NETWORK DETECTIVE™

# QUICK START GUIDE

## Microsoft Cloud Assessment

Instructions to Perform a Microsoft Cloud Assessment

11/2/2023 4:50 PM

# Contents

# Performing a Microsoft Cloud Assessment

## Microsoft Cloud Assessment Overview

Network Detective's **Microsoft Cloud Assessment Module** combines 1) automated data collection with 2) a structured framework for documenting your assessment. To perform a Microsoft Cloud Assessment, you will:

- Download and install the required tools
- Create a site and set up a Microsoft Cloud Assessment project
- Collect Microsoft Cloud Assessment data using the Network Detective Checklist
- Generate Microsoft Cloud Assessment reports

## What Does the Microsoft Cloud Assessment Cover?

This module helps you manage and assess risk across your entire Microsoft Cloud Assessment deployment. It assesses and documents several components, including:

- Microsoft 365 Cloud Services
  - Office 365
  - Teams
  - SharePoint
  - OneDrive (does not scan file content)
  - Outlook/Exchange (does not scan email content)
- Microsoft Azure Cloud Services
  - Azure Active Directory
  - Azure Infrastructure Data Collection (applications, virtual machines, services)

## What Does the Microsoft Cloud Assessment Do?

As the computing world steadily moves more resources into the Cloud, it's getting increasingly difficult for MSPs and other IT professionals to manage assets and configurations that are no longer physically present . . . and that they don't have complete

control over. By periodically running a full assessment on each Microsoft Cloud environment, MSPs can provide themselves, and their clients, with essential reports that will help control the flow, privacy, and security of the organization's data.

Having all this information, organized and at your fingertips, is essential for:

- A new technician who's trying to get a handle on the Microsoft Cloud environment
- A Cloud administrator who is trying to hunt down a misconfiguration that's causing problems
- An MSP who needs to scope a proposal for a prospective new client
- Curbing the sprawl and potential HR headaches of Teams, SharePoint, and OneDrive

# What You Will Need

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

**Note:** You can access these at https://www.rapidfiretools.com/nd.

| Microsoft Cloud Assessment Component | Description |
|---|---|
| **Network Detective** | The Network Detective Application and Reporting Tool guides you through the assessment process from beginning to end. You use it to create sites and assessment projects, configure and use appliances, import scan data, and generate reports. The Network Detective Application is installed on your workstations/laptops; it is not intended to be installed on your client or prospect sites. |
| **Admin Credentials for Microsoft 365 tenant to be assessed (OAUTH method)** | You must have admin credentials for an admin role user who is a member of the Microsoft 365 tenant to be assessed. You will use these credentials to grant permission for Network Detective to connect to the Microsoft Graphs API. The following roles have been verified to work to create this connection:<br><br>• **Privileged role admin** (Recommended)<br>• **Cloud application admin** (Recommended)<br>(Using one these roles will only grant permissions to the individual users who enter their credentials to perform the scan.)<br>• **Global admin** (Using the Global admin role will grant scanning permissions to all non-admin users in the Microsoft 365 tenant who have access to the Site in Network Detective.)<br><br>**If you attempt to sign in with another type of admin role than those listed above, you will be unable to grant the necessary permissions.**<br><br>See Assign Admin Roles in the Microsoft 365 documentation for more details. |

Follow these steps to perform a Microsoft Cloud Assessment:

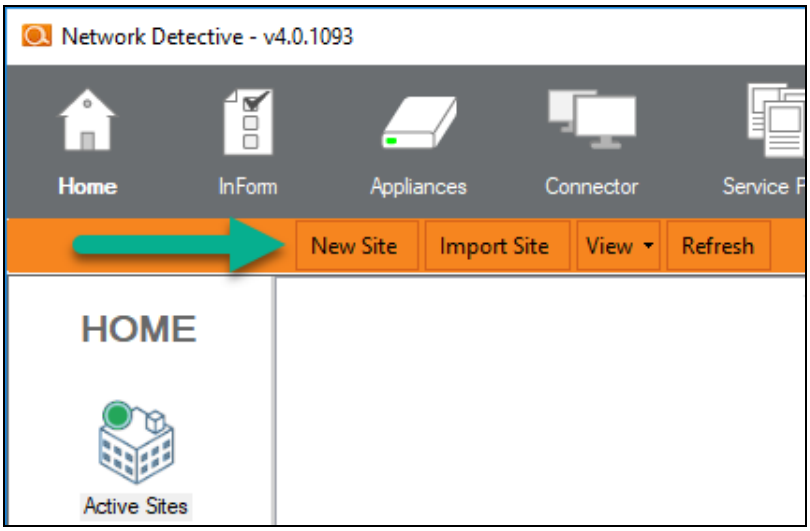
## Step 1 — Download and Install the Network Detective Application

1. Visit https://www.rapidfiretools.com/nd. Download and install the Network Detective Application.
2. Open the app and log in using your credentials.

