# Microsoft Compliance Configuration Analyzer

## Overview

MCCA is a tool which, on execution, generates a report highlighting known issues in your compliance configurations in achieving data protection guidelines and recommends best practices to follow.

### What is Microsoft Compliance Configuration Analyzer (MCCA)?

It is a PowerShell-based utility that will fetch your tenant’s current configurations & validate these configurations against Microsoft 365 recommended best practices. These best practices are based on a set of controls that include key regulations and standards for data protection and general data governance. MCCA then provides you with an actionable status report for improving your compliance posture.

### Why should I use it?

Often tenants face challenges in diagnosing their compliance posture & ensuring that they have the right configurations in place to protect their environment completely. These are largely manual processes which tend to be time consuming & allow for human error. Furthermore, with the evolving compliance landscape the risk of blind spots also increases.

MCCA is a diagnostic tool that will report the status of your current configurations. This allows you to focus efforts more on making the right configurations.

### What is in scope?

This version will provide you recommendations for the M365 Compliance solutions listed below. We will keep adding more solutions & richer recommendations in future versions of this tool.

1. Microsoft Information Protection
   1. [Data Loss Prevention](https://docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention-policies?view=o365-worldwide)
   2. [Information Protection](https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-teams-groups-sites?view=o365-worldwide)
2. Microsoft Information Governance
   1. [Information Governance](https://docs.microsoft.com/en-us/microsoft-365/compliance/manage-information-governance?view=o365-worldwide)
   2. [Records Management](https://docs.microsoft.com/en-us/microsoft-365/compliance/records-management?view=o365-worldwide)
3. Insider Risk
   1. [Communication Compliance](https://docs.microsoft.com/en-us/microsoft-365/compliance/communication-compliance?view=o365-worldwide)
   2. [Insider Risk Management](https://docs.microsoft.com/en-us/microsoft-365/compliance/insider-risk-management?view=o365-worldwide)
4. Discovery & Response
   1. [Audit](https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance?view=o365-worldwide)
   2. [eDiscovery](https://docs.microsoft.com/en-us/microsoft-365/compliance/ediscovery?view=o365-worldwide)

## That is awesome! How do I run it?

### Pre-Requisites

Before running the tool, you should confirm your [Microsoft 365 subscription](https://www.microsoft.com/microsoft-365/compare-all-microsoft-365-plans) and any add-ons. To access and use MCCA, your organization must have one of the following subscriptions or add-ons:

* Microsoft 365 E5 subscription (paid or trial version)
* Microsoft 365 E3 subscription + the Microsoft 365 E5 Compliance add-on

You will be able to run this tool without an E5 subscription or M365 E5 Compliance add-on, but MCCA will still report statuses for E5 workloads & capabilities.

For running the tool:

1. You must have PowerShell version 5.1 or above to run this tool.
2. You must have Exchange Online PowerShell module (You can follow either of the following 2 methods to download the same)

* Exchange Online PowerShell V2 module that is available via the PowerShell gallery:

Install-Module -Name ExchangeOnlineManagement

* Exchange Online PowerShell module (<http://aka.ms/exopsmodule>)

1. You must have appropriate role/user permissions to be able to run this tool. The following table provides details of which roles will have access to which sections of the report.

Other roles within the organisation (not listed in the table below) may not be able to run the tool or they may be able to run the tool with limited information in the final report.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| User Role | MIP | | MIG | | Insider Risk | | Discovery & Response | |
| **DLP** | **IP** | **IG** | **RM** | **IRM** | **CC** | **Audit** | **eDiscovery** |
| Azure Information Protection admin | No | No1 | No | No | No | No | No4 | No |
| Compliance admin | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Compliance Data Admin | Yes | Yes2 | Yes | Yes | Yes | Yes3 | Yes5 | No |
| Customer Lockbox access approver | No | No | No | No | No | No | No | No |
| Exchange Admin | No | No1 | No | No | No | No | No4 | No |
| Global reader | Yes | Yes | Yes | Yes | No | No | Yes | No |
| Helpdesk admin | No | No1 | No | No | No | No | No4 | No |
| Non-Admin User | No | No | No | No | No | No | No | No |
| Reports reader | No | No | No | No | No | No | No | No |
| Security admin | Yes | Yes2 | No | No | No | No | Yes5 | No |
| Security operator | Yes | No | No | No | No | No | Yes5 | No |
| Security reader | Yes | Yes**2** | No | No | No | No | Yes5 | No |
| Service support admin | No | No | No | No | No | No | No | No |
| SharePoint admin | No | No | No | No | No | No | No | No |
| Teams service admin | No | No | No | No | No | No | No | No |
| User admin | No | No | No | No | No | No | No | No |

Exceptions:

1 – User will not be able generate report for IP apart from “Use IRM for Exchange Online” section.

