Go to Form: CMMC - Physical Protection Worksheet'. At the bottom of the task card is a grey button with a checkmark icon labeled 'Mark Complete'.

Specifically, this worksheet asks you to examine:

- Measures to control physical access to site and its resources
- Visitor access control
- Visitor access audit logs
- Physical access control devices and their management

The screenshot shows the 'Acme CMMC Project' interface. On the left is a sidebar with navigation options: Home, Compliance Manager, To Do, Assessments, Dashboard, Forms (selected), Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The main content area is titled 'CMMC Physical Protection Worksheet' and includes a search bar and buttons for 'Select Assessment', 'Current Assessment', 'Add New', 'Save', 'Save and Return', and 'Return'. Below the title, there is a section for '1.1 Control Physical Access - CMMC Ctrl: PE.1.131 - Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals. (NIST 800-171 Rev. 2 Ctrl Ref: 3.35.3)'. This section contains a text input field and a 'Show Guidance' link. Below this is another section for '1.2 Visitor Access Monitoring - CMMC Ctrl: PE.1.532 - Escort visitors and monitor visitor activity. (NIST 800-171 Rev. 2 Ctrl Ref: 3.35.3)'. This section also contains a text input field and a 'Show Guidance' link. At the bottom, there is a section for '1.3 Access Audit Logs - CMMC Ctrl: PE.1.133 - Maintain audit logs of physical access. (NIST 800-171 Rev. 2 Ctrl Ref: 3.35.4)'. This section contains a text input field and a 'Show Guidance' link. The interface also shows a status bar at the bottom indicating '6 required remaining' and buttons for 'Save', 'Save and Return', and 'Return'.

Task 27: Complete CMMC Recovery Worksheet

Complete the CMMC Recovery worksheet. This worksheet should be completed by an Internal Auditor.

The screenshot shows a task card in the 'Compliance Manager > To Do > Details' view. The card has a blue 'Task' label and the text 'This is a task that requires an action to be taken. See below for details.' Below this is a section titled 'Complete CMMC - Recovery Worksheet' with an information icon. The text in this section reads: 'Complete the worksheet to assess compliance with the Recovery control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' Below the text is an orange button labeled 'Go to Form: CMMC - Recovery Worksheet'. At the bottom of the card is a grey button with a checkmark icon labeled 'Mark Complete'.

Specifically, this worksheet asks you to examine:

- Regular performance and testing of data backups
- Protection of CUI data after backup

The screenshot shows the 'CMMC Recovery Worksheet' in the Compliance Manager interface. The left sidebar contains navigation links: Home, Compliance Manager, To Do, Assessments, Dashboard, Forms (selected), Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The main content area is titled 'CMMC Recovery Worksheet' and includes a search bar and buttons for 'Hide #', 'Expand All', 'Collapse All', 'Download', 'Invite Others', 'Save', 'Save and Return', and 'Return'. The worksheet content includes a header '1 CDP - MANAGED BACKUPS (3 REQUIRED REMAINING)' and three sections: 1.1 Regularly Perform and Test Data Backups, 1.2 Protect CUI Backups, and 1.3 Perform Comprehensive Backups. Each section has a description and a 'Show Guidance' link. At the bottom, it indicates '3 required remaining' and has 'Save', 'Save and Return', and 'Return' buttons.

Task 28: Complete CMMC Risk Management Worksheet

Complete the **CMMC Risk Management Worksheet**. This worksheet should be completed by an Internal Auditor.

The screenshot shows the 'To Do' details view for the 'Complete CMMC – Risk Management Worksheet' task. The breadcrumb trail is 'Compliance Manager > To Do > Details'. A 'Task' box states: 'This is a task that requires an action to be taken. See below for details.' Below this is an information icon and the task title 'Complete CMMC – Risk Management Worksheet'. The description reads: 'Complete the worksheet to assess compliance with the Risk Management control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' A prominent orange button says 'Go to Form: CMMC - Risk Management Worksheet'. At the bottom, there is a 'Mark Complete' button with a checkmark icon.

Specifically, this worksheet asks you to examine:

- Risk and vulnerability assessment
- Vulnerability scanning
- Vulnerability remediation

The screenshot shows the 'Acme CMMC Project' interface. On the left is a sidebar with navigation links: Home, Compliance Manager, To Do, Assessments, Dashboard, Forms (selected), Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The main content area is titled 'CMMC Risk Management Worksheet' and includes a search bar, a 'Download' button, and buttons for 'Invite Others', 'Save', 'Save and Return', and 'Return'. The worksheet content includes a header '1.C031 - IDENTIFY AND EVALUATE RISK (3 REQUIRED REMAINING)' and two sections: '1.1 Risk Assessment - CMMC Ctrl: RM.2.343 - Periodically assess the risk to organizational operations...' and '1.2 Vulnerability Scanning - CMMC Ctrl: RM.2.343 - Scan for vulnerabilities in organizational systems and applications...'. Each section has a yellow input field for a response. At the bottom, it says '6 required remaining' and has 'Save', 'Save and Return', and 'Return' buttons.

Task 29: Complete CMMC Security Assessment Worksheet

Complete the CMMC Security Assessment worksheet. This worksheet should be completed by an Internal Auditor.

The screenshot shows the 'CMMC Demo Site 2' interface. On the left is a sidebar with navigation links: Home, Compliance Manager, To Do (selected), Assessments, Settings, and Audit Log. The main content area is titled 'Compliance Manager > To Do > Details' and includes a 'Task' box with the text 'This is a task that requires an action to be taken. See below for details.' Below this is a section titled 'Complete CMMC - Security Assessment Worksheet' with an information icon. The text in this section says 'Complete the worksheet to assess compliance with the Security Assessment control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' Below the text is a button that says 'Go to Form: CMMC - Security Assessment Worksheet'. At the bottom of the main content area is a 'Mark Complete' button with a checkmark icon.

Specifically, this worksheet asks you to examine:

- Existence of a system security plan
- Assessment of the security plan
- Plans of action against vulnerabilities

The screenshot shows the 'CMMC Security Assessment Worksheet' in the Compliance Manager application. The interface includes a sidebar with navigation options like Home, Compliance Manager, To Do, Assessments, Dashboard, Forms, Reports, Issues, Risk Updates, Settings, and Audit Log. The main content area displays the worksheet for 'Acme CMMC Project'. It features a search bar, a 'Select Assessment' dropdown, and a 'Current Assessment' dropdown. The worksheet is divided into sections for different CMMC domains, with a '1.1 System Security Plans' section visible. The section contains a description of the requirement and a table for documenting compliance. The table has columns for 'Control', 'Assessment', and 'Response'. The 'Control' column lists the requirement text, and the 'Assessment' column has a dropdown menu. The 'Response' column is empty. The '1.1 System Security Plans' section is marked as 'REQUIRED REMAINING'. Below it, the '2.1 Security Assessments' section is also marked as 'REQUIRED REMAINING'. At the bottom, there are buttons for 'Save', 'Save and Return', and 'Return'.

Task 30: Complete CMMC System and Communications Protection Worksheet

Complete the **CMMC System and Communications Protection Worksheet**. This worksheet should be completed by an Internal Auditor.

The screenshot shows a task card titled 'Complete CMMC – System and Communications Protection Worksheet'. The card is part of a 'To Do' list in the Compliance Manager application. It includes a 'Task' icon and a description: 'This is a task that requires an action to be taken. See below for details.' Below the description, there is an information icon and the task title. The main content area contains the instruction: 'Complete the worksheet to assess compliance with the Systems and Communication Protection control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' At the bottom of the card, there is a button labeled 'Go to Form: CMMC - Systems and Communication Protection Worksheet' and a 'Mark Complete' button with a checkmark icon.

Specifically, this worksheet asks you to examine:

- Collaborative computing devices
- Session encryption
- Communication boundary definition and protection

The screenshot shows the 'Acme CMMC Project' interface. On the left is a navigation menu with options: Home, Compliance Manager, To Do, Assessments, Dashboard, Forms (selected), Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The main content area is titled 'CMMC System and Communications Protection Worksheet'. It includes a search bar, a 'Select Assessment' dropdown, and buttons for 'Hide #', 'Expand All', 'Collapse All', 'Download', 'Invite Others', 'Save', 'Save and Return', and 'Return'. The worksheet content includes instructions for completion and two sections: '1.1 Collaborative Computing Devices' and '1.2 Session Encryption', each with a text input field and a 'Show Guidance' link. At the bottom, it states '19 required remaining' and has 'Save', 'Save and Return', and 'Return' buttons.

Task 31: Complete CMMC System and Information Integrity Worksheet

Complete the **CMMC System and Information Integrity Worksheet**. This worksheet should be completed by an Internal Auditor.

The screenshot shows the 'Compliance Manager > To Do > Details' view. It features a 'Task' header with the text 'This is a task that requires an action to be taken. See below for details.' Below this is a task card titled 'Complete CMMC – System and Information Integrity Worksheet' with an information icon. The card contains the instruction: 'Complete the worksheet to assess compliance with the System and Information Integrity control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' At the bottom of the card is an orange button labeled 'Go to Form: CMMC - System and Information Integrity Worksheet'. Below the task card is a 'Mark Complete' button with a checkmark icon.

Specifically, this worksheet asks you to:

- Catalog information systems in use and their responsible parties
- Identify and manage information system flaws
- Identify malicious content
- Perform network and system monitoring

Note: For additional guidance in answering worksheet questions 1 through 1.3, please refer to the publication "NIST SP800-18, Guide for Developing Security Plans

for Federal Information Systems," page 19, section 3, "Plan Development." This document is currently available at:

<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-18r1.pdf>

The screenshot shows the 'CMMC Demo Site 2' interface. The left sidebar contains navigation links: Home, Compliance Manager, To Do, Assessments, Dashboard, Forms (selected), Files, Reports, Issues, Settings, and Audit Log. The main content area is titled 'CMMC System and Information Integrity Worksheet'. It includes a search bar, a 'Select Assessment' dropdown set to 'Current Assessment', and buttons for 'Search', 'Hide # | Expand All | Collapse All', 'Download', 'Invite Others', 'Save', 'Save and Return', and 'Return'. Below these, a message states: 'Complete the following worksheet to document the organization's system identification details and compliance with the controls contained within the CMMC - System and Information Integrity (SI) control domain. This worksheet should be completed by an Internal Auditor.' The form has two sections: '1.1 System Name' with a text input field and '1.2 System Categorization' with a text input field. A status bar at the bottom indicates '23 required remaining' and includes 'Save', 'Save and Return', and 'Return' buttons.

Task 32: Complete NIST 800-171 Scoring Supplement (Optional)

In summer 2020, the Department of Defense (DoD) introduced a self-assessment methodology to allow contractors to achieve interim certification before the eventual implementation of the complete CMMC program.

The optional **NIST 800-171 Scoring Supplement** allows you to perform a self-assessment as per the DoD's interim rule. It is based on the DoD NIST SP 800-171 Assessment Methodology, where the final assessment results are communicated in the form of a DoD Assessment Score.

This worksheet should be completed by an Internal Auditor.

The screenshot shows the 'CMMC Demo Site 2' interface with the 'To Do' tab selected in the left sidebar. The main content area displays a task list under the heading 'Compliance Manager > To Do > Details'. The first task is 'Complete NIST 800-171 Scoring Supplement (Optional)'. The task description reads: 'Complete the worksheet to assess compliance CMMC Controls that correspond with NIST 800-171 security requirements not previously assessed during a CMMC Level 2 assessment. You must specify a response to every topic.' Below the description is an orange button labeled 'Go to Form: NIST 800 171 Scoring Supplement Worksheet'. At the bottom of the task card is a 'Mark Complete' button with a checkmark icon.

The NIST 800-171 Scoring Supplement contains and cross-references the CMMC Control Domains that are relevant to the NIST 800-171 Security Requirement.

The screenshot displays the 'Acme CMMC Project' interface. On the left is a navigation sidebar with options: Home, Compliance Manager, To Do, Assessments, Dashboard, Forms (selected), Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The main content area is titled 'Compliance Manager > Assessments > Inform' and shows the 'NIST 800-171 Scoring Supplement' worksheet. At the top right, there's a 'Select Assessment' dropdown set to 'Current Assessment'. Below the title bar are buttons for 'Previous Page', 'Next Page', and 'Page 1 of 2'. The worksheet content includes a search bar, a 'Download' button, and a 'Print' button. The main text area contains the purpose of the worksheet and two sections for controls: '1 ACCESS CONTROL (AC) (REQUIRED REMEDIATION)' and '1.1 Wireless Access and Encryption - CMMC Ctrl: AC.3.052 - Protect wireless access using authentication and encryption. (NIST 800-171 Rev. 2 Ctrl Ref: 3.1.17)'. Each section has a yellow highlighted area for input. At the bottom, there are buttons for 'Previous Page', 'Next Page', 'Page 1 of 2', 'Save', 'Save and Return', and 'Return'.

Note: Issues generated as a result of your responses to the NIST 800-171 Scoring Supplement Worksheet **do not** currently appear in the Compensating Controls Worksheet. Update your responses in the NIST 800-171 worksheet itself to indicate any mitigation measures taken to resolve issues identified. Return to the Worksheet To Do item, click the "Modify" button, and modify the worksheet responses to reflect the remediation actions undertaken.

Complete the Scoring Supplement to access the following compliance reports at the end of your assessment:

- CUI Plan of Action and Milestones Report
- CUI System Security Plan
- NIST 800 171 Scoring Supplement Worksheet
- NIST SP 800 171 DoD Assessment Score Report

Complete Level 3 CMMC Worksheets

Once you choose the Level 3 CMMC assessment, new worksheets will appear in your to do list.

CMMC Demo Site 2			
Complete	9/21/20, 9:01 PM	Running Local Scan of Remote Computers	
Complete	9/22/20, 10:29 AM	Run Local Data Collector (Optional)	
Complete	9/22/20, 10:30 AM	Complete Antivirus Verification Worksheet	
Complete	9/22/20, 10:30 AM	Complete User Access Review Worksheet	
Complete	9/22/20, 10:39 AM	Complete Asset Inventory Worksheet	
Complete	9/22/20, 10:39 AM	Complete Application Inventory Worksheet	
Complete	9/22/20, 10:39 AM	Complete External Information System Worksheet	
Complete	9/22/20, 1:46 PM	Select Level of CMMC Assessment	
Task	9/22/20, 1:46 PM	Complete CMMC – Access Control Worksheet	
Task	9/22/20, 1:46 PM	Complete CMMC – Audit and Accountability Worksheet	
Task	9/22/20, 1:46 PM	Complete CMMC – Awareness and Training Worksheet	
Task	9/22/20, 1:46 PM	Complete CMMC – Configuration Management Worksheet	
Task	9/22/20, 1:46 PM	Complete CMMC – Identification and Authentication Worksheet	
Task	9/22/20, 1:46 PM	Complete CMMC – Incident Response Worksheet	
Task	9/22/20, 1:46 PM	Complete CMMC – Maintenance Worksheet	
Task	9/22/20, 1:46 PM	Complete CMMC – Media Protection Worksheet	

Note Regarding Worksheet Cross References to NIST SP 800-171

Many CMMC worksheets include cross references to items within the NIST SP 800-171 rev1 framework. However, note that CMMC contains additional security requirements, and thus not every CMMC provision references a NIST requirement.

1.2 Protect CUI Backups - CMMC Ctrl: RE.2.138 - Protect the confidentiality of backup CUI at storage locations. (NIST 800-171 Rev. 2 Ctrl Ref: 3.8.9)

Is the confidentiality and integrity of backup CUI protected at the storage location?

Previous Assessment Response: No
[Use Previous Response](#)

No >

Task 17: Complete CMMC Access Control Worksheet

Complete the **CMMC Access Control Worksheet**. This worksheet should be completed by an Internal Auditor.

Compliance Manager > To Do > Details

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

i Complete CMMC – Access Control Worksheet

Complete the worksheet to assess compliance with the Access Control control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.

[Go to Form: CMMC - Access Control Worksheet](#)

[✓ Mark Complete](#)

Specifically, this worksheet asks you to examine:

- Restrictions on internal system access
- Restrictions on access to external information systems
- Restrictions on information posted to public-facing data systems
- Utilization of the principle of least privilege for user accounts and their access to sensitive data

Acme CMMC Project

Compliance Manager > Assessments > To Do

CMMC Access Control Worksheet

Select Assessment
Current Assessment

Search Topics

Hide # | Expand All | Collapse All | Download

Invite Others | Save | Save and Return | Return

Complete the following worksheet regarding the compliance with the CMMC – Access Control (AC) control domain. This worksheet should be completed by an Internal Auditor

1 C001 - ESTABLISH SYSTEM ACCESS REQUIREMENTS (REQUIRED REMAINING)

1.1 Limit system access - CMMC Ctrl: AC.1.001 - Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). (NIST 800-171 Rev. 2 Ctrl Ref: 3.5.1)

Has the company implemented a mechanism to limit information system access to authorized users, processes acting on behalf of authorized users, or devices?

1.2 Privacy and Security Notices - CMMC Ctrl: AC.2.006 - Provide privacy and security notices consistent with applicable CUI rules. (NIST 800-171 Rev. 2 Ctrl Ref: 3.5.9)

Has the company developed and implemented privacy and security notices with applicable CUI rules?

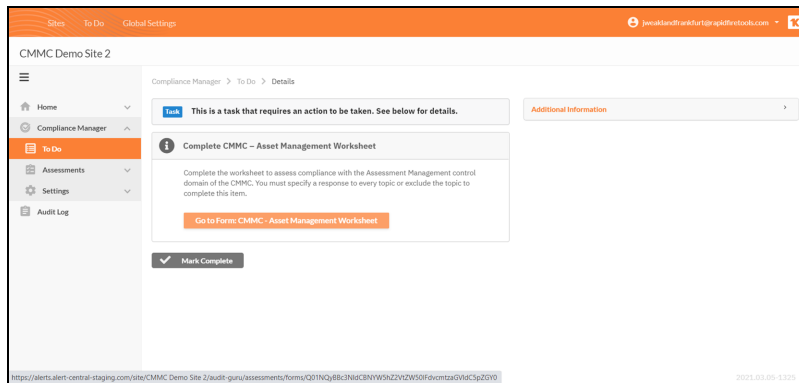
1.3 Limit Portable Storage Device Use - CMMC Ctrl: AC.2.006 - Limit use of portable storage devices on external systems. (NIST 800-171 Rev. 2 Ctrl Ref: 3.5.21)

22 required remaining

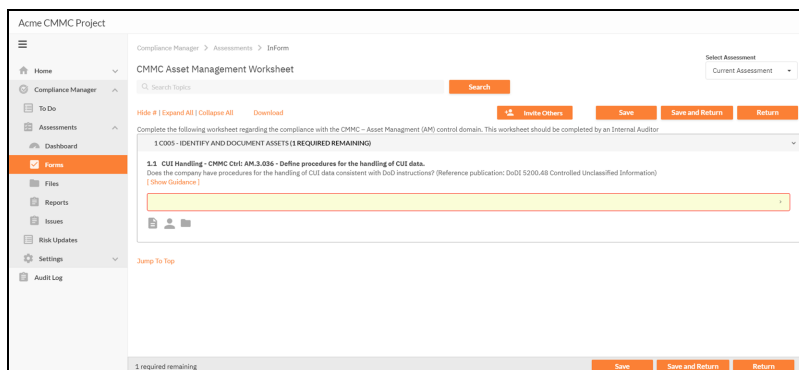
Save | Save and Return | Return

Task 18: Complete Asset Management Worksheet

Complete the **CMMC Asset Management Worksheet**. This worksheet should be completed by an Internal Auditor.

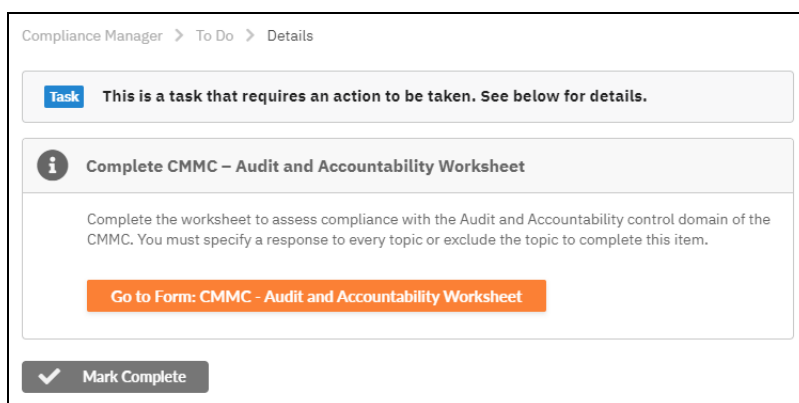


Specifically, this worksheet asks you to examine processes and procedures in place in order to manage "controlled unclassified information" (CUI).



Task 19: Complete CMMC Audit and Accountability Worksheet

Complete the **CMMC Audit and Accountability Worksheet**. This worksheet should be completed by an Internal Auditor.



Specifically, this worksheet asks you to examine:

- Event logging of individual system users and their actions
- Audit log retention
- Audit log review

The screenshot shows the 'CMMC Audit and Accountability Worksheet' in the Compliance Manager interface. The left sidebar contains navigation links: Home, Compliance Manager, To Do, Assessments, Dashboard, Forms (highlighted), Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The main content area displays the worksheet title, a search bar, and buttons for 'Hide #', 'Expand All', 'Collapse All', 'Download', 'Invite Others', 'Save', 'Save and Return', and 'Return'. Below this, a section titled '1 C007 - DEFINE AUDIT REQUIREMENTS (3 REQUIRED REMAINING)' is shown. It includes two sub-sections: '1.1 Event Logging - CMMC Ctrl: AU.3.043 - Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions, (NIST 800-57 Rev. 2 Ctrl Ref: 3.3.2)' and '1.2 Review and Update Logged Events - CMMC Ctrl: AU.3.045 - Review and update logged events, (NIST 800-57 Rev. 2 Ctrl Ref: 3.3.3)'. Each sub-section has a 'Show Guidance' link and a large yellow input field. At the bottom, it indicates '33 required remaining' and has 'Save', 'Save and Return', and 'Return' buttons.

Tip: For helpful, time-saving tips for completing worksheets and surveys, see ["Completing Assessment Worksheets and Surveys" on page 165](#).

Task 20: Complete CMMC Awareness and Training Worksheet

Complete the **CMMC Awareness and Training Worksheet**. This worksheet should be completed by an Internal Auditor.

The screenshot shows a task card in the Compliance Manager interface. The breadcrumb trail at the top reads 'Compliance Manager > To Do > Details'. The card has a 'Task' header with the text 'This is a task that requires an action to be taken. See below for details.' Below this is an information icon and the title 'Complete CMMC - Awareness and Training Worksheet'. The main text states: 'Complete the worksheet to assess compliance with the Awareness and Training control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' At the bottom of the card is an orange button labeled 'Go to Form: CMMC - Awareness and Training Worksheet'. Below the card is a 'Mark Complete' button with a checkmark icon.

Specifically, this worksheet asks you to examine:

- The status of security awareness training at the organization
- The status of role-based security awareness training at the organization

Acme CMMC Project

Compliance Manager > Assessments > Inform

CMMC Awareness and Training Worksheet

Search

Select Assessment
Current Assessment

Hide # | Expand All | Collapse All | Download

Invite Others | Save | Save and Return | Return

Complete the following worksheet to document the organization's compliance with the controls contained within the CMMC – Awareness and Training (AT) control domain. This worksheet should be completed by an Internal Auditor.

1.C011- CONDUCT SECURITY AWARENESS ACTIVITIES (2 REQUIRED REMAINING)

1.1 Security Awareness Training - CMMC Ctrl: AT.2.056 - Ensure that managers, system administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of these systems. (NIST 800-571 Rev. 2 Ctrl Ref: 3.2.3)

Does the company ensure that managers, system administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of these systems?

[Show Guidance]

1.2 Insider Threat Awareness Training - CMMC Ctrl: AT.3.058 - Provide security awareness training on recognizing and reporting potential indicators of insider threat. (NIST 800-571 Rev. 2 Ctrl Ref: 3.2.3)

Does the company ensure that users, managers, and system administrators receive annual training on potential indicators and possible precursors of insider threats and other serious violations of company policies consistent with this control requirement?

[Show Guidance]

2 required remaining

Save | Save and Return | Return

Tip: For helpful, time-saving tips for completing worksheets and surveys, see ["Completing Assessment Worksheets and Surveys" on page 165](#).

Task 21: Complete CMMC Configuration Management Worksheet

Complete the **CMMC Configuration Management Worksheet**. This worksheet should be completed by an Internal Auditor.

Compliance Manager > To Do > Details

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

Complete CMMC – Configuration Management Worksheet

Complete the worksheet to assess compliance with the Configuration Management control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.

Go to Form: CMMC - Configuration Management Worksheet

Mark Complete

Specifically, this worksheet asks you to examine:

- Establish configuration baselines: Ensure principle of least functionality is employed; restrictions on user-installed software.
- Configuration change management: Ensure organization analyzes security configuration changes and establishes and enforces baseline security settings.

The screenshot shows the 'Acme CMMC Project' interface. On the left is a navigation menu with options: Home, Compliance Manager, To Do, Assessments, Dashboard, Forms (selected), Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The main content area is titled 'CMMC Configuration Management Worksheet' and includes a search bar, a 'Download' button, and buttons for 'Invite Others', 'Save', 'Save and Return', and 'Return'. The worksheet content includes instructions to complete the worksheet for organizational compliance with CMMC Configuration Management (CM) controls. It lists two sections: '1.013- ESTABLISH CONFIGURATION BASELINES (REQUIRED REMAINING)' and '1.1 Baseline Configuration - CMMC CM: CM.2.061 - Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. (NIST 800-171 Rev. 2 CM Ref: 3.4.3)'. Below these sections are input fields for responses. At the bottom, it indicates '9 required remaining' and has 'Save', 'Save and Return', and 'Return' buttons.

Tip: For helpful, time-saving tips for completing worksheets and surveys, see ["Completing Assessment Worksheets and Surveys" on page 165](#).

Task 22: Complete CMMC Identification and Authentication Worksheet

Complete the **CMMC Identification and Authentication Worksheet**. This worksheet should be completed by an Internal Auditor.

The screenshot shows the 'To Do' task details in the Compliance Manager interface. The breadcrumb trail is 'Compliance Manager > To Do > Details'. A task card is displayed with the title 'Complete CMMC - Identification and Authentication Worksheet' and an information icon. The task description states: 'Complete the worksheet to assess compliance with the Identification and Authentication control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' Below the description is an orange button labeled 'Go to Form: CMMC - Identification and Authentication Worksheet'. At the bottom of the task card is a 'Mark Complete' button with a checkmark icon.

Specifically, this worksheet asks you to examine:

- User identification procedures and practices
- Password policy, management, and enforcement

The screenshot shows the 'Acme CMMC Project' interface. On the left is a navigation sidebar with options: Home, Compliance Manager, To Do, Assessments, Forms (selected), Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The main content area is titled 'Compliance Manager > Assessments > Inform' and 'CMMC Identification and Authentication Worksheet'. It includes a search bar, a 'Search' button, and buttons for 'Hide #', 'Expand All', 'Collapse All', 'Download', 'Invite Others', 'Save', 'Save and Return', and 'Return'. The worksheet content includes a header 'Complete the following worksheet regarding the compliance with the CMMC – Identification and Authentication (IA) control domain. This worksheet should be completed by an Internal Auditor.' and a section '1.0015 - GRANT ACCESS TO AUTHENTICATED ENTITIES (11 REQUIRED REMAINING)'. Below this are three numbered items: 1.1 User Accounts, 1.2 Identify Users, and 1.3 Password Complexity, each with a description and a 'Show Guidance' link. Each item has a corresponding form field with a dropdown arrow. At the bottom, there are 'Save', 'Save and Return', and 'Return' buttons.

Task 23: Complete CMMC Incident Response Worksheet

Complete the **CMMC Incident Response Worksheet**. This worksheet should be completed by an Internal Auditor.

The screenshot shows the 'Compliance Manager > To Do > Details' view. It features a 'Task' section with the text 'This is a task that requires an action to be taken. See below for details.' Below this is an information icon and the title 'Complete CMMC – Incident Response Worksheet'. The description reads: 'Complete the worksheet to assess compliance with the Incident Response control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' A prominent orange button says 'Go to Form: CMMC - Incident Response Worksheet'. At the bottom, there is a 'Mark Complete' button with a checkmark icon.

Specifically, this worksheet asks you to examine:

- Detail the organization's plan for handling a security incident, including planning, responding, reporting, analyzing, and testing.

The screenshot shows the 'CMMC Incident Response Worksheet' form within the 'Acme CMMC Project' workspace. The left sidebar contains navigation links: Home, Compliance Manager, To Do, Assessments, Dashboard, Forms (selected), Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The main content area has a breadcrumb trail 'Compliance Manager > Assessments > Inform' and a 'Select Assessment' dropdown set to 'Current Assessment'. Below the header, there are buttons for 'Search', 'Download', 'Invite Others', 'Save', 'Save and Return', and 'Return'. The form content includes a title bar 'CMMC Incident Response Worksheet' and a description: 'Complete the following worksheet regarding the compliance with the CMMC – Incident Response (IR) control domain. This worksheet should be completed by an Internal Auditor'. The form is divided into two sections: '1 CS16- INCIDENT PLAN RESPONSE (1 REQUIRED-REMAINING)' and '2 CS17- DETECT AND REPORT EVENTS (2 REQUIRED-REMAINING)'. Each section contains a numbered list of tasks (1.1, 1.2, 2.1, 2.2) with corresponding guidance links and a large yellow text input area. At the bottom, there is a 'Required remaining' status bar and buttons for 'Save', 'Save and Return', and 'Return'.

Task 24: Complete CMMC Maintenance Worksheet

Complete the **CMMC Maintenance Worksheet**. This worksheet should be completed by an Internal Auditor.

The screenshot shows a task card titled 'Complete CMMC – Maintenance Worksheet' within the 'Compliance Manager > To Do > Details' view. The card has a blue 'Task' label and a message: 'This is a task that requires an action to be taken. See below for details.' Below this, there is an information icon and the task title. The main text of the card reads: 'Complete the worksheet to assess compliance with the Maintenance control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' At the bottom of the card, there is an orange button labeled 'Go to Form: CMMC - Maintenance Worksheet' and a grey button with a checkmark labeled 'Mark Complete'.

Specifically, this worksheet asks you to examine:

- Management of IT maintenance tools and management of IT personnel
- Multifactor authentication for remote access maintenance tools

The screenshot shows the 'CMMC Maintenance Worksheet' in the Compliance Manager application. The left sidebar contains navigation links: Home, Compliance Manager, To Do, Assessments, Dashboard, Forms (selected), Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The main content area displays the worksheet title, a search bar, and buttons for 'Initiate Others', 'Save', 'Save and Return', and 'Return'. Below this, a note states: 'Complete the following worksheet to document the organization's compliance with the controls contained within the CMMC - Maintenance (MA) control domain. This worksheet should be completed by an Internal Auditor.' The worksheet content includes three sections: 1.001 - MAINTENANCE (REQUIRED REMAINING), 1.1 Maintenance Tools - CMMC Ctrl: MA.2.111 - Perform maintenance on organizational systems, and 1.2 Controlled Maintenance - CMMC Ctrl: MA.2.132 - Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance. Each section has a yellow highlighted area for input. At the bottom, there is a 'Save' button and a 'Save and Return' button.

Task 25: Complete CMMC Media Protection Worksheet

Complete the **CMMC Media Protection Worksheet**. This worksheet should be completed by an Internal Auditor.

The screenshot shows a 'Task' card in the Compliance Manager application. The card title is 'Complete CMMC - Media Protection Worksheet'. The card content includes a description: 'Complete the worksheet to assess compliance with the Media Protection control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' Below the description is a button labeled 'Go to Form: CMMC - Media Protection Worksheet'. At the bottom of the card is a button labeled 'Mark Complete'.

Specifically, this worksheet asks you to examine:

- Procedures in place to protect CUI (Controlled Unclassified Information) present on both analog and digital media within the organization
- Procedures to destroy or sanitize media devices no longer in use that might contain sensitive data

The screenshot shows the 'Acme CMMC Project' interface. On the left is a navigation menu with options: Home, Compliance Manager, To Do, Assessments, Dashboard, Forms (selected), Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The main content area is titled 'Compliance Manager > Assessments > Inform' and 'CMMC Media Protection Worksheet'. It includes a search bar, a 'Select Assessment' dropdown set to 'Current Assessment', and buttons for 'Hide #', 'Expand All', 'Collapse All', 'Download', 'Invite Others', 'Save', 'Save and Return', and 'Return'. The worksheet content states: 'Complete the following worksheet regarding the compliance with the CMMC – Media Protection (MP) control domain. This worksheet should be completed by an Internal Auditor'. It lists three tasks: 1.023 - PROTECT AND CONTROL MEDIA (3 REQUIRED REMAINING), 1.1 Protect and Control - CMMC Ctrl: MP.2.119 - Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital, (NIST 800-57 Rev. 2 Ctrl Ref: 3.8.5) [Show Guidance], and 1.2 Protect and Control - CMMC Ctrl: MP.2.120 - Limit access to CUI on system media to authorized users, (NIST 800-57 Rev. 2 Ctrl Ref: 3.8.2) [Show Guidance]. Each task has a yellow progress bar. At the bottom, it says '1.3 Protect and Control - CMMC Ctrl: MP.2.122 - Control the use of removable media on system components, (NIST 800-57 Rev. 2 Ctrl Ref: 3.8.7) [Show Guidance]' and '0 required remaining'.

Task 26: Complete CMMC Personnel Security Worksheet

Complete the **CMMC Personnel Security Worksheet**. This worksheet should be completed by an Internal Auditor.

The screenshot shows the 'Compliance Manager > To Do > Details' view. It features a 'Task' box with the text 'This is a task that requires an action to be taken. See below for details.' Below this is an information box with an 'i' icon, titled 'Complete CMMC – Personnel Security Worksheet'. The text inside says: 'Complete the worksheet to assess compliance with the Personnel Security control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' Below the text is an orange button labeled 'Go to Form: CMMC - Personnel Security Worksheet'. At the bottom is a grey button with a checkmark icon labeled 'Mark Complete'.

Specifically, this worksheet asks you to examine:

- Procedures to screen individuals before employment and access to sensitive data
- Procedures to restrict employee data access after they leave the organization

The screenshot shows the 'Acme CMMC Project' interface. On the left is a navigation menu with options: Home, Compliance Manager, To Do, Assessments, Dashboard, Forms (selected), Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The main content area is titled 'CMMC Personnel Security Worksheet' and includes a search bar, a 'Download' button, and buttons for 'Invite Others', 'Save', 'Save and Return', and 'Return'. Below this, a summary states: 'Complete the following worksheet to document the organization's compliance with the controls contained within the CMMC – Personnel Security (PS) control domain. This worksheet should be completed by an Internal Auditor.' The worksheet is divided into two sections: '1 CO26 - SCREEN PERSONNEL (1 REQUIRED REMAINING)' and '2 CO27 - PROTECT CUI DURING PERSONNEL ACTIONS (1 REQUIRED REMAINING)'. Each section contains a specific control question and a yellow progress bar. The first question is '1.1 Personnel Screening - CMMC CnE PS.2.327 - Screen individuals prior to authorizing access to organizational systems containing CUI. (NIST 800-171 Rev. 2 CUI Ref. 3.9.3) Does the company screen individuals requiring access before access is granted?'. The second question is '2.1 Personnel Termination and Transfer - CMMC CnE PS.2.328 - Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers. (NIST 800-171 Rev. 2 CUI Ref. 3.9.3) Does the company disable information system access prior to employee termination or transfer?'. At the bottom, it indicates '2 required remaining' and provides 'Save', 'Save and Return', and 'Return' buttons.

Task 27: Complete CMMC Physical Protection Worksheet

Complete the **CMMC Physical Protection Worksheet**. This worksheet should be completed by an Internal Auditor.

The screenshot shows a 'Task' notification in the 'Compliance Manager > To Do > Details' view. The task title is 'Complete CMMC – Physical Protection Worksheet'. The description states: 'Complete the worksheet to assess compliance with the Physical Protection control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' Below the description is an orange button labeled 'Go to Form: CMMC - Physical Protection Worksheet'. At the bottom, there is a 'Mark Complete' button with a checkmark icon.

Specifically, this worksheet asks you to examine:

- Measures to control physical access to site and its resources
- Visitor access control
- Visitor access audit logs
- Physical access control devices and their management

The screenshot shows the 'Acme CMMC Project' interface. On the left is a sidebar with navigation links: Home, Compliance Manager, To Do, Assessments, Dashboard, Forms (highlighted), Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The main content area is titled 'Compliance Manager > Assessments > InfoForm' and displays the 'CMMC Physical Protection Worksheet'. It includes a search bar, a 'Select Assessment' dropdown, and a 'Current Assessment' dropdown. The worksheet content includes a header 'CMMC Physical Protection Worksheet' and a sub-header '1 C208-LIMIT PHYSICAL ACCESS (6 REQUIRED REMAINING)'. Below this, there are two sections: '1.1 Control Physical Access - CMMC Ctrl: PE.1.131 - Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals. (NIST 800-171 Rev. 2 Ctrl Ref: 3.35.3)' and '1.2 Visitor Access Monitoring - CMMC Ctrl: PE.1.132 - Escort visitors and monitor visitor activity. (NIST 800-171 Rev. 2 Ctrl Ref: 3.35.3)'. Each section has a 'Show Guidance' link and a large yellow input field. At the bottom, there is a section for '1.3 Access Audit Logs - CMMC Ctrl: PE.1.133 - Maintain audit logs of physical access. (NIST 800-171 Rev. 2 Ctrl Ref: 3.35.4)' with a '6 required remaining' status and 'Save', 'Save and Return', and 'Return' buttons.

Task 28: Complete CMMC Recovery Worksheet

Complete the CMMC Recovery worksheet. This worksheet should be completed by an Internal Auditor.

The screenshot shows the 'Compliance Manager > To Do > Details' view. It features a 'Task' card with the text 'This is a task that requires an action to be taken. See below for details.' Below this is an information card titled 'Complete CMMC – Recovery Worksheet' with an information icon. The card contains the text: 'Complete the worksheet to assess compliance with the Recovery control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' Below the text is an orange button labeled 'Go to Form: CMMC - Recovery Worksheet'. At the bottom of the card is a 'Mark Complete' button with a checkmark icon.

Specifically, this worksheet asks you to examine:

- Regular performance and testing of data backups
- Protection of CUI data after backup

The screenshot shows the 'Acme CMMC Project' interface. On the left is a navigation menu with options: Home, Compliance Manager, To Do, Assessments, Dashboard, Forms (selected), Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The main content area is titled 'CMMC Recovery Worksheet' and includes a search bar and buttons for 'Hide #', 'Expand All', 'Collapse All', 'Download', 'Invite Others', 'Save', 'Save and Return', and 'Return'. Below this, a section titled '1 CDP - MANAGED BACKUPS (3 REQUIRED REMAINING)' contains three tasks: 1.1 Regularly Perform and Test Data Backups, 1.2 Protect CUI Backups, and 1.3 Perform Comprehensive Backups. Each task has a description and a 'Show Guidance' link. At the bottom, it indicates '3 required remaining' and has 'Save', 'Save and Return', and 'Return' buttons.