## Step 2 — Create a New Site

To create a new site:

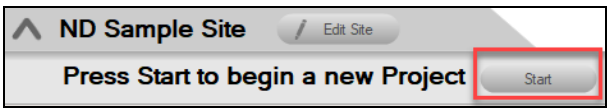
1. Click **New Site** to create a new Site for your assessment project.



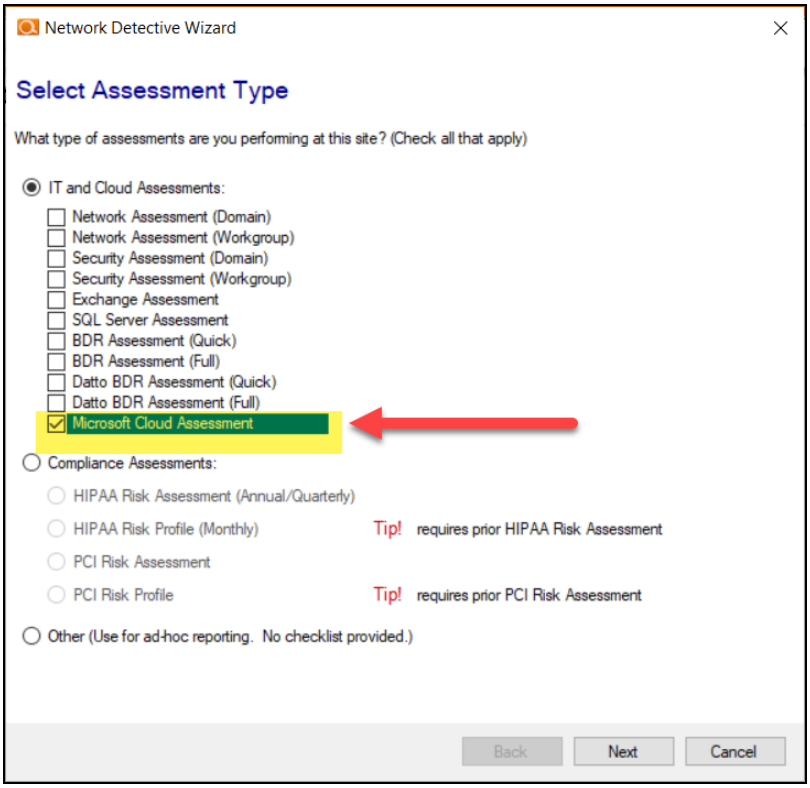

2. Enter a **Site Name** and click **OK**.

## Step 3 — Start a Microsoft Cloud Assessment Project

1. From within the Site Window, click **Start** to begin the assessment.



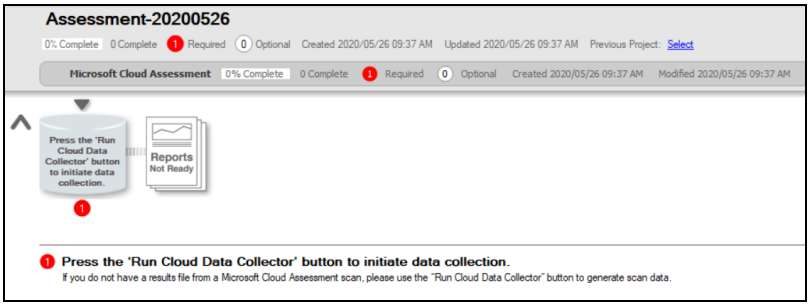
2. Next, select **IT and Cloud Assessments**, and then select Microsoft Cloud Assessment.




3. Then follow the prompts presented in the Network Detective Wizard to start the new Assessment.

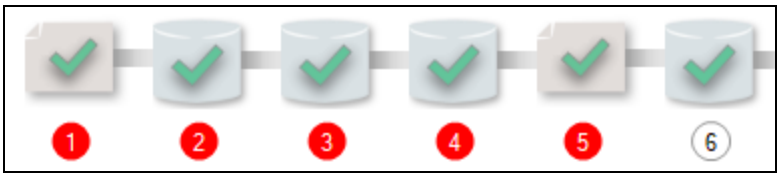
## Use the Microsoft Cloud Assessment Checklist

Once you begin the Microsoft Cloud Assessment, a **Checklist** appears in the Assessment Window. The **Checklist** presents the **Required** 1 and **Optional** 1 steps that are to be performed during the assessment process. The **Checklist** will be updated with additional steps to be performed throughout the assessment process.




Complete the required **Checklist Items** in the exact numerical order presented. Use the **Refresh Checklist** feature to guide you through the assessment process at each step until completion.

When you complete a step, that item will be updated with a green check mark  in the checklist. Different assessment types have a different number of steps to complete.




You may also print a copy of the **Checklist** for reference purposes by using the **Printed Checklist** feature.

