

# M365 DLP Migration Assistant (v1.0): User Guide

## Contents

M365 DLP Migration Assistant: User Guide .....	1
Introduction.....	2
What is M365 DLP Migration Assistant? .....	2
Migration tasks that M365 DMA performs .....	2
How does the M365 DLP Migration Assistant work? .....	3
Understanding mapping of Symantec DLP elements to M365 DLP elements.....	4
Before You Start.....	8
A. Have Appropriate M365 Subscription .....	8
B. Have Appropriate User Role & Privileges.....	8
C. Install Exchange Online Management PowerShell Module .....	8
D. Export Symantec DLP Policies.....	8
Installation Steps.....	9
Start Migration .....	12
Step 1: Log into your account.....	13
Step 2: Upload your Symantec policy .....	15
Step 3: Review policy mapping .....	17
Step 4: Optimize & Fix validation errors (if any).....	21
Step 5: Extend Coverage.....	23
Step 6: Connect & import policy .....	24
View your migration report!.....	25
Output PowerShell scripts & rule package XMLs.....	27
Next Steps: After policy import.....	28
Reporting Errors & Providing Feedback.....	30
Telemetry Notice .....	30

## Introduction

---

Welcome to the User Guide for the M365 DLP Migration Assistant (MDMA). Here you will find all details about the MDMA tool along with step-by-step instructions on using MDMA to migrate your policies to Microsoft's Unified DLP Platform.

## What is M365 DLP Migration Assistant?

---

The MDMA tool is a Windows based desktop application that will migrate your DLP policies from other DLP platforms to our Unified DLP platform.

Our tool takes you through a simple five-step migration process. It accepts Symantec DLP policy XML exports, performs mapping, and creates equivalent Unified DLP policies through PowerShell scripts.

You can safely use the MDMA tool to create DLP policies in test mode, which does not affect your live data or interact with current environment.

## Migration tasks that M365 DMA performs

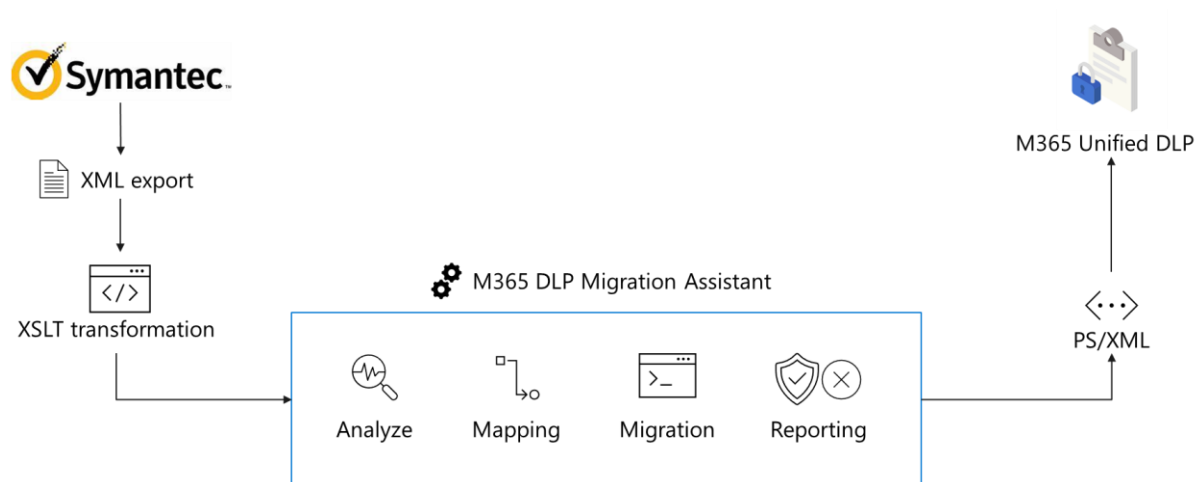
---

MDMA takes over many of the difficult or tedious tasks involved in a DLP migration project:

- In traditional migration scenario, you need to perform feasibility analysis between source & target DLP platforms, map features, migrate policies manually, and test and tweak DLP policies. Your migrated DLP policies can be up and running within minutes of starting the M365 DMA process.
- With M365 DMA, you can scale up your migration project quickly from moving a single policy manually to multiple policies at the same time.
- M365 DMA automatically identifies Sensitive Information Types (SITs) or Data Identifiers in source policies and creates Custom SITs in your Microsoft tenant moving over all your custom regular expressions and keywords in a few clicks.
- M365 DMA detects which conditions, exclusions & actions are currently being used in source policies and automatically creates new rules with the same conditions, exclusions & actions.
- M365 DMA provides you with a detailed migration report with policy wise migration status and recommendations.
- M365 DMA ensures that your DLP policy migration project is completely private and takes place within the boundaries of your organization.
- M365 DMA supports policy migration from Symantec Data Loss Prevention 15.7 or earlier.

## How does the M365 DLP Migration Assistant work?

The following diagram illustrates the MDMA migration process.



During a given instance of migration, the M365 DLP Migration Assistant works in five phases:

1. Input  
*MDMA ingests one or more Symantec DLP policy XML files.*
2. Analyze  
*MDMA interprets the files & identifies Symantec DLP policy constructs.*
3. Rationalize  
*MDMA maps the identified Symantec DLP policy constructs to Unified DLP capabilities. It performs validations for Unified DLP platform limitations.*
4. Migrate  
*MDMA executes PowerShell scripts for the DLP scenarios identified & supported by the UDLP platform.*
5. Reporting  
*MDMA provides the user with a detailed migration report about which policies were migrated successfully, partially and/or not migrated. It also provides recommendations to improve the migration fidelity further.*

## Understanding mapping of Symantec DLP elements to M365 DLP elements

The following section describes how MDMA translates different policy elements from Symantec DLP to M365 DLP.

### Supported Workloads

MDMA migrates policies into MIP only for the workloads listed in the following table.

Workload	MDMA Support
Exchange (EXO)	Yes
Share Point Online (SPO)	Yes (Limited)
One Drive for Business (ODB)	Yes (Limited)
Teams Chat and Channel messages	Yes (Limited)
Devices	Yes (Limited)
Microsoft Cloud App Security (MCAS)	Yes (Limited)

For workloads other than Exchange (EXO), MDMA provides the ability to create simple policies with the 'Content contains Sensitive Information' condition scoped to the entire tenant.

### Classification Elements

The following table details the mapping of classification elements that MDMA uses while translating Symantec DLP policies.

Symantec Classification Element	M365 DLP Classification Element
Regular Expression	Create new custom SIT with regular expression.
Keyword	Create new custom SIT with a keyword list or keyword dictionary.
Keyword Pair	Create new custom SIT with first keyword list as primary element & second keyword list as a supporting element with 300 char proximity.
Data Identifier	Map to OOB SIT if equivalent available else, create new custom SIT.
Classification	Not supported

The following table details the mapping of optional validators for Sensitive Information Types (a.k.a. Data Identifiers in Symantec DLP) that MDMA uses while translating Symantec DLP policies.

Symantec Optional Validators	M365 DLP Optional Validators
Exclude exact match	Exclude specific matches
Exact Match Data Identifier Check	NA
Exclude beginning characters	Starts or does not start with characters
Exclude ending characters	Ends or does not end with characters
Exclude prefix	Include or Exclude prefixes
Exclude suffix	Include or Exclude prefixes

Number Delimiter	NA
Require beginning characters	Starts or does not start with characters
Exact Match	NA
Duplicate digits	Exclude duplicate characters
Require ending characters	Ends or does not end with characters
Find keywords	Available as both primary & supporting elements

### *Regular Expressions – Potential validation issues to be aware of*

When you upload your rule package XML file, the system validates the XML and checks for known bad patterns and obvious performance issues. Here are some known issues that the validation checks for — a regular expression:

- Cannot begin or end with alternator "|", which matches everything because it's considered an empty match.
  - For example, "|a" or "b|" will not pass validation.
- Cannot begin or end with a "{0,m}" pattern, which has no functional purpose and only impairs performance.
  - For example, "{0,50}ASDF" or "ASDF.{0,50}" will not pass validation.
- Cannot have "{0,m}" or "{1,m}" in groups, and cannot have ".\*" or ".\*" in groups.
  - For example, "{0,50000}" will not pass validation.
- Cannot have any character with "{0,m}" or "{1,m}" repeaters in groups.
  - For example, "(a\*)" will not pass validation.
- Cannot begin or end with "{1,m}"; instead, use just "."
  - For example, "{1,m}asdf" will not pass validation; instead, use just ".asdf".
- Cannot have an unbounded repeater (such as "\*" or "+") on a group.
  - For example, "(xx)\*" and "(xx)+" will not pass validation.