Task 29: Complete CMMC Risk Management Worksheet

Complete the **CMMC Risk Management Worksheet**. This worksheet should be completed by an Internal Auditor.

The screenshot shows the 'Compliance Manager > To Do > Details' page. It features a 'Task' box with the text: 'This is a task that requires an action to be taken. See below for details.' Below this is an information box with an 'i' icon, titled 'Complete CMMC – Risk Management Worksheet'. The text inside says: 'Complete the worksheet to assess compliance with the Risk Management control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' A prominent orange button reads 'Go to Form: CMMC - Risk Management Worksheet'. At the bottom, there is a 'Mark Complete' button with a checkmark icon.

Specifically, this worksheet asks you to examine:

- Risk and vulnerability assessment
- Vulnerability scanning
- Vulnerability remediation

The screenshot shows the 'Acme CMMC Project' interface. On the left is a navigation menu with options: Home, Compliance Manager, To Do, Assessments, Dashboard, Forms (selected), Files, Reports, Issues, Risk Updates, Settings, and Audit Log. The main content area is titled 'CMMC Risk Management Worksheet' and includes a search bar, a 'Download' button, and buttons for 'Invite Others', 'Save', 'Save and Return', and 'Return'. The worksheet content includes a header '1.C031 - IDENTIFY AND EVALUATE RISK (3 REQUIRED REMAINING)' and two sections: '1.1 Risk Assessment - CMMC Ctrl: RM.2.343 - Periodically assess the risk to organizational operations...' and '1.2 Vulnerability Scanning - CMMC Ctrl: RM.2.343 - Scan for vulnerabilities in organizational systems and applications...'. Each section has a yellow input field for a response. At the bottom, it says '6 required remaining' and has 'Save', 'Save and Return', and 'Return' buttons.

Task 30: Complete CMMC Security Assessment Worksheet

Complete the CMMC Security Assessment worksheet. This worksheet should be completed by an Internal Auditor.

The screenshot shows the 'CMMC Demo Site 2' interface. On the left is a navigation menu with options: Home, Compliance Manager, To Do (selected), Assessments, Settings, and Audit Log. The main content area is titled 'Compliance Manager > To Do > Details'. It features a 'Task' box with the text 'This is a task that requires an action to be taken. See below for details.' Below this is a task card titled 'Complete CMMC - Security Assessment Worksheet' with an information icon. The card text says 'Complete the worksheet to assess compliance with the Security Assessment control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' Below the text is a button that says 'Go to Form: CMMC - Security Assessment Worksheet'. At the bottom of the task card is a 'Mark Complete' button with a checkmark icon.

Specifically, this worksheet asks you to examine:

- Existence of a system security plan
- Assessment of the security plan
- Plans of action against vulnerabilities

The screenshot shows the 'CMMC Security Assessment Worksheet' in the Compliance Manager interface. The left sidebar contains navigation links: Home, Compliance Manager, To Do, Assessments, Dashboard, Forms (selected), Reports, Issues, Risk Updates, Settings, and Audit Log. The main content area displays the worksheet for 'Acme CMMC Project'. It includes a search bar, a 'Select Assessment' dropdown, and a 'Current Assessment' dropdown. The worksheet is divided into sections for '1 CO34- DEVELOP AND MANAGE A SYSTEM SECURITY PLAN (3 REQUIRED REMAINING)' and '2 CO35- DEFINE AND MANAGE CONTROLS (3 REQUIRED REMAINING)'. Each section contains a task description and a 'Show Guidance' link. At the bottom, there are buttons for 'Save', 'Save and Return', and 'Return', and a status bar indicating '5 required remaining'.

Task 31: Complete Situational Awareness Worksheet

Complete the **CMMC Situational Awareness Worksheet**. This worksheet should be completed by an Internal Auditor.

The screenshot shows the 'CMMC Demo Site 2' interface. The left sidebar contains navigation links: Home, Compliance Manager, To Do (selected), Assessments, Settings, and Audit Log. The main content area displays a task titled 'Complete CMMC – Situational Awareness Worksheet'. The task description states: 'Complete the worksheet to assess compliance with the Situational Awareness control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.' Below the description is a button labeled 'Go to Form: CMMC - Situational Awareness Worksheet'. At the bottom, there is a 'Mark Complete' button.

Specifically, this worksheet asks you to examine how the organization becomes aware of and/or identifies potential cyber threats.

The screenshot shows the 'CMMC Situational Awareness Worksheet' in the Compliance Manager interface. The left sidebar contains navigation links: Home, Compliance Manager, To Do, Assessments, Dashboard, Forms (selected), Reports, Issues, Risk Updates, Settings, and Audit Log. The main content area displays the worksheet for 'Acme CMMC Project'. It includes a search bar, a 'Select Assessment' dropdown, and a 'Current Assessment' dropdown. The worksheet is divided into sections for '1 CO37- IMPLEMENT THREAT MONITORING (3 REQUIRED REMAINING)' and '1.1 Threat Monitoring - CMMC Ctl: SA.3.3.69 - Resolve and respond to cyber threat intelligence from information sharing forums and sources and communicate to stakeholders'. Each section contains a task description and a 'Show Guidance' link. At the bottom, there are buttons for 'Save', 'Save and Return', and 'Return', and a status bar indicating '1 required remaining'.

Task 32: Complete CMMC System and Communications Protection Worksheet

Complete the **CMMC System and Communications Protection Worksheet**. This worksheet should be completed by an Internal Auditor.

Compliance Manager > To Do > Details

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

Complete CMMC – System and Communications Protection Worksheet

Complete the worksheet to assess compliance with the Systems and Communication Protection control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.

[Go to Form: CMMC - Systems and Communication Protection Worksheet](#)

☒ Mark Complete

Specifically, this worksheet asks you to examine:

- Collaborative computing devices
- Session encryption
- Communication boundary definition and protection

Acme CMMC Project

Compliance Manager > Assessments > 3dForm

CMMC System and Communications Protection Worksheet

Select Assessment: Current Assessment

Search Topics

Hide # | Expand All | Collapse All | Download

14 | Invite Others | Save | Save and Return | Return

Complete the following worksheet regarding the compliance with the controls contain within the CMMC - System and Communications Protection (SC) control domain. This worksheet should be completed by an Internal Auditor.

1 CO38 - DEFINE SECURITY REQUIREMENTS FOR SYSTEMS AND COMMUNICATIONS (15 REQUIRED REMAINING)

1.1 Collaborative Computing Devices - CMMC Ctrl: SC.2.378 - Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device. (NIST 800-57 Rev. 2 Ctrl Ref: 3.3.3.2)

Does the company prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device?

[Show Guidance]

1.2 Session Encryption - CMMC Ctrl: SC.2.379 - Use encrypted sessions for the management of network devices.

Does the company employ mechanisms to encrypt sessions during the management of network devices?

[Show Guidance]

19 required remaining

Save | Save and Return | Return

Task 33: Complete CMMC System and Information Integrity Worksheet

Complete the **CMMC System and Information Integrity Worksheet**. This worksheet should be completed by an Internal Auditor.

Compliance Manager > To Do > Details

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

Complete CMMC – System and Information Integrity Worksheet

Complete the worksheet to assess compliance with the System and Information Integrity control domain of the CMMC. You must specify a response to every topic or exclude the topic to complete this item.

[Go to Form: CMMC - System and Information Integrity Worksheet](#)

☒ Mark Complete

Specifically, this worksheet asks you to:

- Catalog information systems in use and their responsible parties
- Identify and manage information system flaws
- Identify malicious content
- Perform network and system monitoring

Note: For additional guidance in answering worksheet questions 1 through 1.3, please refer to the publication "NIST SP800-18, Guide for Developing Security Plans for Federal Information Systems," page 19, section 3, "Plan Development." This document is currently available at:

<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-18r1.pdf>

CMMC Demo Site 2

Compliance Manager > Assessments > InForm

CMMC System and Information Integrity Worksheet

Select Assessment: Current Assessment

Search Topics

Hide # | Expand All | Collapse All Download Invite Others Save Save and Return Return

Complete the following worksheet to document the organization's system identification details and compliance with the controls contained within the CMMC – System and Information Integrity (SI) control domain. This worksheet should be completed by an Internal Auditor.

1 INFORMATION SYSTEM NAME AND TITLE (3 REQUIRED REMAINING)

1.1 System Name
State the name of the system in the field below. Spell out acronyms.

Required Response

1.2 System Categorization
Enter the System Categorization in the field below.

Required Response

1.3 required remaining

Save Save and Return Return

Generate CMMC Reports

In this phase, the Internal Auditor will document any compensating controls before generating and reviewing the assessment reports.

Complete the Compensating Controls Worksheet

Use this worksheet to document any compensating controls used to mitigate the risks detected during the assessment.

The screenshot shows the 'Compensating Control Worksheet' in the CMMC Demo Site 2. The left sidebar contains navigation links: Home, Compliance Manager, To Do, Assessments, Dashboard, Forms (selected), Files, Reports, Issues, Settings, and Audit Log. The main content area has a breadcrumb trail 'Compliance Manager > Assessments > Inform' and a 'Select Assessment' dropdown set to 'Current Assessment'. Below this is a search bar and a 'Search' button. Action buttons include 'Hide # | Expand All | Collapse All', 'Download', 'Save', 'Save and Return', and 'Return'. The worksheet content shows a green checkmark icon and the title '1 PROCEDURES AND MECHANISMS REQUIRED TO PERFORM PERIODIC AND REAL-TIME SCANS OF FILES FROM EXTERNAL SOURCES'. The status is 'NOT IMPLEMENTED'. The description reads: 'time scans of files from external sources as files are downloaded, opened, or executed.' Below this is a section for '1.1 Procedures and Mechanisms Required to Perform Periodic and Real-Time Scans of Files from External Sources not Implemented' with a prompt to confirm the issue status. A 'Valid' dropdown menu is present. At the bottom, it says '0 required remaining' and has 'Save', 'Save and Return', and 'Return' buttons.

Note: Once you complete the Compensating Controls Worksheet, your CMMC Assessment reports will become available to review. You will receive an email notification when the reports are ready to view. This process may take a few minutes.

When you are finished entering your responses, click **Save**. You can also click **Save and Return** to return to the To Do task details page. If you do not wish to save changes, click **Return**.

This close-up shows the bottom of the worksheet interface. It includes the 'Worksheet' label, a language dropdown set to 'English (US)', and the 'Select Assessment' dropdown set to 'Current Assessment'. A purple arrow points to the 'Save' button, which is highlighted in yellow. The 'Save and Return' button is also visible next to it.

Click **Mark Complete** on the task To Do page when you are ready to finalize the worksheet and continue the assessment.

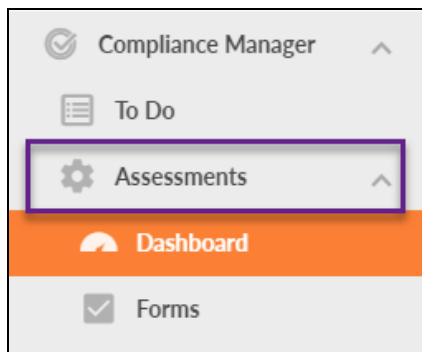
Review Final Reports

After documenting the compensating controls, the assessment reports and supporting documentation will become available for review.

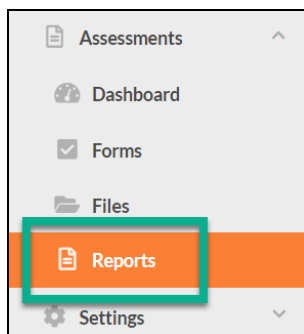
Note: It may take several minutes for the reports to appear once you reach this step.

To review the reports and findings:

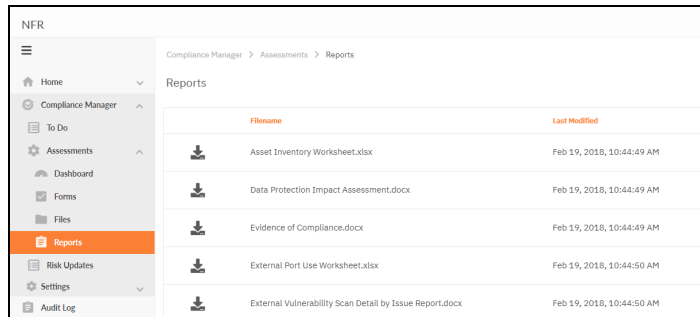
1. From your Site, go to **Compliance Manager > Assessments**.



2. Click **Reports** from the left menu to access a list of generated reports.



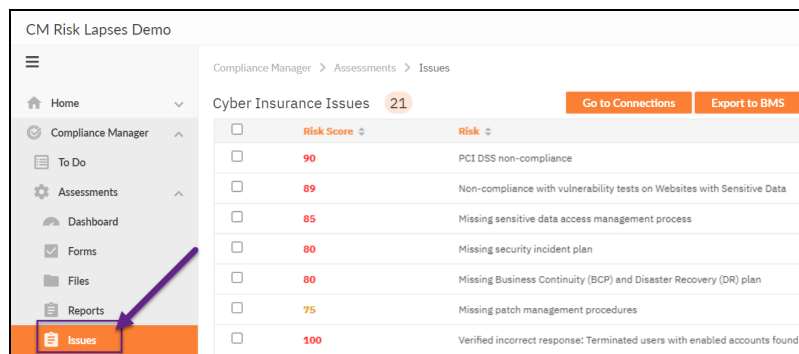
3. The Reports page will appear. Click the download icon next to the report that you wish to download and view.



4. Once you have reviewed the reports, click **Mark Complete** on the task details page.

Manage Assessment Issues

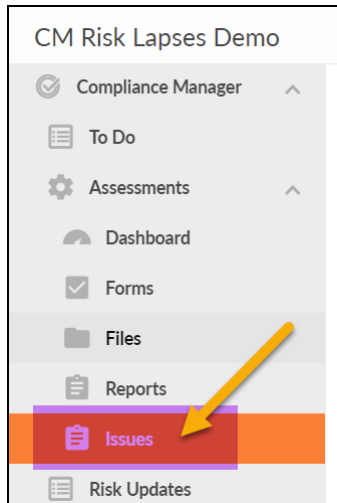
Once you generate assessment reports and review them, you can view specific issues identified in the assessment — organized by risk score — from the **Issues** tab. These issues supplement the detailed data in your reports with immediate action items — and likewise allow you to perform ["Optional Task: Export Issues to Kaseya BMS" on page 133.](#)



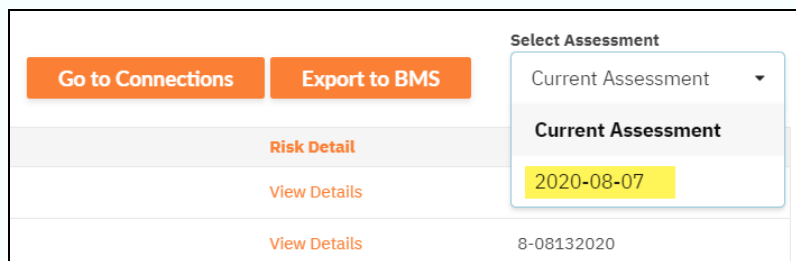
View Assessment Issues

To view identified assessment issues:

1. From your chosen Site, navigate to **Compliance Manager > Assessments > Issues**.



Note: In order to see issues for the current assessment, you must have an active assessment in which you have generated reports. Otherwise, you can view issues from previous assessments. To do this, select the previous assessment from the drop-down menu.



- Click on the **Risk Score** field to organize issues by their numerical risk scores. Address the highest risk issues first for maximum effect.

Compliance Manager > Assessments > Issues



Cyber Insurance Issues 21

Go to Connections Export to BMS

<input type="checkbox"/>	Risk Score	Risk
<input type="checkbox"/>	90	PCI DSS non-compliance
<input type="checkbox"/>	89	Non-compliance with vulnerability tests on Websites with Sensitive Data
<input type="checkbox"/>	85	Missing sensitive data access management process
<input type="checkbox"/>	80	Missing security incident plan
<input type="checkbox"/>	80	Missing Business Continuity (BCP) and Disaster Recovery (DR) plan
<input type="checkbox"/>	75	Missing patch management procedures
<input type="checkbox"/>	100	Verified incorrect response: Terminated users with enabled accounts found

3. Finally, you can click **View Details** next to an issue to see the brief recommendation.

Risk Score ▾	Risk ▾	Risk Detail
90	PCI DSS non-compliance	View Details
89	Non-compliance with vulnerability tests on Websites with Sensitive Data	View Details


High Risk PCI DSS Non-Compliance			
Risk Score 90	Recommendations Address all issues with non-compliance with PCI DSS in a timely manner.	Severity 	Probability 
Close			

Optional Task: Export Issues to Kaseya BMS

Step 1 — Gather Credentials and Set Up Kaseya BMS

Before you begin, you will need:

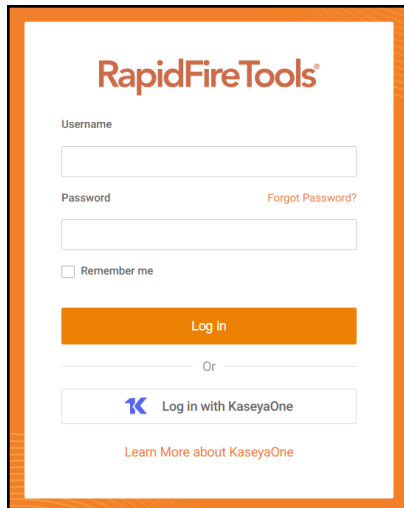
- Valid Login Credentials for RapidFire Tools Portal
- A RapidFire Tools Portal Compliance Manager "Site" for which you wish to export tickets
- Valid Login Credentials and details for Kaseya BMS (refer to the table below)

PSA System	PSA Prerequisites
	<ul style="list-style-type: none"> • Kaseya Username • Kaseya Password • Kaseya Tenant (i.e. company name) • Kaseya API URL, example: "https://bms.kaseya.com" (you should receive the exact URL in an email from Kaseya)

Step 2 — Set Up a Connection to your Kaseya BMS

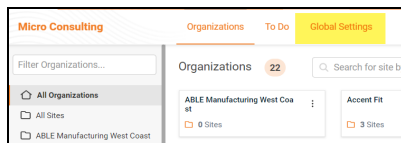
Follow these steps to set up a Connection to Kaseya BMS.

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

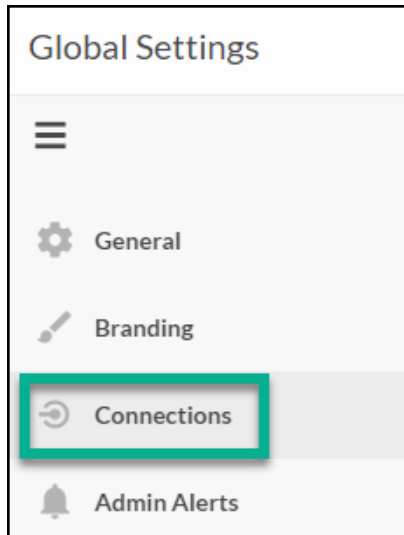


Note: In order to configure the Settings in the Portal, you must have the **All** or **Admin** global access level.

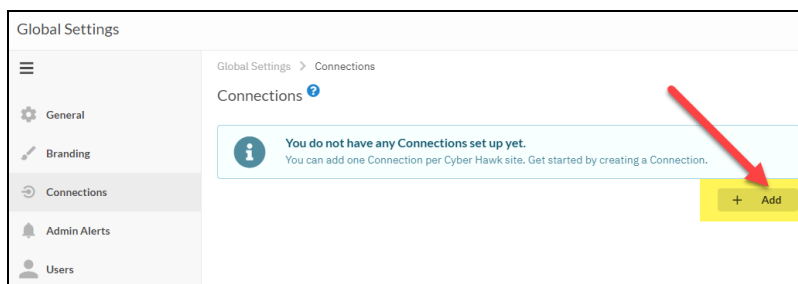
2. Click **Global Settings**.



3. Click **Connections**.

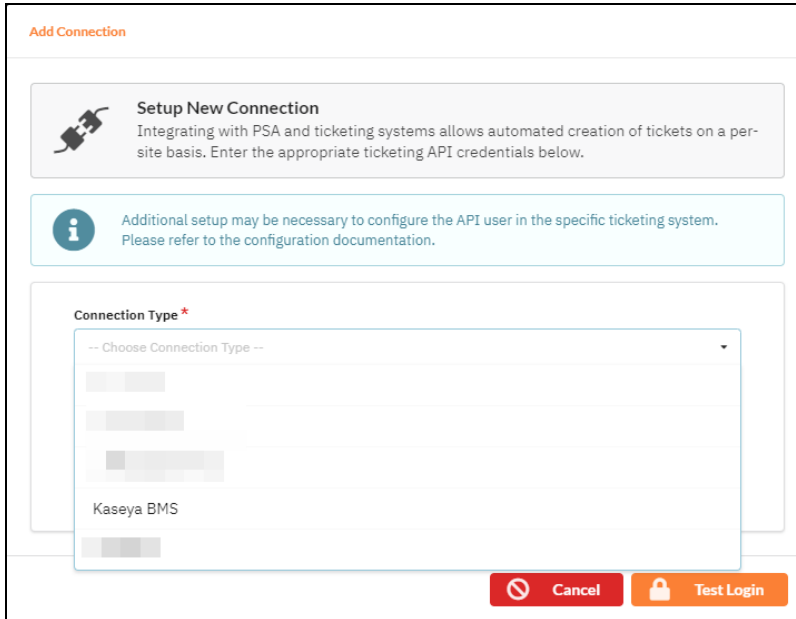


4. Click **Add** to create a new Ticketing System/PSA Connection.



5. In the Setup New Connection window, select **Connection Type** and choose **Kaseya BMS**.

Note: Compliance Manager can only be integrated with Kaseya BMS at this time.



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*

-- Choose Connection Type --

Kaseya BMS


Cancel Test Login


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

This information will include:

- Username and Password
- API URL
- Tenant name (Company name)

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 *

Username *

Password *


Tenant *

API URL *

[Cancel](#) [Test Login](#)

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

Add Connection

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

Account *

-- Choose Account --

Location *

-- Choose Location --

Contact *

-- Choose Contact --

Ticket Source *

-- Choose Ticket Source --

Ticket Type *

-- Choose Ticket Type --

Priority *

-- Choose Priority --

Status *

-- Choose Status --


Queue *

-- Choose Queue --

Primary Assignee *

-- Choose Primary Assignee --


← Back


 Test Ticket

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

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


Add Connection

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



 **Connection**

Connection Name *

Type	Kaseya BMS
Login	<input type="password"/>


 **Ticketing**


Account	NFR RapidFire Tools	Location	NFR RapidFire Tools
Contact	Leo Tolstoy	Ticket Source	Verbal
Ticket Type	Problem	Priority	Medium
Status	Completed	Queue	Level Three Support
Primary Assignee	RFT Test		

 Back  Save

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

Connections ⓘ

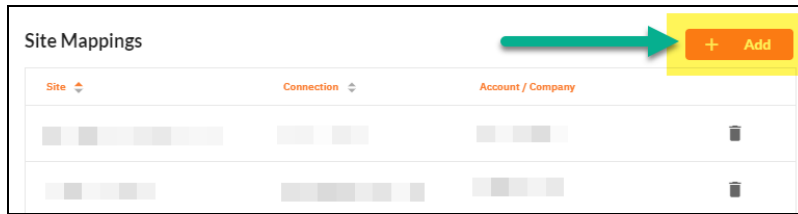
Your Connections 

Name	Type	Login	
BMS Export CM Issues	Kaseya BMS	<input type="password"/>	 

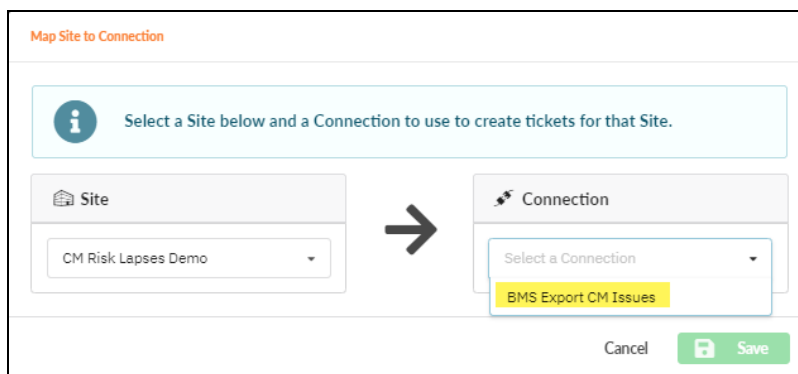
Step 3 — Map your Compliance Manager's Site to a Kaseya BMS Connection

Follow these steps to map a Kaseya BMS Connection to the RapidFire Tools Portal Site associated with your Compliance Manager assessment.

1. From the **Global Settings > Connections** menu, scroll down and click **Add** under Site Mappings. The Map Site to Connection window will be displayed.



2. Select the RapidFire Tools Portal Compliance Manager **Site** you want to assign to the Kaseya BMS Integration.
3. Next, **select the name of the Connection** that you want use to link the Site to Kaseya BMS.



4. Click **Save**. The Site's mapping will be saved and listed in the Site Mappings list.

You can now export Issues as tickets for the RapidFire Tools Portal Site you selected.



Step 4 — Export Issues to Kaseya BMS

The final step is to select issues and export them. To do this:

1. Navigate to the site with the issues you want to export. Go to **Compliance Manager > Assessment > Issues**.
2. Check the box next to each issue to be exported.
3. Click **Export to BMS** and confirm.

CM Risk Lapses Demo

Compliance Manager > Assessments > Issues

CYBERINSURANCE Issues 21

Go to Connections Export to BMS

Select Assessment
Current Assessment

	Risk Score	Risk	Risk Detail	BMS Ticket #
✓	90	PCI DSS non-compliance	View Details	Not Submitted
✓	89	Non-compliance with vulnerability tests on Websites with Sensitive Data	View Details	Not Submitted
✓	85	Missing sensitive data access management process	View Details	Not Submitted
✓	80	Missing security incident plan	View Details	Not Submitted
✓	80	Missing Business Continuity (BCP) and Disaster Recovery (DR) plan	View Details	Not Submitted
✓	75	Missing patch management procedures	View Details	Not Submitted
✓	100	Verified incorrect response: Terminated users with enabled accounts found	View Details	Not Submitted
✓	100	Verified incorrect response: Credit Card Numbers found	View Details	Not Submitted
✓	97	Unsupported operating systems	View Details	Not Submitted

Each successfully exported issue will receive a ticket number. The issues will now be available as tickets in Kaseya BMS.

Compliance Manager > Assessments > Issues

CYBERINSURANCE Issues 21

Go to Connections Export to BMS

Select Assessment
Current Assessment

	Risk Score	Risk	Risk Detail	BMS Ticket #
	90	PCI DSS non-compliance	View Details	12-08102020
	89	Non-compliance with vulnerability tests on Websites with Sensitive Data	View Details	16-08102020
	85	Missing sensitive data access management process	View Details	14-08102020
	80	Missing security incident plan	View Details	11-08102020
	80	Missing Business Continuity (BCP) and Disaster Recovery (DR) plan	View Details	13-08102020

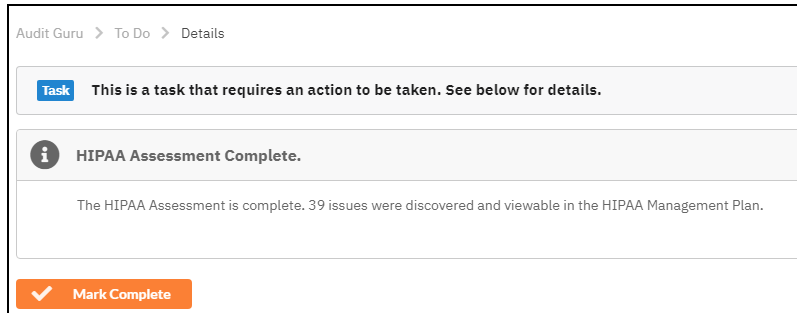
Note: Once the ticket is exported, you can continue to view its details, but you cannot export it twice.

Complete and Archive your CMMC Assessment

After you have reviewed your generated CMMC assessment reports, you are ready to complete and archive your assessment.

Task 22: CMMC Assessment Complete

In this step, after you have reviewed your CMMC assessment reports, the CMMC assessment will be complete. Compliance Manager will also note the number of compliance and security issues detailed for further review in the Risk Assessment report.



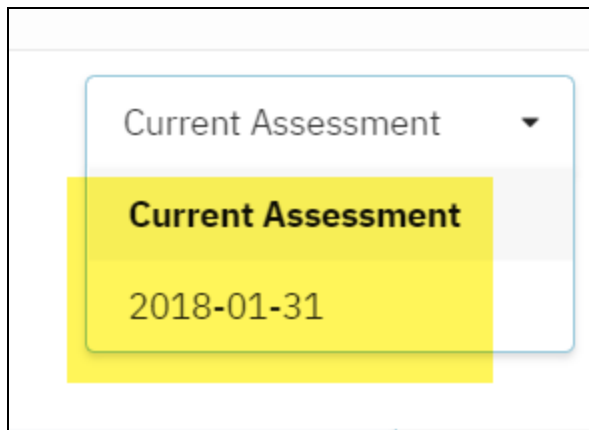
Click **Mark Complete** to archive a copy of your completed CMMC Assessment.

Tip: Congratulations! That's all there is to completing your CMMC Assessment. If you were doing an in-house test-run, now you're ready to set up sites for your clients.

View an Archived Assessment

When you complete an assessment, that assessment will be archived. You can review an archived copy of the assessment and the generated reports and compliance documentation. To do this:

1. Navigate to the **Assessments** tab.



2. Click on the drop-down menu from the right side of the screen.
3. Select the archived assessment you wish to review.

Note: Your archived assessment will be named: **YYYY-MM-DD** where the date is the start date of the assessment.

See also: ["Ongoing CMMC Assessments" on page 155](#).

CMMC Assessment Reports

Compliance Manager for CMMC can generate the following reports and supporting documents:

CMMC Compliance Reports

These reports show where you are in achieving CMMC compliance. In addition, these documents identify and prioritize issues that must be remediated to address CMMC related security vulnerabilities through ongoing managed services.

Report Type	Description	Level 1	Level 2	Level 3
CMMC Assessor Checklist	The CMMC Assessor Checklist gives you a high-level overview of how well the organization complies with the CMMC (Cybersecurity Maturity Model Certification) requirements. The checklist details specific compliance items, their status, and helpful references. Use the checklist to quickly identify potential issues to be re-mediated in order to achieve compliance.	✓	✓	✓
CMMC Evidence of Compliance	Compiles compliance information from automated scans, augmented data, and questionnaires. Gathers evidence into one document to back up the CMMC Assessor Checklist with real data.	✓	✓	✓
CMMC Risk Analysis	CMMC Risk Analysis is the foundation for the entire CMMC compliance and IT security program. The CMMC Risk Analysis identifies what protections are in place and where there is a need for more. The Risk Analysis results in a list of items that must be remediated to ensure the security and confidentiality of sensitive data at rest and/or during its transmission.	✓	✓	✓
CMMC Risk Treatment Plan	Based on the findings in the CMMC	✓	✓	✓

Report Type	Description	Level 1	Level 2	Level 3
	Compliance Assessment, the organization must create a Risk Treatment Plan with tasks required to minimize, avoid, or respond to risks. Beyond gathering information, CMMC Manager provides a risk scoring matrix that an organization can use to prioritize risks and appropriately allocate money and resources and ensure that issues identified are issues solved. The Risk Treatment plan defines the strategies and tactics the organization will use to address its risks.			
CUI Plan of Actions and Milestones Report*	The CUI Plan of Action is organized by the NIST security control requirements and cross references the CMMC control domains. It details the status of implementation for each control, and provides suggestions for resolving the issues identified. <i>(Requires Level 2 assessment and completion of NIST SP 800 171 DoD Assessment Scoring Supplement Worksheet)</i>		✓	✓
CUI System Security Plan*	This document supplements the Risk Analysis, Risk Treatment Plan, and NIST SP 800 - 171 DoD Assessment Scoring report and offers substantiation and verification of compliance with control requirements. <i>(Requires Level 2 assessment and completion of NIST SP 800 171 DoD Assessment Scoring Supplement Worksheet)</i>		✓	✓
NIST 800 171 Scoring Supplement Worksheet*	The optional NIST 800-171 Scoring Supplement allows you to perform a self-assessment as per the DoD's interim rule. It is based on the DoD NIST SP 800-171 Assessment Methodology, where the final assessment results are communicated in		✓	

Report Type	Description	Level 1	Level 2	Level 3
	the form of a DoD Assessment Score. <i>(Requires Level 2 assessment and completion of NIST SP 800 171 DoD Assessment Scoring Supplement Worksheet)</i>			
NIST SP 800 171 DoD Assessment Score Report*	This report details the DoD Assessment Score as per the DoD Assessment methodology. It details the control point value deductions, as well as the implementation status for each required control. <i>(Requires Level 2 assessment and completion of NIST SP 800 171 DoD Assessment Scoring Supplement Worksheet)</i>		✓	✓

Supporting Documentation

These documents show the detailed information and raw data that backs up the compliance reports. These documents include the various interviews and worksheets, as well as detailed data collections on network assets, shares, login analysis, etc.

Report Type	Description
CMMC Full Detail Excel Export	The CMMC Full Detail Excel Export includes every detail uncovered during the CMMC assessment's network and computer endpoint scanning process. Details are presented in line-item fashion in an editable Excel workbook document. The report is organized by titled worksheets to help you locate the specific findings of interest, and problem areas are conveniently highlighted in red, making it easy to spot individual problems to be rectified
CMMC Login History Report	This report presents user login history by computer to enable workforce members responsible for IT Security to audit access to computers connected to a company's network. Quite useful, in particular, for looking at a commonly accessed machines (file server, domain controller, etc.) – or a particularly sensitive “CUI” computers that are used to collect, process, transmit, or store CUI for failed login attempts.
CMMC Windows Patch Assurance Report	The CMMC Windows Patch Assurance Report helps verify the effectiveness of the client's patch management program. The report uses scan data to detail which patches are missing on the network.
External Vulnerability Scan Detail by Issue	Detailed report showing security holes and warnings, informational items including CVSS scores as scanned from outside the target network. External vulnerabilities could allow a malicious attacker access to the internal network.

Worksheets by Assessment Level

Report Type	Description	Level 1	Level 2	Level 3
CMMC Access Control Worksheet	This worksheet is used to collect information required to demonstrate compliance with the CMMC “Access Control” control domain requirements that cannot be discovered and assessed through automated scans.	✓	✓	✓
CMMC Antivirus Verification Worksheet	Compliance Manager will automatically detect any anti-virus software installed on PCs on the target network. The Anti-virus Verification Worksheet details whether each endpoint on the network has anti-virus software installed. It also displays the type of anti-virus software.	✓	✓	✓
CMMC Application Inventory Worksheet	This worksheet is used to document the “necessity” of the applications identified as being installed on the computer endpoints operating within the network.	✓	✓	✓
CMMC Asset Inventory Worksheet	The Asset Inventory Worksheet is used to augment the asset data that was collected during the internal network scan. Details include the asset owner, acceptable use, environment, backup agent status, as well as device and asset criticality classification. The asset criticality classification is used to determine the risk to the organization in the event of a security incident where the asset’s access or availability is compromised.	✓	✓	✓
CMMC Asset Management Worksheet	This worksheet is used to collect information required to demonstrate compliance with the CMMC “Asset Management Worksheet” control domain requirements that cannot be discovered and assessed through			✓

Report Type	Description	Level 1	Level 2	Level 3
	automated scans.			
CMMC Audit and Accountability Worksheet	This worksheet is used to collect information required to demonstrate compliance with the CMMC “Audit and Accountability” control domain requirements that cannot be discovered and assessed through automated scans.		✓	✓
CMMC Awareness and Training Worksheet	This worksheet is used to collect information required to demonstrate compliance with the CMMC “Awareness and Training” control domain requirements that cannot be discovered and assessed through automated scans.		✓	✓
CMMC Configuration Management Worksheet	This worksheet is used to collect information required to demonstrate compliance with the CMMC “Configuration Management” control domain requirements that cannot be discovered and assessed through automated scans.		✓	✓
CMMC External Information System Worksheet	This worksheet is used to document external information systems used by your organization. Add entries for each external information system along with a description, purpose for using the system, name of the business owner of the system, along with its criticality. Examples of external information systems include Salesforce, QuickBooks Online, and Office 365.	✓	✓	✓
CMMC External Port Use Worksheet	This worksheet allows you to document business justifications for all of the allowed external ports, the protocol configured to use a specific port, and the	✓	✓	✓

Report Type	Description	Level 1	Level 2	Level 3
	documentation of any insecure configurations implemented and in use for a given protocol.			
CMMC Identification and Authentication Worksheet	This worksheet is used to collect information required to demonstrate compliance with the CMMC “Identification and Authentication” control domain requirements that cannot be discovered and assessed through automated scans.	✓	✓	✓
CMMC Incident Response Worksheet	This worksheet is used to collect information required to demonstrate compliance with the CMMC “Incident Response” control domain requirements that cannot be discovered and assessed through automated scans.		✓	✓
CMMC Maintenance Worksheet	This worksheet is used to collect information required to demonstrate compliance with the CMMC “Maintenance” control domain requirements that cannot be discovered and assessed through automated scans.		✓	✓
CMMC Media Protection Worksheet	This worksheet is used to collect information required to demonstrate compliance with the CMMC “Media Protection” control domain requirements that cannot be discovered and assessed through automated scans.	✓	✓	✓
CMMC Personnel Security Worksheet	This worksheet is used to collect information required to demonstrate compliance with the CMMC “Personnel Security” control domain requirements that cannot be discovered and assessed through automated scans.		✓	✓

Report Type	Description	Level 1	Level 2	Level 3
CMMC Physical Protection Worksheet	This worksheet is used to collect information required to demonstrate compliance with the CMMC “Physical Protection” control domain requirements that cannot be discovered and assessed through automated scans.	✓	✓	✓
CMMC Recovery Worksheet	This worksheet is used to collect information required to demonstrate compliance with the CMMC “recovery” control domain requirements that cannot be discovered and assessed through automated scans.		✓	✓
CMMC Risk Management Worksheet	This worksheet is used to collect information required to demonstrate compliance with the CMMC “Risk Management” control domain requirements that cannot be discovered and assessed through automated scans.		✓	✓
CMMC Security Assessment Worksheet	This worksheet is used to collect information required to demonstrate compliance with the CMMC “Security Assessment” control domain requirements that cannot be discovered and assessed through automated scans.		✓	✓
CMMC Situation Awareness Worksheet	This worksheet is used to collect information required to demonstrate compliance with the CMMC “Situation Awareness Worksheet” control domain requirements that cannot be discovered and assessed through automated scans.			✓
CMMC System and Communications Protection	This worksheet is used to collect information required to demonstrate compliance with the CMMC “System	✓	✓	✓

Report Type	Description	Level 1	Level 2	Level 3
Worksheet	and Communications Protection” control domain requirements that cannot be discovered and assessed through automated scans.			
CMMC System and Information Integrity Worksheet	This worksheet is used to collect information required to demonstrate compliance with the CMMC “System and Information Integrity” control domain requirements that cannot be discovered and assessed through automated scans.	✓	✓	✓
CMMC User Access Review Worksheet	The User Access Worksheet is used to augment the user data that was collected during the internal network scan. Complete the worksheet to provide the additional information requested.	✓	✓	✓
NIST 800 171 Scoring Supplement Worksheet	The optional NIST 800-171 Scoring Supplement allows you to perform a self-assessment as per the DoD's interim rule. It is based on the DoD NIST SP 800-171 Assessment Methodology, where the final assessment results are communicated in the form of a DoD Assessment Score.		✓	

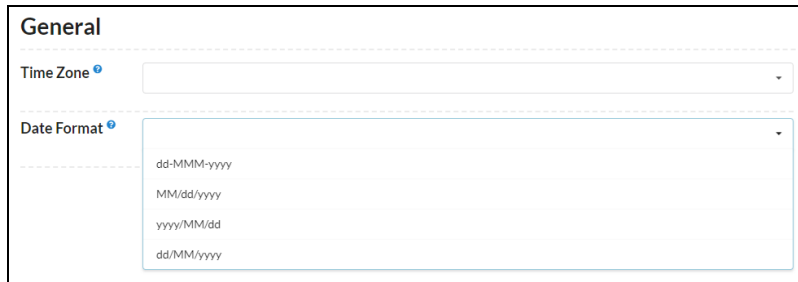
CMMC Risk Update Assessment Reports

Report Type	Description
CMMC Change Summary Report	Every time you use Compliance Manager for CMMC to run a CMMC Risk Update Assessment on a given network, Compliance Manager for CMMC generates the CMMC Change Summary report. This report compares the results the last Full CMMC Assessment with the Risk Update Assessment's network scan, local computer scan(s), and external vulnerability scan results performed during the Risk Update Assessment process. This report details changes in the network's User Accounts, Local Computer Accounts, Active Directory (A/D) Computers, Non-A/D Computers, Non-A/D Devices, External Vulnerabilities, along with a Windows computer Patch Summary.
CMMC Risk Treatment Plan Update	Based on the findings in the CMMC Risk Update Assessment, the organization must create a CMMC Risk Treatment Plan with tasks required to minimize, avoid, or respond to identified risks to IT security. The CMMC Risk Treatment Plan Update contains a list of tasks that can be executed to mitigate identified IT Security risks.
CMMC Risk Analysis Update	The CMMC Risk Analysis Update report lists IT Security risks identified during a Risk Update Assessment that impact the state of IT network security. The CMMC Risk Analysis Update identifies what protections are in place and where there is a need for more. The CMMC Risk Analysis Update report presents results in a list of items that must be remediated to ensure the security and confidentiality of sensitive or confidential information at rest and/or during its transmission.
External Vulnerability Scan Detail**	Detailed report showing security holes and warnings, informational items including CVSS scores as scanned from outside the target network. External vulnerabilities could allow a malicious attacker access to the internal network.