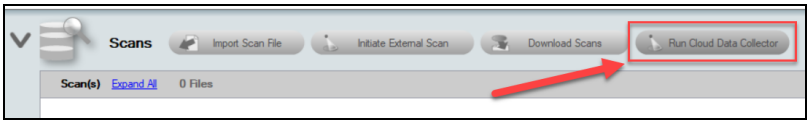

## Step 4 — Run the Cloud Data Collector

See "Modify Report Privacy Options in Microsoft 365 Admin Center" on page 25 to troubleshoot issues with how data appears in your reports.

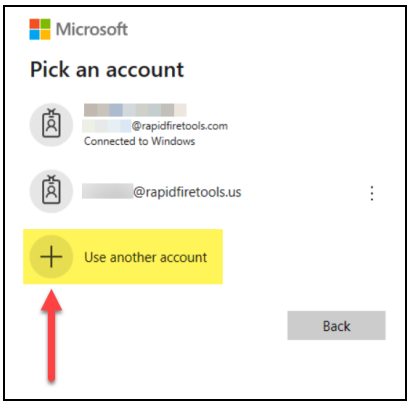
## Perform Scan Using OAUTH Credentials

> **Note:** Before you can Run the Cloud Data Collector, you need admin credentials for the Microsoft 365 tenant to be assessed.

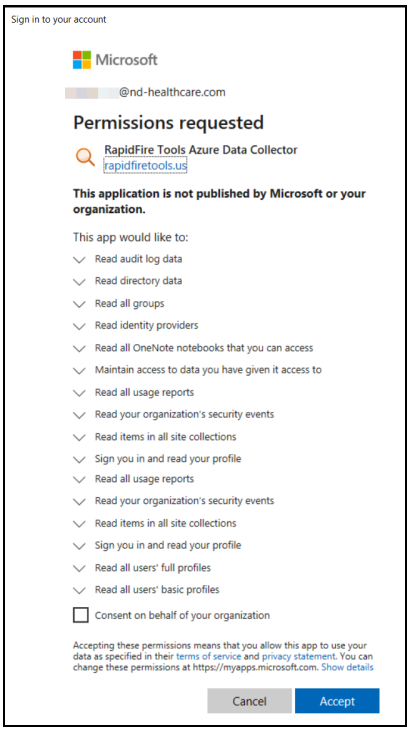
1. To start your assessment, click **Run Cloud Data Collector** under Scans.



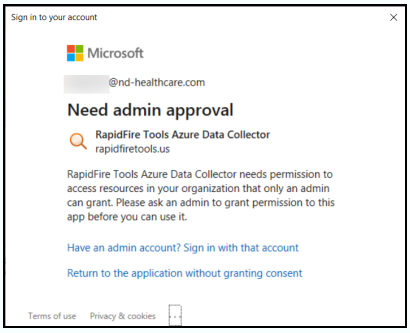

2. A Microsoft login window will appear. Enter admin credentials for the Microsoft Cloud environment to be assessed. To do this, click **Use Another Account**.




3. Consent to the permissions needed for Network Detective to scan the Microsoft Cloud environment. Check the box and click **Accept**.

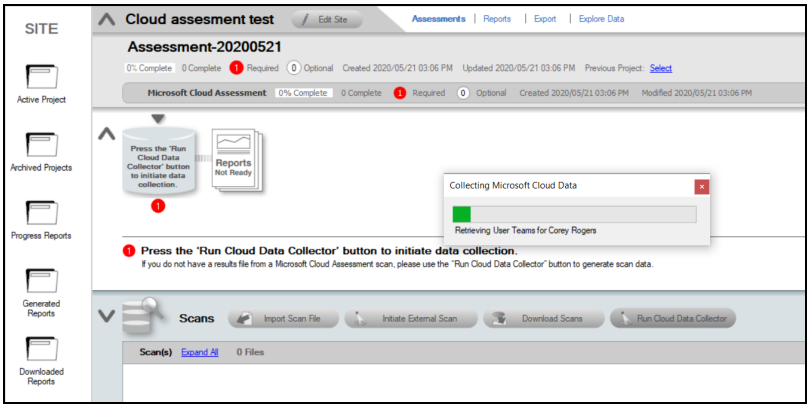



**Note:** If you attempt to sign in with an account that does not have the required admin access, you will be prompted to sign in with an admin account. See "Admin Credentials for Microsoft 365 tenant to be assessed (OAUTH method)" on page 5 for the specific admin roles.