### *Condition and Exception Mapping*

The following table details the mapping of condition and exception elements for Exchange (EXO) workload that MDMA uses while translating Symantec DLP policies.

- *Exchange Workload*

Condition/Exception in Symantec	Condition/Exception in M365 DLP
Content Matches Regular Expression	Content contains SIT
Content Matches Keyword	Content contains SIT
Content Matches Data Identifier	Content contains SIT
Content Matches Classification	Not supported
File Properties	Not supported

Message Attachment or File Type Match	One or more of the following: <ul style="list-style-type: none"> <li>Attachment is password protected</li> <li>Attachment's file extension is</li> </ul>
Message Attachment or File Size Match	Document size equals or is greater than
Message Attachment or File Name Match	One or more of the following: <ul style="list-style-type: none"> <li>Document name contains words or phrases</li> <li>Document name matches patterns</li> </ul>
Message/Email Properties and Attributes	Not supported
Sender/User Matches Pattern	One or more of the following: <ul style="list-style-type: none"> <li>Sender is</li> <li>Sender is a member of</li> <li>Sender domain is</li> <li>Sender address contains words</li> <li>Sender address matches patterns</li> <li>Sender IP address is</li> </ul>
Recipient Matches Pattern	One or more of the following: <ul style="list-style-type: none"> <li>Recipient is a member of</li> <li>Recipient domain is</li> <li>Recipient is</li> <li>Recipient address contains words</li> <li>Recipient address matches patterns</li> </ul>
Sender/User based on a Directory Server Group	Not supported
Recipient based on a Directory Server Group	Not supported
Content Matches Exact Data from an Exact Data Profile (EDM)	Not supported
Content Matches Document Signature from an Indexed Document Profile (IDM)	Not supported
Detect using Vector Machine Learning profile (VML)	Not supported
Protocol Monitoring <ul style="list-style-type: none"> <li>SMTP protocol</li> </ul>	Exchange (EXO) DLP policy

- *Endpoint Devices, SharePoint Online, OneDrive & Other Workloads*

Condition/Exception in Symantec	Condition/Exception in M365 DLP
Content Matches Regular Expression	Content contains SIT
Content Matches Keyword	Content contains SIT
Content Matches Data Identifier	Content contains SIT

Message Attachment or File Type Match	Document's file extension is
Protocol Monitoring <ul style="list-style-type: none"> <li>• HTTP</li> <li>• HTTPS</li> <li>• FTP</li> </ul>	Cross-workload DLP policy(s)
Protocol Monitoring: Endpoint Device Type <ul style="list-style-type: none"> <li>• CD/DVD</li> <li>• Removable storage</li> <li>• Copy to network share</li> <li>• Printer/Fax</li> <li>• Clipboard</li> <li>• Cloud storage</li> <li>• Application File Access</li> <li>• SEP Intensive Protection</li> </ul>	One or more of the following (Devices): <ul style="list-style-type: none"> <li>• Copy to USB removable media</li> <li>• Copy to network share</li> <li>• Copy to clipboard</li> <li>• Print</li> <li>• Upload to cloud service domains or access by unallowed browsers</li> </ul>

### Response Rules

The following table details the mapping of Symantec response rules to M365 DLP actions that MDMA uses while translating Symantec DLP policies.

Symantec Response Rule	M365 DLP Action
Generate DLP Incident	Generate Alert
Logging (Syslog)	Audit logs
Network Prevent: Modify SMTP Message <ul style="list-style-type: none"> <li>• Modify email subject</li> <li>• Modify header</li> </ul>	One or more of the following: <ul style="list-style-type: none"> <li>• Prepend subject</li> <li>• Set headers</li> </ul>
Network Prevent: Block SMTP Message <ul style="list-style-type: none"> <li>• Bounce message to sender</li> <li>• Redirect message to this address</li> </ul>	One or more of the following: <ul style="list-style-type: none"> <li>• Block / Restrict access</li> <li>• Send user notification</li> <li>• Redirect message to</li> </ul>
Send Email Notification	Send User Notification
Endpoint Prevent <ul style="list-style-type: none"> <li>• Notify</li> <li>• Notify with Cancel</li> <li>• Block</li> </ul>	One or more of the following (Endpoint Devices) <ul style="list-style-type: none"> <li>• Notify</li> <li>• Block</li> <li>• Audit</li> </ul>
User Cancel	One or more of the following: <ul style="list-style-type: none"> <li>• Block / Restrict access</li> <li>• User Overrides</li> </ul>