2 – User will be able generate report for IP apart from “Use IRM for Exchange Online” section.

3 – User will be able generate report for IP apart from “Enable Communication Compliance in O365” section.

4 – User will not be able generate report for IP apart from “Enable Auditing in Office 365” section.

5 – User will be able generate report for IP apart from “Enable Auditing in Office 365” section.

### Install Guide

#### Step 1: Download & unzip MCCA

First, you will need MCCA ([link](https://microsoft-my.sharepoint.com/:f:/p/karashah/Et_vgioEZWJGie3qN2EDGKABVt-tIP-JIvcGxkRoxzMXcw?e=yLbKef)). Download and then unzip the MCCA folder to a location of your preference (Say C:\ drive)

#### Step 2: Open PowerShell or EOM Shell

If you are a non-MFA enabled user then you may directly run the following commands from PowerShell.

If you are a MFA-enabled user then you will need the Exchange Online Management Shell (<http://aka.ms/exopsmodule>).

* For Non-MFA users:
  + Open PowerShell in administrator mode
* For MFA users
  + Open Exchange Online Management Shell

#### Step 3: Run MCCA

Next you need to run a set of commands to get the MCCA report.

Within the console navigate to the location you unzipped the MCCA folder in Step 1.

cd C:\MCCA

Import MCCA

Set-ExecutionPolicy -ExecutionPolicy Bypass -Scope Process

.\RunMCCAReport.ps1

#### Step 4: Generate MCCA Report

Use the following cmdlet to generate the MCCA report.

Get-MCCAReport

This will generate a report based on the geolocation of your tenant. If an error occurs while fetching your tenant’s geolocation, you will get a report covering all supported geolocations.

You can learn more about this cmdlet by running the following.

Get-Help Get-MCCAReport

### Input Parameters

You can also get a tailored report based on specific input parameters listed below.

1. **Geolocation**

Get-MCCAReport -Geo @(1,7)

This will generate a report based on the geolocations entered by you.

You need to input appropriate numbers from the following list corresponding to the regions.

|  |  |
| --- | --- |
| Input | Region |
| 1 | Asia-Pacific |
| 2 | Australia |
| 3 | Canada |
| 4 | Europe (excl. France) / Middle East / Africa |
| 5 | France |
| 6 | India |
| 7 | Japan |
| 8 | Korea |
| 9 | North America (excl. Canada) |
| 10 | South America |
| 11 | South Africa |
| 12 | Switzerland |
| 13 | United Arab Emirates |
| 14 | United Kingdom |

**Note:** As an add-on, the report will always include MCCA supported international sensitive information types like SWIFT Code, Credit Card Number etc.

1. **Solutions**

Get-MCCAReport -Solution @(1,7)

This will generate a report only for the solutions entered by you.

You need to input appropriate numbers from the following list corresponding to the solution.

|  |  |
| --- | --- |
| Input | Solution |
| 1 | Data Loss Prevention |
| 2 | Information Protection |
| 3 | Information Governance |
| 4 | Records Management |
| 5 | Communication Compliance |
| 6 | Insider Risk Management |
| 7 | Audit |
| 8 | eDiscovery |

1. **Multiple Parameters**

Get-MCCAReport -Solution @(1,7) -Geo @(9)

This will generate a report only on for the solutions entered by you and based on the regions you have selected.

In either of the case, there will be a prompt to enter your credentials. Once you enter your credentials, MCCA will run for a while and an HTML report will be generated.

### License

We use the following open source components in order to generate the report:

* Bootstrap, MIT License - <https://getbootstrap.com/docs/4.0/about/license/>
* Fontawesome, CC BY 4.0 License - <https://fontawesome.com/license/free>
* clipboard.js v1.5.3, MIT License - <https://cdn.jsdelivr.net/clipboard.js/1.5.3/clipboard.min.js>

## Frequently Asked Questions (FAQ)

### Will this tool make any changes to my existing settings, policies, etc.?

MCCA is a diagnostic tool that is “read-only”. It fetches information about your current configurations to generate a report but will not alter any of your existing configurations.

### What different sections do I see in my report?

The report provides you with:

* Solutions summary: It provides a break-down of statuses at a solution level. Each solution has counters that tell you how many recommendations are informational, require improvement and are OK.
* Solution drill-down: Following solutions summary, each solution has a separate section that provides detailed information about configurations & their status.
  + Each solution may have 1 or more improvement actions which will further be broken down into finer configurations. MCCA will provide you a status both at an improvement action level & also for finer configurations.