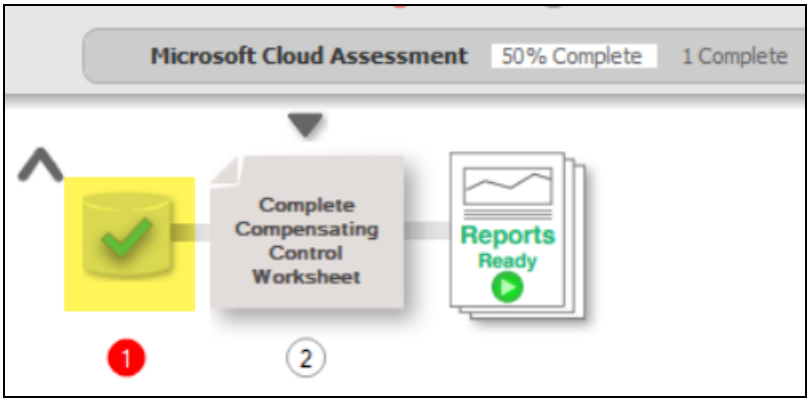



## Scan in Progress

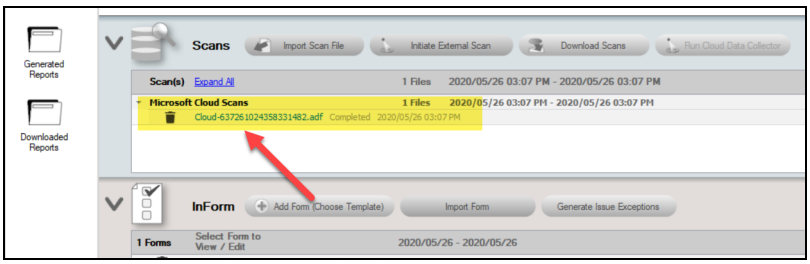
Once you initiate the scan using either method detailed above, the scan will begin and a progress window will appear. This process may take several minutes.



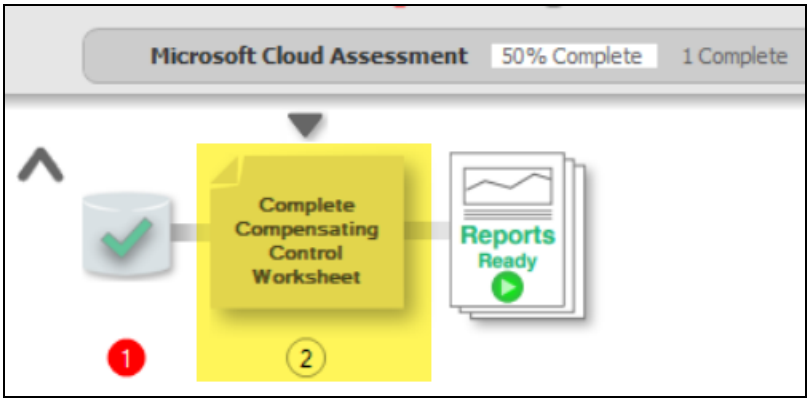

When the scan completes, the "Run Cloud Data Collector" step will be marked complete in the Checklist.



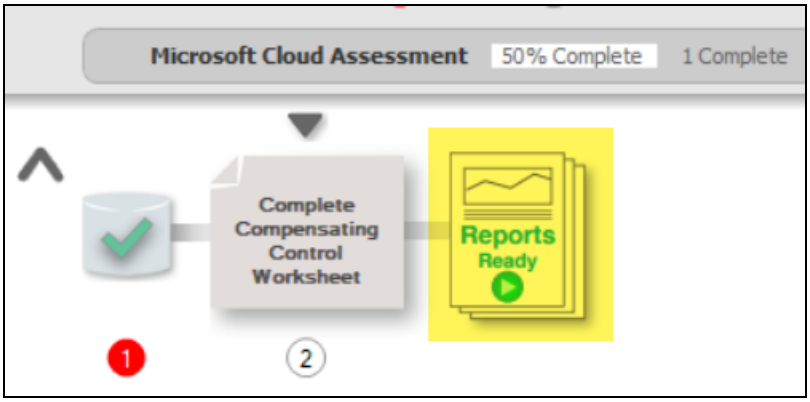

At the same time, the data file will appear in the Scans menu under Microsoft Cloud Scans.




The optional **Compensating Controls Worksheet** will then become available to complete.



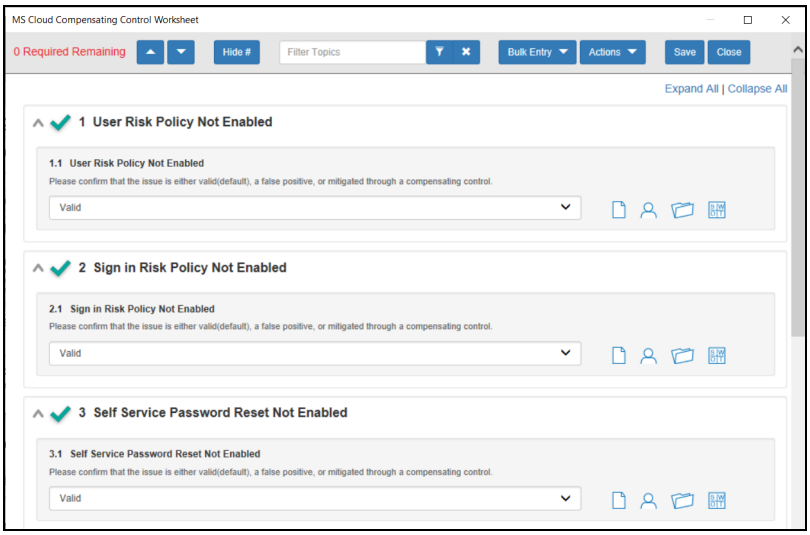

Finally, you can choose to generate reports based on the current scan data without choosing to enter information on Compensating Controls.