Report Date Format (Global Settings)

You can set the **Date Format** for the reports and compliance documentation generated by Compliance Manager. You can do this from **Global Settings > General** settings.

1. Select your preferred format from the **Date Format** drop down menu.



The screenshot shows the 'General' settings section. Under 'Date Format', a dropdown menu is open, displaying the following options: dd-MMM-yyyy, MM/dd/yyyy, yyyy/MM/dd, and dd/MM/yyyy.

2. Click **Save**.

Your documentation will now appear with your chosen date format.

The table below shows examples of the date formats converted to actual calendar dates.

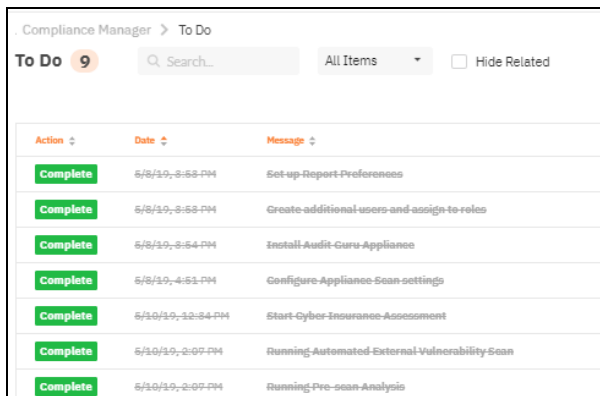
Date Format	Example
dd-MMM-yyyy	31-Jan-2000
MM/dd/yyyy	01/31/2000
yyyy/MM/dd	2000/01/31
dd/MM/yyyy	31/01/2000

Ongoing CMMC Assessments

After you finish your first CMMC assessment, you have a few options for performing ongoing CMMC assessments. You can read about these below:

Start a New CMMC Assessment after Completing a Previous Assessment

When you complete a CMMC Assessment, your To Do list will show all items as **Complete**.

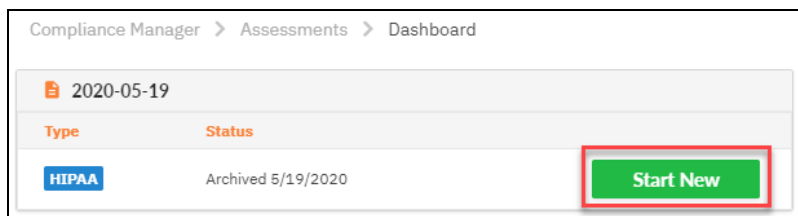


The screenshot shows the 'To Do' list in the Compliance Manager interface. The header includes 'Compliance Manager > To Do', a 'To Do 9' badge, a search bar, and a dropdown menu set to 'All Items'. A 'Hide Related' checkbox is also present. The table below lists seven tasks, all of which are marked as 'Complete' in a green box. The tasks and their completion dates are:

Action	Date	Message
Complete	5/8/20, 3:53 PM	Set up Report Preferences
Complete	5/8/20, 3:53 PM	Create additional users and assign to roles
Complete	5/8/20, 3:54 PM	Install Audit-Curu Appliance
Complete	5/8/20, 4:51 PM	Configure Appliance Scan settings
Complete	5/10/20, 12:54 PM	Start Cyber Insurance Assessment
Complete	5/10/20, 2:07 PM	Running Automated External Vulnerability Scan
Complete	5/10/20, 2:07 PM	Running Pre-scan Analysis

To start a new assessment, follow these steps:

1. Go to **Compliance Manager > Assessments > Dashboard**.
2. Click **Start New**.



The screenshot shows the 'Assessments > Dashboard' page in Compliance Manager. It displays a date filter for '2020-05-19'. Below this is a table with two columns: 'Type' and 'Status'. The table contains one entry: 'HIPAA' with a status of 'Archived 5/19/2020'. A green 'Start New' button is highlighted with a red box in the bottom right corner of the table.

Type	Status
HIPAA	Archived 5/19/2020

Your To Do List will be reset. The **Start CMMC Assessment** To Do item will be added to your To Do list.

3. Click the **Start CMMC Assessment** To Do item.

4. In the To Do item details page, click **Start Assessment**.

Your new assessment will start. New worksheets will become available, and the Compliance Manager server will initiate Internal and External network scans. See ["Collect Initial CMMC Assessment Data" on page 62](#) for step by step instructions.

Generate Risk Update Reports

You can generate **Risk Update Reports** to identify changes at the target Site that might pose a security risk. This allows you to quickly determine what action you might need to take to remain in compliance with a particular assessment protocol. Risk Update Reports also keep track of this activity for your ongoing compliance documentation tasks.

Note: Before you can generate Risk Update Reports, be sure that:

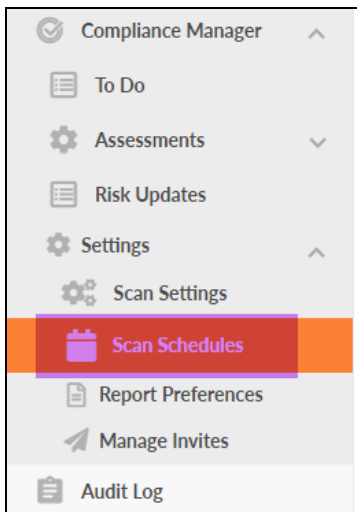
- Scan Settings and network pre-requisites are current and in place
- Last assessment must be marked "Complete" and no assessment is in progress,
- Start Assessment To Do item cannot be present in the To Do list

You can choose to generate Risk Update Reports automatically or manually. To do this, see:

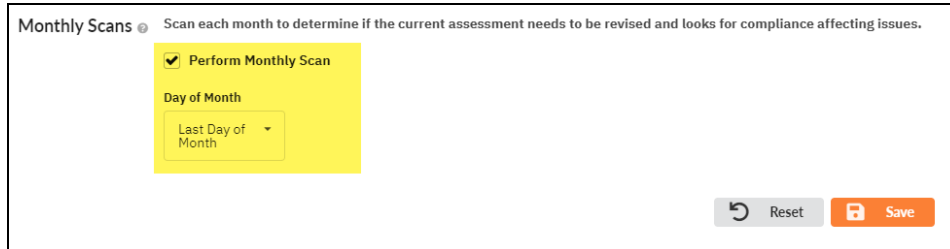
Automatically Generate Risk Update Reports

You can set up your Site to *automatically* generate Risk Update Reports on a monthly basis. To do this:

1. From your Site, go to **Settings > Scan Schedules**.



2. Select **Perform Monthly Scan** and choose a **Day of the Month**.

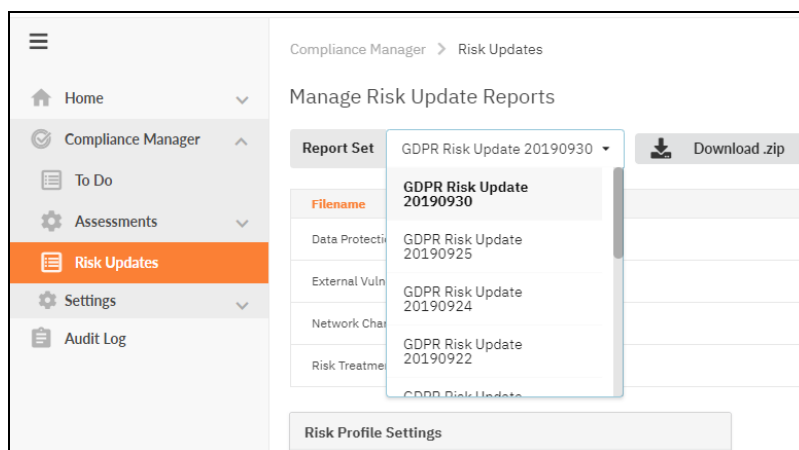


Note: See also ["Monthly Scan Requirements" on page 213](#)

3. When the scheduled monthly scan occurs and reports are generated successfully, the Review Risk Update Reports To Do item will appear.

Note: The Default Risk Update Scan Time is set for 00:00 Eastern Standard Time (5:00 UTC).

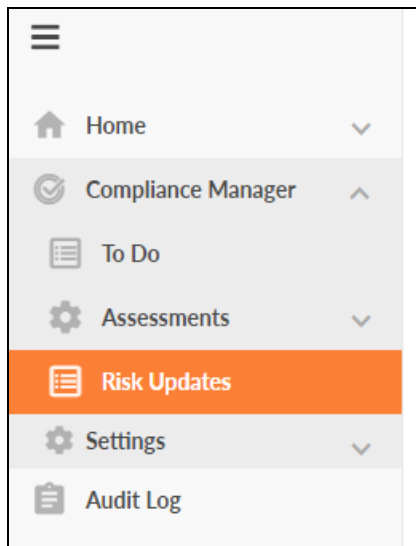
4. The Site Admin, Technician, and Internal Auditor will receive a To Do notification and can access the Portal to review the Risk Update Reports.
5. You can access each of the Risk Reports from **Compliance Manager > Risk Updates**. You can access Risk Report sets by date from the drop-down menu.



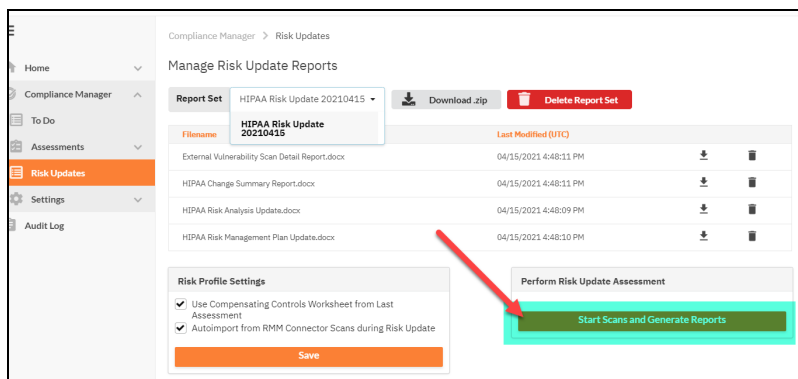
Manually Generate Risk Update Reports

You don't need to wait for the monthly scan to generate Risk Update Reports. To *create reports right away*:

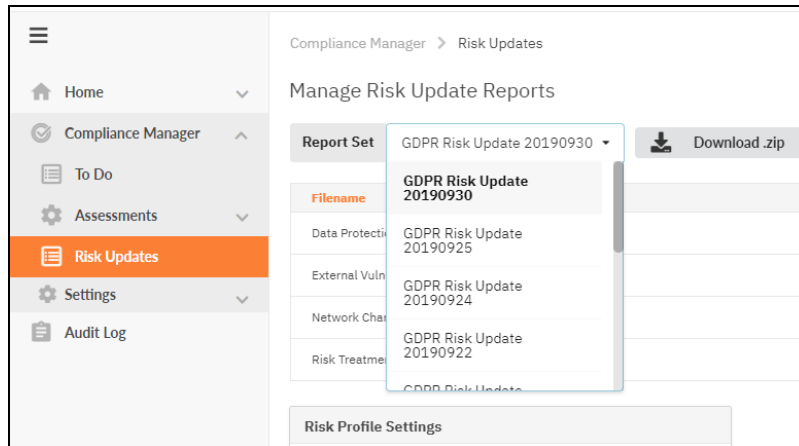
1. From your Site, go to **Compliance Manager > Risk Updates**.



2. Click the **Start Scans and Generate Reports** button. This will immediately initiate a scan.

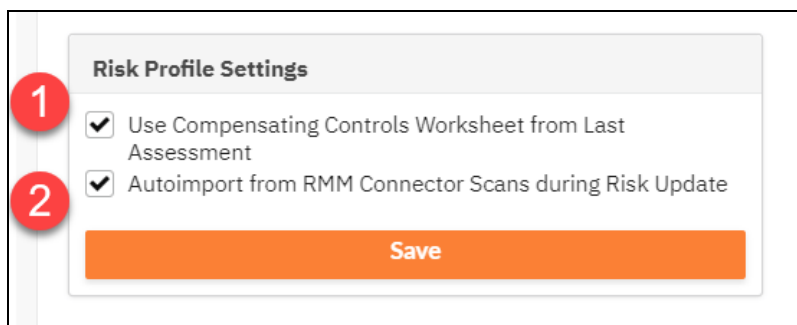


3. When the scan completes and reports are generated successfully, the Review Risk Update Reports To Do item will appear.
4. The Site Admin, Technician, and Internal Auditor will receive a To Do notification and can access the Portal to review the Risk Update Reports.
5. You can access each of the Risk Reports from **Compliance Manager > Risk Updates**. You can access Risk Report sets by date from the drop-down menu.



Risk Profile Settings

You can select optional risk profile settings as part of your Risk Update Reports. These include:



1. **Use Compensating Controls Worksheet from Last Assessment:** When you select this option, issues that you marked as mitigated in your last complete assessment will also be represented as mitigated in your Risk Update Reports.
2. **Auto import from RMM Connector Scans during Risk Update:** If you are using Kaseya VSA to perform scans on the target network, you can choose to import these scans during the Risk Update. Also see ["Integration with VSA Agents for Local Data Collection \(Compliance Manager\)" on page 226](#).

If you select one or both options, click **Save** to confirm your settings.

List of Risk Update Reports

You can find your Site's Risk Update Reports under **Compliance Manager > Risk Updates**. These reports include:

Module	Reports
HIPAA	<ul style="list-style-type: none"> • HIPAA Risk Analysis Update Report (limited to only IT Security Risks) • HIPAA Risk Management Plan Update (limited to only IT Security Risks) • External Vulnerability Scan Detail Report • HIPAA Change Summary Report* • Exception Report (in case of failed scans)
Cyber Insurance	<ul style="list-style-type: none"> • Cyber Risk Analysis Update Report (limited to only IT Security Risks) • Cyber Risk Management Plan Update (limited to only IT Security Risks) • External Vulnerability Scan Detail by Issue Report • Cyber Insurance Change Summary Report* • Exception Report (in case of failed scans)
GDPR	<ul style="list-style-type: none"> • Data Protection Impact Assessment Update Report (limited to only IT Security Risks) • Risk Treatment Plan Update (limited to only IT Security Risks) • External Vulnerability Scan Detail by Issue Report • GDPR Change Summary Report*
NIST CSF	<ul style="list-style-type: none"> • NIST CSF Risk Analysis Update • NIST CSF Change Summary Report* • NIST CSF Management Plan Update • External Vulnerability Scan Detail • Exception Report (in case of failed scans)
CMMC	<ul style="list-style-type: none"> • CMMC Risk Analysis Update • CMMC Change Summary Report* • CMMC Treatment Plan Update • External Vulnerability Scan Detail • Exception Report (in case of failed scans)

Note: *: The **Change Summary Report** compares the results the latest complete assessment with a new network scan, local computer scan(s), and external vulnerability scan. This report details changes in the network's User Accounts, Local Computer Accounts, Active Directory (A/D) Computers, Non-A/D Computers, Non-A/D Devices, and External Vulnerabilities, along with a Windows Computer Patch

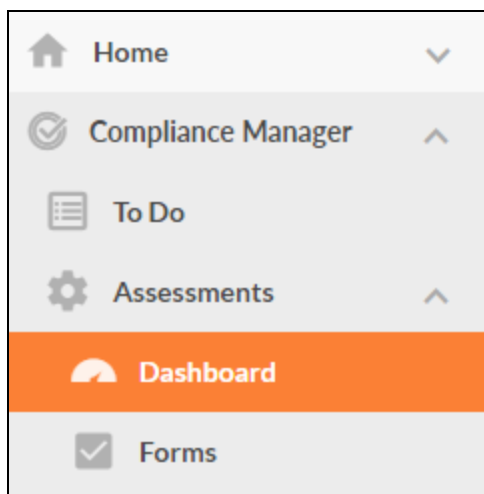
Summary. Changes in the form of additions are noted in **green** text font. Changes in the form of removals are noted in **red** text font.

Additional Compliance Manager Assessment Features

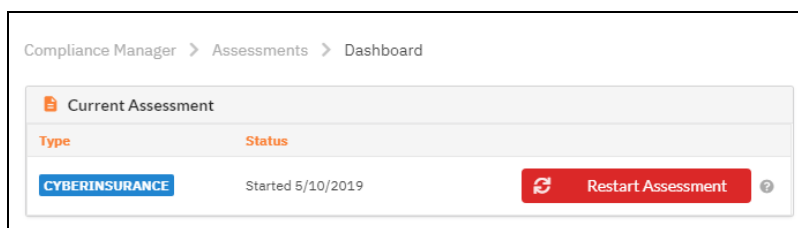
Restart an Compliance Manager Assessment before it is Complete

You may wish to restart your Assessment before it is complete. This might be useful, for example, if you want to change scan settings or restart a scan. You can restart your Compliance Manager Assessment by following these steps:

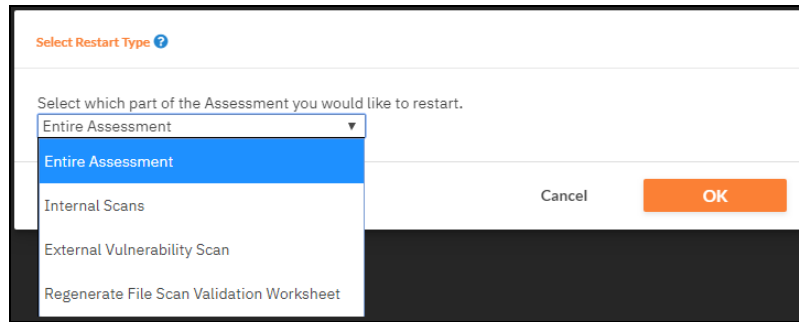
1. Go to **Compliance Manager > Assessments > Dashboard** tab to open the Assessments page.



2. Click **Restart Assessment**.



3. Select which part of the Assessment you wish to restart. You can choose to restart the:



- **Entire Assessment**

Restart Entire Assessment will restart both the internal network scan and external vulnerability scans. All worksheets and questionnaires will be reset, too.

Note: When you restart the entire assessment, Compliance Manager will automatically begin performing a pre-scan analysis. You will need to allow the pre-scan analysis to complete before you can begin the internal network scan. Use the pre-scan analysis to ensure your scan and network configurations are still optimal.

- **Internal Network Scan**

Restart Internal Scan will restart all internal network scans. Any worksheet that draws data from these scans will be reset in the current assessment.

- **External Vulnerability Scan**

Restart External Vulnerability Scan will restart just the external vulnerability scan. The External Port Use Worksheet and Compensating Control Worksheet will be reset.

Completing Assessment Worksheets and Surveys

Throughout the assessment process, you will use worksheets, surveys, and questionnaires to collect information about the site that cannot be discovered solely through automated scans. This section details some helpful instructions and time-saving tips that you can use to breeze through your assessment documentation.

EXAMPLE:

To complete an InForm worksheet (or survey or questionnaire), follow these steps:

- i. Review the *Topic* (i.e. the specific field or question within the form).

The screenshot shows a form titled "1 POLICY AND PROCEDURES (23 REQUIRED REMAINING)". A purple arrow points to the "Section" label. Below it, "1.1 HIPAA Policy and Procedures" is labeled as the "Topic/Question". A purple arrow points to the question text: "Has your organization implemented the HIPAA Policy and Procedures included with Audit Guru? If you have imp". Below the question is a yellow "Answer field". A purple arrow points to the "Instructions" area, which contains icons for a document, a person, and a folder.

- ii. Review the *Instructions*. The instructions appear immediately below the topic label. Instructions provide guidance and are not included in the reports.
- iii. Enter the *Response*. There are three types of responses:

Response Type	Description	Example Use
Text Response	Free-form text response	"Describe the condition of the data center."
Multiple Choice	Multiple fixed responses	"Does the firewall have IPS?" (Yes/No)
Checklist Item	An item that is marked off if completed	"Check the security of the door locks."

Note: With few exceptions, you must respond to each form entry to complete the all of the surveys within the CMMC Assessment process.

- iv. (Optional) Enter any *Notes* relevant to the topic's response.

- v. (Optional) Enter the name of *Respondent* (i.e. the person who provided you with the information, if applicable).

When you complete a section of the worksheet, a **green check mark** indicator will appear.

The screenshot shows a worksheet section titled "1 SECURITY OFFICER" with a green checkmark icon. A purple arrow points from the "Section Complete" label to the section title. Below the title, the text reads: "HIPAA requires a named Security Officer as a central point of contact." Underneath, there is a sub-section "1.1 Name" with a "Show Help" button. The instruction says: "Enter the name of the Security Officer for the covered entity." A text input field contains the text "Security Official".

- vi. Longer worksheets have separate pages. You can navigate pages using the buttons at the top of the form. Your responses will remain on the previous page if you proceed when you proceed to the next one.

The screenshot shows a worksheet titled "Cyber Liability Questionnaire". At the top, there is a breadcrumb trail: "Audit Guru > Assessments > InForm". Below the title, there is a search bar with the text "Search Topics" and a "Search" button. Below the search bar, there are links: "Hide # | Expand All | Collapse All" and a "Download" button. Below these links, there are three buttons: "Previous Page", "Next Page", and "Page 1 of 2". At the bottom, there is a green checkmark icon and the text "1 TYPE OF SENSITIVE DATA".

- vii. **Save** frequently. When you are done, click **Save and Return**.

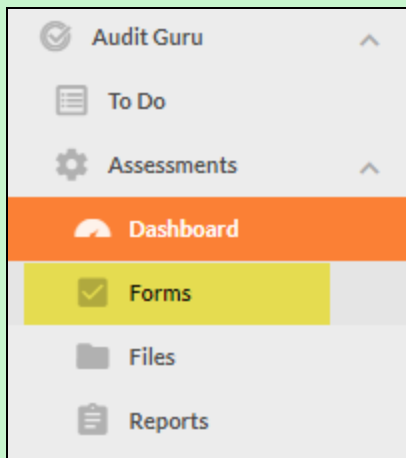
The screenshot shows a worksheet with a "Worksheet" label and a dropdown menu set to "English (US)". To the right, there is a "Select Assessment" dropdown menu set to "Current Assessment". At the bottom, there are two buttons: "Save" and "Save and Return". A purple arrow points to the "Save" button.

- viii. When you are ready to finalize the worksheet and move on the next assessment To Do item, click **Mark Complete** in the task details page.



Important: Once you mark a worksheet as complete, you cannot re-open that worksheet unless you restart the assessment. Only mark a worksheet as complete when you are ready to finalize it and move on to the next assessment To Do item.

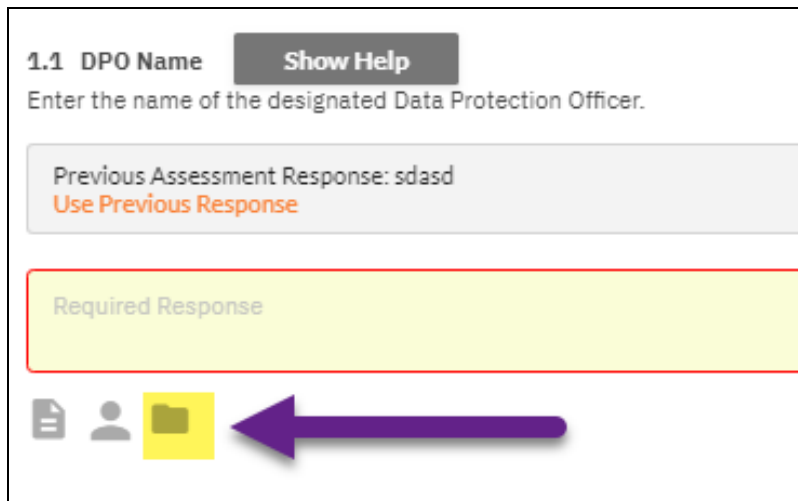
Click the **Forms** button from the left-hand menu to access and edit worksheets and forms — *that you have not already marked Complete* — at any time.



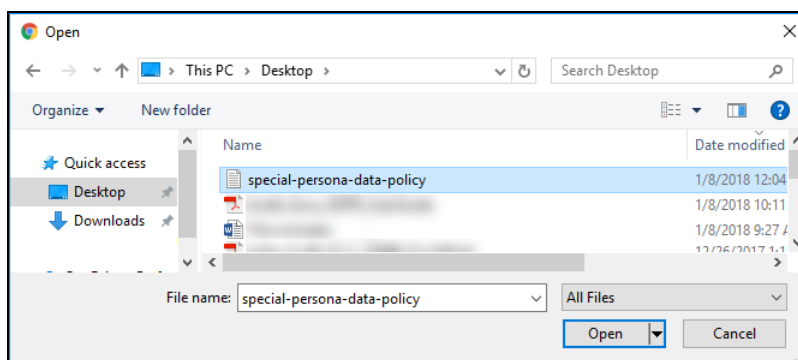
Attach Supporting Documents

As evidence of compliance, you can add supporting documents that will be included as attachments when you generate assessment and compliance reports with Compliance Manager. To attach a supporting document:

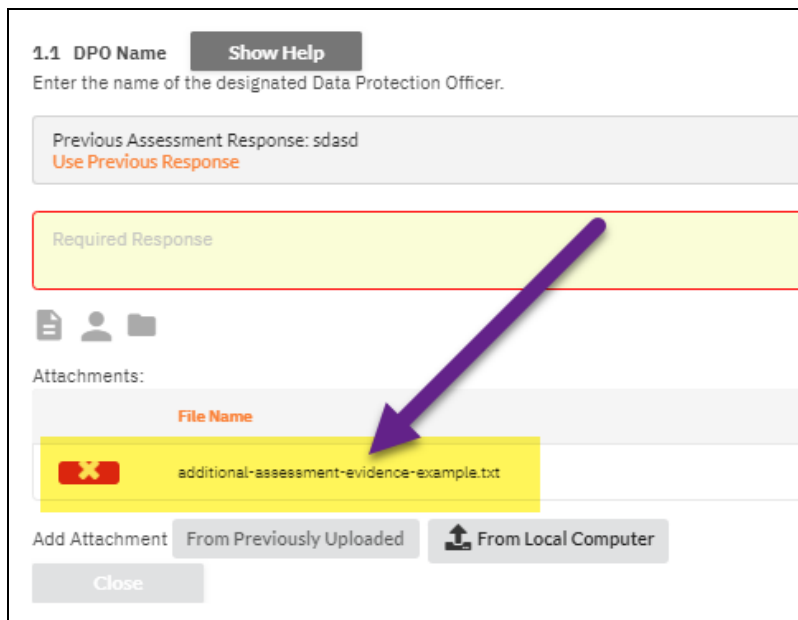
1. Click on the folder icon underneath the appropriate questionnaire field.



2. Choose whether to Add Attachment from **Previously Uploaded** or from your **Local Computer**.
3. Select the file you wish to upload and click Open. The selected file(s) will appear in the attachments queue.



4. The file will be added to the assessment document as an attachment.



The screenshot shows a web form titled "1.1 DPO Name" with a "Show Help" button. Below the title is the instruction "Enter the name of the designated Data Protection Officer." There is a text input field containing "Previous Assessment Response: sdasd" and a link "Use Previous Response". Below this is a "Required Response" section with a red border. Underneath is an "Attachments:" section with a table. The table has a header "File Name" and one row with a red 'X' icon and the filename "additional-assessment-evidence-example.txt". A purple arrow points from the "Required Response" section to the attachment row. At the bottom are buttons for "Add Attachment", "From Previously Uploaded", "From Local Computer", and "Close".

Note: The attachment will appear in your supporting documents and reports that are generated at the end of the assessment process.

Select Multiple Fields

In worksheets that have tables with multiple fields, you can select several or all fields at once in order to enter responses more quickly. To select multiple fields:

1. Click the left mouse button and hold on the first field you would like to include in the selection.

1 ISSUE CHECKLIST

1.1 Issue Checklist
As you walk through the site environment, check to see if any of the following security issues are present. Check the box next to any issues that you find. Check the box next to any issues that you find necessary to achieve the ISO 27001 standard.

Previous Assessment Response: Multiple Responses
[View Previous Responses](#)

<input type="checkbox"/>	Removable media not secure. Left on desks in unsecured office or cubicles or in public areas. (8.3.1)
<input type="checkbox"/>	Hard drives or defunct systems with media left in unsecured offices or cubicles or in public areas. (8.3.2)
<input type="checkbox"/>	Servers or devices containing sensitive information reside in an insecure area (11.1.1a)
<input type="checkbox"/>	Perimeter of building or site is not physically sound allowing easy break-in (11.1.1b)
<input type="checkbox"/>	Lack of physical access control either manned or unmanned (11.1.1c)
<input type="checkbox"/>	Fire doors on security perimeter found that are not alarmed or monitored (11.1.1e)
<input type="checkbox"/>	Lack of physical intrusion detection system (11.1.1f)
<input type="checkbox"/>	Processing facilities maintained by external parties co-located with the organisation's information processing facilities (11.1.1g)
<input type="checkbox"/>	Visitors allowed entry to secured areas without recording date and time (11.1.2a)
<input type="checkbox"/>	Visitors allowed to move unsupervised through secured areas (11.1.2a)

2. While holding the left mouse button, drag and select your desired fields.

1 ISSUE CHECKLIST

1.1 Issue Checklist
As you walk through the site environment, check to see if any of the following security issues are present. Check the box next to any issues that you find. Check the box next to any issues that you find necessary to achieve the ISO 27001 standard.

Previous Assessment Response: Multiple Responses
[View Previous Responses](#)

<input type="checkbox"/>	Removable media not secure. Left on desks in unsecured office or cubicles or in public areas. (8.3.1)
<input type="checkbox"/>	Hard drives or defunct systems with media left in unsecured offices or cubicles or in public areas. (8.3.2)
<input type="checkbox"/>	Servers or devices containing sensitive information reside in an insecure area (11.1.1a)
<input type="checkbox"/>	Perimeter of building or site is not physically sound allowing easy break-in (11.1.1b)
<input type="checkbox"/>	Lack of physical access control either manned or unmanned (11.1.1c)
<input type="checkbox"/>	Fire doors on security perimeter found that are not alarmed or monitored (11.1.1e)
<input type="checkbox"/>	Lack of physical intrusion detection system (11.1.1f)
<input type="checkbox"/>	Processing facilities maintained by external parties co-located with the organisation's information processing facilities (11.1.1g)
<input type="checkbox"/>	Visitors allowed entry to secured areas without recording date and time (11.1.2a)
<input type="checkbox"/>	Visitors allowed to move unsupervised through secured areas (11.1.2a)
<input type="checkbox"/>	Lack of authentication mechanism to secure areas (11.1.2b)
<input type="checkbox"/>	Lack of physical or electronic audit trail for all access to secure areas (11.1.2c)
<input type="checkbox"/>	Employees, contractors, or external parties in secure area without visible identification (11.1.2d)

3. You can use this feature to copy and paste multiple responses at once. See ["Copy and Paste Responses" below](#).

Copy and Paste Responses

Some worksheets allow you to copy and paste the responses you entered, much like a spreadsheet. This saves you time by allowing you to enter many responses at once. To do this:

1. First answer one or more questions that require a response. Enter your response within the field.

Note: You can copy and paste both free-form and multiple choice entries.

(such as privileges) with the covered entity. For active employees and vendors, indicate if the user is

Last Login	ePHI Access
4/3/2018 4:16:37 AM	Employee - ePHI authorization
9/12/2018 6:25:29 AM	Employee - ePHI authorization
10/8/2018 9:14:33 AM	Employee - no ePHI authorization
1/16/2019 12:43:04 PM	Vendor - ePHI authorization
10/8/2018 9:29:47 AM	Vendor - no ePHI authorization
12/3/2018 9:20:19 AM	Former Employee
4/9/2018 4:17:06 AM	Employee - ePHI authorization

2. Use your mouse to drag and select multiple rows that contain the responses you wish to copy.

	ePHI Access
	Employee - ePHI authorization
	Employee - ePHI authorization
	Employee - ePHI authorization
	Employee - ePHI authorization
	Vendor - ePHI authorization
	Vendor - ePHI authorization
	Vendor - ePHI authorization
	Vendor - ePHI authorization
	Vendor - ePHI authorization
	Vendor - ePHI authorization
	Vendor - ePHI authorization

3. On your keyboard, press **CTRL+C**.
4. Use your mouse to drag and select the rows you wish to paste the responses into.
5. On your keyboard, click **CTRL+V**. Your pasted responses will appear in the worksheet.

ty. For active employees and vendors, indicate if the user is

	ePHI Access
	Employee - ePHI authorization
	Employee - ePHI authorization
	Employee - ePHI authorization
	Employee - ePHI authorization
	Employee - ePHI authorization
	Employee - ePHI authorization
	Employee - ePHI authorization
	Employee - ePHI authorization
	Vendor - ePHI authorization
	Vendor - ePHI authorization
	Vendor - ePHI authorization

Use this feature to save time completing worksheet responses that can be answered with the same answer.

Dynamic Guidance for Worksheets and Surveys in the RapidFire Tools Portal

Need help with answering questions in worksheets and surveys when completing assessments? When working with a form, you can click **Show Guidance** to open a sidebar with more detailed guidance for answering each question.

Note: This feature is currently available for selected Compliance Manager assessment worksheets.

To access dynamic guidance for worksheet or survey:

1. Open the assessment worksheet or survey from your Site in the RapidFire Tools Portal.
2. Next to a question you want more help with, click **Show Guidance** where it appears.

Note: If the button does not appear, there is no additional help currently available for that question.

Compliance Manager > Assessments > InForm

CMMC Awareness and Training Worksheet

Search Topics

Select Assessment
Current Assessment

Hide # | Expand All | Collapse All | Download | Invite Others | Save | Save and Return | Return

Complete the following worksheet to document the organization's compliance with the controls contained within the CMMC – Awareness and Training (AT) control domain. This worksheet should be completed by an Internal Auditor.

1 C011 - CONDUCT SECURITY AWARENESS ACTIVITIES (2 REQUIRED REMAINING)

1.1 Security Awareness Training - CMMC Ctr: AT.2.056 - Ensure that managers, system administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems. (NIST 800-171 Rev. 2 Ctr Ref: 3.2.2)

Does the company ensure that managers, system administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems?

[Show Guidance]

1.2 Insider Threat Awareness Training - CMMC Ctr: AT.3.058 - Provide security awareness training on recognizing and reporting potential indicators of insider threat. (NIST 800-171 Rev. 2 Ctr Ref: 3.2.3)

Does the company ensure that users, managers, and system administrators receive annual training on potential indicators and possible precursors of insider threats and other serious violations of company policies consistent with this control requirement?

[Show Guidance]

3 required remaining

Save | Save and Return | Return

A sidebar will open with more information to help you respond.

CMMC Awareness and Training Worksheet

Search Topics Search

Hide # | Expand All | Collapse All Download Invite Others Save Save and Return Return

Complete the following worksheet to document the organization's compliance with the controls contained within the CMMC – Awareness and Training (AT) control domain. This worksheet should be completed by an Internal Auditor.

1 CO11 - CONDUCT SECURITY AWARENESS ACTIVITIES (2 REQUIRED REMAINING)

1.1 Security Awareness Training - CMMC Ctrl: AT.2.056 - Ensure that managers, system administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems. (NIST 800-171 Rev. 2 Ctrl Ref: 3.2.1)

Does the company ensure that managers, system administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems?

[Hide Guidance]

1.2 Insider Threat Awareness Training - CMMC Ctrl: AT.3.058 - Provide security awareness training on recognizing and reporting potential indicators of insider threat. (NIST 800-171 Rev. 2 Ctrl Ref: 3.2.3)

Does the company ensure that users, managers, and system administrators receive annual training on potential indicators and possible precursors of insider threats and other serious violations of company policies consistent with this control requirement?