## Before You Start

---

Before you use M365 DLP Migration Assistant (MDMA) for the first time, complete the following tasks:

- A. Check your M365 subscription license
- B. Verify your role & privileges
- C. Install pre-requisite Exchange Online PowerShell module
- D. Export policy XMLs from Symantec DLP

### A. Have Appropriate M365 Subscription

---

To migrate your DLP policies with highest fidelity across all Microsoft workloads (Exchange, SharePoint Online, OneDrive for Business, Teams, Endpoint Devices) as well as third party cloud apps (like Box, Google Drive, etc.), your organization should have one of the following subscriptions:

- Microsoft 365 E5 or Office 365 E5 subscription
- Microsoft 365 E3 subscription with E5 Compliance add-on

### B. Have Appropriate User Role & Privileges

---

You need to have a *Global Administrator* or *Compliance Administrator* role to be able to use MDMA.

### C. Install Exchange Online Management PowerShell Module

---

You need to have the Exchange Online Management PowerShell module installed on the same machine where MDMA will be installed to be able to successfully run the scripts that MDMA generates.

To install, please follow these steps:

1. Open PowerShell in Administration mode
2. Run the following command:

```
Install-Module ExchangeOnlineManagement
```

### D. Export Symantec DLP Policies

---

Also, before you begin the migration process with MDMA, you will also need your Symantec DLP policies.

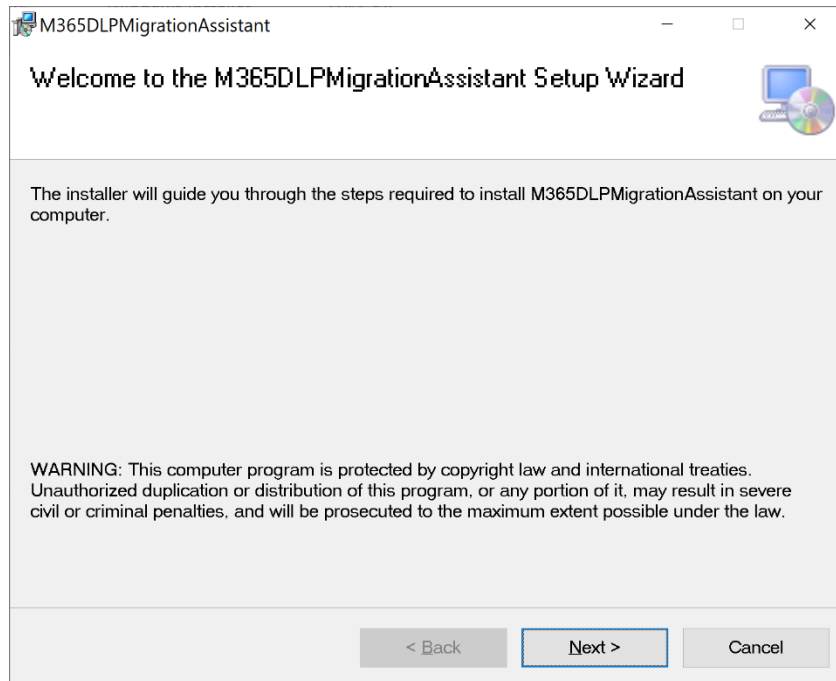
You will need to export these policies as XMLs from Symantec DLP. You can export these as explained [here](#).