## Step 5 — *(Optional)* Document Compensating Controls

Next, complete the optional **Compensating Controls Worksheet** (CCW). While not necessary to generate reports, the CCW details security exceptions that will be (or have been) implemented to mitigate risks in the cloud environment. Here you can document and explain why various discovered items are not true issues and possible false positives.

1. Double click on the **Compensating Controls Worksheet** from the assessment checklist.

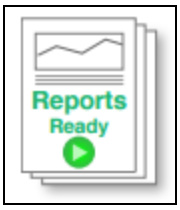



2. Ensure you save your changes to the form before you close it.
3. You may add notes, respondent names, SWOT details, responses, and file attachments.

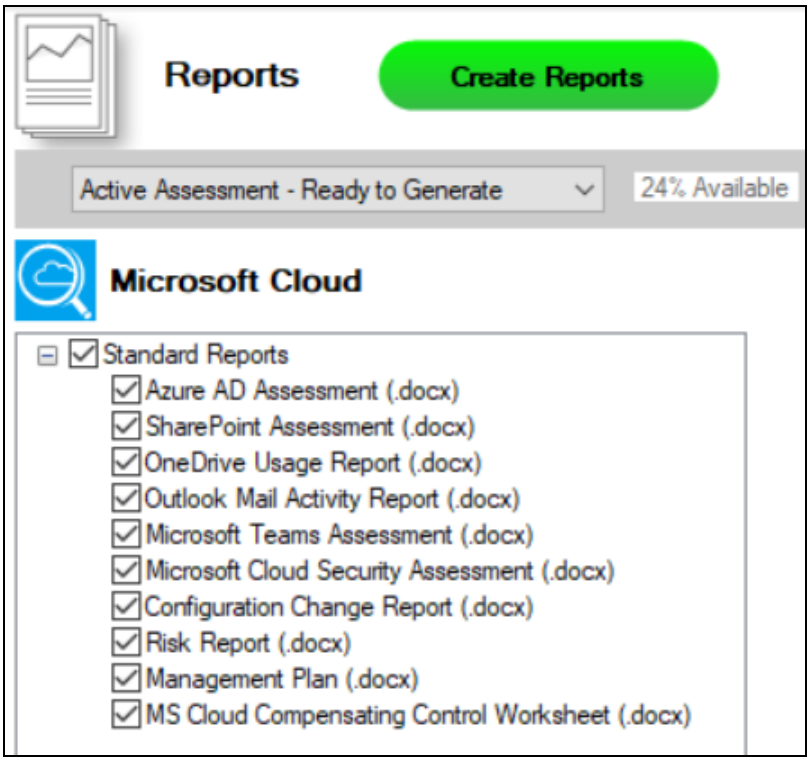
   When you complete all of the fields, this step will appear as complete in the check list.

## Step 6 — Generate Reports

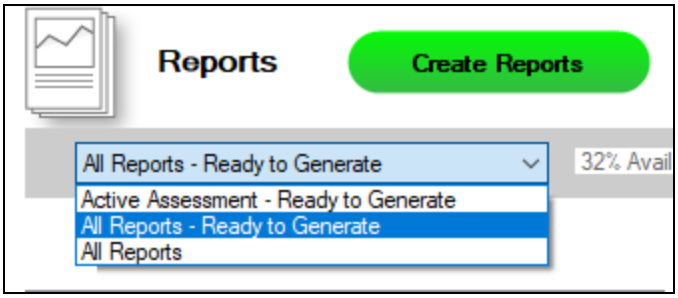
1. From your site, click the **Reports Ready** button at the end of the assessment checklist.




2. Select which of the Microsoft Cloud Assessment reports that you want to generate.

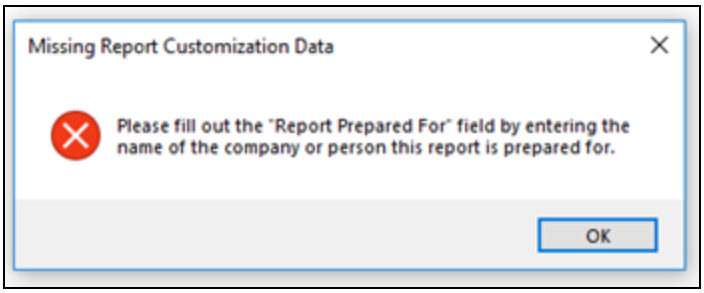



You can use the Reports drop-down menu to filter reports related to the active assessment project, reports that are ready to generate, or to browse all available reports.