[Show Guidance]

3 required remaining Save Save and Return Return

AT.2.056

Ensure that managers, system administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

- (a) security risks associated with organizational activities involving CUI are identified;
- (b) policies, standards, and procedures related to the security of the system are identified;
- (c) managers, system administrators, and users of the system are made aware of the security risks associated with their activities; and
- (d) managers, system administrators, and users of the system are made aware of the applicable policies, standards, and procedures related to the security of the system.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

3. Click **Hide Guidance** if you wish to dismiss the sidebar.

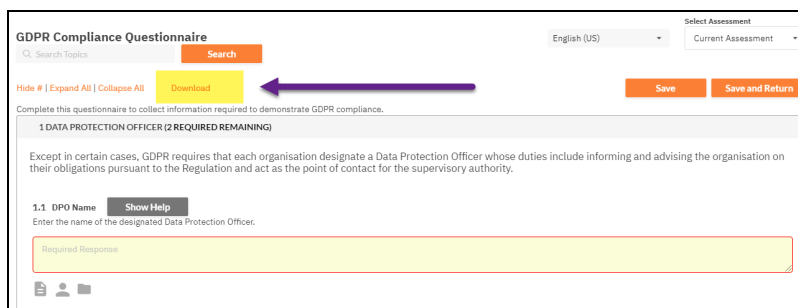
Download and Print Assessment Forms

You can download and print questionnaires and worksheets presented for completion during the assessment process.

Note: The form will be converted to Microsoft Word format.

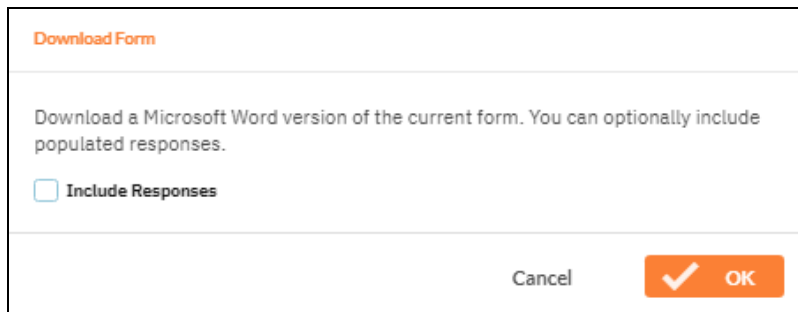
To do this:

1. Open the form you wish to download and/or print. You can do this from **Assessments > Forms**, or by opening the form from its **To Do** item.



The screenshot shows the 'GDPR Compliance Questionnaire' interface. At the top, there's a search bar and a 'Search' button. Below that, there are buttons for 'Hide #', 'Expand All', 'Collapse All', and 'Download'. A purple arrow points to the 'Download' button. To the right of the 'Download' button are 'Save' and 'Save and Return' buttons. The main content area shows the questionnaire text, including a section for '1 DATA PROTECTION OFFICER (2 REQUIRED REMAINING)' and a text input field for '1.1 DPO Name'.

2. Click **Download**.
3. Select **Include Responses** if you wish to also download the information already in the form.



The screenshot shows a 'Download Form' dialog box. It contains the text: 'Download a Microsoft Word version of the current form. You can optionally include populated responses.' Below this text is a checkbox labeled 'Include Responses' which is currently unchecked. At the bottom right of the dialog are 'Cancel' and 'OK' buttons.

4. Click **OK**. Your download will begin. You can then edit or print the form in MS Word format.

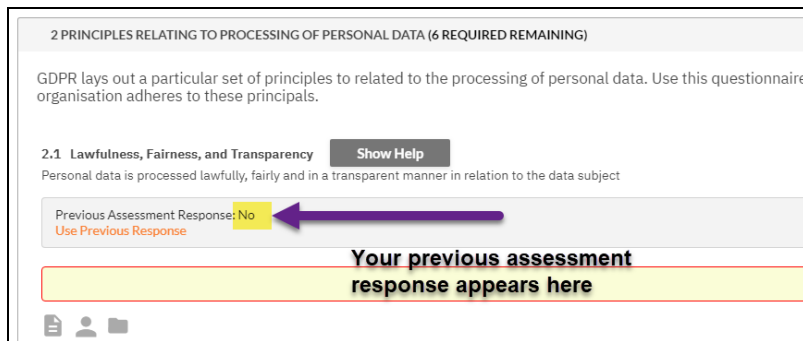
Re-use Previous Responses in Questionnaires

Compliance Manager saves your completed assessment forms and allows you to use them as a starting point for new assessment projects, thus saving you valuable time. This requires that you have at least one completed assessment. To re-use form responses, open the *new* form from the To Do Item or from **Assessments > Forms**.

You then have several options depending on the type of data you wish to re-use:

Simple Form Entries

1. For *simple form entries*, you can see your **Previous Assessment Response** immediately below the form question.

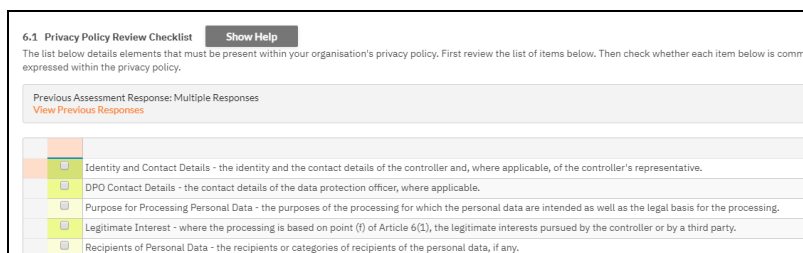


The screenshot shows a questionnaire titled "2 PRINCIPLES RELATING TO PROCESSING OF PERSONAL DATA (6 REQUIRED REMAINING)". Below the title, there is a paragraph of text: "GDPR lays out a particular set of principles to related to the processing of personal data. Use this questionnaire organisation adheres to these principals." Below this, there is a section titled "2.1 Lawfulness, Fairness, and Transparency" with a "Show Help" button. Below the section title, there is a paragraph of text: "Personal data is processed lawfully, fairly and in a transparent manner in relation to the data subject". Below the text, there is a field labeled "Previous Assessment Response: No" with a "Use Previous Response" link. A purple arrow points from the "Use Previous Response" link to a yellow box below the field. The yellow box contains the text "Your previous assessment response appears here".

2. Click **Use Previous Response**. This will copy and paste the previous response into the new form field.

Tables and Checklists

1. For *tables or checklists*, click **View Previous Responses**.



The screenshot shows a checklist titled "6.1 Privacy Policy Review Checklist" with a "Show Help" button. Below the title, there is a paragraph of text: "The list below details elements that must be present within your organisation's privacy policy. First review the list of items below. Then check whether each item below is commu expressed within the privacy policy." Below the text, there is a section labeled "Previous Assessment Response: Multiple Responses" with a "View Previous Responses" link. Below the link, there is a table with 5 rows and 2 columns. The first column contains checkboxes and the second column contains text descriptions of the items to be reviewed.

<input type="checkbox"/>	Identity and Contact Details - the identity and the contact details of the controller and, where applicable, of the controller's representative.
<input type="checkbox"/>	DPO Contact Details - the contact details of the data protection officer, where applicable.
<input type="checkbox"/>	Purpose for Processing Personal Data - the purposes of the processing for which the personal data are intended as well as the legal basis for the processing.
<input type="checkbox"/>	Legitimate Interest - where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party.
<input type="checkbox"/>	Recipients of Personal Data - the recipients or categories of recipients of the personal data, if any.

2. You can then preview all of your responses in a pop-up window.

Previous Entries

The table below shows the answers supplied in the previous assessment.

<input checked="" type="checkbox"/>	Identity and Contact Details - the identity and the contact details of the controller and, where applicable, of the controller's representative.
<input checked="" type="checkbox"/>	DPO Contact Details - the contact details of the data protection officer, where applicable.
<input checked="" type="checkbox"/>	Purpose for Processing Personal Data - the purposes of the processing for which the personal data are intended as well as the legal basis for the processing.
<input type="checkbox"/>	Legitimate Interest - where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party.
<input type="checkbox"/>	Recipients of Personal Data - the recipients or categories of recipients of the personal data, if any.
<input type="checkbox"/>	Intent to Transfer (if applicable) - where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.
<input type="checkbox"/>	Retention Period - the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period.
<input type="checkbox"/>	Access and Erasure Rights - the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability.
<input type="checkbox"/>	Right to Withdraw Consent - where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal.

- Click **Use Previous Responses** from the pop-up menu containing your previously entered answers. This will copy and paste the previous responses into the new form fields.

Re-Use All Previous Responses

If you wish to use all of your previous responses and enter them into the form, click **Use All Previous Responses** at the top of the form. All of your previous responses will be copied and pasted into the form.

GDPR Compliance Questionnaire Use All Previous Responses Download Expand All Collapse All

11 Required Remaining Hide # Filter Topics T X Invite Others Save Save and Return Return

Complete this questionnaire to collect information required to demonstrate GDPR compliance.


1 DATA PROTECTION OFFICER (2 Required Remaining)

Except in certain cases, GDPR requires that each organisation designate a Data Protection Officer whose duties include informing and advising the organisation on their obligations pursuant to the Regulation and act as the point of contact for the supervisory authority.

1.1 DPO Name
Enter the name of the designated Data Protection Officer.

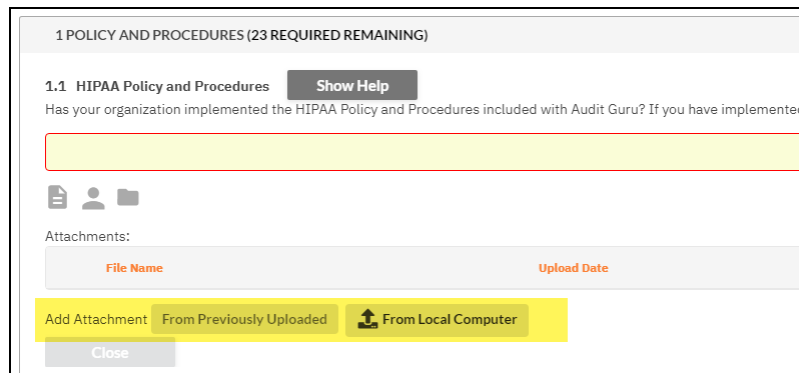
Previous Assessment Response: **Example Response**

Use Previous Response Required Response



Compliance Manager Assessment Files (Document Repository)

When completing questionnaires forms and worksheets, you can upload supporting documents as a part of answering a question. These will be added as exhibits within the compliance documentation that will be generated at the end of the assessment process. Once you upload a file once, you can choose whether to re-use that file in other worksheets or questionnaires performed at that Site.



1 POLICY AND PROCEDURES (23 REQUIRED REMAINING)

1.1 HIPAA Policy and Procedures [Show Help](#)

Has your organization implemented the HIPAA Policy and Procedures included with Audit Guru? If you have implemented

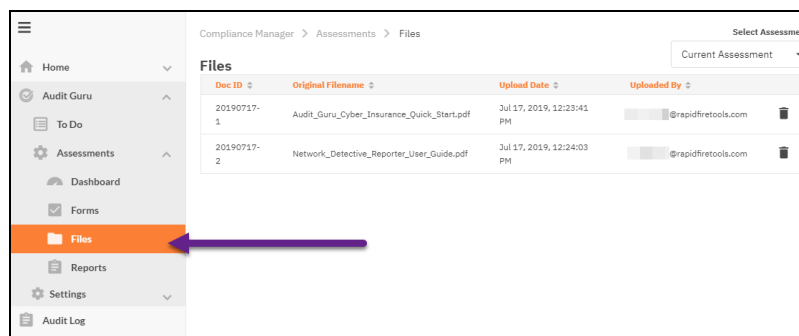
Attachments:

File Name	Upload Date
-----------	-------------

[Add Attachment](#) [From Previously Uploaded](#) [From Local Computer](#)

[Close](#)

From your Site, you can view and choose to delete these documents from **Your Site** > **Compliance Manager** > **Assessments** > **Files**. You cannot download them.

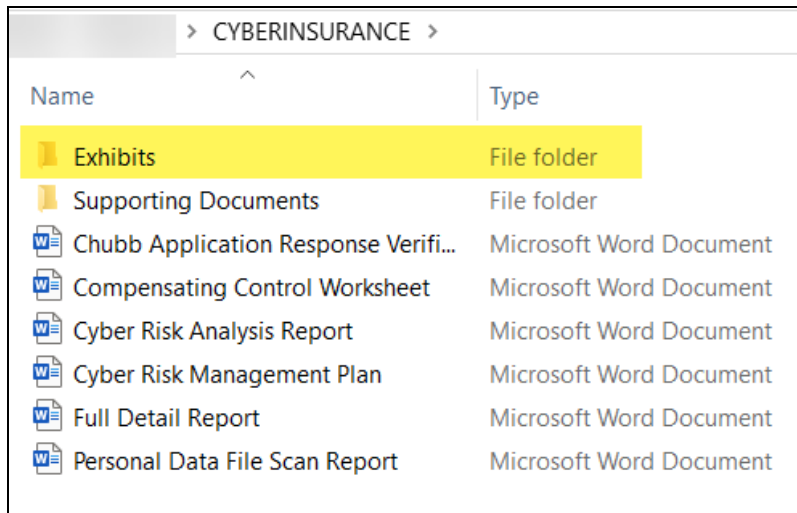
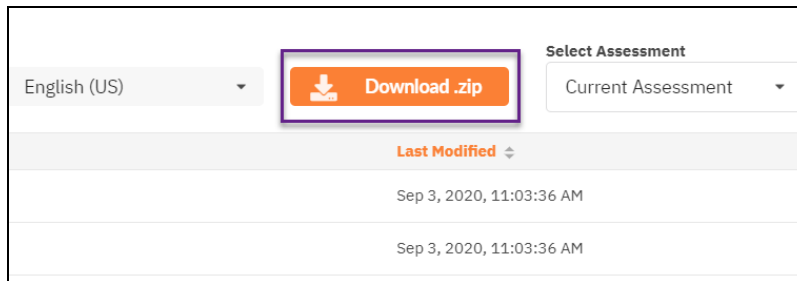


Compliance Manager > Assessments > Files

Select Assessment
Current Assessment

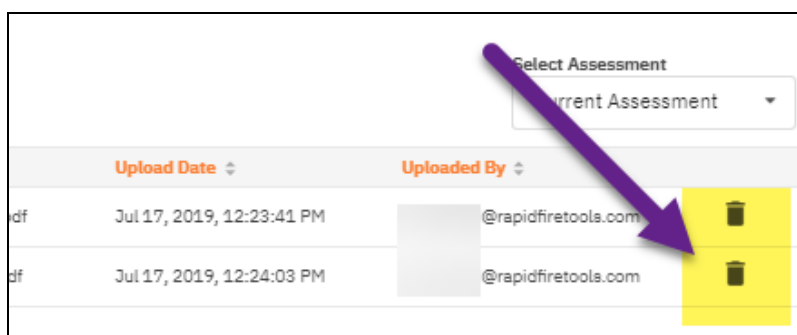
Doc ID	Original Filename	Upload Date	Uploaded By
20190717-1	Audit_Guru_Cyber_Insurance_Quick_Start.pdf	Jul 17, 2019, 12:23:41 PM	@rapidfiretools.com
20190717-2	Network_Detective_Reporter_User_Guide.pdf	Jul 17, 2019, 12:24:03 PM	@rapidfiretools.com

However, you can access files that you attached to worksheets once you generate reports. They will be located in the **Exhibits** folder once you download the report .zip file from **Reports**.



Delete an Assessment File

You can choose to delete a file from the **Assessments > Files** page by clicking on the **trash can** button.

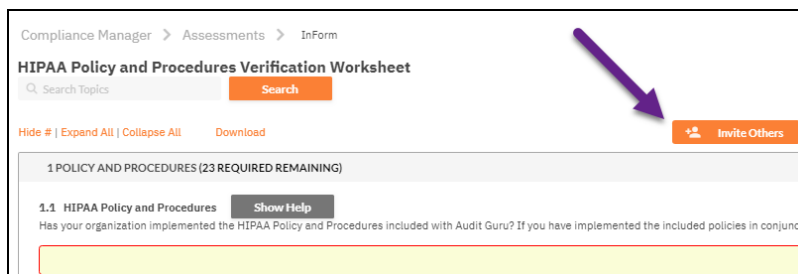


Note: You cannot delete a file if it is being used in a current or previous assessment.

Invite Subject Matter Experts (SMEs) to Complete Forms

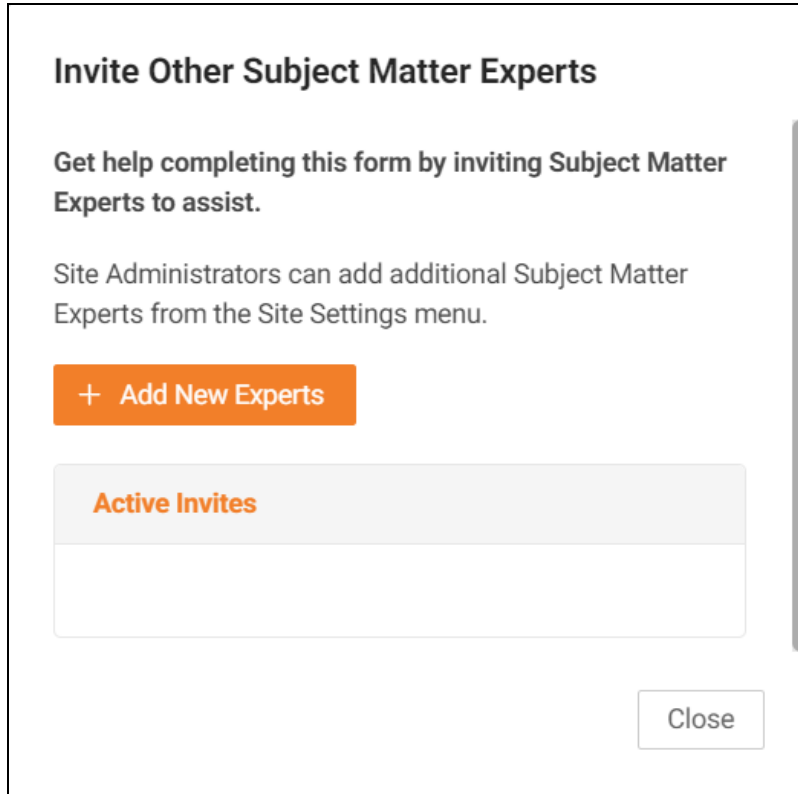
You can invite Subject Matter Experts (SMEs) from within your organization to assist you in responding to worksheets and surveys. To invite an SME:

1. First ensure that one or more users are added to the **Subject Matter Expert** Project Role under **[Your Site] > Home > Roles**.
2. Open the worksheet for which you would like to invite an SME. You can do this either from the **Compliance Manager** tab > **Assessments > Forms** or from the **Task** item in the **To Do** list.
3. With the worksheet open, click **Invite Others**.



The Invite Other Subject Matter Experts screen will appear.

4. Click **Add New Experts** to invite new SMEs.



Invite Other Subject Matter Experts

Get help completing this form by inviting Subject Matter Experts to assist.

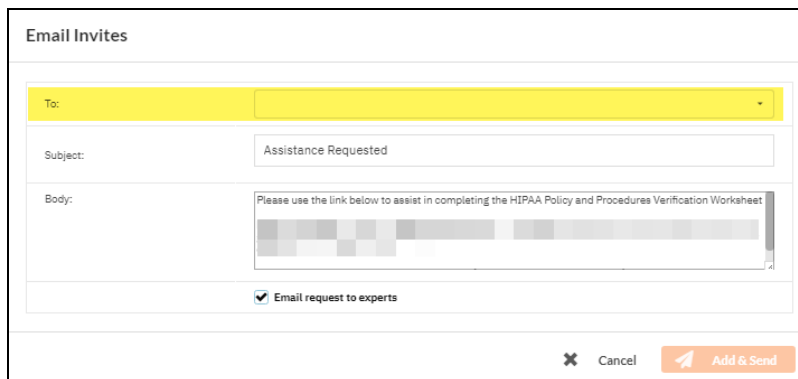
Site Administrators can add additional Subject Matter Experts from the Site Settings menu.

+ Add New Experts

Active Invites

Close

- Click **To** and select the SMEs whom you wish to invite. Edit your email's Subject and add any additional information in the body of your email.



Email Invites

To: [Dropdown menu]

Subject: Assistance Requested

Body: Please use the link below to assist in completing the HIPAA Policy and Procedures Verification Worksheet
[Text area with a link placeholder]

☒ Email request to experts

Cancel Add & Send

- Click **Add and Send**.

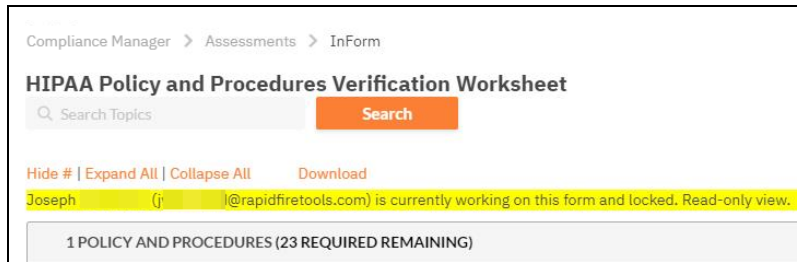
Once you invite the SME, they will receive an email with a link to access the worksheet. The SME can then contribute to and edit the worksheet.

Tip: See also: ["Completing Assessment Worksheets and Surveys" on page 165.](#)

Multiple Contributors and Locking Forms

Multiple contributors can make changes to forms, but only one user can access a form at a time. This helps prevent conflicting changes.

If another user is working with the form you will see a notification at the top of the form:



Compliance Manager > Assessments > InForm

HIPAA Policy and Procedures Verification Worksheet

Search Topics Search

Hide # | Expand All | Collapse All Download

Joseph (j@rapidfiretools.com) is currently working on this form and locked. Read-only view.

1 POLICY AND PROCEDURES (23 REQUIRED REMAINING)

If you are working on the form, your "lock" will expire after 20 minutes of inactivity. The form will then become available for other users to edit.

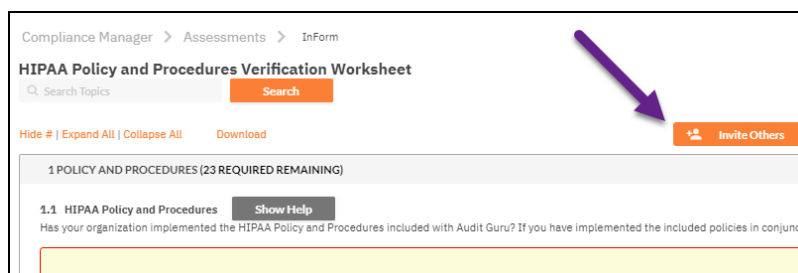
Revoke (Un-Invite) SME Invitation

You can revoke (or un-invite) the invitation to an SME to contribute to a worksheet.

Note: You may wish to do this if:

- You invite the wrong SME.
- You no longer want the SME to be able to edit the form.

1. Open the worksheet for which you would like to un-invite an SME. You can do this either from **Assessments > Forms** or from the **Task** item in the **To Do** list.
2. With the worksheet open, click **Invite Others**.



Compliance Manager > Assessments > InForm

HIPAA Policy and Procedures Verification Worksheet

Search Topics Search


Hide # | Expand All | Collapse All Download Invite Others

1 POLICY AND PROCEDURES (23 REQUIRED REMAINING)

1.1 HIPAA Policy and Procedures Show Help

Has your organization implemented the HIPAA Policy and Procedures included with Audit Guru? If you have implemented the included policies in conjunction with the Audit Guru, please check the box below.

The Invite Other Subject Matter Experts screen will appear.

3. Click the **Trash** icon  next to the user to revoke their invitation.

Invite Other Subject Matter Experts

Get help completing this form by inviting Subject Matter Experts to assist.

Site Administrators can add additional Subject Matter Experts from the Site Settings menu.

+ Add New Experts

Active Invites	
<div></div> i@rapidfiretools.com	
Unitrends Example User (unitrends-example-user@unitrends.com)	

X Close

4. Click **OK**. The SME will no longer be able to access or edit the form.

Manage SME Invites to Contribute to Questionnaires and Worksheets

From the **Manage Invites** page, you can manage which *Subject Matter Experts* (SMEs) you have invited to complete specific worksheets and surveys as part of the assessment process. When you invite an SME, they will receive an email invitation to contribute to the form.

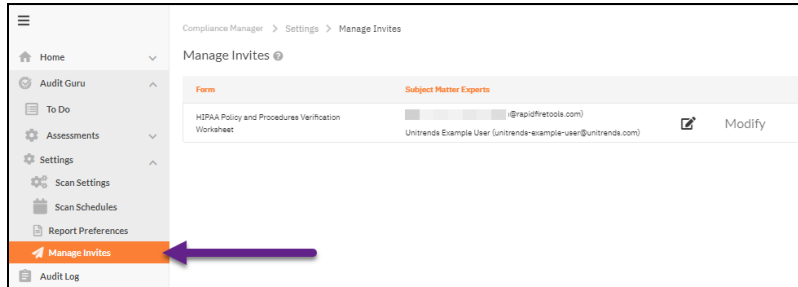
You can invite new Subject Matter Experts, or revoke the invitation of SMEs whom you previously invited to contribute to your forms.

Note: Only Site Admin users can access this page and manage invites.

To Manage Invites:

1. Navigate to your Site, then to **Compliance Manager > Settings > Manage Invites**.

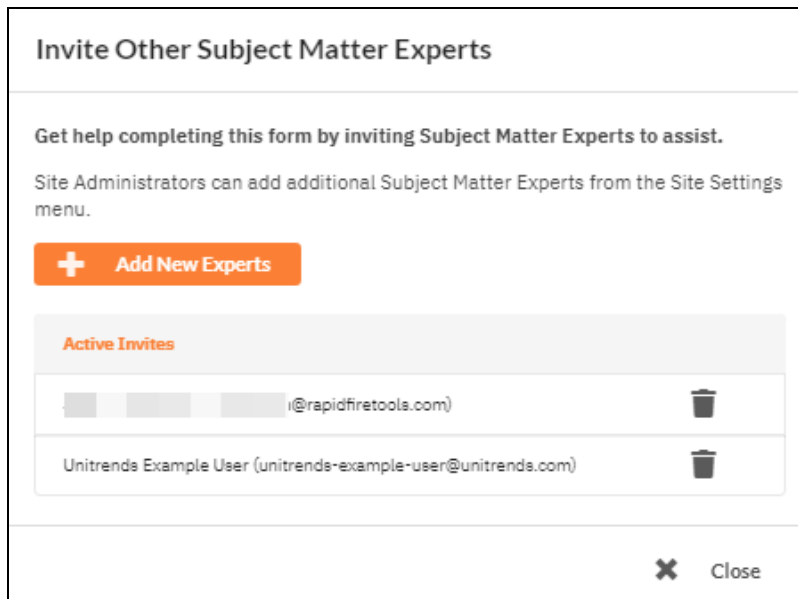
Here you will see the questionnaire or worksheets for which you have active invitations.



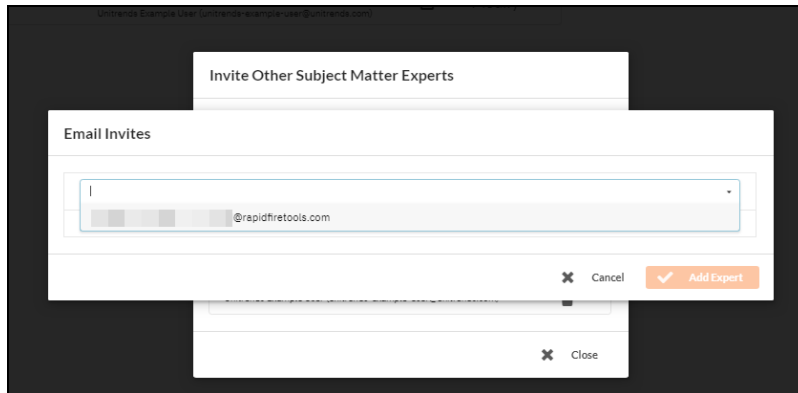
2. Click **Modify**.

Note: In order to Add the SME, you must first have added the **User** to your Site. You must also have added that user to the Subject Matter Expert project **Role**.


3. Click **Add New Experts** to invite a new SME.



4. Select the SME from the drop-down menu. Also select whether to email the request to the SME.



Note: If you do not choose to email the request, the SME will need to log in to the RapidFire Tools Portal in order to access and contribute to forms.

5. Click **Add Expert**. The SME will then receive an email invitation with a link to contribute to the form.
6. Alternatively, you can click **the trash icon**  to rescind the invitation of the SME. This can be useful when are ready to finalize a particular worksheet and no longer wish for it to be modified by the SME previously invited to complete the form.

Project Roles in the CMMC Assessment

The table below details the Project Roles relevant to your CMMC assessment.

Note: See ["CMMC To Do Task Complete List" on page 270](#) for a breakdown of the sequence of steps in the assessment process, as well as which roles perform which tasks.

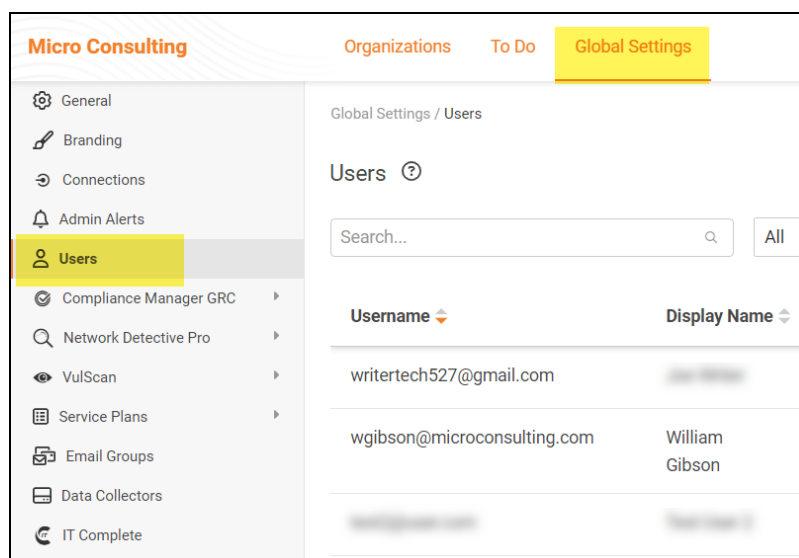
Role	Assessment Responsibilities
Site Administrator	<ul style="list-style-type: none"> • The Master or Admin who creates the site will be designated the Site Administrator. • The Site Administrator user can be used to perform all tasks performed by each role. • The Site Administrator will see all To Do list items for each role. A user assigned the Site Admin role can perform the entire assessment by themselves.
Technician	<ul style="list-style-type: none"> • Installs the server app. • Validates that the server is installed successfully and connected to the network. • Configures the server schedules and scans. • Enters credentials for the technical portions of managing the server. • Works with the Internal Auditor as the technical expert. • Performs the work for remediation. • Knowledgeable about the target network.
Internal Auditor	<ul style="list-style-type: none"> • Completes To Do list tasks to perform the assessment. • Completes worksheets and surveys. • Invites Subject Matter Experts to contribute to forms.
Subject Matter Expert	<ul style="list-style-type: none"> • Receives email invitations to contribute to worksheets and surveys. • Can only see and edit forms; cannot access any other portal features. • Does not receive To Do tasks. <div style="border: 2px solid red; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p>Important: Do not assign the SME role to users with other role assignments. Doing so will limit their access to the portal.</p> </div>

Manage Portal Users and Access

This section covers how portal admins can create and manage users. This includes assigning users the appropriate level of access for their intended roles. Likewise, here you can review how individual users can manage how they authenticate their access to the portal.

Manage Users (Global Level)

You can manage users associated with your account from **Global Settings > Users**.



From the **Users** page, you can see a list of users associated with your account. This includes their *Global Access* and *Site Access* role. You can see each site that a user is associated with, as well as the **Roles** they have been assigned to each site.

Username	Display Name	Global Access Level	Site Level Access	2FA	
billfoyers@itsolutions.com	Bill Foyers	Site Restricted	Salient Industries (Client)	Yes	
bv-admin@microsolutions.com		Admin	All / (Site Admin), Test CIS V8 IG1 site (Site Admin)	No	
chuckp@microconsulting.com	Chuck Palahniuk	Site Restricted	Micro Consulting MSP (Unassigned)	No	
example-user@rapidfiretools.com	Example User 1	Site Restricted	Sample HIPAA Assessment (Unassigned)	No	

Users and Global Access Roles

Note: Global Access Level vs. Site Level Access

- *Global Access Level* determines the level of access a user has to the RapidFire Tools Portal account, including which features and sites a user can access.
- *Site Access Level*, on the other hand, represents 1) the **Sites** to which a user has been assigned and 2) the **Role(s)** the user has been assigned at a Site. Roles include Site Admin, Technician, Internal Auditor, or SME. A user's level of Global Access does not limit the project role they can be assigned for a particular site.

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

Global Access Role	Description
MASTER/ALL	<p>Has global access to all Organizations and Sites and the ability to manage billing, technical information, and confidential data/notes. Has access to <i>Site Settings</i> and <i>Global Settings</i>. Can access API Keys from Global Settings.</p> <p>Who should I assign this level to?</p> <p>IT Managers within your operation who have your highest level of trust, and who will:</p> <ul style="list-style-type: none"> • be the "primary" admin for the RapidFire Tools Portal • handle sensitive data for all of your clients • purchase and provision additional RapidFire Tools Products • create and assign the appropriate security permissions for users within — and outside — of your operation who access the Portal
ADMIN	<p>Has global access to multiple sites. Has access to <i>Site Settings</i> and <i>Global Settings</i>.</p> <p>Who should I assign this level to?</p> <ul style="list-style-type: none"> • Users you trust within your operation to be "secondary" admins for the RapidFire Tools Portal • Users you trust with sensitive data for all of your clients • Users you trust to create and assign the appropriate security permissions for users within — and outside — of your operation

Global Access Role	Description
	who access the Portal
RESTRICTED	<p>Does not have global access to multiple organizations/sites. Site access must be defined by a Site Admin.</p> <p>Users in the Restricted Role can log in to the Network Detective application.</p> <p>Who should I assign this level to?</p> <ul style="list-style-type: none"> • Techs or others in your operation who should only access specific Sites as a Site Admin or Technician • Techs or others in your operation who should also access sites in the Network Detective application <div style="border: 2px solid red; padding: 10px; margin-top: 10px;"> <p>Important: Users should not be assigned the Restricted Role unless you are using the Network Detective app in tandem with other RapidFire Tools Products. Instead, use the Site Redistricted Role.</p> </div>
SITE RESTRICTED	<p>Does not have global access to multiple organizations/sites. Site access must be defined by a Site Admin.</p> <p>Who should I assign this level to?</p> <ul style="list-style-type: none"> • Techs who should only access specific Sites as a Site Admin or Technician • Client users working with your team to perform IT or compliance assessments in the role of Technician, Internal Auditor, or SME

From the Users page, you can also:

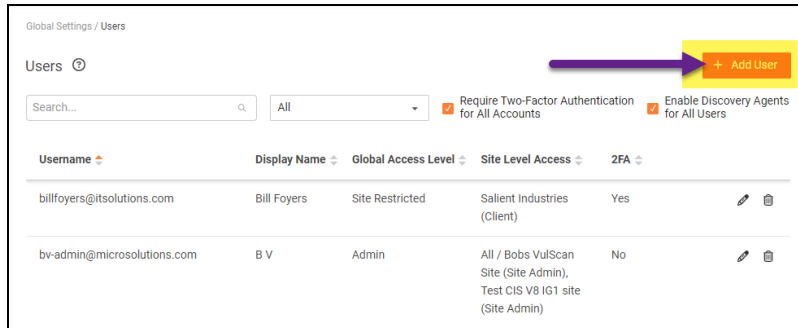
- ["Add User at Global Level" below](#)
- ["Edit User at Global Level" on page 192](#)

Add User at Global Level

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

You can add users to your account at the global level from the **Global Settings > Users** page. To do this:

1. Click **Add User**.



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

The 'Add User' form contains the following fields and options:

- Username/Email Address:** * micro-pro@user.com
- First Name:** * Micro
- Last Name:** * Pro
- Password:** *
- Confirm Password:** *
- Global Access Role:** * Site Restricted

At the bottom right, there are two buttons: 'Close' and '+ Add'.

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

3. Choose a **Global Access Role** for the User.

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

Global Access Role	Description
MASTER/ALL	<p>Has global access to all Organizations and Sites and the ability to manage billing, technical information, and confidential data/notes. Has access to <i>Site Settings</i> and <i>Global Settings</i>. Can access API Keys from Global Settings.</p> <p>Who should I assign this level to?</p> <p>IT Managers within your operation who have your highest level of trust, and who will:</p> <ul style="list-style-type: none"> • be the "primary" admin for the RapidFire Tools Portal • handle sensitive data for all of your clients • purchase and provision additional RapidFire Tools Products • create and assign the appropriate security permissions for users within — and outside — of your operation who access the Portal
ADMIN	<p>Has global access to multiple sites. Has access to <i>Site Settings</i> and <i>Global Settings</i>.</p> <p>Who should I assign this level to?</p> <ul style="list-style-type: none"> • Users you trust within your operation to be "secondary" admins for the RapidFire Tools Portal • Users you trust with sensitive data for all of your clients • Users you trust to create and assign the appropriate security permissions for users within — and outside — of your operation who access the Portal
RESTRICTED	<p>Does not have global access to multiple organizations/sites. Site access must be defined by a Site Admin.</p> <p>Users in the Restricted Role can log in to the Network Detective</p>

Global Access Role	Description
	<p>application.</p> <p>Who should I assign this level to?</p> <ul style="list-style-type: none"> • Techs or others in your operation who should only access specific Sites as a Site Admin or Technician • Techs or others in your operation who should also access sites in the Network Detective application <div style="border: 2px solid red; padding: 5px; margin-top: 10px;"> <p>Important: Users should not be assigned the Restricted Role unless you are using the Network Detective app in tandem with other RapidFire Tools Products. Instead, use the Site Redistricted Role.</p> </div>
SITE RESTRICTED	<p>Does not have global access to multiple organizations/sites. Site access must be defined by a Site Admin.</p> <p>Who should I assign this level to?</p> <ul style="list-style-type: none"> • Techs who should only access specific Sites as a Site Admin or Technician • Client users working with your team to perform IT or compliance assessments in the role of Technician, Internal Auditor, or SME

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

Edit User at Global Level

Note: Only *Master* and *Admin* users can edit users. And only Master users can edit other Master users. See ["Manage Users \(Global Level\)" on page 187](#) for more details.

To edit users:

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

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

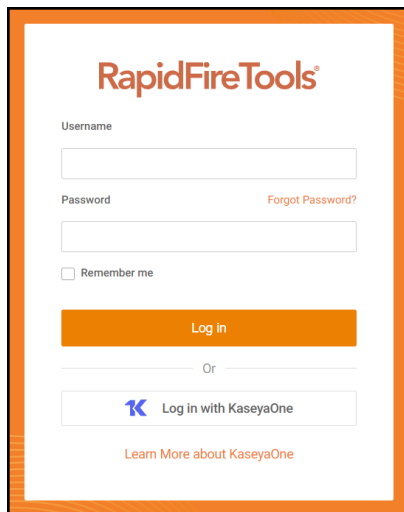
3. Click **Save**.