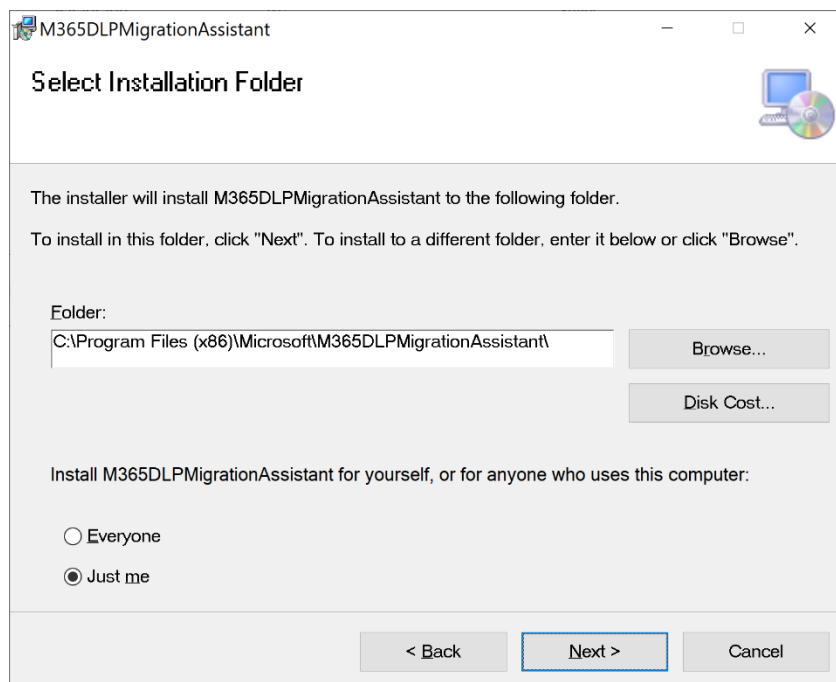
## Installation Steps

Please follow the steps given to install M365 DLP Migration Assistant (MDMA).

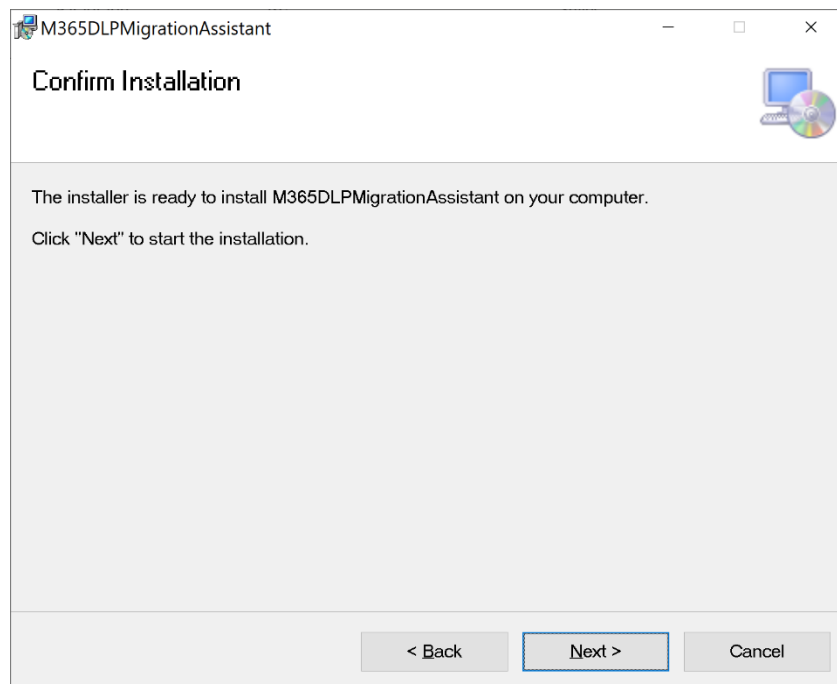
1. [Download](#) and launch **M365DLPMigrationAssistant.msi** file.
2. The following dialog box will open. Click 'Next'.