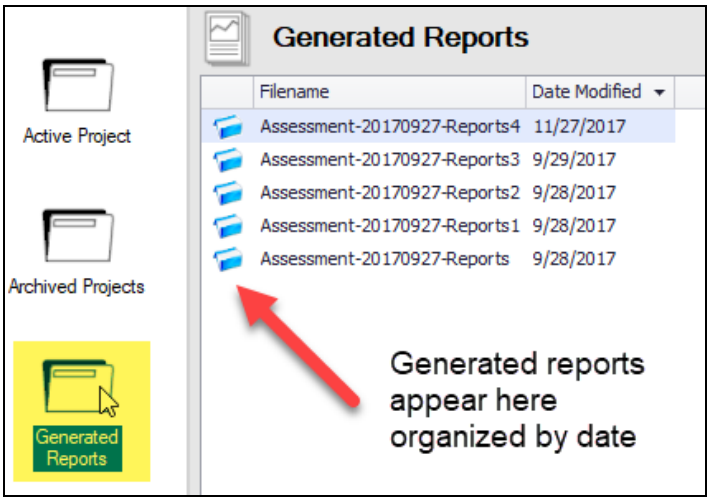



3. Click the **Create Reports** button and follow the prompts to generate the reports you selected.

    i. If you have not previously edited your Report Preferences, you will be prompted to do so before generating reports.




Click **Generated Reports** from the left-hand Site menu to access previously generated reports. Double click a set of assessment reports to open the folder in Windows Explorer.



# Microsoft Cloud Assessment Reports

The Microsoft Cloud Assessment allows you to generate the following reports and supporting documents:

| Report Name | Description |
|---|---|
| **Azure AD Detail Report** | The Azure AD Detail Report goes through the entire Azure Active Directory environment and documents all organizations, domains, and support services that are turned on for the AD environment. Every detail is presented in line-item fashion in an editable report document, including: installed special applications, web URLs to those apps, organizational contacts, distribution lists, proxy addresses, Microsoft service plans and SKUs being used, groups, users, permissions, devices, and more. The report is organized by section with a table of contents 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. |
| **Cloud Management Plan** | The Cloud Management Plan takes issues identified in the Risk Report, organizes them by severity, and includes specific recommendations on how to remediate them. The report's information is pulled directly from the Microsoft controls from multiple Cloud components, including SharePoint, OneDrive, Teams, Azure AD itself. It also identifies other types of issues related to misconfigurations and operations. |
| **Cloud Risk Report** | The Cloud Risk Report, like the Risk Reports in all of our other Network Detective modules, spans all of the Microsoft Cloud components. It includes an overall Risk Score, an overall Issues Score, as well as a summary list of issues discovered. The issues come from both the Microsoft controls as well as other best practices. It identifies specific risks that are due to misconfigurations as well as risks created from turning on or off specific running components. |
| **Compensating Control Worksheet** | The report is used present the details associated with security exceptions and how Compensating Controls will be or have been implemented to mitigate risks in the cloud environment. Here you can explain document and explain why various discovered items are not true issues and possible false positives. The benefit of this feature is that it adds back in the human element into the assessment and allows for explanation of special circumstances and specific environment |

| Report Name | Description |
|---|---|
| | requirements. The Compensating Controls Worksheet does not alleviate the need for safe guards but allows for description of alternative means of mitigating the identified security risk. |
| **Microsoft Cloud Configuration Change Report** | The Microsoft Cloud Configuration Change Report is a very detailed technical report that identifies entity and configuration changes. The changes are grouped by properties, showing the old values vs. the new values, and then the changes are grouped together into bands called “Change Sets.” This report gives you the ability to look at a group of changes together, as well as see how all the properties have changed for that particular time period. This is useful for change management and for capturing and documenting unwanted changes in the event you need to roll back those changes in the user interface. |
| **Microsoft Cloud Security Assessment** | The Microsoft Cloud Security Assessment report brings together all of the security aspects of Microsoft Cloud under one umbrella. It not only includes your own Microsoft Control Score and Secure Score from Microsoft; it also shows your trending against the average score of your peers. |
| **Microsoft Teams Assessment Report** | The Microsoft Teams Assessment Report provides detail about each team in the system, including who the owners are, what channels they have, and what kind of user identity audits have been conducted on the channels. There are individual entries that can be used for audits of the member settings, the guest settings, the message settings, the fun settings, the tab settings. This information goes beyond the Microsoft security score controls and includes other types of misconfigurations that might cause security problems, such as having guest members that are able to remove and delete channels. |
| **OneDrive Assessment Report** | The OneDrive Assessment Report provides a high-level summary report of all OneDrive usage. This is critical to know, since it includes every user the system has, all the Teams, and all the sites created by the client. This overview report gives you a solid handle on how the OneDrive platform is growing, and looks for spikes in that growth that need to be managed. It also looks for spikes in activity that may need to be investigated. The report provides trends over of 30-, 60-, and 90-day increments to give you a solid indicator of storage and bandwidth utilization. |
| **Outlook Mail Activity Report** | The Outlook Mail Activity Report is the perfect complement to the Network Detective Exchange Assessment module, which provides |