Set Up Portal Branding

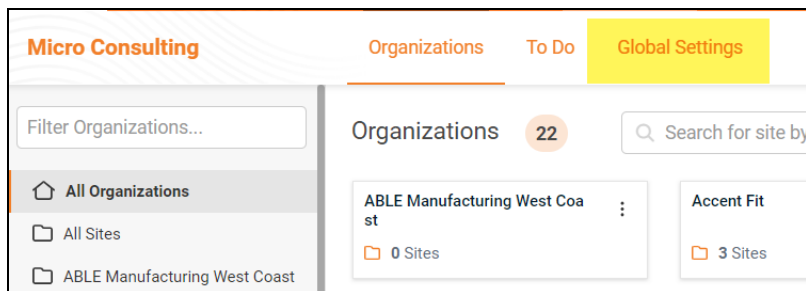
The RapidFire Tools Portal allows you to customize many elements to fit with your organization's brand and identity. This topic covers how you can modify the Portal's look and feel.

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

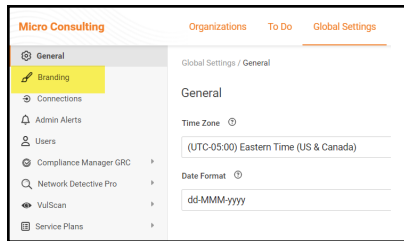
Note: In order to configure the settings in the Portal, the login credentials you use to access the Portal will require the Master User rights.



2. Click **Global Settings**.



3. Click **Branding**.



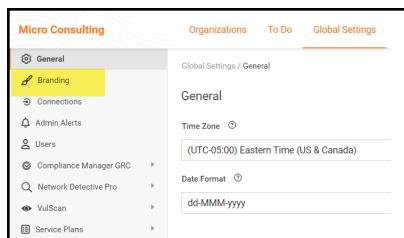
From this page, you can then:

- ["Set Custom Portal Theme" below](#)
- ["Set Custom Portal Subdomain" on the facing page](#)
- ["Set Custom Company Name" on page 197](#)
- ["Set Custom Company Logo" on page 198](#)

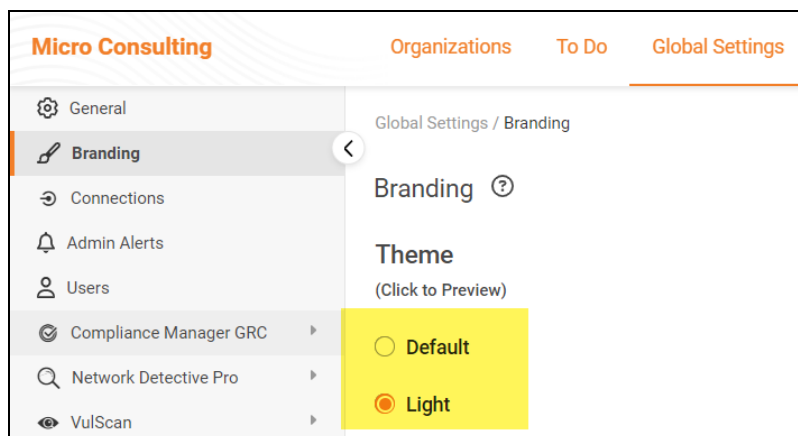
Set Custom Portal Theme

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

1. From **Global Settings > Branding**, select the *Default* or *Light* under theme.



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

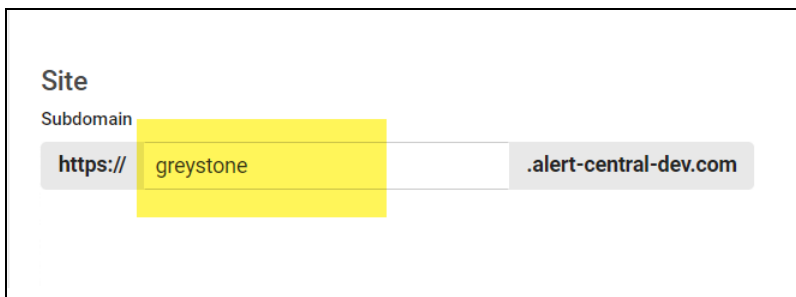


- When you select the theme, you can click around the Portal and preview it. You must click **Save** from **Global Settings > Branding** to apply your changes. This change will apply to all users.

Set Custom Portal Subdomain

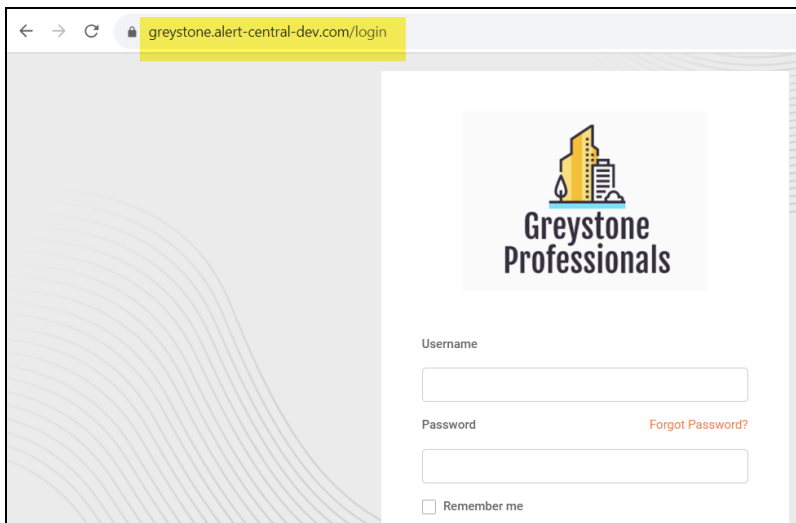
You can enter a custom subdomain to communicate your company name/brand to users when they access the URL for the portal. To do this:

- From **Global Settings > Branding**, scroll down and enter the custom **Subdomain** name in the Site Subdomain field.



The screenshot shows a configuration form for the 'Site Subdomain'. The label 'Site Subdomain' is at the top. Below it, the text 'https:// greystone .alert-central-dev.com' is displayed. The word 'greystone' is highlighted in a yellow box, indicating the custom subdomain being entered.

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

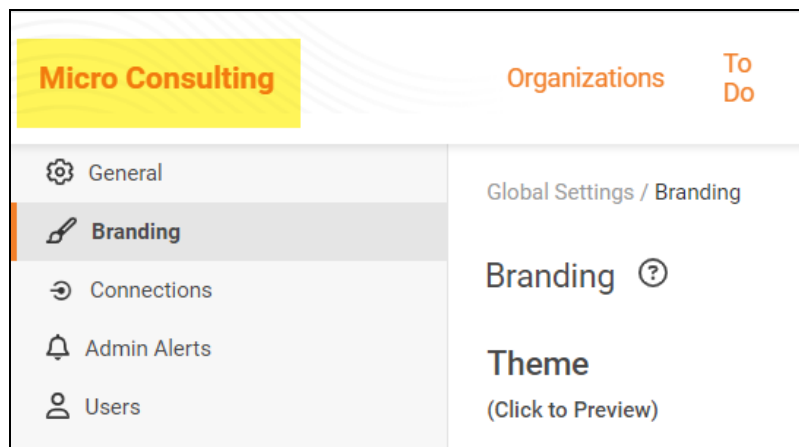


The screenshot shows a web browser displaying the login page for 'Greystone Professionals'. The address bar shows the URL 'greystone.alert-central-dev.com/login'. The login form includes a 'Username' field, a 'Password' field, a 'Forgot Password?' link, and a 'Remember me' checkbox. The Greystone Professionals logo is displayed at the top of the form.

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.

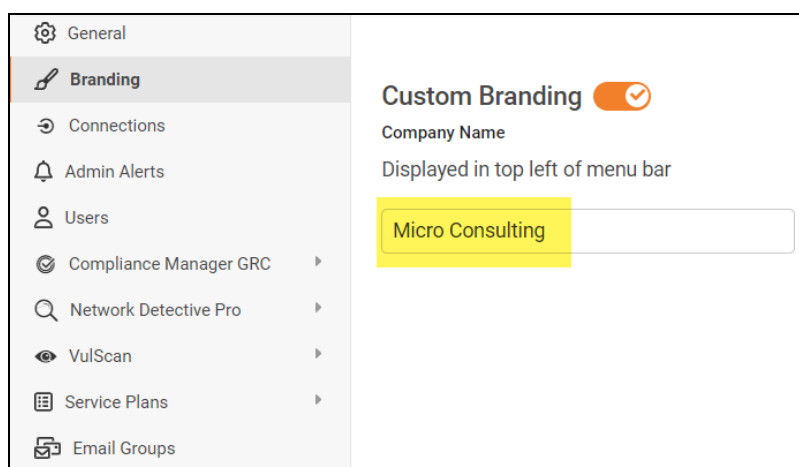
Set Custom Company Name

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 > 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 > Branding**, click **Select** under Company Logo and **Upload** a custom image.

Company Logo

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


Browse

 or drop file

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

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

login screen.



The logo for Greystone Professionals features a stylized illustration of a city skyline with a yellow building and a blue building, with a blue line representing a river or path in front of them. Below the illustration, the text "Greystone Professionals" is written in a bold, black, sans-serif font.

Username

Password [Forgot Password?](#)

☐ Remember me

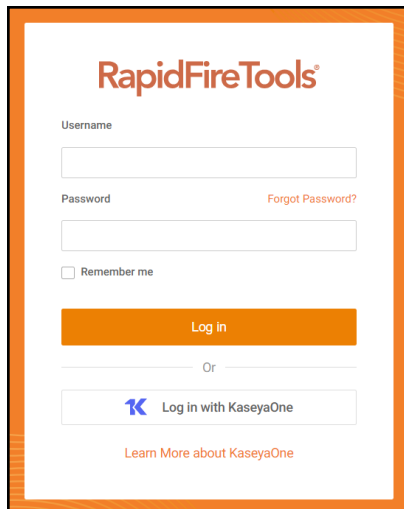
[Log in](#)

[Learn More about KaseyaOne](#)

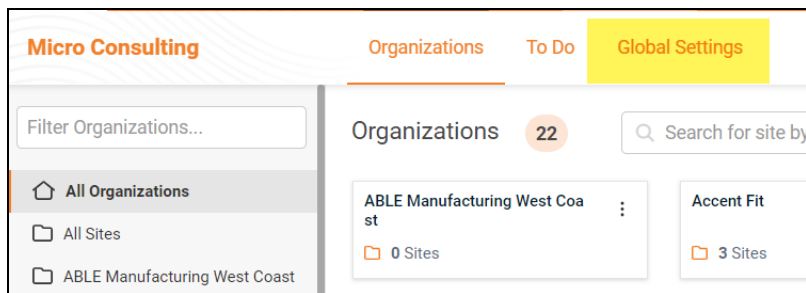
Set Up a Custom Subdomain to Access the RapidFire Tools Portal

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

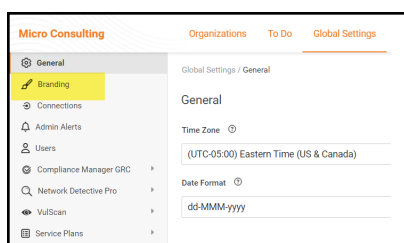
Note: In order to configure the settings in the Portal, the login credentials you use to access the Portal will require the Master User rights.



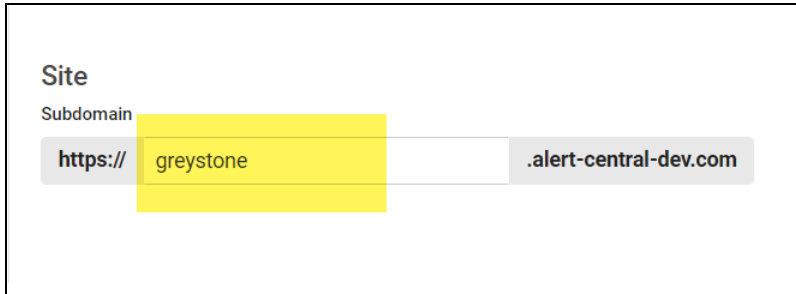
2. Click **Global Settings**.



3. Click **Branding**.

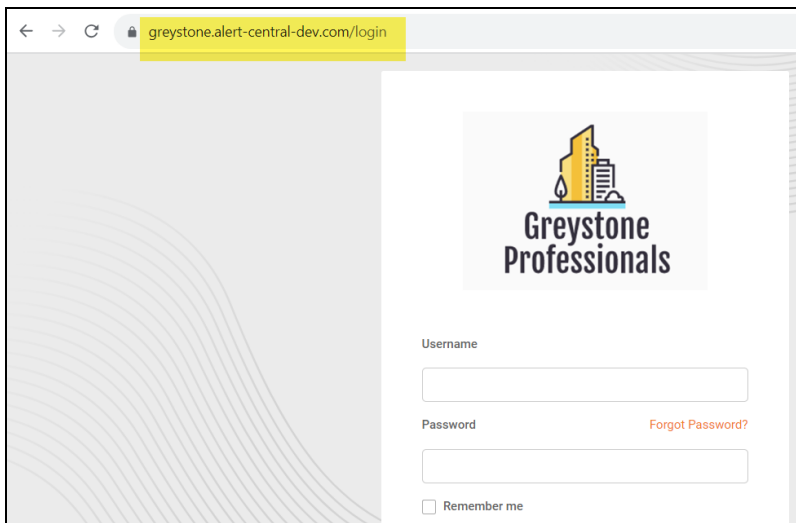


4. Enter the **Subdomain** name you desire in the Site Subdomain field.



The screenshot shows a configuration form for a site. The 'Site' section is expanded, showing the 'Subdomain' field. The 'Subdomain' field is highlighted in yellow and contains the text 'greystone'. The 'URL' field is also visible, showing 'https://' and '.alert-central-dev.com'.

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



The screenshot shows a web browser window with the URL 'greystone.alert-central-dev.com/login' in the address bar. The page displays the 'Greystone Professionals' logo, which features a stylized building icon. Below the logo, there are input fields for 'Username' and 'Password'. A 'Remember me' checkbox is located below the password field. A 'Forgot Password?' link is also visible next to the password field.

Log Out of RapidFire Tools Portal

To maintain data security, log out of the RapidFire Tools Portal when you are not using it.

1. From the portal, click the user icon  in the top right hand corner of the screen.
2. Click **Logout**.
3. You will return to the RapidFire Tools Portal Login page.

Compliance Manager Resources

Compliance Manager comes with additional resources to help you sell your Compliance and IT Assessment services to your customers. This includes marketing collateral, brochures, videos, and so on.

To access these resources:

1. Log into the RapidFire Tools Portal with your credentials.
2. From the portal, click the user icon  in the top right hand corner of the screen.
3. Click **Compliance Manager Resources**.

The Compliance Manager Resources page will appear.

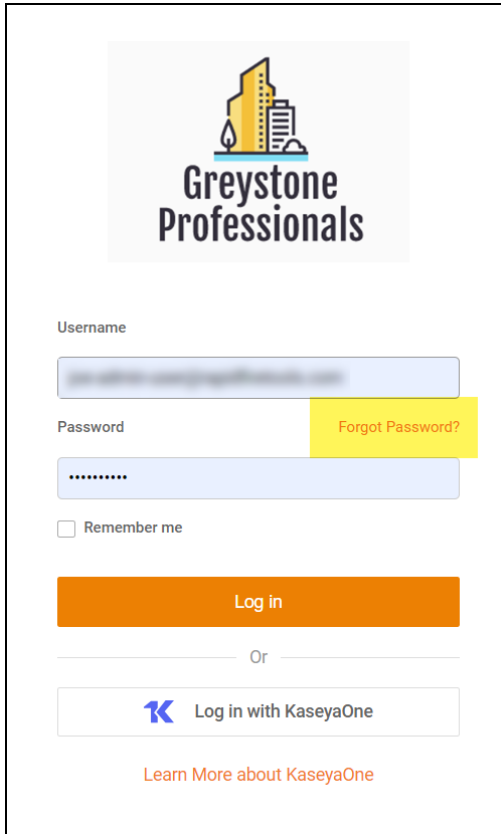


From here you can access user guides, marketing collateral, and also view a price list for Compliance Manager licenses based on the currency you used for your initial purchase.

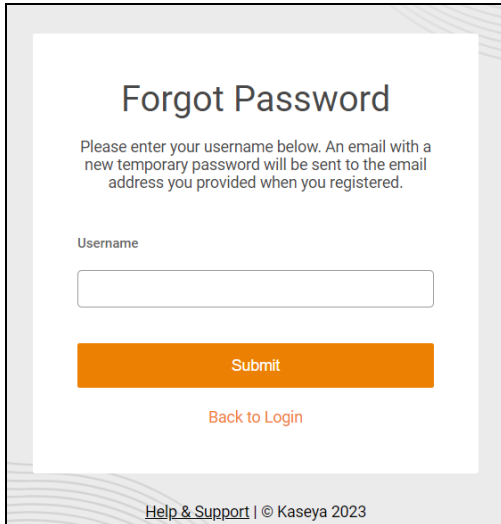
Recover Forgotten Password

To recover a forgotten password:

1. Open the RapidFire Tools Portal at <https://www.youritportal.com>.



2. Click **Forgot Password?**
3. Enter your user account's **email address**.



Forgot Password

Please enter your username below. An email with a new temporary password will be sent to the email address you provided when you registered.

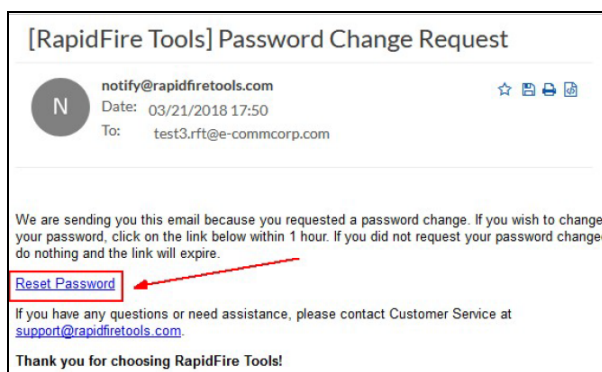
Username

Submit

[Back to Login](#)

[Help & Support](#) | © Kaseya 2023


4. Click **Submit**. You will receive an email with a link to change your password. Click **Reset Password**.

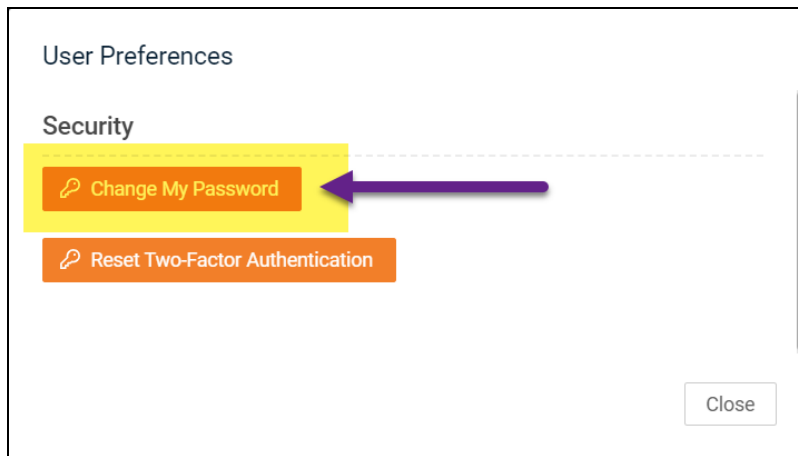


5. Follow the on-screen prompts to complete recovering your password.

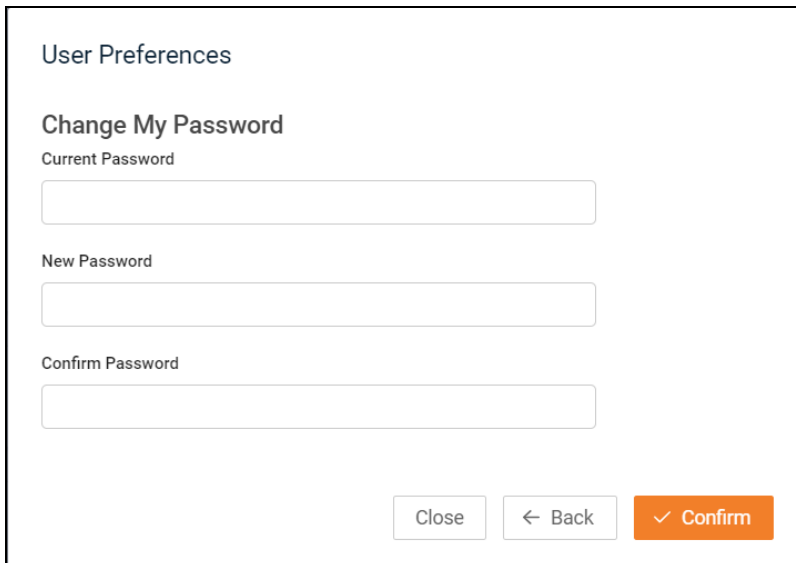
Change your Password

To change your password in the RapidFire Tools Portal:

1. Log into the RapidFire Tools Portal with your credentials.
2. From the portal, click the user icon  in the top right hand corner of the screen.
3. Click **User Preferences**.
4. Click **Change My Password**.



5. Then enter your new password and confirm it again.



6. Click **Confirm**.

Your password will then be changed.

Scans for Compliance Manager Assessments

This section covers configuring and performing network scans with Compliance Manager for your compliance assessments.

Compliance Manager Server Firewall Requirements

IT admins and end customers using RapidFire Tools servers/appliances should configure the firewall rules on their networks to enable access to the following RapidFire Tools URLs.

- gatekeeper.rapidfiretools.com
- go.rapidfiretools.com
- au.rapidfiretools.com
- go-eu.rapidfiretools.com
- go-au.rapidfiretools.com
- wcflb.rapidfiretools.com
- wcflb-eu.rapidfiretools.com
- wcflb-au.rapidfiretools.com
- api.ndglue.com
- networkdetective.s3.amazonaws.com
- download.rapidfiretools.com

The RapidFire Tools Server and Discovery Agent requires access to **port 443**.

The Virtual Appliance requires access to the Greenbone Community Feed at `feed.community.greenbone.net` using **port 873**.

View Assessment Scan Status

On a Site's home page, consult the **Assessment Scan Status** bar to quickly review the current scan for your assessment.

The screenshot shows the Compliance Manager dashboard. At the top, there's a 'Current Assessment' section with a 'Type' of 'HIPAA' and a 'Status' of 'Running'. Below this is the 'Assessment Scan Status' bar, which is highlighted in yellow. It shows a 'Scan Type' of 'Push Scan', a 'Status' of 'Running', a 'Start Date UTC' of '27-Jul-2020 6:11:33 PM', and a 'Last Scan Details' of 'Running. Total: 286, Success: 5, Failed: 1, Remaining: 287 (Elapsed 00:00:36)'. To the right of the bar is a 'View All' link. Below the bar are two sections: 'To Do's' with 12 items and 'Audit Log' with 23 items. The 'To Do's' section lists tasks like 'Set up Report Preferences', 'Create additional users and assign to roles', 'Install Compliance Manager Appliance', 'Configure Appliance Scan settings', and 'Start HIPAA Assessment'. The 'Audit Log' section lists events like 'Scan Started', 'New Task Created', 'Scan Completed', 'Status was updated to Complete', and 'Form Modified'.

Specifically, you can:

- See the progress of the current scan (refresh the page to update)
- See when a scan is complete
- See when a scan has failed

To view more details, including completed scans, click **View Details**.

The screenshot shows the 'Assessment Scan Status' bar. It has a title 'Assessment Scan Status' and a 'View All' link. Below the title is a message 'No Running Scans - See View All' with an information icon. A red arrow points from the message to the 'View All' link.

A list will appear detailing all scans, including completed and failed scans.

The screenshot shows a list of assessment scans. The table has columns for 'Scan Type', 'Status', 'Start Date UTC', 'End Date UTC', and 'Last Scan Details'. The list shows three completed scans: 'Network Scan', 'Push Scan', and 'External Vulnerability Scan'. Each scan has a unique reference number and a description of the scan results.

Scan Type	Status	Start Date UTC	End Date UTC	Last Scan Details
Network Scan	Completed	27-Jul-2020 5:23:43 PM	27-Jul-2020 5:33:39 PM	Network Data Collection (ref #12798345): Scan completed successfully.
Push Scan	Completed	27-Jul-2020 6:11:33 PM	27-Jul-2020 6:45:27 PM	PUSH Scan (ref #12798674, File Scan: HIPAA Quick): Scan completed successfully.
External Vulnerability Scan	Completed	27-Jul-2020 3:18:05 PM	27-Jul-2020 3:37:32 PM	External Vulnerability Scan completed successfully

The various scans include:

- Pre-scan Analysis
- External Vulnerability Scan
- Network Scans for Active Directory and Workgroup Networks
- Internal Vulnerability Scans
- Quick Remote Local Computer Scans
- Deep Remote Local Computer Scans

Important Notes for Scan Status

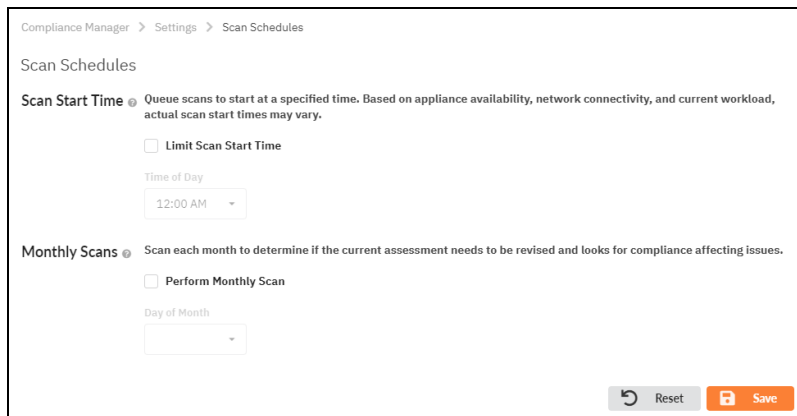
- Only the most recent scans for each scan "type" are displayed, eg. network scan, push deploy scan, external vulnerability scan, etc. You can view comprehensive details for all scans and site activity from the ["Audit Log " on page 268](#).
- There may sometimes be a delay of a few minutes between when a scan is completed and when a new To Do item appears. For example, the scan status may appear as "No Running Scans," even while the scan task remains incomplete in the To Do list. During this delay, the backend is working to prepare the new To Do item. Check the To Do list again in a few minutes.
- If you have scheduled a start time for scans, the scan will not appear in Scan Status until the scheduled time. You cannot view queued or pending scans in the Scan Status. See also ["Scan Schedules" on the facing page](#).

Scan Schedules

From the **Scan Schedules** page, you can configure the time of day at which your scans will begin for a particular site. You can also schedule recurring monthly rescans for ongoing IT and compliance assessment on a Site by Site basis.

Note: Only the Site Admin and Technician can access Scan Schedules.

To configure scan schedules, navigate to **Compliance Manager > Settings > Scan Schedules**.



The screenshot shows the 'Scan Schedules' configuration page. At the top, there is a breadcrumb trail: 'Compliance Manager > Settings > Scan Schedules'. Below this, the title 'Scan Schedules' is displayed. The first section is 'Scan Start Time', which includes a description: 'Queue scans to start at a specified time. Based on appliance availability, network connectivity, and current workload, actual scan start times may vary.' There is a checkbox labeled 'Limit Scan Start Time'. Below this checkbox is a 'Time of Day' dropdown menu currently set to '12:00 AM'. The second section is 'Monthly Scans', with a description: 'Scan each month to determine if the current assessment needs to be revised and looks for compliance affecting issues.' It includes a checkbox labeled 'Perform Monthly Scan' and a 'Day of Month' dropdown menu. At the bottom right of the form, there are two buttons: 'Reset' and 'Save'.

Scan Start Time

Use the **Limit Scan Start Time** option to control the time of day at which the internal and external network scans will begin. By default, this will be in Eastern US Standard time (UTC-05:00).

Note: Be sure that you have set your time zone before proceeding (see ["Set Time Zone" on page 265](#)).

The scan will begin at this time as soon as the server becomes available (i.e., as soon as it finishes a previous scan or regains network connectivity).

Tip: Use this feature to schedule the scan during office down-time to avoid affecting network performance during office hours.

Important: If you select Limit Scan Start Time, and you initiate a scan from the To Do list, your scan will NOT begin immediately. Instead, your scan will be put into a queue and will begin at your assigned start time. If you need to perform several scans, note that it may take several days to complete your assessment. This is because only one scan can begin at the Scan Start Time each day.

Scan Start Time Feature Impact on Compliance Manager Automated Scan Job Performance

The scan “Start Time” feature enables the Technician to schedule External Vulnerability, Network, and Remote Local Computer scans to start and be performed at scheduled times over a number of days during the assessment process.

Scan Start Time enables the Site’s “Technician” user to minimize the impact of the automated scans on the use of the company’s network during business hours.

When the scan Start Time feature is used, automated scans jobs will be scheduled to be started at the Start Time’s scheduled time over a period of four (4) days.

Scan Start Time Chronology Example

Below is an example of the scan start timing when the scan Start Time is set to schedule scan starts at 1:00 AM Eastern Time (ET).

Automated Scan Action Type	Scan Start Time and Associated To Do item Events	The Day the Scan is Started
Pre-Scan	When Assessment is started	Immediately after assessment is started (Day 1)
External Vulnerability Scan	Will be scheduled to start at 1:00 AM ET on Day 2	Day 2
Network Scan	Will be scheduled to run at 1:00 AM ET on Day 2 if the	Day 2

Automated Scan Action Type	Scan Start Time and Associated To Do item Events	The Day the Scan is Started
	<p>user marks the assessment's "Review Pre-scan Analysis Results and Recommendations" To Do</p> <p>item task on Day 1</p>	
Remote Local Computer Scan (Quick)	Will be scheduled to run at 1:00 AM ET on Day 3 if the "Running Automated Scan of the Internal Network" To Do item is automatically completed by the end of Day 2	Day 3
Remote Local Computer Scan (Deep)	Will be scheduled to run at 1:00 AM ET on Day 4 if the user marks the assessment's "File Scan System Selection Worksheet" To Do task complete on Day 3	Day 4

Monthly Scans

The Monthly Scans feature is used to ["Generate Risk Update Reports" on page 157](#) and schedule them to run on a monthly basis.

Configure Monthly Scans from **Compliance Manager > Settings > Scan Schedules**. You can choose a day of the month on which to perform the monthly scan.

Compliance Manager > Settings > Scan Schedules

Scan Schedules

Scan Start Time ⓘ Queue scans to start at a specified time. Based on appliance availability, network connectivity, and current workload, actual scan start times may vary.

☐ Limit Scan Start Time

Time of Day

12:00 AM

Monthly Scans ⓘ Scan each month to determine if the current assessment needs to be revised and looks for compliance affecting issues.

☐ Perform Monthly Scan

Day of Month

Reset Save

See ["Scan Schedules" on page 210](#) for details.

Note: If you do not select a day, the scan will begin on the first of the month.

When you select this option, every month, Compliance Manager will initiate the Risk Update Assessment scans and generate the Risk Update Assessment reports.

The Risk Update Assessment reports can be accessed on the Manage Risk Update reports page by accessing the **Compliance Manager > Risk Updates** menu option.

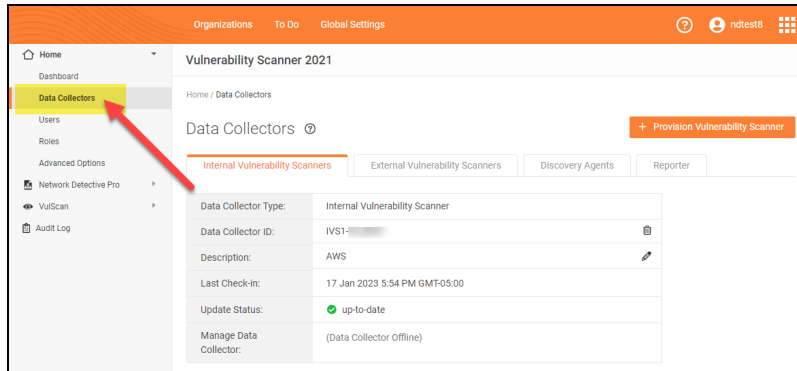
Monthly Scan Requirements

In order for Compliance Manager to perform successful monthly scans, ensure your project meets the requirements below:

- i. The Assessments Status on the Assessments page in the Portal must be set to "Archived".
- ii. There must be no Active Assessment (meaning an assessment that has been started or is currently underway) in the Site.
- iii. The Site's Scan settings must be current and operational.
- iv. The computer(s) operating the Scan Hosts must be available and the Compliance Manager Server turned on.

Manage Site Data Collectors

From the **Data Collectors** page, you can manage the available Data Collectors (also called "**appliances**") deployed for your Site.

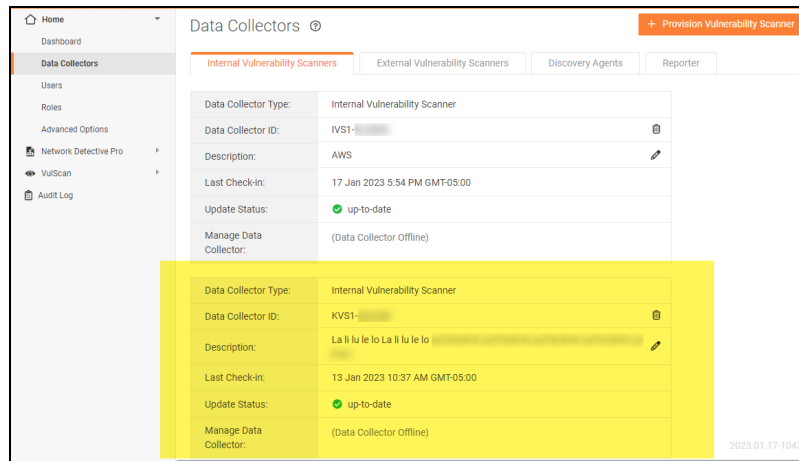


The **Data Collectors** page presents each "data collector" – also known as an *appliance* or *server* - deployed on the Site network. This includes data collectors for the various managed services: Cyber Hawk, Compliance Manager, Reporter, and other product types.

Note: Data Collectors may be referred to as "appliances" or "servers" throughout this document.

Important: You cannot manage the "Local Data Collector" from this menu; the Local Data Collector is used on a case-by-case basis for individual workstations that cannot be scanned remotely.

If multiple data collectors have been provisioned for a Site, they will appear one below the other.

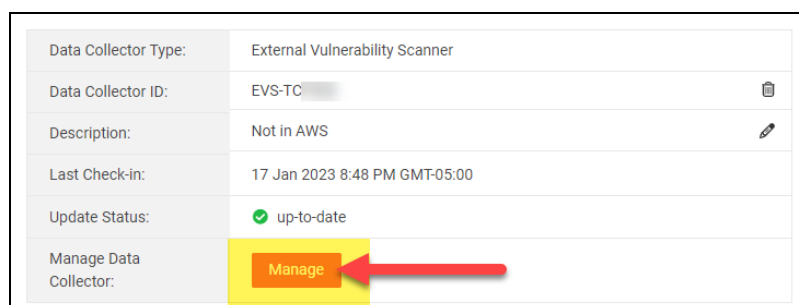


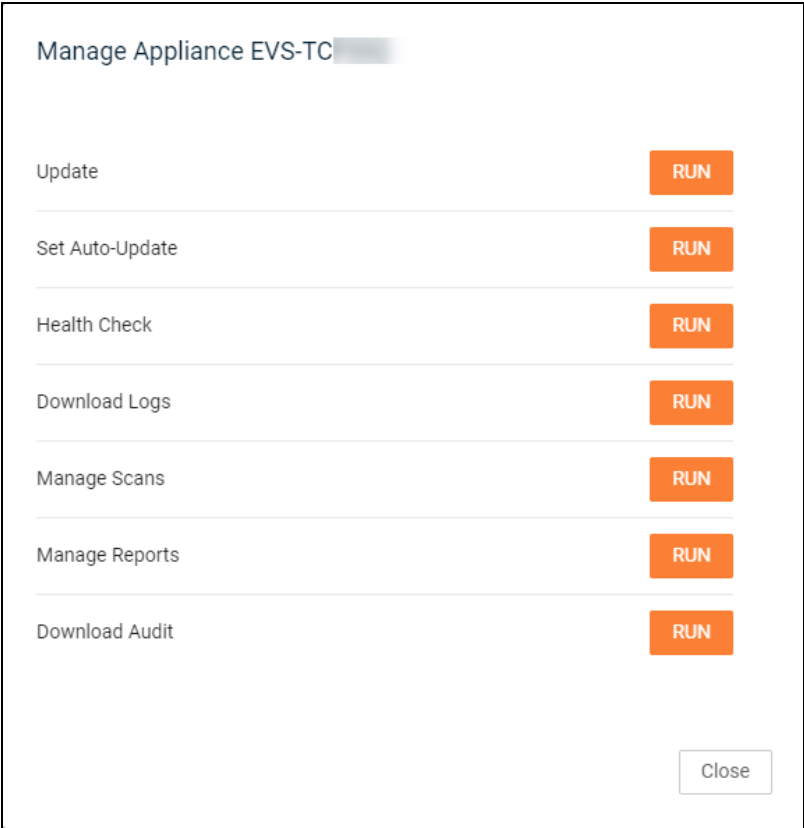
For each data collector, you can quickly see:

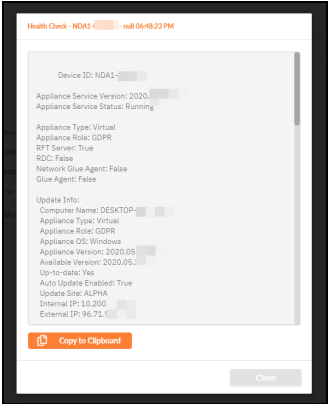
Data Collector Type	For example: Compliance Manager, Reporter, Cyber Hawk
Data Collector ID	Useful for troubleshooting purposes
Last check-in	Useful for troubleshooting purposes and indicates active status
Update status	Indicates whether the data collector has the latest update. In most cases the data collector should update automatically once an update becomes available.
Manager data collector	Select one of several "Data Collector Commands " below from the drop-down menu. If the Data Collector is not available, "Data Collector Offline" will appear.