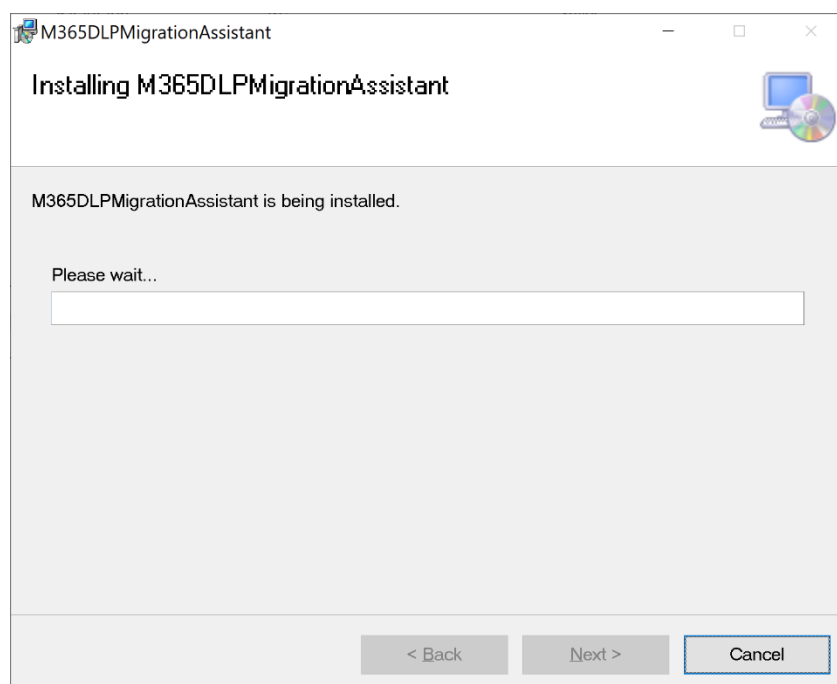
3. Please select the location where you want to install MDMA and click 'Next'.



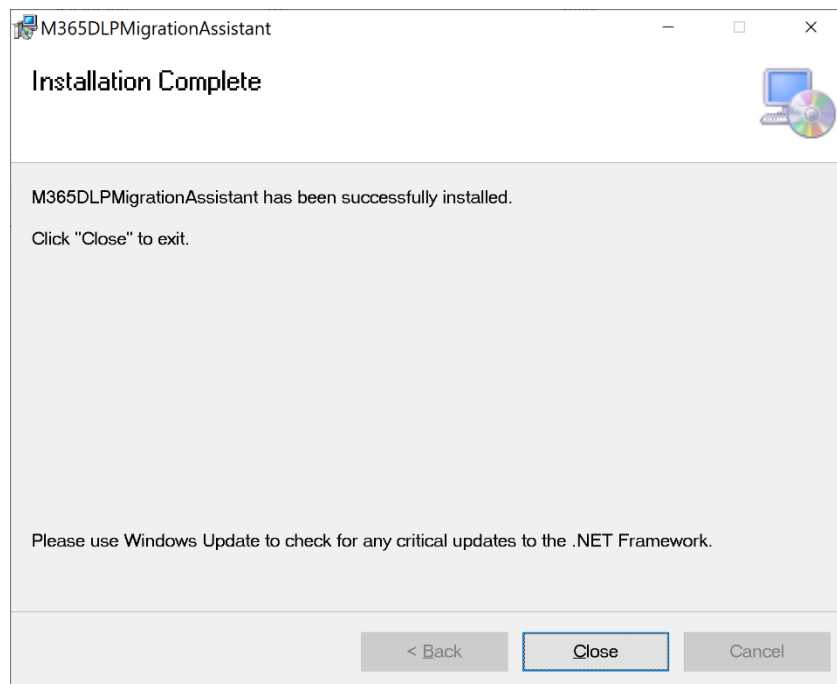
4. Once installer is ready, click 'Next' to begin installation.



5. Please wait while MDMA is being installed.



6. Once MDMA is installed, you can close the dialog box.



## Start Migration

---

To perform a DLP policy migration, you do the following:

- Complete the steps in the [Before You Start](#) section.
- You input XML files of your DLP policies exported from Symantec DLP 15.7 or earlier.
- You make selections and/or tweaks to your DLP policy.
- You create a new DLP policy in your M365 tenant equivalent to your input policy.

Thereafter, you test your DLP policies and make any further changes to your DLP policies through the M365 Unified DLP platform.