| Report Name | Description |
|---|---|
| | deep dive information about Office 365 usage. The Outlook Mail Activity Report provides a high-level summary of what emails are being sent and received by your top 10 active senders and active receivers for the reporting period. This report is meant to be run month-over-month to identify the power users who may need more capacity, and which mailboxes are not being read at all and likely represent recently inactive users that need to be cleaned up. |
| **SharePoint Assessment Report** | The SharePoint Assessment Report is a detailed assessment that shows the total number of sites started under management, how many active SharePoint sites there are, what storage requirements there are, and includes daily trends in the number of sites and storage usage. It then takes the site collections and breaks down all the individual sites so you can understand what is being published in each, how they are organized, and even what groups they contain. Among other things, the report helps understand growth trends and better predicts backup needs. |

# Appendices

Refer to the appendices listed below for the supplementary information referenced in this user guide:

# Pre-Scan Network Configuration Checklist

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

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

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

## Checklist for Domain Environments

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

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

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

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

## Checklist for Workgroup Environments

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

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

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

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

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

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

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

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

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

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

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

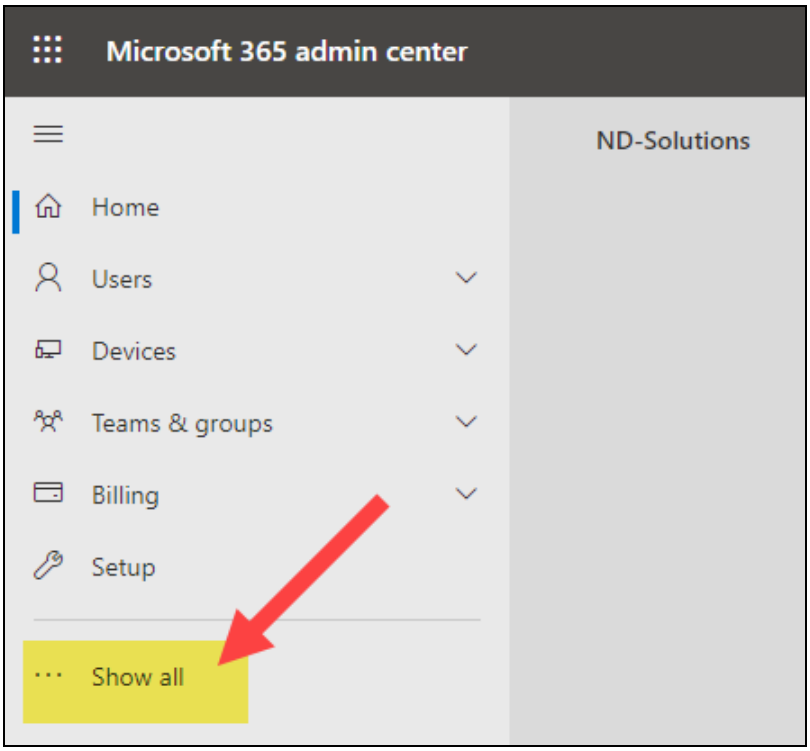
| Complete? | Workgroup Configuration |
|---|---|
| | **Network Settings** |
| ☐ | • *Admin$* must be present on the computers you wish to scan, and be accessible with the login credentials you provide for the scan |
| ☐ | • *File and printer sharing* must be enabled on the computers you wish to scan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

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

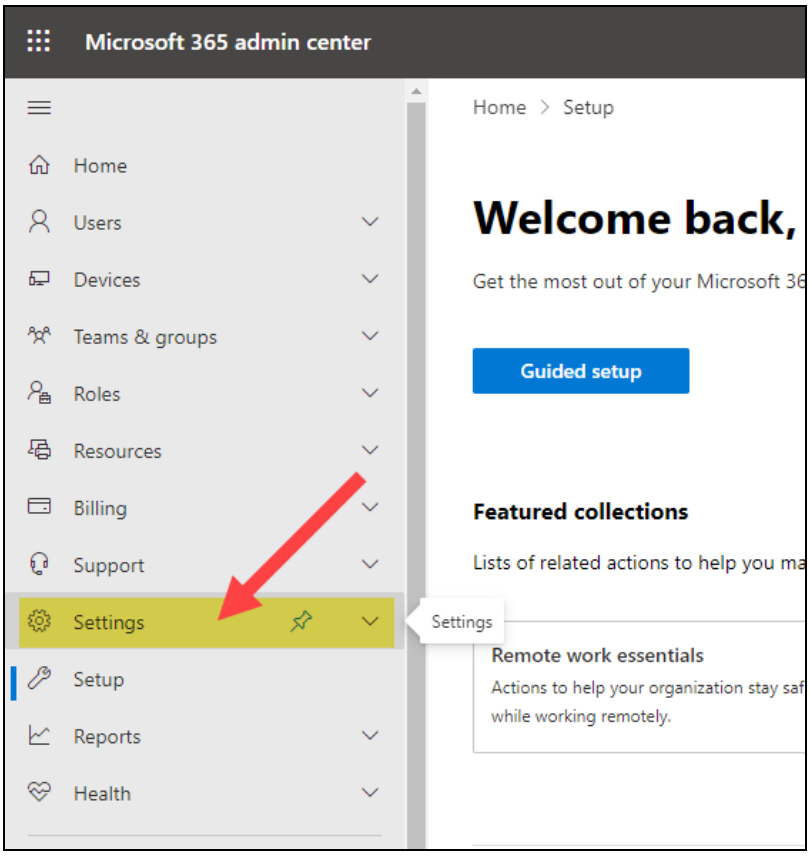
# Modify Report Privacy Options in Microsoft 365 Admin Center