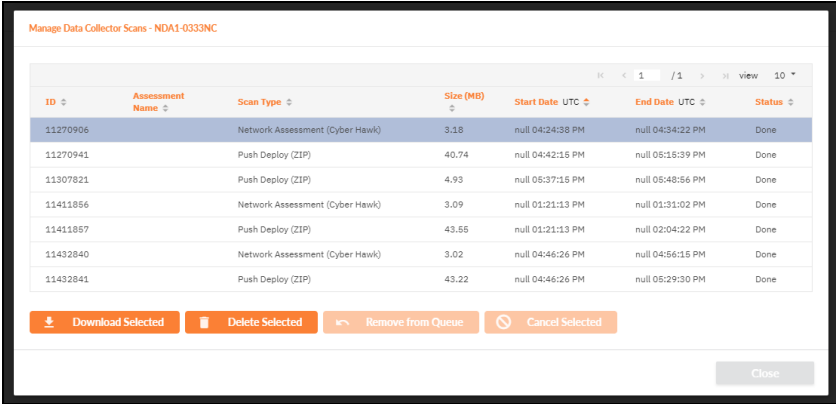
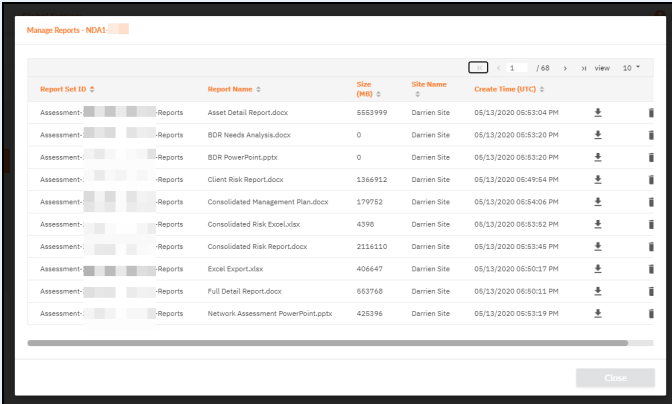
Data Collector Commands

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





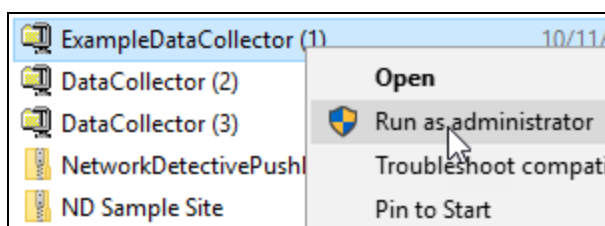
Update	Update the data collector to the latest version. Note that this will cancel all current scans.
Set Auto-Update	Order the data collector to automatically update itself when a new version becomes available.
Health Check	<div>Access technical information about the data collector's current status. Can be copied as a text file for troubleshooting.</div> <div></div>

Download Logs	Download log files for troubleshooting purposes.
Manage Scans	<p>View and manage all scans assigned to the appliance.</p>  <p>Here you can:</p> <ul style="list-style-type: none"> • Download scan files • Delete completed scans and their associated files • Remove queued scans • Cancel scans in progress
Manage Reports (Reporter only)	<p>Access and manage reports stored on the Reporter appliance.</p> 
Download Audit	Download the audit log for the appliance.

Run CMMC Local Data Collector

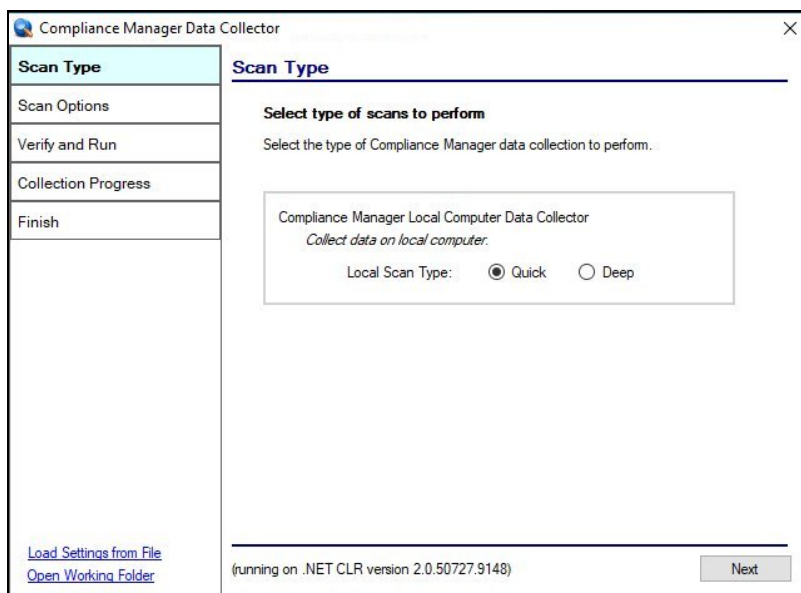
The steps below detail how to run the local Data Collector on computers that could not be scanned automatically via the Compliance Manager server. See ["Local Computer Scans" on page 222](#) for more details, including troubleshooting information.

1. If you have not done so already, visit the RapidFire Tools software download website at <https://www.rapidfiretools.com/cm> and download the CMMC Data Collector.
2. Run the **CMMC Data Collector** executable program as an Administrator (**right click>Run as administrator**).



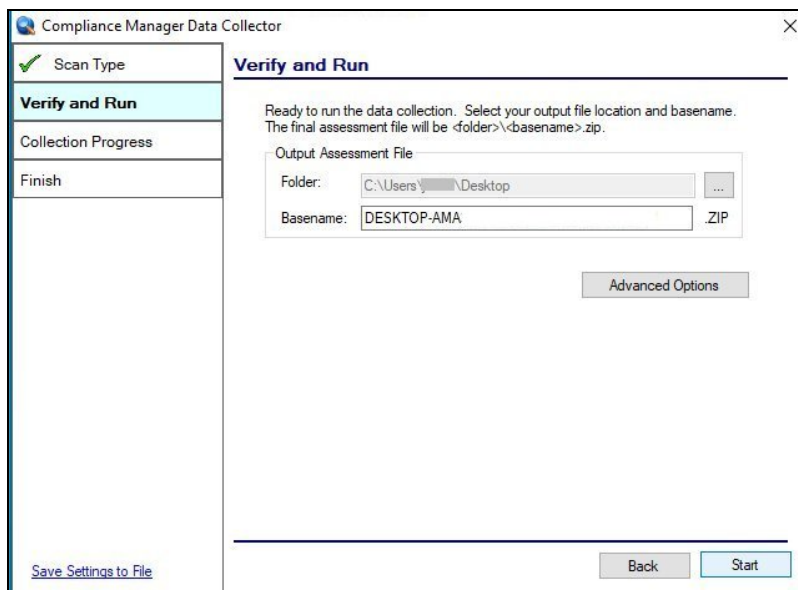
Important: For the most comprehensive scan, you **MUST** run the data collector as an **ADMINISTRATOR**.

3. **Unzip** the files into a temporary location. The CMMC Data Collector's self-extracting ZIP file does not install itself on the client computer.
4. The CMMC Data Collector Scan Type window will appear.



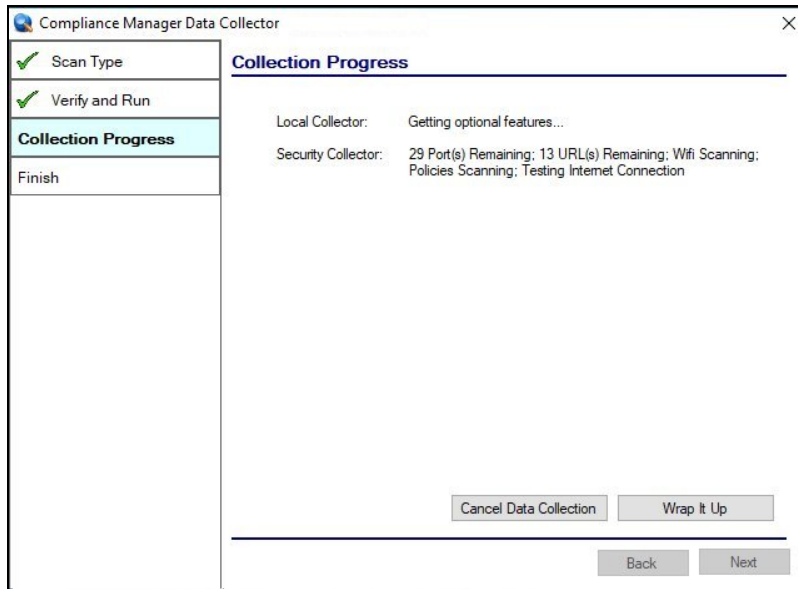
5. Select whether you wish to run a **Quick** or **Deep** scan.
 - Run a **Quick Scan** on computers that were not available for scanning during the “**Running Local Scan of Remote Computers**” task’s scanning process.
 - Run a **Deep Scan** on computers that were not available for scanning during the “**Running File Scan**” task’s scanning process.

The Verify and Run window will be displayed. The **Verify and Run** window enables you to change the output location for the scan data, change the name of the file, and add comments.



6. After setting the **Output Assessment File**’s **folder location**, the **Basename** of the scan’s output file, and adding a **Comment**, select **Start** to initiate the scan.

The **Collection Progress** window will be displayed during the scan process.

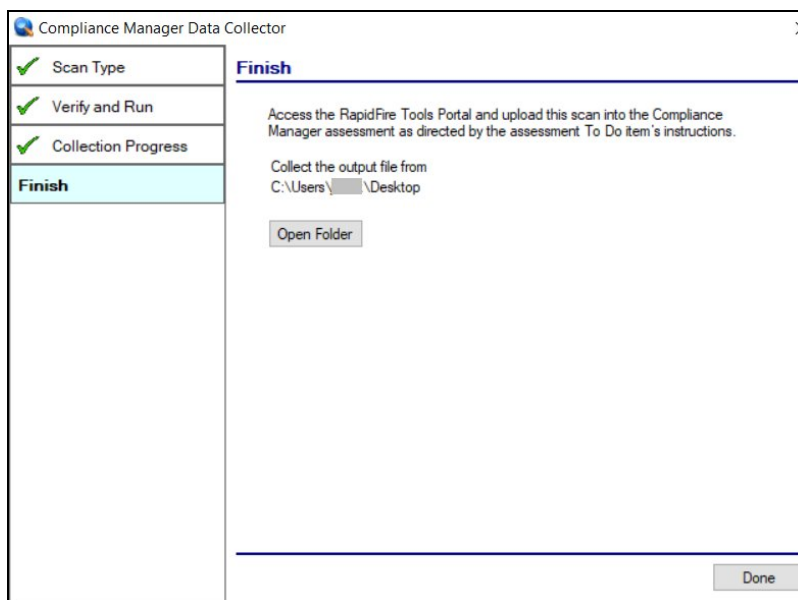


Track the scan's progress through the **Collection Progress** window.

At any time you may **Cancel Data Collection** without saving any data.

You may select **Wrap It Up** to stop a scan and use the incomplete data that was collected.

Upon the completion of the scan, the **Finish** window will be displayed.



Note the scan **output file's** location and click on the **Done** button to complete the process.

The scan file will appear in the assigned location in the directory.

How to Upload the Local Scan Files

Once you have used the Cyber Insurance Local Data Collector to create scan files for all computers that you wish to scan, upload them into the assessment project. To do this:

1. Extract the data file's contents to the desired location. (Optional)
2. In the RapidFire Tools Portal, click on the To Do task to open the task details page.
3. Click on the **Upload Scans** button.
4. Select the scan file that you wish to upload.
5. Click **OK**. The scan file will be integrated into the assessment.
6. When you have successfully uploaded all scan files, click **Mark Complete** to continue the assessment.

Local Computer Scans

Local Computer Scans are performed during assessments performed through the use of the “Local Data Collectors” utilized within the Network Detective, Reporter, Inspector, and Compliance Manager products..

The Local Computer Scanning program itself and scanning engine contained within the Local Data Collector is used for both “Quick” Local Computer Scans and “Deep” Local Computer Scans.

The Local Computer Scanning program is designed to collect information a number of sources including the Windows registry, Windows log files, Windows Management Instrumentation (WMI), installed browser histories, the computers file system, and contents of files being examined.

Local Computer Scanning Dependencies and Recommendations

Both the speed and ability to complete a Local Computer Scan (Quick or Deep) depends on a number of dependencies and factors.

Dependencies and factors include:

Scanning Process and Scanning Surface Area

- Type of Local Computer Scan performed: Quick Computer Scan, Quick Security Scan, Deep ePHI Scan, Deep PCI Scan, Deep EU Personal Data Scan, and Deep PII Scan.
- Data recording actions undertaken when EU Personal Data, PII, ePHI, and Cardholder Data is detected and examined
- Types of files scanned (.txt, .log, .docx, .xlsx, .pdf, and other text file types)
- Size of files scanned
- Number of folders/files scanned

Computer Resource Related

- Total disk size and used space (number of files to be scanned and examined during Deep data collection)
- Free disk space size
- Available CPU resources
- Available computer memory resources
- Other background applications and processes

- Impact of uninstalled Windows Updates
- Computer disk fragmentation state

Scan Interference Factors

- Interference from unknown malware and spyware programs operating on the computer
- Installed Anti-malware and anti-virus program interference
- Interference from other security scanning software scanning at the same time as Quick and Deep Local Computer Scans
- User interference caused by the user interacting with the computer during Quick and Deep Local Computer Scans
- Computer disk fragmentation

Recommendations to Improve Local Computer Scan Performance

Quick Local Computer Scans

During the Quick Local Computer Scan, computer users should see little impact from the scan's effect on the computer endpoint's performance. Exceptions: when installed antivirus/anti-malware interference computer scans occurs or when computer disk, CPU, or memory resources are low during scan time.

Recommendations:

- Temporarily disable antivirus/anti-malware
- Increase availability of computer resources during scan time
- Address computer disk fragmentation issues by optimizing computer disk resources through the use of disk optimization tools such as Defrag and other third party products

Deep Local Computer Scans

Along side of the factors associated with the Quick Local Computer Scans that are also factors that affect Deep Local Computer Scans, there are a series of recommendations that specifically pertain to Deep Local Computer Scan performance and scan time length.

Recommendations:

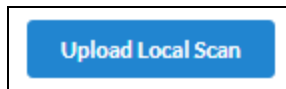
- Remove temporary/junk files
- During Deep Scan time, close all applications operating on the computer endpoint

- Scan the computer endpoint during times when the computer is not in use or during periods of low utilization
- Ensure that the computer's Windows operating system and applications are up to date
- Temporarily disable resource intensive background services
- Verify that the computer endpoint is free of malware and PUPs (potentially unwanted programs) that are unnecessarily consuming computer resources

Performing Scans on Mac and Linux Computers

In order to scan Mac and Linux workstations, you will need to perform manual local computer scans with the Mac Computer Data Collector and the Linux Computer Data Collector. This will add the computers to the Asset Inventory Worksheet. To do this:

1. Download the computer data collectors from www.rapidfiretools.com/nd or from the links provided below.
2. Run the computer data collectors on all target systems.
3. Once the scans are completed and you have collected the scan files, upload the scans into the Assessment. Use the **Upload Local Scan** button on the task details page in order to do this.



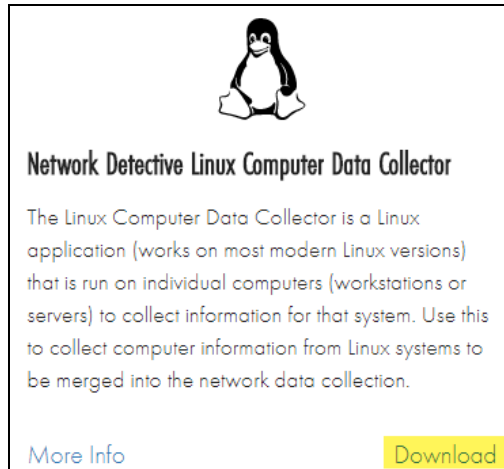
The Mac and Linux computers will later be listed in the **Asset Inventory Worksheet** when it is generated.

Important: Mac and Linux computers **CANNOT** be included in the **GDPR PD**, **HIPAA ePHI**, or **Cyber Insurance Sensitive Data** Scan processes, even if these computers are listed in the Scan System Selection worksheets.



Mac OS Computer Data Collector

<https://www.rapidfiretools.com/nd/downloads/>



Linux Computer Data Collector

<https://www.rapidfiretools.com/nd/downloads/>

Integration with VSA Agents for Local Data Collection (Compliance Manager)

Purpose

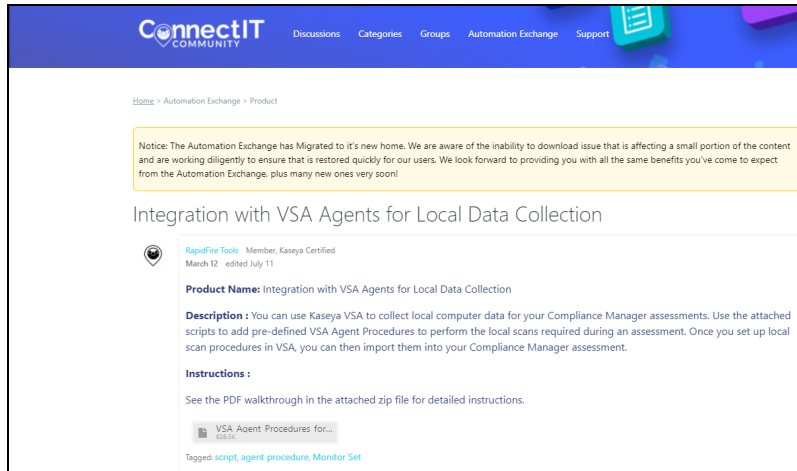
This topic presents step-by-step instructions on how to add predefined VSA procedures to perform the local scans required during the Compliance Manager assessment process. Once you set up and perform local scan procedures in VSA, you can then ["Import RMM Connector Scans" on page 233](#) during your Compliance Manager assessment.

Requirements

- Login for Kaseya Automation Exchange (www.community.connectit.com)
- Compliance Manager Subscription
- Kaseya VSA Subscription

Step 1: Download ZIP file from Kaseya Automation Exchange

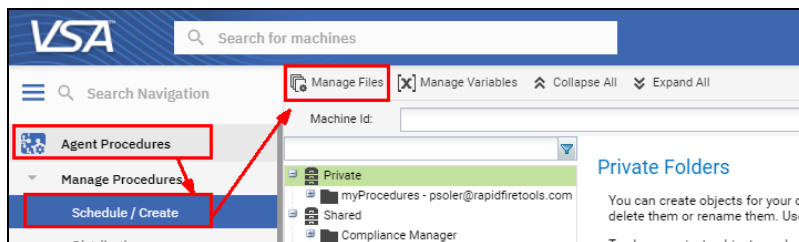
In order to access the agent procedures to upload to VSA, visit www.community.connectit.com. Navigate to **"Integration with VSA Agents for Local Data Collection"** and download the attached ZIP file.



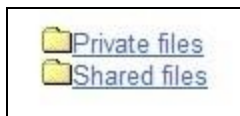
Step 2: Upload the Compliance Manager Resources to Files to VSA

Kaseya VSA can automate the distribution of files to managed computers. First, an administrator must upload these files to VSA.

1. In the Kaseya application, navigate to **Agent Procedures > Schedule / Create**. Click the **Manage Files** button as shown below.



2. A dialog box will appear with a choice of directories to store your files. Select **Shared files**.

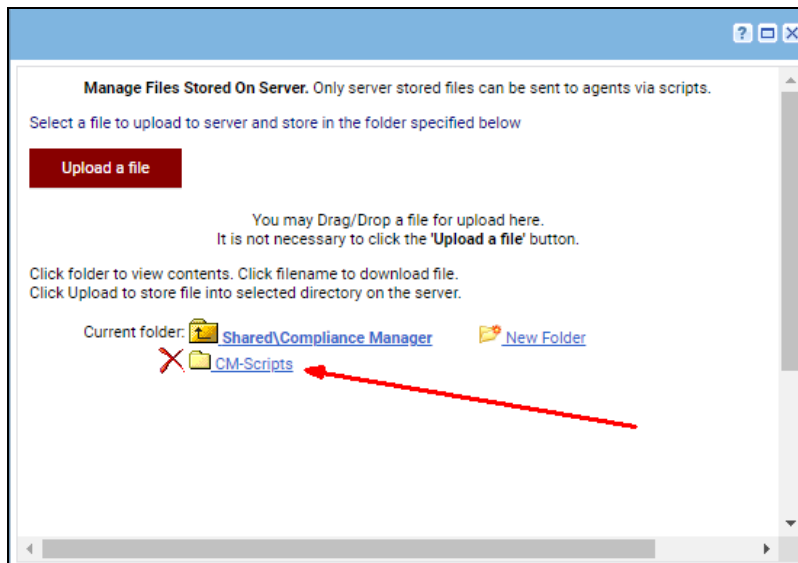


3. Click the **New Folder** link.

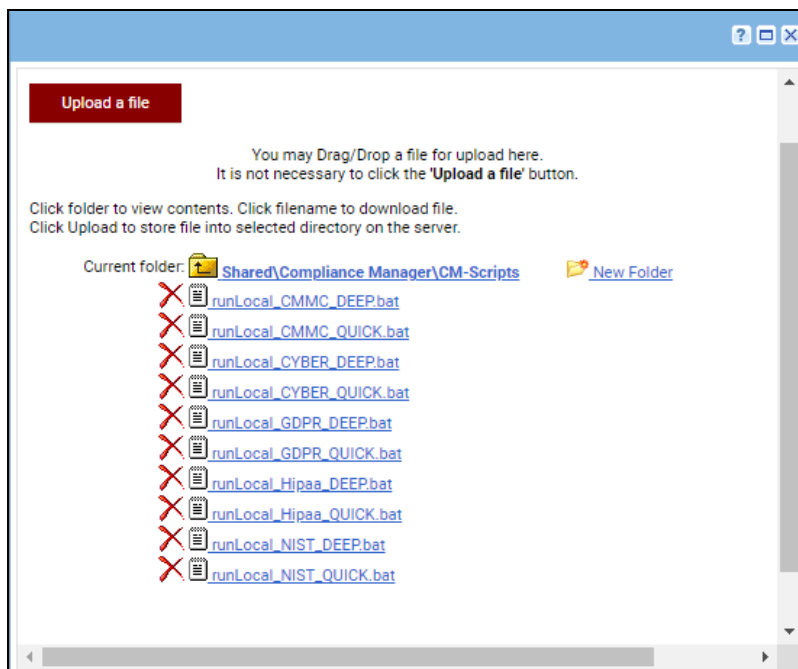


4. For the purpose of this example and to ensure your Compliance Manager procedures will work out of the box, create a new folder named "**Compliance Manager**" under Shared files.

- Once the folder has been created, open the folder and create a new subfolder named **“CM-Scripts”** as shown below.



- Upload the following files (provided with this document) into the CM-Scripts folder:



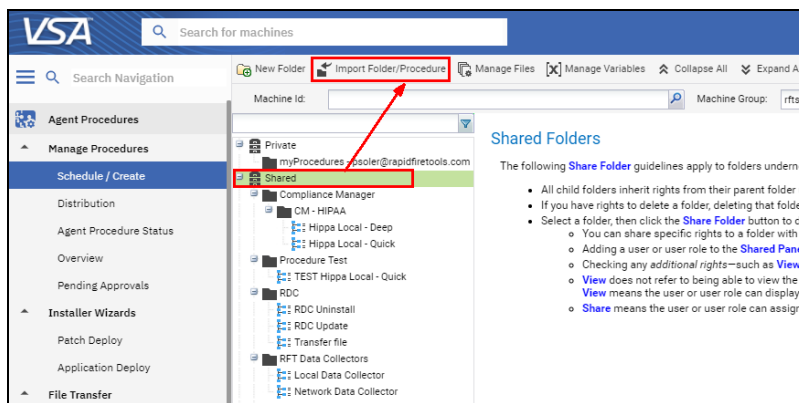
These files correspond to the local scan tasks that can be performed in a Compliance Manager assessment. For example:

- **runLocal_Hipaa_Quick.bat** is used to perform the local scan required to complete Task 9.2: Run Local Data Collector of the Compliance Manager Hipaa Assessment (see page 68 of the [Compliance Manager HIPAA User Guide](#))
- **runLocal_Hipaa_Deep.bat** is used to perform the local scans required to complete Task 18: Unable to scan all selected systems of the Compliance Manager Hipaa Assessment (see page 76 of the [Compliance Manager HIPAA User Guide](#))

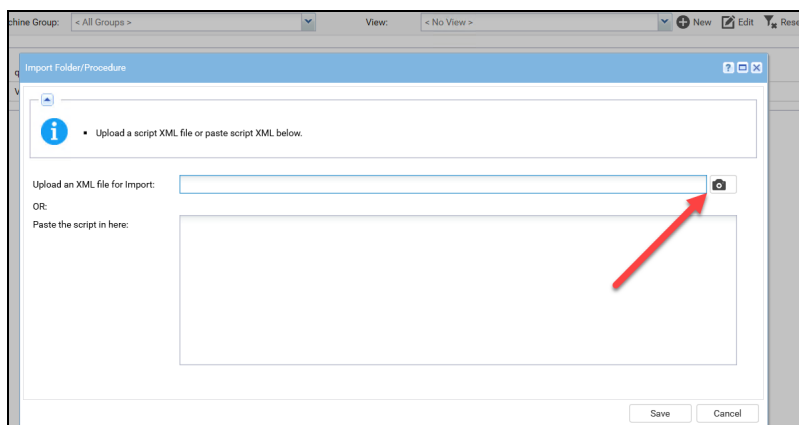
Step 3: Import Kaseya VSA Procedures for Compliance Manager local scans

Next, import the provided XML file containing the agent procedures into Kaseya VSA.

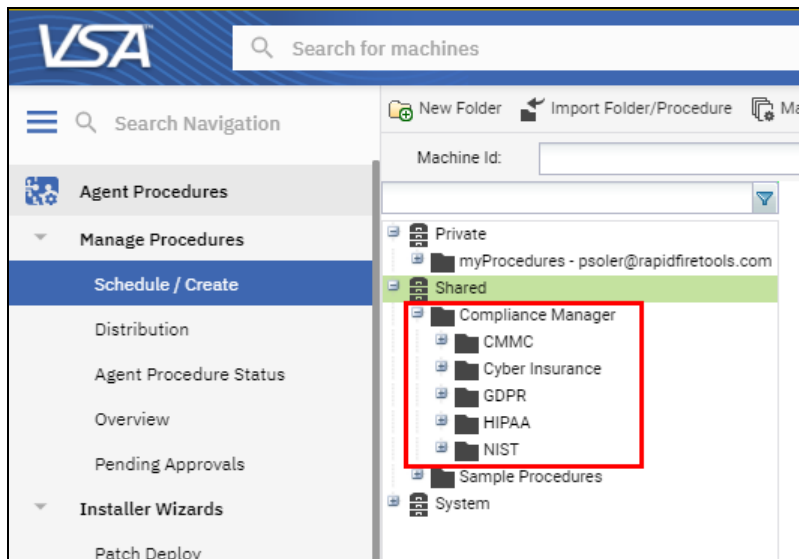
1. Navigate to **Agent Procedures > Schedule / Create**. Choose the procedure where you wish to place your Compliance Manager procedure folder and click the **Import Folder/Procedure** button as seen below. In the example below, we have selected the Shared folder as the location, but you may select the folder of your choice.



2. Select the XML file **Procedure Folder Compliance Manager** included in the ZIP file with this package and click **Save**.



3. Once you have imported the procedure XML, you should see the following folders containing the VSA local scan procedures for each of the Compliance Manager Assessment types (see below).

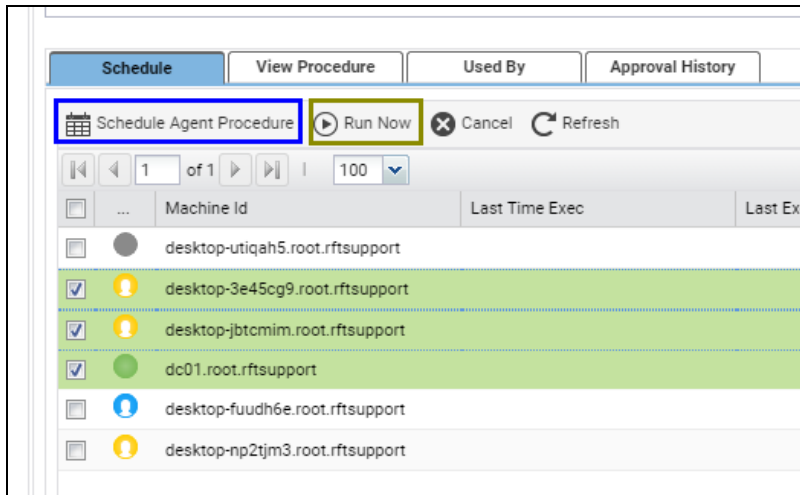


Important: Do not edit these procedures after they have been imported. These procedures are only supported by RapidFire Tools with their current “out of the box” configuration.

Step 4: Executing Local Data Procedures

Once the Agent Procedures have been imported, they can be run on demand or on a schedule.

1. To run a procedure, highlight the desired local scan procedure and select the machines you would like to scan from the list of machines in the lower right-hand quadrant of the browser.



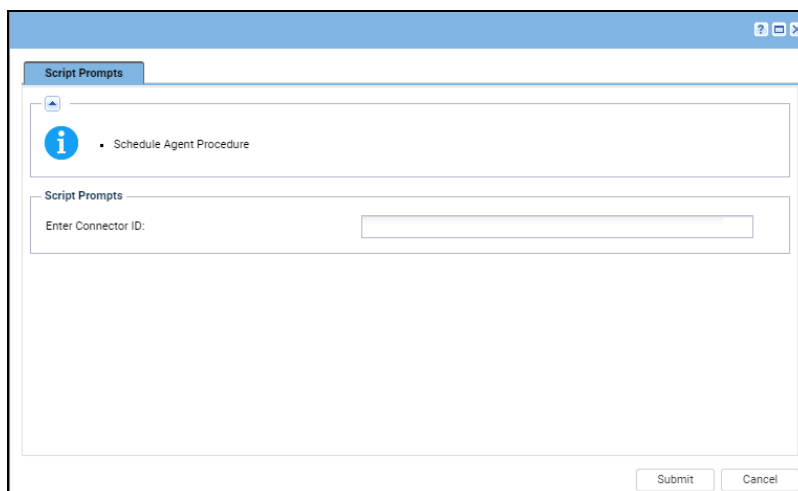
2. To run the procedure on demand, select the machine(s) and then click the **Run Now** button.



3. To run the procedure later, select the machine and click the **Schedule Agent Procedure** button.

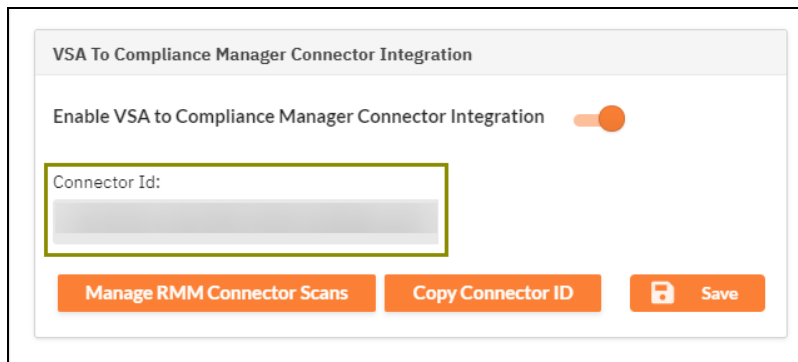


4. When the procedure is initiated, you will be prompted to enter the **Connector ID** associated with the site in the Compliance Manager Portal.



5. To access the Connector ID for your Compliance Manager site, open your site and go to **Compliance Manager > Settings > IT Complete**. Under **VSA to**

Compliance Manager Connector Integration, click the slider and copy the Connector ID.

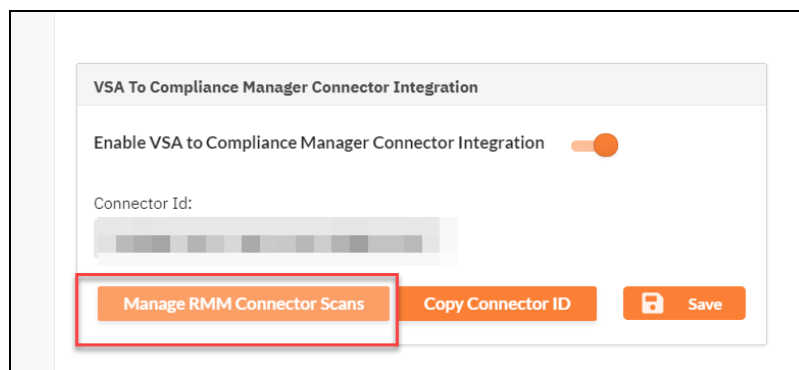


6. Returning to VSA, enter the ID and click **Submit**. At this point, your data collection will begin.

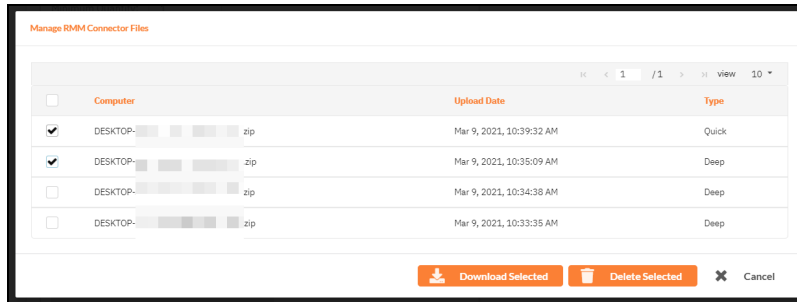
Step 5: Verifying successful Collection

Once the agent procedures have been completed, log into the Compliance Manager Portal to review a list of scans that have been uploaded to the site.

Open your site and go to **Compliance Manager > Settings > IT Complete**. Under VSA to Compliance Manager Connector Integration, click **Manage RMM Connector Scans**.



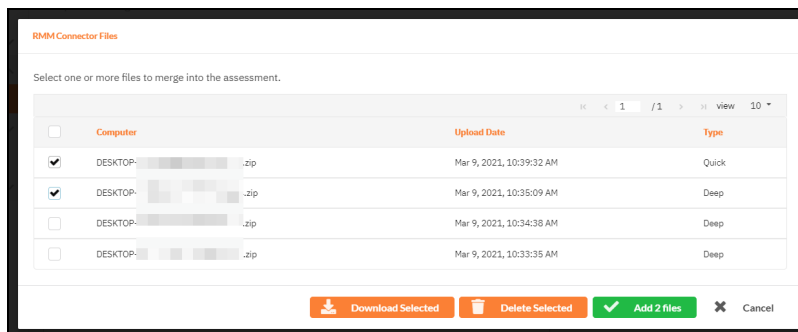
From this screen you can download or delete RMM scans.



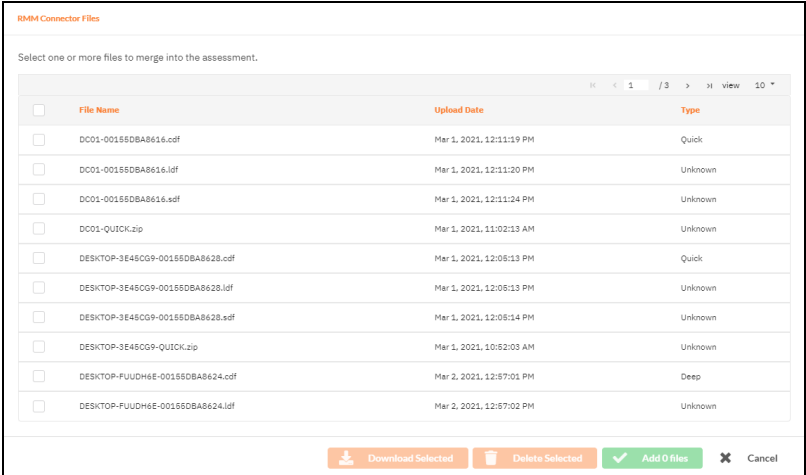
Import RMM Connector Scans

Once you set up ["Integration with VSA Agents for Local Data Collection \(Compliance Manager\)" on page 226](#), you can import local scan files into your Compliance Manager assessment. Here's how this works:

1. You must have performed one or more local scans on the target network using agent procedures in Kaseya VSA.
2. You can then import local scan files from VSA at several points during your assessment. Specifically, you can import local scans whenever a local scan or related to do item appears in your assessment.



3. To import the scan file, open the To Do item and click **Import from RMM Connector Scans**. Select the scans to import then click **Add**.



4. The selected local scan files will then be merged into your assessment. Once the merge is complete, mark the To Do item complete and proceed with your assessment.

Appendices

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

<u>Configuring Report Preferences</u>	238
Set Reports Text Preferences	240
Set Reports Logo Preferences	241
Set Themes Preferences	242
Access Updated Report Styles	243
Set Reports Cover Images Preferences	244
Set Company Information Preferences	245
Use Network Detective to Add Your MSP Name to Report Headers	245
<u>Upgrade your Site License (MSPs Only)</u>	247
Site License Options	248
Account-wide License Options (MSP and SMB)	248
<u>Enable BMS Contract Updates for Compliance Manager GRC</u>	250
Step 1 — Gather Credentials for Kaseya BMS	250
Step 2 — Set Up a Connection to your Kaseya BMS	251
Step 3 — Map your Compliance Manager's Site to a Kaseya BMS Connection	256
Step 4 — Enable BMS Billing Integration from Site	257
<u>Delete a Site</u>	264
<u>Set Time Zone</u>	265
<u>Admin Alerts (RapidFire Tools Portal)</u>	266
Admin Alerts: Global Settings vs. Site Settings	266
Configure Admin Alerts	266
<u>Audit Log</u>	268
Compliance Manager Audit Log Details	268
Examples of Audit Log Entries	269
Creation of To Do Task Items	269
Automated Scanning Start and Completion Activity	269
Assessment Questionnaire and Worksheet Form Access and Modification Activity	270
<u>CMMC To Do Task Complete List</u>	270
<u>Import Worksheet Attachments from ITGlue</u>	275

Augment Antivirus Verification Worksheets to Detect Antivirus Apps 280

 Step 1 — Augment Reports in Network Detective280

 Step 2 — Generate Antivirus Verification Worksheet282

License Usage (Global Settings)284

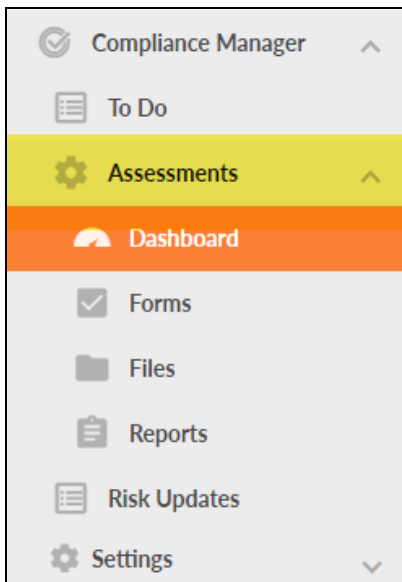
Configuring Report Preferences

Before you perform your first assessment using Compliance Manager, you should configure the report generation tool to use your company's logos, color themes, and other details. This ensures your assessment reports conform to your company's corporate branding and image standards.

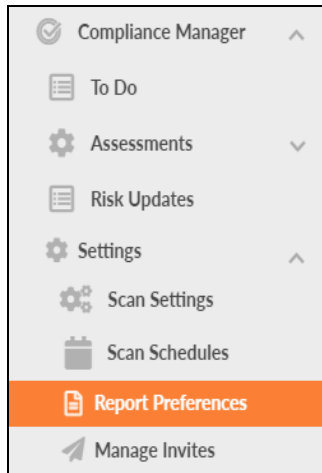
Tip: The reports produced by Compliance Manager are delivered to you as Microsoft Word and/or Excel documents. You are able to add information to the report, extract information to be included in your own documentation, sort and analyze in Excel, etc.

To access and configure Report Preferences:

1. From your Site Home Page, go to **Compliance Manager > Settings**.



Next, click **Report Preferences** to access the customization settings. This includes company information, images, and design elements for this site's reports.