### Can I generate report for specific sections within the report?

Yes, you can generate report for specific sections within the report. You can use the solution input parameter (–solution <input solution number>) to generate the report for a specific solution from the following list:

|  |  |
| --- | --- |
| Input | Solution |
| 1 | Data Loss Prevention |
| 2 | Information Protection |
| 3 | Information Governance |
| 4 | Records Management |
| 5 | Communication Compliance |
| 6 | Insider Risk Management |
| 7 | Audit |
| 8 | eDiscovery |

For e.g. If you wanted to create report for the DLP solution only then you can run the following command:

Get-MCCAReport –solution @(1)

You can learn more about this input parameter in the Input Parameters section within the Install Guide above.

### What does Recommendation, Informational, Improvement & OK messages mean?

All recommendations provided by MCCA report are categorized in 3 types of status:

1. Recommendations: These are best practices that your tenant should follow.   
   *Note: The support for these messages is limited in the current version so you may not see any recommendations in your report.*
2. Informational: These messages/statuses represent information in your current environment & are non-actionable in nature.
3. Improvement: These messages/statuses highlight areas that need your attention & are actionable. Sections which are marked as “Improvement” would generally have 1 or more configurations marked as “Improvement”.
4. OK: These messages/statuses indicate that a given area is configured efficiently to meet data protection baselines.

### Why don’t I see my tenant’s name on the report?

Due to a technical error, the tool would not have been able to fetch your tenant’s name. In the event of such error, you may not see your tenant name on the report. Please try running the tool again after some time. If the issue persists, please reach out to us at [MCCAhelp@microsoft.com](mailto:mecahelp@microsoft.com) and/or contact your Microsoft partner.

### Why do I see “No active policy defined” when I already have policies defined?

The policies created by you may be protecting a subset of information, workloads, user groups and/or other criteria. “No active policy defined” highlights the areas that are not protected by your current policies and need an action on your part.

We provide “Remediation Scripts” which you can run from your PowerShell console & the required policies will automatically be set up.

Please refer to “Remarks” section in your report to understand why you are seeing “Improvement”. If you still have concerns, please reach out to us at [MCCAhelp@microsoft.com](mailto:mecahelp@microsoft.com) or contact your Microsoft partner.

### Why do I see “Policy defined but not protected on 1 or more workloads” when I already have policies defined?

Often there is a case where a given area (sensitive information, workloads, user groups and/or other criteria) may be protected in 1 or more policies in your environment but would not be protected across your entire environment.

E.g. Your current policy configurations may U.S. / U.K. Passport Number on SharePoint & Exchange but not on OneDrive & Teams. This puts you at risk.

To avoid such cases, MCCA will highlight all the affected areas. You will need to review these and either tweak your current policies and/or create new ones to accommodate these areas.

### What are remediation scripts?

When MCCA identifies if your current policies have zero coverage for certain sensitive information types, it provides you with “Remediation Scripts” to help you avoid the hassle of manually setting up these policies. These policies will be created in *Test* mode and you will still have review & enable it manually.

You should review script parameters & then run these scripts from your *Windows PowerShell ISE* console. You would need to connect to [Connect to Security & Compliance Center PowerShell](https://docs.microsoft.com/en-us/powershell/exchange/connect-to-scc-powershell?view=exchange-ps) or [Connect to Exchange Online Center PowerShell](https://docs.microsoft.com/en-us/powershell/exchange/connect-to-exchange-online-powershell?view=exchange-ps) to execute these scripts. On successful execution of the scripts, the required policies will automatically be set up.

Note: These scripts are pre-configured and may need tweaking to achieve best results for your organization. We are working on improving these scripts in future versions of this tool.

### Why is the report asking me to protect Sensitive Information Types which I do not have in my environment?

This version of the tool aims to protect all possible sensitive information types across multiple geographies and/or industries.

Future versions of this tool will provide recommendations to you based on the nature of information you have in your environment.

### Can I generate the report to get recommendations for Sensitive Information Types applicable to my tenant’s geographic regions?

Yes, you can generate the report for specific geographic regions.

By default, the tool will generate a report based on the geolocation for your tenant. If you wish to run the report for specific geos then while running the *Get-MCCAReport* cmdlet, you can input an extra parameter by *–Geo* followed by 1 or more region numbers supported by MCCA.

Please refer the *Install Guide* section above for more detailed steps.

### How do I save my report?

Please use the “Print” button provided on top right corner of the report to export a PDF (subject to your browser and/or system support for printing as a PDF) or print a physical copy of your report.

### This tool is awesome! How do I provide feedback and suggestions for future versions?

Please share your feedback & suggestions with us at [MCCAhelp@microsoft.com](mailto:mecahelp@microsoft.com). Alternatively, reach out to your Microsoft partner to share your feedback and suggestions.

### My issue is not listed here. I am facing issues in running the tool and/or interpreting the report, what do I do?

Please share your concerns with us at [MCCAhelp@microsoft.com](mailto:mecahelp@microsoft.com). Alternatively, reach out to your Microsoft partner and we will help you solve your issue at the earliest.