By default, the Microsoft Cloud will conceal user information such as usernames, groups, and sites for certain reports. This can affect how data is presented in your Microsoft Cloud Assessment reports. If you are missing details in your reports, follow these steps to resolve the issue:

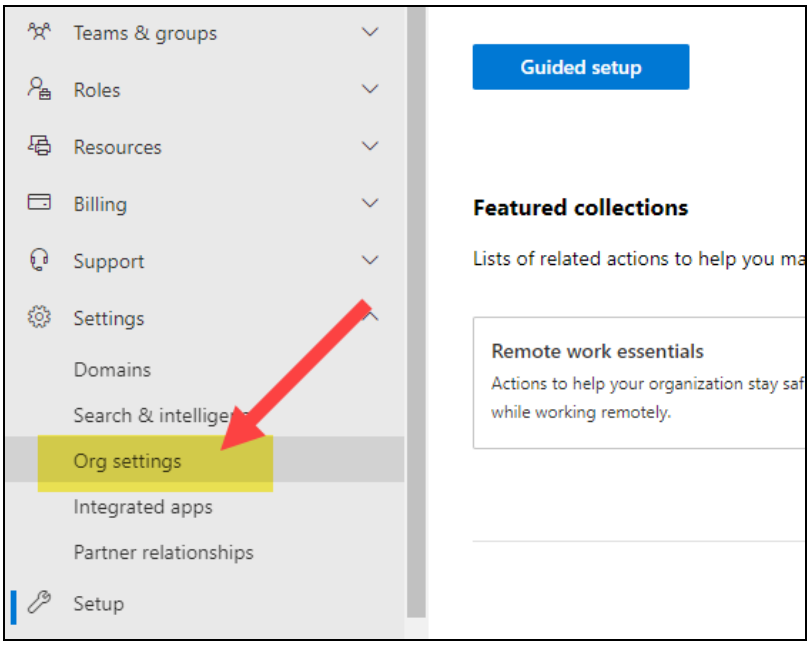
1. From your browser, access the Microsoft 365 admin center at admin.microsoft.com.
2. From the home page, click **Show all** from the side menu.



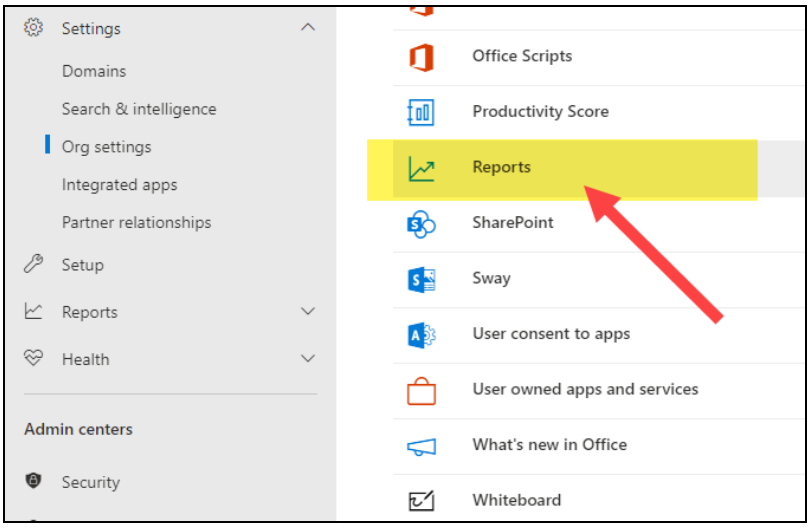

3. Then click **Settings**.




4. Then open **Org settings**.




5. From the list of Services, scroll down and click **Reports**.




6. From the right-hand menu, **DESELECT** the **Display concealed user, group, and site names in all reports** option. Then click **Save**. Disabling this option will ensure your Microsoft Cloud Assessment reports have more detailed data.