2. Customize your reports. This includes company information, images, and design elements for this site's reports.

A screenshot of the 'Report Preferences' configuration page. The breadcrumb trail at the top reads 'Compliance Manager GRC / Settings / Report Preferences'. The page title is 'Report Preferences'. There are four tabs: 'Text' (selected and underlined in orange), 'My Logo', 'Theme', and 'Cover Image'. Under the 'Text' tab, there are four input fields: 'Report Prepared For:' with the value 'Advent Technologies', 'Report Prepared By:' with the value 'Micro Consulting', 'Footer:' with the value 'PROPRIETARY & CONFIDENTIAL', and 'Cover Page Disclaimer:' with a text area containing a confidentiality note. The note reads: 'CONFIDENTIALITY NOTE: The information contained in this report d of the client specified above and may contain confidential, privileged information. If the recipient of this report is not the client or address prohibited from reading, photocopying, distributing or otherwise usir any way.'

You can also Select Target Language for Assessment Reports. **LANGUAGES OTHER THAN ENGLISH ARE ONLY AVAILABLE FOR COMPLIANCE MANAGER FOR EU GDPR.**

3. Once you finish configuring Report Preferences, return to the item in the To Do list and click **Mark Complete**. Do this each time you complete a task in the To Do list.



This section details each of the available configuration options.

Set Reports Text Preferences

Set the report text preferences to customize the report's language for a specific client.

The screenshot shows the 'Report Preferences' page with the 'Text' tab selected. The page has a breadcrumb trail: 'Compliance Manager GRC / Settings / Report Preferences'. Below the title 'Report Preferences', there are four tabs: 'Text' (active), 'My Logo', 'Theme', and 'Cover Image'. The 'Text' tab contains several input fields: 'Report Prepared For:' with the value 'Advent Technologies', 'Report Prepared By:' with the value 'Micro Consulting', 'Footer:' with the value 'PROPRIETARY & CONFIDENTIAL', and 'Cover Page Disclaimer:' with a text area containing a confidentiality note. At the bottom, there are three more fields: 'Target Language(s):' with a dropdown set to 'English (US)', 'Paper Sizes:' with a dropdown set to 'Letter (8.5"x11")', and 'Currency Symbol:' with a dropdown set to '\$'.

1. Click the **Text** tab from the Report Preferences side menu.
2. Enter your responses within each field.
3. Click **Save** when you are finished.

Text Configuration Option	Description
Report Prepared For:	This is the client for whom you are assessing and for whom you are preparing the reports.
Report Prepared By:	This is you, your company, your DBA.
Footer:	This is the footer of the document, and appears on all pages. By default it reads, "PROPRIETARY & CONFIDENTIAL"
Cover Page Disclaimer:	By default this is a confidentiality disclaimer, but could also could serve well for Copyright.

Text Configuration Option	Description
Target Language*:	Select the language to be used when producing reports. Target languages include English, German, Spanish, French (Canadian), and Italian. *GDPR only
Paper Sizes:	Select the default page size to be used when reports are generated and formatted.
Currency Symbol:	Set the currency symbol to use in the generated reports.
Conversion Factor:	Set the conversion factor for other currencies to their value in USD (United States Dollars).

Set Reports Logo Preferences

Incorporate your company's logos into the Reports generated by Compliance Manager.

Compliance Manager GRC / Settings / Report Preferences

Report Preferences

Text **My Logo** Theme Cover Image

Logos

Cover Logo Image:
(600x150)

600 × 150

Browse or drop file

Allowed file types: JPG, PNG. Max file size: 2MB

Header Logo Image:
(300 x 75 or 600 x 150)

600 × 150

Browse or drop file

1. Click the **My Logo** tab from the Report Preferences side menu.
2. Click the **Upload** button underneath the Cover Logo Image.

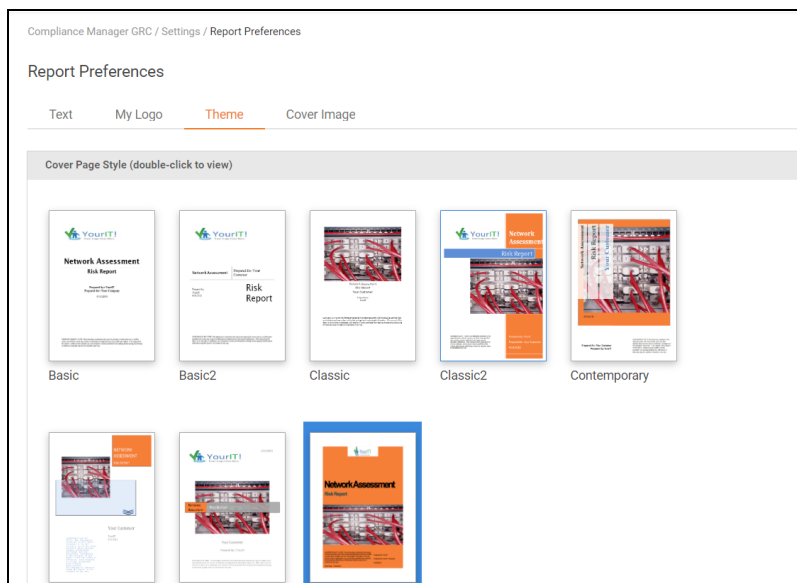
3. Select the Cover Logo image from your computer.
4. Repeat this process for the Header Logo Image.
5. Click **Save** when you are finished.

Note: The Cover Logo image must be 600 x 150 pixels.

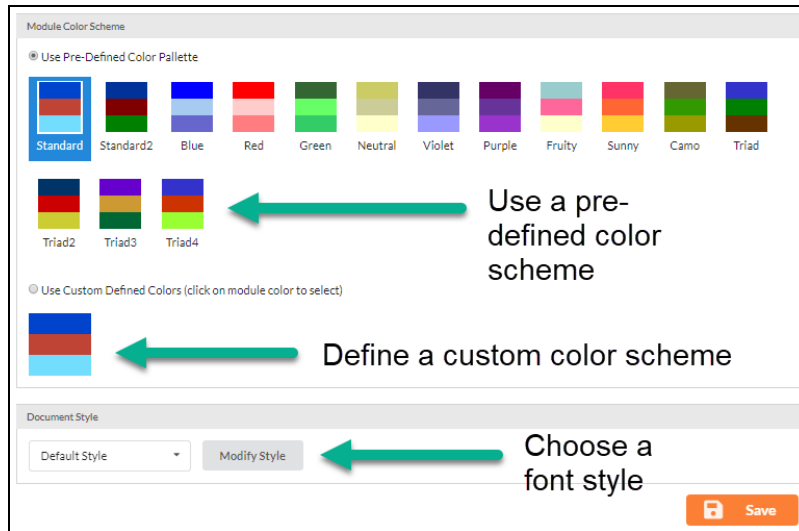
The Header Logo must be 300 x 75 or 600 x 150 pixels.

Set Themes Preferences

Each report generated follows a pre-built theme and is color-coded. Using this option, you can assign a report color palette to be used with each module during report generation.



1. Click the **Themes** tab from the Report Preferences side menu.
2. Click on theme from the available options to select it to apply to your reports.
3. You can also select custom color schemes and fonts.

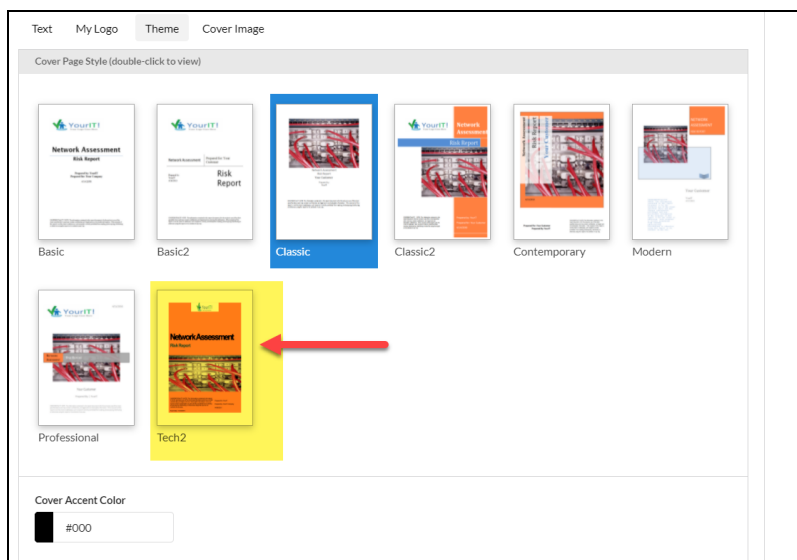


4. Click **Save** when you are finished.

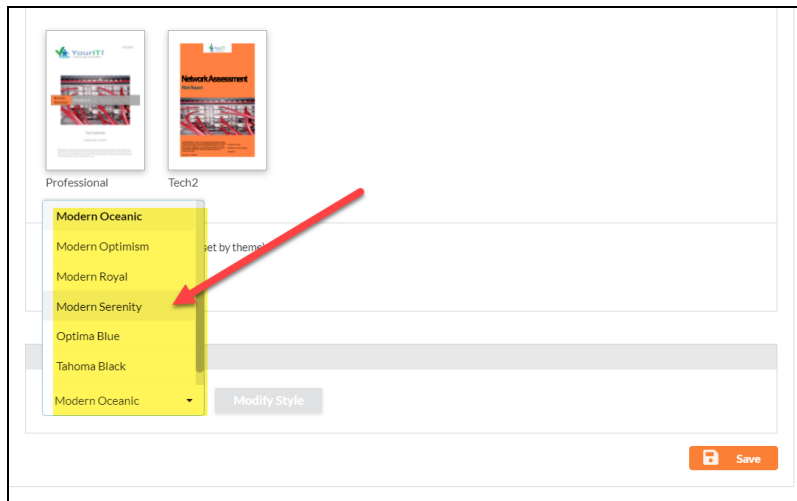
Access Updated Report Styles

You can access several updated report styles from **Report Preferences > Themes**.

Specifically, you can access the **Tech2** cover page style:

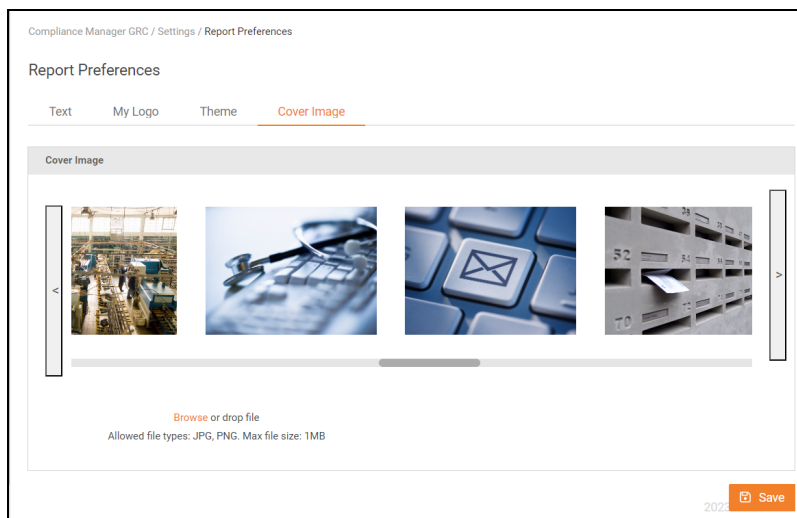


Also, under **Document Style**, you can access several updated "Modern" report styles that enhance the overall look and feel of your assessment documentation:



Set Reports Cover Images Preferences

You can define the image that should be displayed within the Reports Cover Page when a report document is generated.



1. Click the **Cover Images** tab from the Report Preferences side menu.
2. Click on an image from the available options to select it to apply to your reports.

3. Click **Save** when you are finished.

Set Company Information Preferences

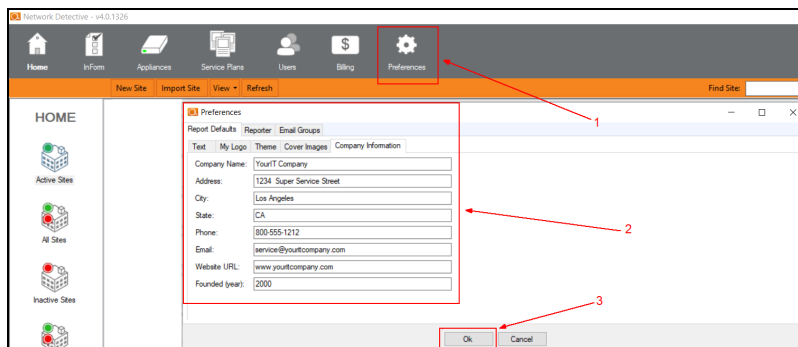
The Company Information Preferences contain basic details and contact information for your company to include in the reports.

1. Click the **Company Information** tab from the Report Preferences side menu.
2. Enter your responses within each field.
3. Click **Save** when you are finished.

Use Network Detective to Add Your MSP Name to Report Headers

You can use Network Detective to add your company MSP name to your Compliance Manager GRC report headers. To do this:

1. Download and install the Network Detective application from <https://www.rapidfiretools.com/nd-downloads>.
2. As the Master User for the Compliance Manager GRC account, log into Network Detective.
3. From the Network Detective top menu, open **Preferences > Report Defaults > Company Information**. Populate the fields with your Company Name and other information.



4. When you're finished, click **OK** to save your changes.
5. When Compliance Manager GRC next generates reports, your MSP's information will appear in the report's header.

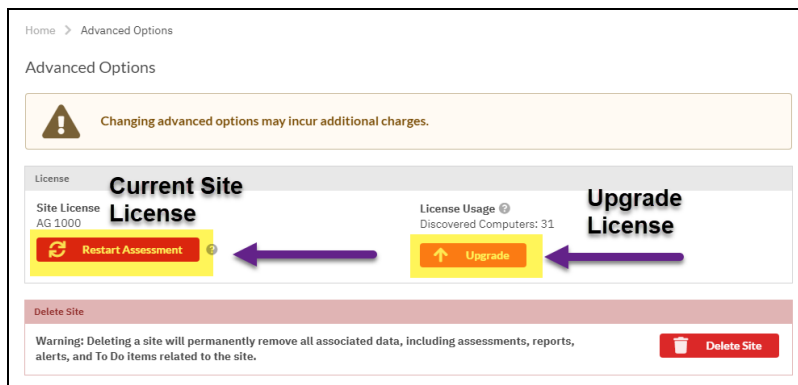
After you have finished setting the Reports Defaults preferences, you can proceed to performing assessments and generating reports that will use your company's branding.

Upgrade your Site License (MSPs Only)

Note: Only MSP account users can upgrade an individual site license. If you are a direct-to-customer or SMB user, please contact your account representative to upgrade your license.

Your site must be licensed for the number of computers on the target network. If the network scan discovers more computers on the site network than are covered in your license, you will need to upgrade your license to continue the assessment. To do this:

1. Select the site from the Sites page that you wish to upgrade.
2. From the site's Home tab, click **Advanced Options**.



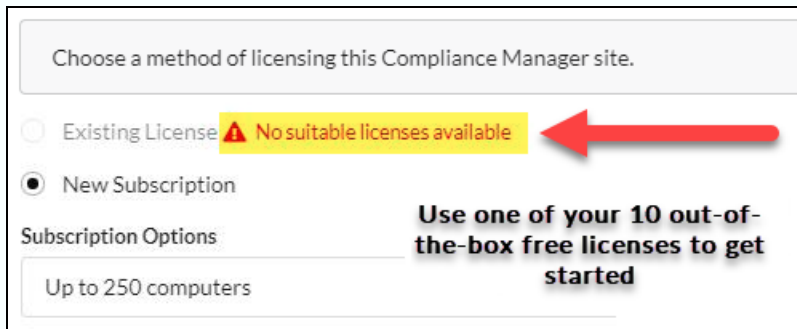
Note: Subscriptions cannot be downgraded or canceled until the end of the subscription period.

3. Click **Upgrade**.
4. Select a license from the **Available Licenses** tab.

If you have a license violation, it will be removed and you can continue with your assessment. See below for more information on the available licenses.

Site License Options

Note: You have **10 FREE** Site licenses as part of your initial Compliance Manager subscription. Each of these licenses can cover a site with up to 250 computers. *Select one of these free licenses for use with your first 10 new Sites.* We suggest that you use 1 of the 10 licenses for your own internal use, such as familiarizing yourself with the product and assessment processes.



Choose a method of licensing this Compliance Manager site.

☐ Existing License **⚠ No suitable licenses available**

☒ New Subscription

Subscription Options

Up to 250 computers

Use one of your 10 out-of-the-box free licenses to get started

If you wish to purchase additional licenses or upgrade to a higher license (500 and above), you will be billed extra. Contact your Sales Representative for more details.

You can upgrade your Site licenses to one of the available options below. You upgrade on a Site by Site basis.

Note: Upgrading a license will incur additional costs.

License	Limit
250	Up to 250 computers
500	Up to 500 computers
1000	Up to 1000 computers
2000	Up to 2000 computers

Account-wide License Options (MSP and SMB)

There are two licensing "models" for RapidFire Tools accounts:

- **MSP:** For resellers who offer managed services to clients. License upgrades are purchased site-by-site.

- **SMB:** For end-users who are deploying services on their own networks/sites. Account-wide license covers a certain number of sites and computers. Contact account representative to upgrade.

Enable BMS Contract Updates for Compliance Manager GRC

You can export contract updates from your compatible sites (Compliance Manager; VulScan) into Kaseya BMS. This will automatically update the BMS contract with billing data from the site based on successful scan/assessment data.

Specifically, you can update the quantity of units for a Service associated with a Contract in BMS. You can choose to quantify several types of units, including:

- Endpoints from latest assessment
- Current employees from latest assessment
- Users from latest assessment


For example, you can smartly bill a client based on the number of active users identified at the site during regular assessment scans. As active users are added to or removed from the network, your BMS contract will automatically be updated to reflect this.

To enable BMS contract updates:

Step 1 — Gather Credentials for Kaseya BMS

Before you begin, you will need:

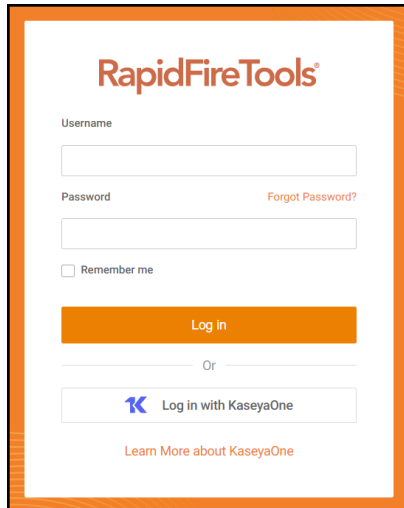
- Valid Login Credentials for RapidFire Tools Portal
- A RapidFire Tools Portal Compliance Manager "Site" for which you wish to export tickets
- Valid Login Credentials and details for Kaseya BMS (refer to the table below)

PSA System	PSA Prerequisites
	<ul style="list-style-type: none">• Kaseya Username• Kaseya Password• Kaseya Tenant (i.e. company name)• Kaseya API URL, example: "https://bms.kaseya.com" (you should receive the exact URL in an email from Kaseya)

Step 2 — Set Up a Connection to your Kaseya BMS

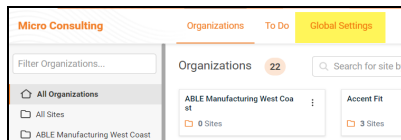
Follow these steps to set up a Connection to Kaseya BMS.

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

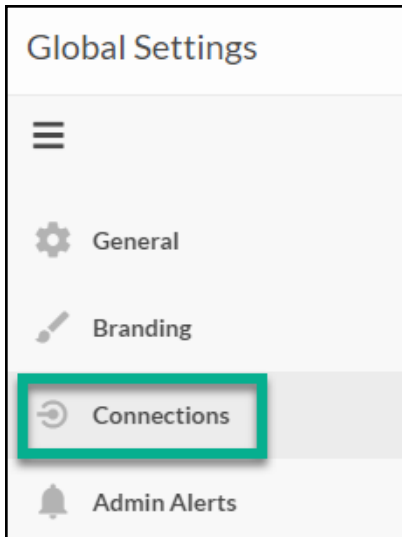


Note: In order to configure the Settings in the Portal, you must have the **All** or **Admin** global access level.

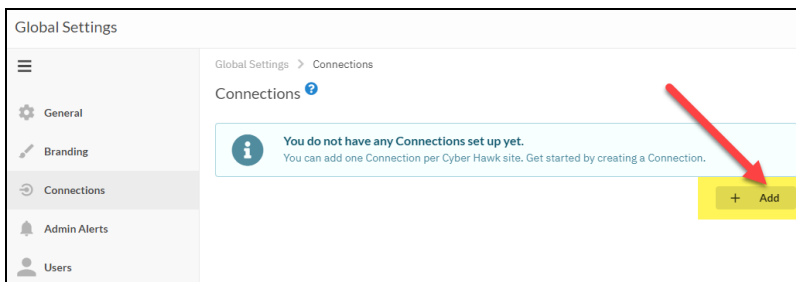
2. Click **Global Settings**.



3. Click **Connections**.




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




5. In the Setup New Connection window, select **Connection Type** and choose **Kaseya BMS**.

Note: Compliance Manager can only be integrated with Kaseya BMS at this time.

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 *

-- Choose Connection Type --

-
-
-
- Kaseya BMS
-


 

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


This information will include:

- Username and Password
- API URL
- Tenant name (Company name)

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 *

Username *

Password *


Tenant *

API URL *

[Cancel](#)[!\[\]\(d78c549529259e418b25695fc4d34f70_img.jpg\) **Test Login**](#)

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

Add Connection

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

Account *
-- Choose Account --

Location *
-- Choose Location --

Contact *
-- Choose Contact --

Ticket Source *
-- Choose Ticket Source --

Ticket Type *
-- Choose Ticket Type --


Priority *
-- Choose Priority --

Status *
-- Choose Status --

Queue *
-- Choose Queue --

Primary Assignee *
-- Choose Primary Assignee --

← Back

 **Test Ticket**

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

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

Add Connection

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

Connection

Connection Name *

Type

Kaseya BMS

Login

Ticketing

Account	NFR RapidFire Tools	Location	NFR RapidFire Tools
Contact	Leo Tolstoy	Ticket Source	Verbal
Ticket Type	Problem	Priority	Medium
Status	Completed	Queue	Level Three Support
Primary Assignee	RFT Test		

Back
 Save

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

Connections

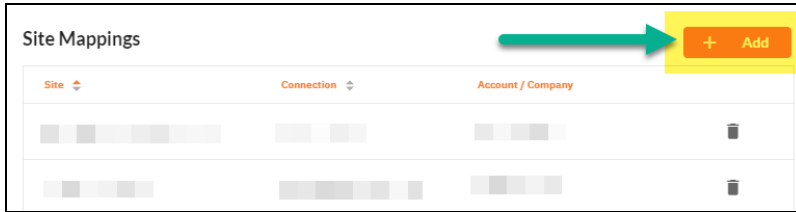
Your Connections + Add

Name	Type	Login	
BMS Export CM Issues	Kaseya BMS	<input type="password"/>	

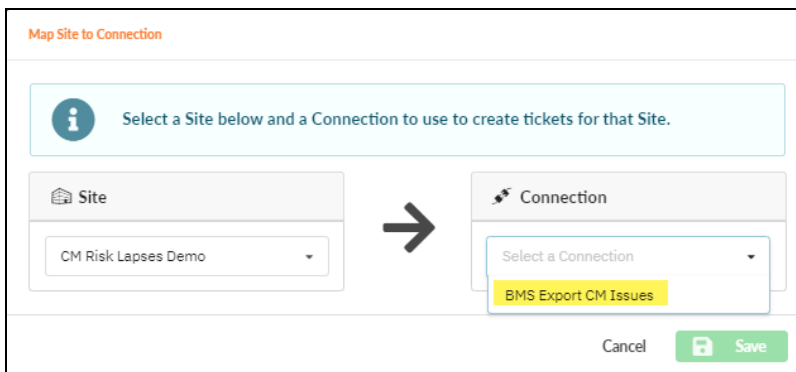
Step 3 — Map your Compliance Manager's Site to a Kaseya BMS Connection

Follow these steps to map a Kaseya BMS Connection to the RapidFire Tools Portal Site associated with your Compliance Manager assessment.

1. From the **Global Settings > Connections** menu, scroll down and click **Add** under Site Mappings. The Map Site to Connection window will be displayed.



2. Select the RapidFire Tools Portal Compliance Manager **Site** you want to assign to the Kaseya BMS Integration.
3. Next, **select the name of the Connection** that you want use to link the Site to Kaseya BMS.



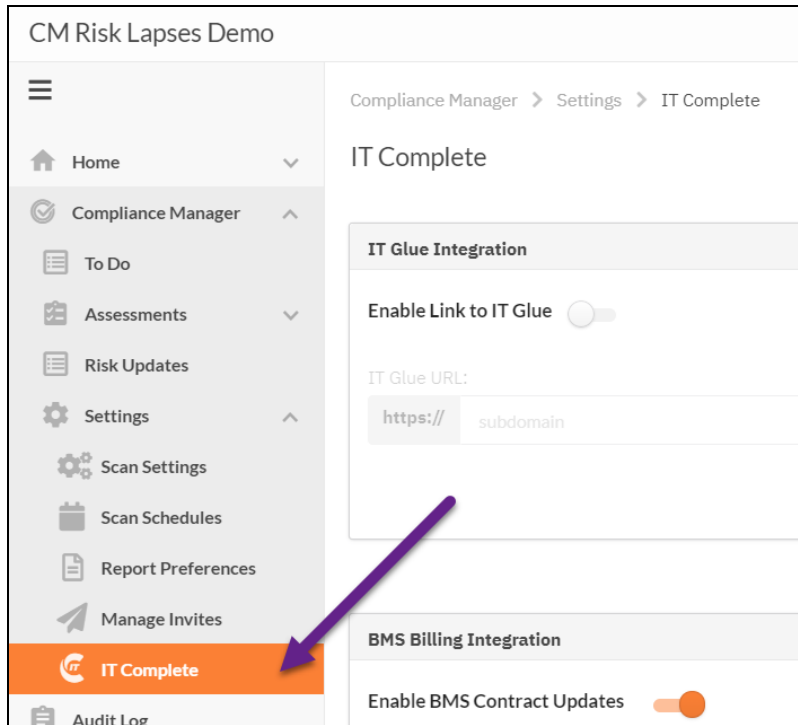
4. Click **Save**. The Site's mapping will be saved and listed in the Site Mappings list.

You can now export Issues as tickets for the RapidFire Tools Portal Site you selected.

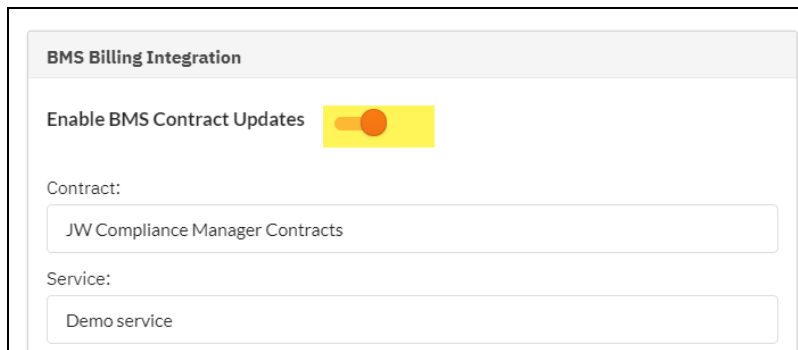


Step 4 — Enable BMS Billing Integration from Site

1. From your selected site, navigate to **Compliance Manager > Settings > IT Complete**.



2. Scroll down to **BMS Billing Integration**.
3. Click the slider to **Enable BMS Contract Updates**.



4. Select the contract for which you want to enable billing updates. You can select from among those contracts associated with your account in BMS.

BMS Billing Integration

Enable BMS Contract Updates

Contract:

Alternative Contract

JW Compliance Manager Contracts

Bill By:

☒ Endpoints (Latest Assessment: 36)

☐ Current Employees (Latest Assessment: 0)

☐ Users (Latest Assessment: 34)

Minimum Quantity:

1

Maximum Quantity:

-1

☒ Unlimited

5. Next, select the particular BMS **Service** to associate with the Site. You can select from the Services that you have associated with your Contract in BMS.

BMS Billing Integration

Enable BMS Contract Updates

Contract:

JW Compliance Manager Contracts

Service:

Demo service

MANUAL SYNC

REGULAR ASSESSMENT SERVICE

RISK UPDATE SERVICE

Users (Latest Assessment: 34)

Minimum Quantity:

1

Maximum Quantity:

-1

☒ Unlimited

Last Sync: 12/23/2020 6:18:26 PM (Quantity: 36)

Sync Now

Undo Changes

Save

6. Next, select how you want to bill for the Site. Choose the exact unit that will be quantified based on your billing preferences. The options include:

Unit	Description
Endpoints	Endpoints represents the active computers for which local data was collected or which have logged in within the last 30 days. Includes both automated and manual collection.
Current Employees	“Current Employees” are marked on the User Access Review Worksheet during the assessment.
Users	Users represents the number of total users found. This corresponds to the number of rows on the User Access Review Worksheet. Includes both automated and manual collection.

BMS Billing Integration

Enable BMS Contract Updates

Contract:

JW Compliance Manager Contracts

Service:

Demo service

Bill By:

☒ Endpoints (Latest Assessment: 36)

☐ Current Employees (Latest Assessment: 0)

☐ Users (Latest Assessment: 34)

Minimum Quantity:

1

Maximum Quantity:

-1

☒ Unlimited

Last Sync: 12/23/2020 6:18:26 PM (Quantity: 36)

Sync Now

Undo Changes

Save

- Next, choose the minimum and maximum quantity to be billed. This quantity is based on the unit you select to bill by in the earlier step.

Bill By:

☒ Endpoints (Latest Assessment: 36)

☐ Current Employees (Latest Assessment: 0)

☐ Users (Latest Assessment: 34)

Minimum Quantity:

1

Maximum Quantity:

-1

☒ Unlimited

Last Sync: 12/23/2020 6:18:26 PM (Quantity: 36)

Sync Now

Undo Changes

Save

- Click **Save**.
- Then click **Sync Now** to update the Service in BMS with the correct quantity/units.

- If the assessment value is less than the minimum quantity, the minimum quantity is sent to BMS. For example, if 5 users are detected, and you set a minimum of 10 users, BMS will be updated with 10 users.
- If the assessment value is greater than the maximum quantity, the maximum quantity is sent to BMS – unless set to unlimited.

Contract:
JW Compliance Manager Contracts

Service:
Demo service

Bill By:

☐ Endpoints (Latest Assessment: 36)

☐ Current Employees (Latest Assessment: 0)


☒ Users (Latest Assessment: 34)

Minimum Quantity:

Maximum Quantity: ☒ Unlimited

Last Sync: 12/24/2020 7:01:44 PM (Quantity: 34) [Sync Now](#)

[Undo Changes](#) [Save](#)

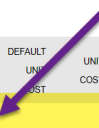


10. The **Unit** number for the designated service will be updated based on the data from Compliance Manager. This will help streamline your automated billing in BMS.

Contract Billing Price: *
\$450.00

[Add](#) [Delete](#)

	SERVICE NAME	DESCRIPTION	EFFECTIVE DATE	UNITS	DEFAULT UNIT COST	UNIT COST	TOTAL COST	DEFAULT UNIT PRICE	UNIT PRICE	TOTAL PRICE	SORT ORDER
<input type="checkbox"/>	GDPR	REGULAR ASSESSMENT	11/01/2020	36	\$8.00	\$8.00	\$288.00	\$10.00	\$10.00	\$360.00	2
<input checked="" type="checkbox"/>	Demo service	MANUAL SYNC	11/01/2020	2	\$10.00	\$10.00	\$20.00	\$10.00	\$10.00	\$20.00	3
<input type="checkbox"/>	REGULAR ASSESSMENT SERVICE	REGULAR ASSESSMENT SERVICE	11/01/2020	3	\$10.00	\$10.00	\$30.00	\$10.00	\$10.00	\$30.00	4
<input type="checkbox"/>	RISK UPDATE SERVICE	RISK UPDATE SERVICE	11/01/2020	4	\$10.00	\$10.00	\$40.00	\$10.00	\$10.00	\$40.00	5



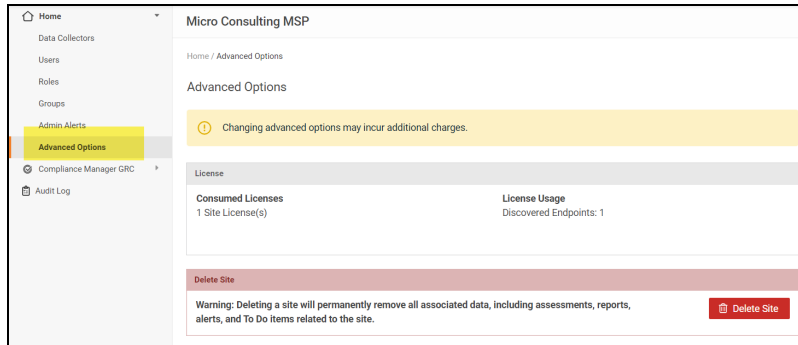
11. The Unit for BMS contract/services will also be automatically updated when:

- You complete a Compliance Manager assessment
- You complete a Risk Update

Delete a Site

If you wish to delete a site, follow these steps:

1. Select the site from the Sites page that you wish to delete.
2. From the site's **Home** tab, click on **Advanced Options**.



3. Click **Delete Site**.

Important: Deleting a site will permanently remove all associated data, including assessments, reports, alerts, and To Do items related to the site.

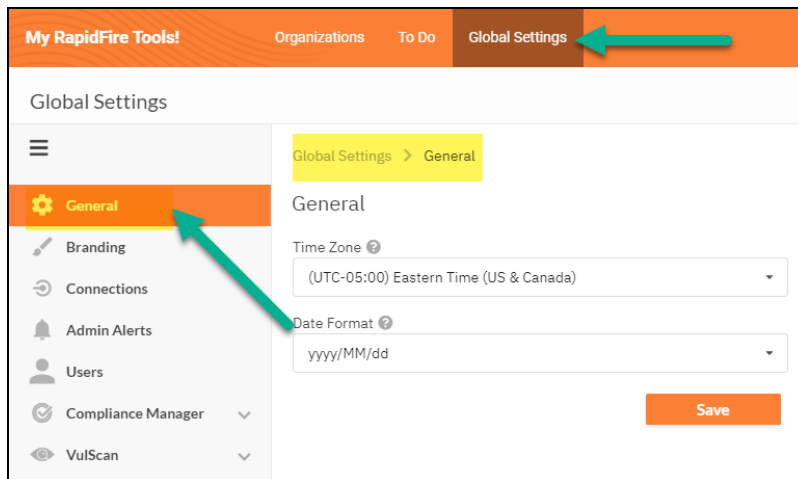
4. Confirm that you wish to delete the site by typing the site's name. Then click **Yes**. The site will then be removed from the system.

A screenshot of the 'Delete Site' confirmation dialog. The title is 'Delete Site'. It features a red warning icon and the text: 'Are you sure? Deleting a site will permanently remove all associated data, including assessments, reports, alerts, and To Do items related to the site.' Below this, it says: 'To delete the site, type the site name (Micro Consulting MSP) in the box below:'. There is a text input field labeled 'Site Name'. At the bottom, there are two buttons: 'Cancel' and 'Delete Site'.

Set Time Zone

You can set your time zone from **Global Settings > General**. Set your time zone to schedule automated scans at your preferred local time. To configure time zones:

1. Go to **Global Settings > General**.



2. Select your time zone from the drop down menu.
3. Click **Save**.

Note that the time zone setting is relatively narrow in scope. For example, To Do task creation time is shown based on your browser's local time, *not* the time zone setting in Global Settings. The time zone setting effects a few items, including:

- start time for scans when using the limit scan start time feature for a site
- last modified date of risk update reports
- last sync date and time for Kaseya BMS billing integration

Admin Alerts (RapidFire Tools Portal)

Within the RapidFire Tools Portal, you can set and configure Admin Alerts to inform you of events such as a completed or failed scan or notification error.

Admin Alerts: Global Settings vs. Site Settings

There are two levels at which you can configure Admin Alerts:

- From **Global Settings > Admin Alerts**, you can set the default Admin Alert settings for all of your Sites within the RapidFire Tools Portal. This can be useful if one group of recipients should receive admin alerts for all of your Sites.
- From **[Your Site] > Home > Admin Alerts**, you can override the default Global Settings for Admin Alerts. Your changes will be specific to that Site. This can be useful if you want different groups of recipients to receive admin alerts for different sites.

Configure Admin Alerts

To configure Admin Alerts:

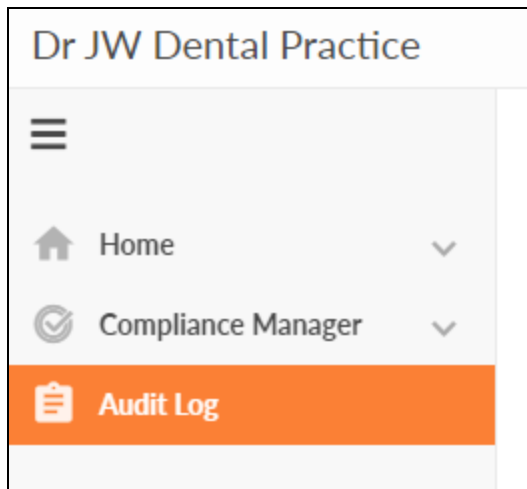
1. Decide whether you want to change the Admin Alert settings for:
 - A. All of your Sites (Navigate to **Global Settings > Admin Alerts**)
 - B. Just for one specific Site (**[Your Site] > Home > Admin Alerts**)
2. Then, enter the email addresses for the users who will receive the Admin Alerts.

The screenshot shows the 'Global Settings / Admin Alerts' configuration page in the RapidFire Tools Portal. The left sidebar contains a navigation menu with options: General, Branding, Connections, Admin Alerts (highlighted), Users, Compliance Manager GRC, Network Detective Pro, VulScan, Service Plans, Email Groups, Data Collectors, and IT Complete. The main content area is titled 'Global Settings / Admin Alerts' and 'Admin Alerts'. It includes a text input field for 'Email Addresses (Separate multiple addresses with a comma (""))' and a section for 'Notices (Subject Prefix (added before notice type))' with a text input field containing '%%SITE%% -'. Below this, there are four checkboxes: 'Scan Failed' (checked), 'Notification Error' (unchecked), 'Scan Complete' (checked), and 'Reports Generated' (checked).

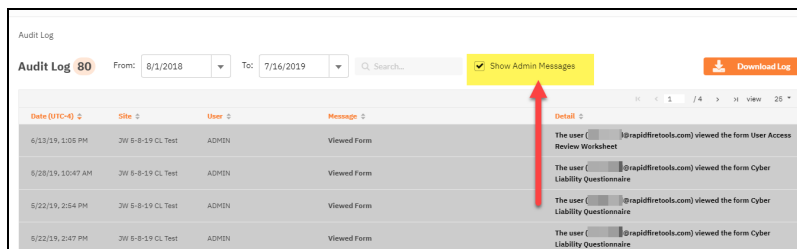
3. Add a Subject Prefix that will be included in email's subject line before the notice type.
4. Select which types of alerts to send to the listed users.
5. Click **Save**. You can also choose to **Reset** to Global Settings.

Audit Log

The **Audit Log** allows you to see all of the activity in the RapidFire Tools Portal.



Click **Show Admin Messages** to see even more detail. This includes notices that scans were started, completed, failed, etc.



Compliance Manager Audit Log Details

The Compliance Manager Audit Log records and presents the following information pertaining to an assessment:

- The creation of Assessment To Do task items
- The start and completion of automated scans including:
 - Pre-Scan
 - External vulnerability scan
 - Network Scan
 - “Quick” Remote Local Computer Scans
 - “Deep” Remote Local Computer Scans

- The viewing and modification of the worksheet and questionnaire forms by users assigned Site Admin, Technicians, Internal Auditor, and Subject Matter Expert roles
- Subject Matter Expert invitations to participate in the assessment project
- Report generation

Examples of Audit Log Entries

Below are examples of audit log entries illustrating To Do task creation, automated scan activity, and assessment form access and modification activity.

Creation of To Do Task Items

Insured Entity					
Audit Log					
Audit Log 26 From: 2/27/2020 To: 2/28/2020 Search... Show Admin Messages					
Date (UTC-05:00)	Site	User	Message	Detail	
2/26/20, 1:14 PM	Insured Entity		New Task Created	Cyber Insurance Assessment Complete.	
2/26/20, 12:50 PM	Insured Entity		New Task Created	Review Final Reports	
2/26/20, 12:50 PM	Insured Entity		New Task Created	Complete the Compensating Control Worksheet	
2/26/20, 12:49 PM	Insured Entity		New Task Created	Complete Cyber Liability Questionnaire	
2/26/20, 12:47 PM	Insured Entity		New Task Created	Complete Insurance Selection Worksheet	
2/26/20, 12:47 PM	Insured Entity		New Task Created	Complete Antivirus Verification Worksheet	
2/26/20, 12:47 PM	Insured Entity		New Task Created	Complete User Access Review Worksheet	
2/26/20, 12:46 PM	Insured Entity		New Task Created	Complete the File Scan Validation Worksheet	
2/26/20, 7:36 AM	Insured Entity		New Task Created	Unable to scan all selected systems	
2/26/20, 6:58 AM	Insured Entity		New Task Created	Running File Scan	
2/26/20, 6:57 AM	Insured Entity		New Task Created	File Scan System Selection Worksheet	
2/26/20, 12:21 AM	Insured Entity		New Task Created	Run Local Data Collector (Optional)	
2/27/20, 11:21 PM	Insured Entity		New Task Created	Running Local Scan of Remote Computers	
2/27/20, 10:52 PM	Insured Entity		New Task Created	Running Automated Scan of the Internal Network	
2/27/20, 10:36 PM	Insured Entity		New Task Created	Complete External Port Use Worksheet	
2/27/20, 10:03 PM	Insured Entity		New Task Created	Running Automated External Vulnerability Scan	
2/27/20, 10:03 PM	Insured Entity		New Task Created	Running Pre-scan Analysis	

Automated Scanning Start and Completion Activity

Insured Entity					
Audit Log					
Audit Log 37 From: 2/28/2020 To: 2/28/2020 Search... Show Admin Messages					
Date (UTC-05:00)	Site	User	Message	Detail	
2/28/20, 7:36 AM	Insured Entity		New Task Created	Unable to scan all selected systems	
2/28/20, 7:33 AM	Insured Entity	ADMIN	Local scan files merged	Local scan files were merged into the primary scan	
2/28/20, 7:09 AM	Insured Entity	ADMIN	Scan Completed	PDGM Scan (ref #F920723) Scan completed successfully.	
2/28/20, 6:58 AM	Insured Entity		New Task Created	Running File Scan	
2/28/20, 7:09 AM	Insured Entity	ADMIN	Scan Completed	PDGM Scan (ref #F920723) Scan completed successfully.	
2/28/20, 6:58 AM	Insured Entity		New Task Created	Running File Scan	
2/28/20, 6:58 AM	Insured Entity	ADMIN	Scan Started	PDGM Scan (ref #F920723)	
2/28/20, 6:57 AM	Insured Entity		New Task Created	File Scan System Selection Worksheet	
2/28/20, 12:21 AM	Insured Entity		New Task Created	Run Local Data Collector (Optional)	
2/28/20, 12:01 AM	Insured Entity	ADMIN	Local scan files merged	Local scan files were merged into the primary scan	
2/27/20, 11:57 PM	Insured Entity	ADMIN	Scan Completed	PDGM Scan (ref #F976987, File Scan: C1 Quick) Scan completed successfully.	
2/27/20, 11:21 PM	Insured Entity	ADMIN	Scan Started	PDGM Scan (ref #F976987, File Scan: C1 Quick)	
2/27/20, 11:21 PM	Insured Entity		New Task Created	Running Local Scan of Remote Computers	
2/27/20, 11:21 PM	Insured Entity	ADMIN	Scan Started	PDGM Scan (ref #F976987, File Scan: C1 Quick)	
2/27/20, 11:21 PM	Insured Entity		New Task Created	Running Local Scan of Remote Computers	
2/27/20, 10:03 PM	Insured Entity	ADMIN	Scan Completed	Network Data Collection (ref #F976989) Scan completed successfully.	
2/27/20, 10:02 PM	Insured Entity		New Task Created	Running Automated Scan of the Internal Network	
2/27/20, 10:02 PM	Insured Entity	ADMIN	Scan Started	Network Data Collection (ref #F976989)	

Assessment Questionnaire and Worksheet Form Access and Modification Activity

The screenshot shows the 'Insured Entity' page with the 'Audit Log' tab selected. The log displays a list of activities with columns for Date/Time, User, Message, and Detail. The activities include viewing and modifying various forms such as the Compensating Control Worksheet, Cyber Liability Questionnaire, Insurance Selection Worksheet, User Access Review Worksheet, Audits/Verification Worksheet, File Scan Validation Worksheet, and System Selection Worksheet.

Date/Time	User	Message	Detail
2/28/2020 12:50 PM	Insured Entity	Form Modified	The Form Compensating Control Worksheet was modified by
2/28/2020 12:50 PM	Insured Entity	Form Modified	The user viewed the Form Compensating Control Worksheet
2/28/2020 12:50 PM	Insured Entity	Form Modified	The user viewed the Form Cyber Liability Questionnaire
2/28/2020 12:50 PM	Insured Entity	Form Modified	The user viewed the Form Cyber Liability Questionnaire
2/28/2020 12:50 PM	Insured Entity	Form Modified	The user viewed the Form Insurance Selection Worksheet
2/28/2020 12:50 PM	Insured Entity	Form Modified	The user viewed the Form Insurance Selection Worksheet
2/28/2020 12:50 PM	Insured Entity	Form Modified	The user viewed the Form User Access Review Worksheet
2/28/2020 12:50 PM	Insured Entity	Form Modified	The user viewed the Form User Access Review Worksheet
2/28/2020 12:50 PM	Insured Entity	Form Modified	The user viewed the Form Audits/Verification Worksheet
2/28/2020 12:50 PM	Insured Entity	Form Modified	The user viewed the Form Audits/Verification Worksheet
2/28/2020 12:50 PM	Insured Entity	Form Modified	The user viewed the Form File Scan Validation Worksheet
2/28/2020 12:50 PM	Insured Entity	Form Modified	The user viewed the Form File Scan Validation Worksheet
2/28/2020 12:50 PM	Insured Entity	Form Modified	The user viewed the Form System Selection Worksheet
2/28/2020 12:50 PM	Insured Entity	Form Modified	The user viewed the Form System Selection Worksheet

CMMC To Do Task Complete List

The list below outlines all To Do tasks in the CMMC Assessment To Do list.

Note: The items below may appear in a different order in your To Do list. This depends on the order in which you choose to complete certain tasks.

	Task	Project Role
<input type="checkbox"/>	Create additional users and assign to roles (Home tab > Settings > Users; Roles) <i>Add and invite users to participate in the assessment. Then assign these users to project roles.</i>	Site Admin
<input type="checkbox"/>	Set up Report Preferences (Compliance Manager tab > Settings > Report Preferences) <i>Configure the reports for the Site that will be generated at the end of the assessment. This includes visual elements and client details.</i>	Site Admin
<input type="checkbox"/>	Install Compliance Manager Server (Installed on client network) <i>Compliance Manager Server on the target network.</i>	Technician
<input type="checkbox"/>	Configure Server Scan Settings (Compliance Manager tab > Settings > Scan Settings) <i>Once server is installed, enter information to set up scans.</i>	Technician

	Task	Project Role
<input type="checkbox"/>	Start CMMC Assessment (Compliance Manager tab > To Do) <i>Initial start of assessment. Starts automated scans and generates forms to complete.</i>	Internal Auditor
<input type="checkbox"/>	Running Pre-Scan Analysis (Automated Scan) <i>The server will check for issues that might prevent a complete network scan.</i>	Compliance Manager Server
<input type="checkbox"/>	Review Pre-Scan Analysis Results and Recommendations (Compliance Manager tab > To Do) <i>Review and fix potential scan problems before starting the internal scans.</i>	Technician
<input type="checkbox"/>	Running the Automated Internal Network Scan (Automated Scan) <i>An automated scan will begin on the client's internal network.</i>	Compliance Manager Server
<input type="checkbox"/>	Running Local Scan of Remote Computers (Automated Scan) <i>An automated scan will begin on the client's internal network targeting remote computers.</i>	Compliance Manager Server
<input type="checkbox"/>	Unable to scan all selected systems (Compliance Manager tab > To Do) <i>Perform and upload computer scans on machines that could not be reached during the internal scan.</i>	Technician
<input type="checkbox"/>	Run Local Data Collector (optional) (Compliance Manager tab > To Do) <i>Perform and upload computer scans on machines that could not be reached during the internal scan.</i>	Technician
<input type="checkbox"/>	Running the Automated External Vulnerability Scan (Automated Scan) <i>An automated external vulnerability scan will begin on the designated IP addresses.</i>	Compliance Manager Server
<input type="checkbox"/>	Complete External Port Use Worksheet (Compliance Manager tab > To Do)	Technician

	Task	Project Role
	<i>Enter information about external ports discovered during the external scan.</i>	
<input type="checkbox"/>	Complete Antivirus Verification Worksheet (Compliance Manager tab > To Do) <i>Assess</i>	Internal Auditor
<input type="checkbox"/>	Complete User Access Review Worksheet (Compliance Manager tab > To Do) <i>Assess</i>	Internal Auditor
<input type="checkbox"/>	Complete Asset Inventory Worksheet (Compliance Manager tab > To Do) <i>Document any</i>	Internal Auditor
<input type="checkbox"/>	Complete Application Inventory Worksheet (Compliance Manager tab > To Do) <i>Document how</i>	Internal Auditor
<input type="checkbox"/>	Complete External Information System Worksheet (Compliance Manager tab > To Do) <i>Document any</i>	Internal Auditor
<input type="checkbox"/>	Select Level of CMMC Assessment (Compliance Manager tab > To Do) <i>Optionally can choose to add additional worksheets to your assessment to identify additional issues.</i>	Internal Auditor
<input type="checkbox"/>	Complete CMMC Access Control Worksheet (Level 1 and Level 2) (Compliance Manager tab > To Do) <i>Conduct</i>	Internal Auditor
<input type="checkbox"/>	Complete CMMC Audit and Accountability Worksheet (Level 2) (Compliance Manager tab > To Do) <i>Conduct an inventory of all .</i>	Internal Auditor

	Task	Project Role
<input type="checkbox"/>	Complete CMMC Awareness and Training Worksheet (Level 2) (Compliance Manager tab > To Do) <i>Conduct an inventory of all</i>	Technician
<input type="checkbox"/>	Complete CMMC Configuration Management Worksheet (Level 2) (Compliance Manager tab > To Do) <i>Select</i>	Internal Auditor
<input type="checkbox"/>	Complete CMMC Identification and Authentication Worksheet (Level 1 and Level 2) (Automated Scan) <i>An automated scan of the client network will begin checking for .</i>	Internal Auditor
<input type="checkbox"/>	Complete CMMC Maintenance Worksheet (Level 2) (Automated Scan) <i>An automated scan of the client network will begin checking for .</i>	Internal Auditor
<input type="checkbox"/>	Complete CMMC Media Protection Worksheet (Level 1 and Level 2) (Automated Scan) <i>An automated scan of the client network will begin checking for .</i>	Internal Auditor
<input type="checkbox"/>	Complete CMMC Personnel Security Worksheet (Level 2) (Automated Scan) <i>An automated scan of the client network will begin checking for .</i>	Internal Auditor
<input type="checkbox"/>	Complete CMMC Physical Protection Worksheet (Level 1 and Level 2) (Automated Scan) <i>An automated scan of the client network will begin checking for .</i>	Internal Auditor
<input type="checkbox"/>	Complete CMMC Recovery Worksheet (Level 2) (Automated Scan) <i>An automated scan of the client network will begin checking for .</i>	Internal Auditor
<input type="checkbox"/>	Complete CMMC Risk Management Worksheet (Level 2) (Automated Scan) <i>An automated scan of the client network will begin checking for .</i>	Internal Auditor

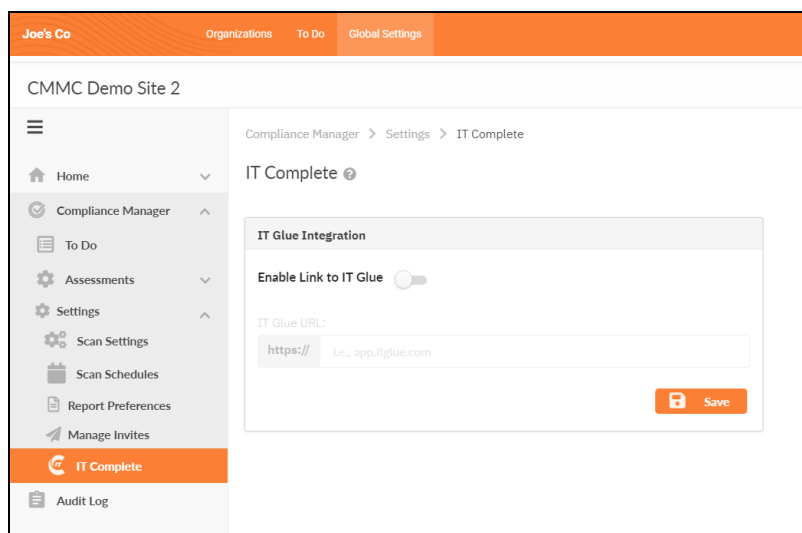
	Task	Project Role
<input type="checkbox"/>	Complete CMMC Security Assessment Worksheet (Level 2) (Automated Scan) <i>An automated scan of the client network will begin checking for .</i>	Internal Auditor
<input type="checkbox"/>	Complete CMMC System and Communications Protection Worksheet (Level 1 and Level 2) (Automated Scan) <i>An automated scan of the client network will begin checking for .</i>	Internal Auditor
<input type="checkbox"/>	Complete CMMC System and Information Integrity Worksheet (Level 1 and Level 2) (Automated Scan) <i>An automated scan of the client network will begin checking for .</i>	Internal Auditor
<input type="checkbox"/>	Review Final Reports (Compliance Manager tab > To Do) <i>Examine the final reports and supporting documents to demonstrate compliance or begin remediating issues.</i>	Internal Auditor
<input type="checkbox"/>	Complete CMMC Assessment (Compliance Manager tab > To Do) <i>Finish and archive your CMMC Assessment. You can review the archived documentation at any time.</i>	Internal Auditor

Import Worksheet Attachments from ITGlue

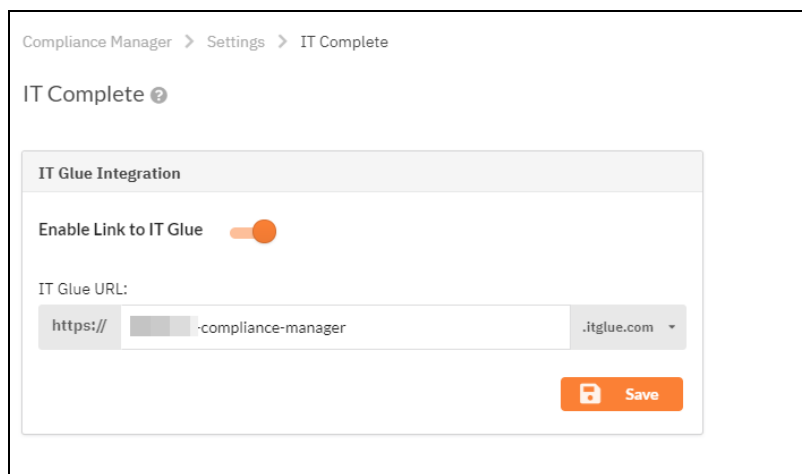
If you use the **ITGlue** documentation tool (www.itglue.com), you can import documents from ITGlue as attachments into your Compliance Manager assessment worksheets and surveys. If you are already maintaining technical documents about the site's IT resources in ITGlue, then use this feature to save time by leveraging this data directly within your Compliance Manager assessment.

Follow these steps to import items from ITGlue into your assessment documentation:

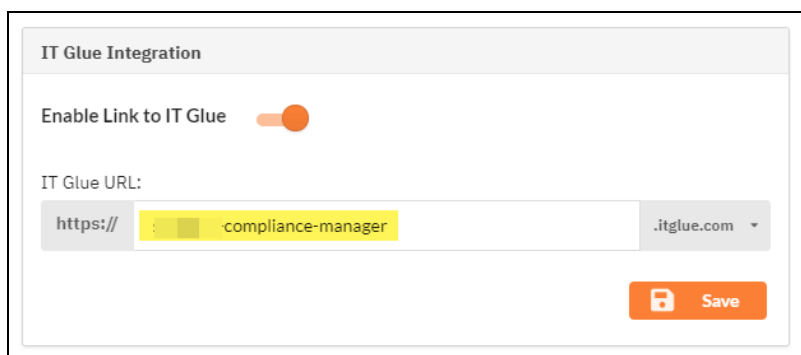
1. Open the assessment site that you want to enhance with documentation from ITGlue.
2. From your Site, go to **Settings > ITComplete**.



3. Under **ITGlue Integration**, click the **Enable Link to ITGlue slider** button.

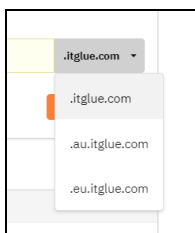


4. Next enter the IT Glue URL. Be sure to enter it in the appropriate format. We make it easy. For example, if your entire IT Glue URL is "https://my-it-company.itglue.com," just enter "my-it-company" in the field.

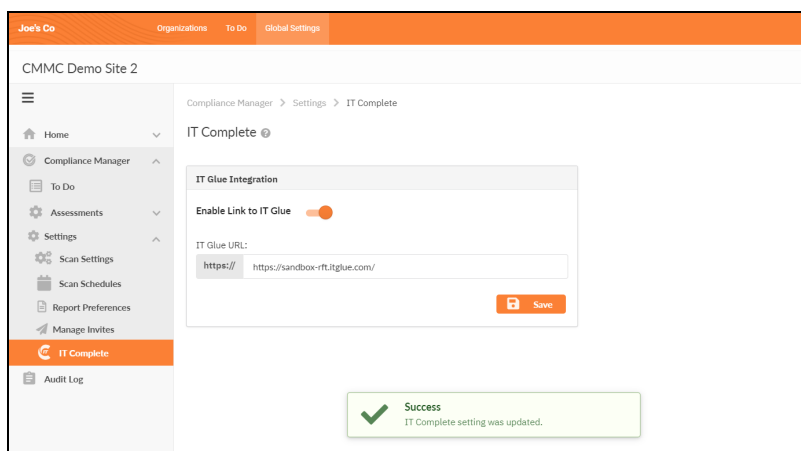


The screenshot shows a form titled "IT Glue Integration". It has a toggle switch for "Enable Link to IT Glue" which is turned on. Below this is a text field for "IT Glue URL:" containing "https://", a highlighted input field with "compliance-manager", and a dropdown menu showing ".itglue.com". A "Save" button is at the bottom right.

5. If you are in the EU, select **.eu.itglue.com** from the drop down menu.

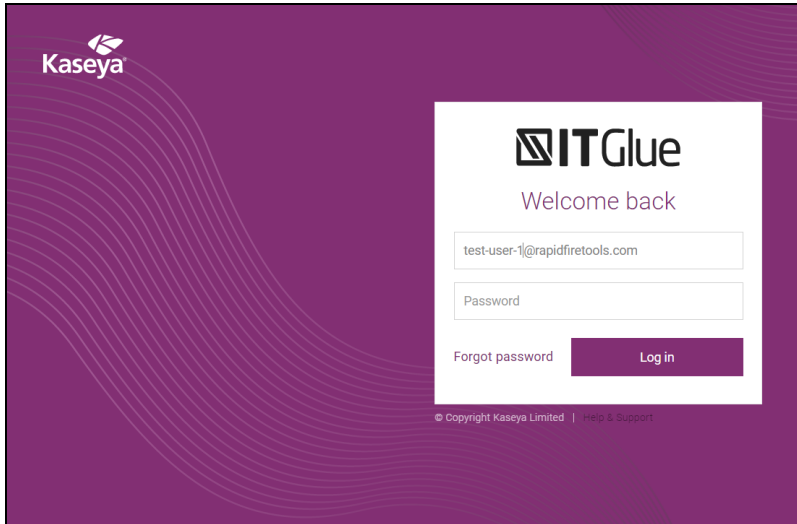


6. Click **Save** to confirm your IT Glue integration details.

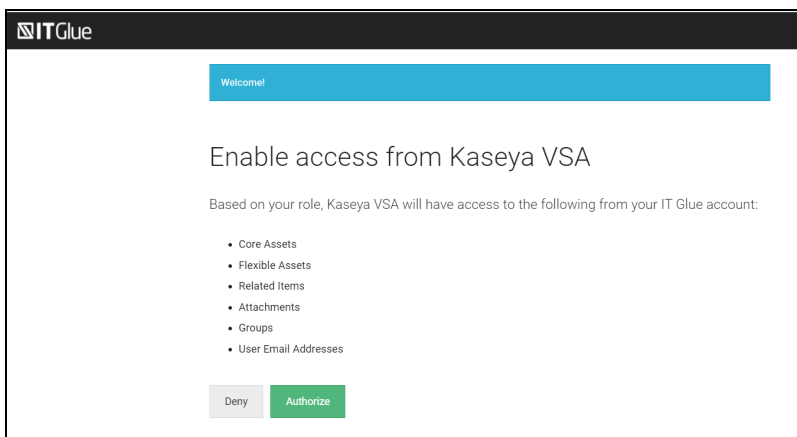


The screenshot shows the "IT Complete" settings page in a web application. The page has a sidebar with navigation links: Home, Compliance Manager, To Do, Assessments, Settings, Scan Settings, Scan Schedules, Report Preferences, Manage Invites, IT Complete (selected), and Audit Log. The main content area shows the "IT Complete" settings, including the "IT Glue Integration" section with the "Enable Link to IT Glue" toggle and the "IT Glue URL:" field containing "https://sandbox-rt.itglue.com/". A "Save" button is at the bottom right. A green success message box at the bottom center reads "Success IT Complete setting was updated."

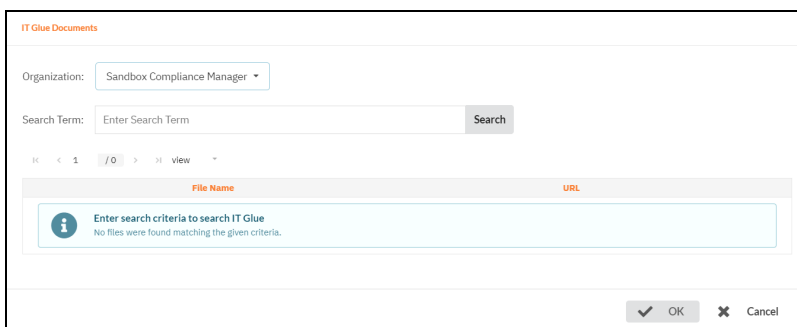
7. Next, from your Site's To Do list, open the assessment worksheet for which you want to attach ITGlue documents.
8. Choose a worksheet question and click the folder icon.



11. Confirm that you want to grant the necessary data permissions to attach documents to your Compliance Manager worksheets. Click **Authorize**.



12. When you enter your login credentials, you will connect to ITGlue. Compliance Manager will reopen and you can then browse for documents in ITGlue. To do this, enter a search term and click **Search** to find IT Glue documents to attach to your worksheets as evidence of compliance.



13. Once you enter the appropriate search term, select each document to attach and click **OK**.

IT Glue Documents

Organization: Compliance Manager

Search Term: compliance Search

Select one or more attachments to attach to the selected topic.

1 / 2 view

	File Name	URL
<input type="checkbox"/>	OAuth client in EU Prod	https://compliance-manager.itglue.com/passwords
<input type="checkbox"/>	OAuth client in EU Staging	https://compliance-manager.itglue.com/passwords
<input type="checkbox"/>	OAuth client in NA Prod	https://compliance-manager.itglue.com/passwords
<input type="checkbox"/>	OAuth client in NA Staging	https://compliance-manager.itglue.com/passwords
<input type="checkbox"/>	New Document	https://compliance-manager.itglue.com/DOC-
<input type="checkbox"/>	New Document	https://compliance-manager.itglue.com/DOC-
<input type="checkbox"/>	New Document	https://compliance-manager.itglue.com/DOC-

OK Cancel

The selected documents will be attached to your worksheet.

Attachments:

	File Name	Upload Date	Uploaded By
<input checked="" type="checkbox"/>	Account Management (IT Glue - https://compliance-manager.itglue.com/passwords)	Nov 2, 2020, 10:43:18 AM	@rapidfiretools.com
<input checked="" type="checkbox"/>	Vendor Management (e.g. Sage) (IT Glue - https://compliance-manager.itglue.com/passwords)	Nov 2, 2020, 10:43:18 AM	@rapidfiretools.com
<input checked="" type="checkbox"/>	Remote Management & Monitoring (RMM) (IT Glue - https://compliance-manager.itglue.com/passwords)	Nov 2, 2020, 10:43:18 AM	@rapidfiretools.com

Add Attachment From Previously Uploaded From Local Computer From IT Glue

Close

Augment Antivirus Verification Worksheets to Detect Antivirus Apps

Occasionally, your customer may have an antivirus or antispyware service installed that was not detected by Compliance Manager. For example, your customer may have a very old or very new release of an existing product. This topic covers how to ensure your Compliance Manager reports always present the complete picture of your customer's unique circumstances.

By using the Compliance Manager in tandem with the Network Detective app, you can customize your data analysis to better suit each of your customers. If an antivirus service is not listed in our database, you may add it through the Network Detective application. Then, re-generate the reports in Compliance Manager and the service will be properly included and displayed.

You can use this feature with the following modules:

- NIST
- Cyber Insurance
- CMMC

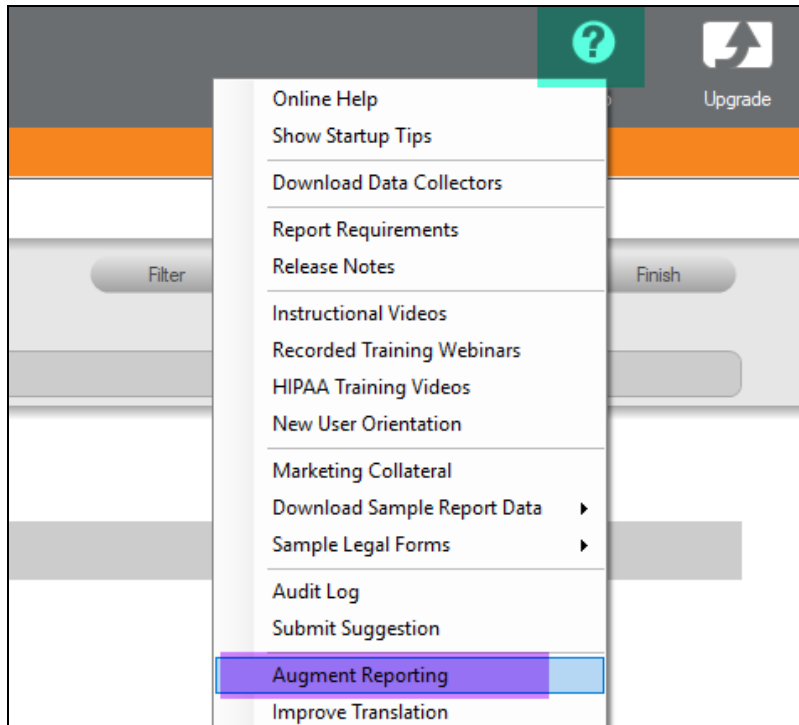
To augment your reports:

Step 1 — Augment Reports in Network Detective

1. First, download and install Network Detective from <https://www.rapidfiretools.com/nd-downloads>.
2. Open the app and log in with your credentials. Your Compliance Manager credentials will allow you to access Network Detective.

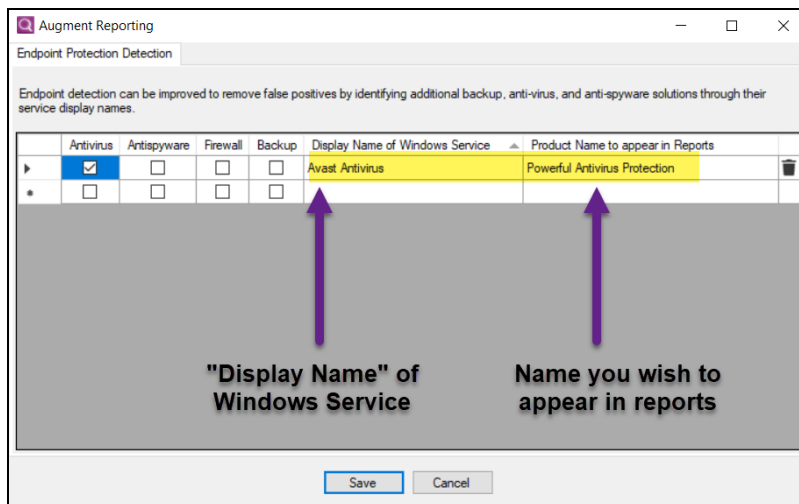
Important: If you are **not** a Network Detective subscriber, in order to augment antivirus detection you must access Network Detective using the account credentials assigned to you when purchasing Compliance Manager. If you **are** a Network Detective subscriber, you can log in with a Compliance Manager user who has at least the "Admin" level of global access.

3. In Network Detective, go to **Help > Augment Reporting**.



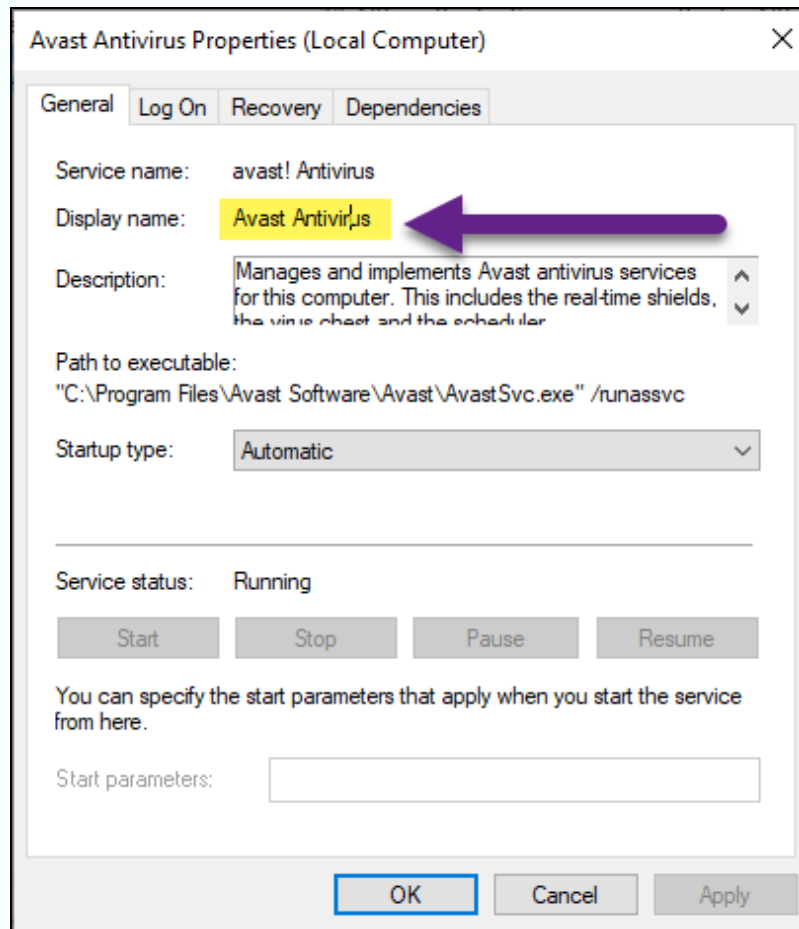
The **Endpoint Protection Detection** screen will appear.

4. For each application you wish to add to your reports, select the type of application: *Antivirus*, *Antispyware*, *Firewall*, and/or *Backup*.



5. Then enter the *Display Name* for the Windows Service.

Note: You can find the *Display Name* by opening the Windows Services app from your desktop. **Right click** on the service and click **Properties**.



6. Next enter the **Product Name** for use with reporting. You can choose any name you wish for the Product Name for your Reports.
7. Repeat these steps for each app you wish to add to your reports.
8. Click **OK**.

Step 2 — Generate Antivirus Verification Worksheet

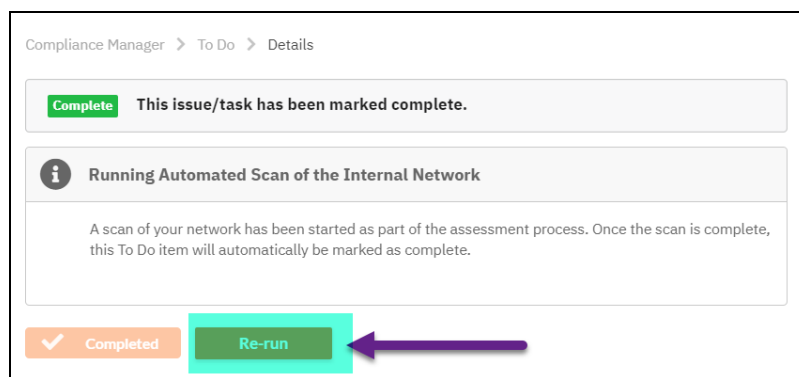
After you set up augmented reporting in Network Detective, the next step is to generate the Antivirus Verification **Worksheet**. You can do this two ways:

- A. If you have not already started your assessment, proceed through your assessment. When you reach the **Complete Antivirus Verification Worksheet** to

do item, the proper AV software should appear for each endpoint listed in the worksheet if you followed Step 1 correctly.

- B. If you have already generated your Antivirus Verification Worksheet, you must re-run the Internal Network Scan. This will rescan the assigned endpoints and reset your Antivirus Verification Worksheet. With the updated worksheet, the proper AV software should appear for each endpoint if you followed Step 1 correctly. To do this:

1. From your site To Do list, return to the **Running Automated Scan of the Internal Network** To Do item.
2. Open the To Do item and click **Re-run**. Note that this will reset several worksheets for the current assessment, including the **Antivirus Verification Worksheet**.



3. The internal network scan will then begin. Once it finishes, the automated local scan will also begin. Finally, you have the option to manually scan any workstations that could not be reached during the internal scan.
4. Once the internal scans are all marked complete, the updated antivirus worksheet will become available. The worksheets will detail which endpoints host your selected antivirus software.

Hide # | Expand All | Collapse All | Download

1 TEST.PERFORMANCEIT.COM

1.1 test.performanceit.com
Please verify the following antivirus software are present.

Previous Assessment Response: Multiple Responses
View Previous Responses

Computer	IP Address	AV Detected	Detected Antivirus	Assessment
DESKTOP-108DGL1	fe80:c252b2a24ba2f4b15%4.10.2	Yes	Windows Defender	Verified Present
DESKTOP-191JQL	fe80:f107b4c6d101cca%17.10.2	Yes	Windows Defender	Verified Present
DESKTOP-35EQCC	fe80:a03d798735a47be%5.10.2	Yes	Windows Defender	Verified Present
DESKTOP-4171ARO	fe80:a190a4648544551%6.10.2	Yes	Avast Antivirus, Powerful Antivirus Protection, Windows Defender	Verified Present
DESKTOP-4PF2ICP	10.200.1.177	Yes	Windows Defender	Verified Present
DESKTOP-534MS45	fe80:4ce7d92ca7cb498b%10.10.	Yes	Windows Defender	Verified Present
DESKTOP-85BJGT	fe80:d88c596c5403420%12.10.	Yes	Windows Defender	Verified Present
DESKTOP-AMB2RC8	fe80:219c316416ad24fb%5.10.2	Yes	Windows Defender	Verified Present

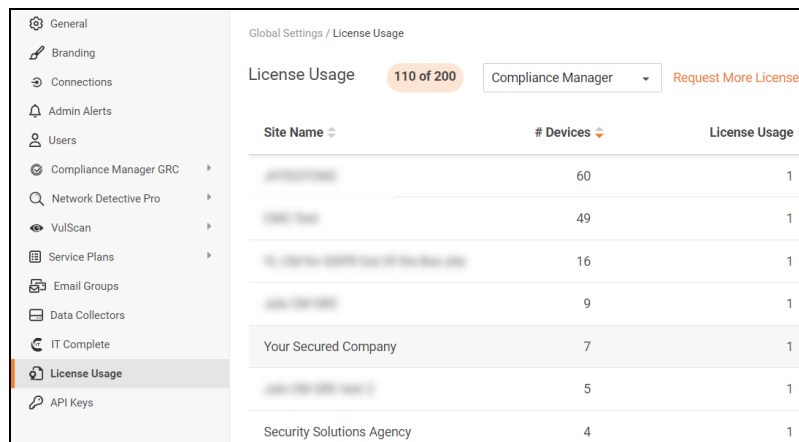
0 required remaining

Save Save and Return Return

License Usage (Global Settings)

From **Global Settings > License Usage**, you can see a breakdown of your available licenses for Compliance Manager.

Here you can see a license usage for each site – including the number of computers identified at the site during the most recent scan. Contact your sales representative to request additional licenses.



Site Name	# Devices	License Usage
[REDACTED]	60	1
[REDACTED]	49	1
[REDACTED]	16	1
[REDACTED]	9	1
Your Secured Company	7	1
[REDACTED]	5	1
Security Solutions Agency	4	1

A Site License will be automatically consumed whenever the number of detected devices exceeds 250. For example:

- When 0 to 250 devices are detected, one Site License will be used
- When 251 Devices are detected, a second Site License will be used
- When 501 Devices are detected, a third Site License will be used, and so on

Use the drop-down menu to filter between Compliance Manager, VulScan, and Cyber Hawk site license usage.