You can follow the following steps to perform a DLP policy migration:

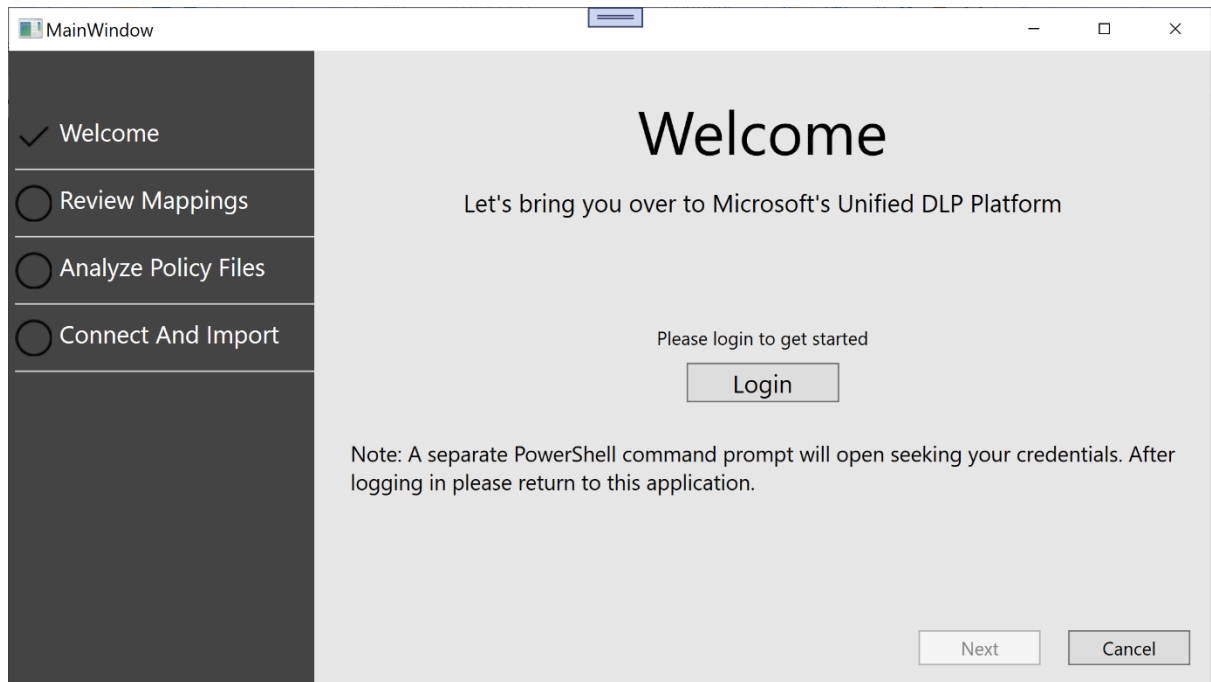
- [Step 1: Log into your account](#)
- [Step 2: Upload your Symantec policy](#)
- [Step 3: Review policy mapping](#)
- [Step 4: Optimize & Fix validation errors \(if any\)](#)
- [Step 5: Extend coverage](#)
- [Step 6: Connect & import policy](#)
- [View your migration report!](#)
- [Next Steps: After policy import](#)

## Step 1: Log into your account

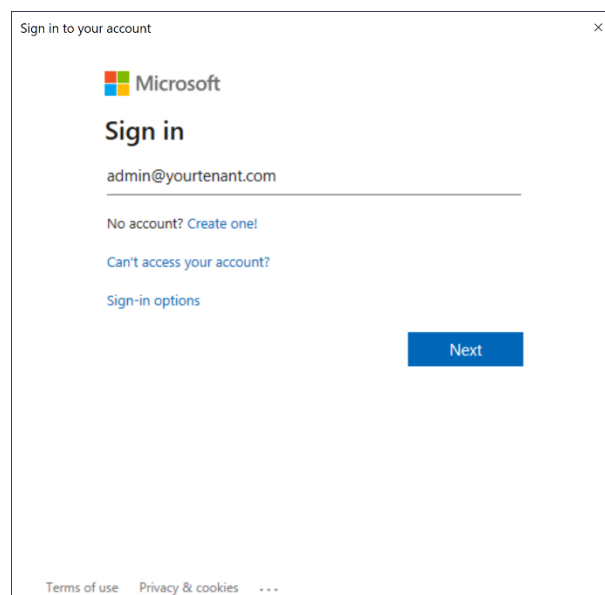
---

After you have installed & launched the M365 DLP Migration Assistant, the first thing that you need to do is to login.

1. You will be greeted with a Welcome screen. Here, you can then click the login button to get started.



2. You will have another pop-up where you need to enter your login credentials.



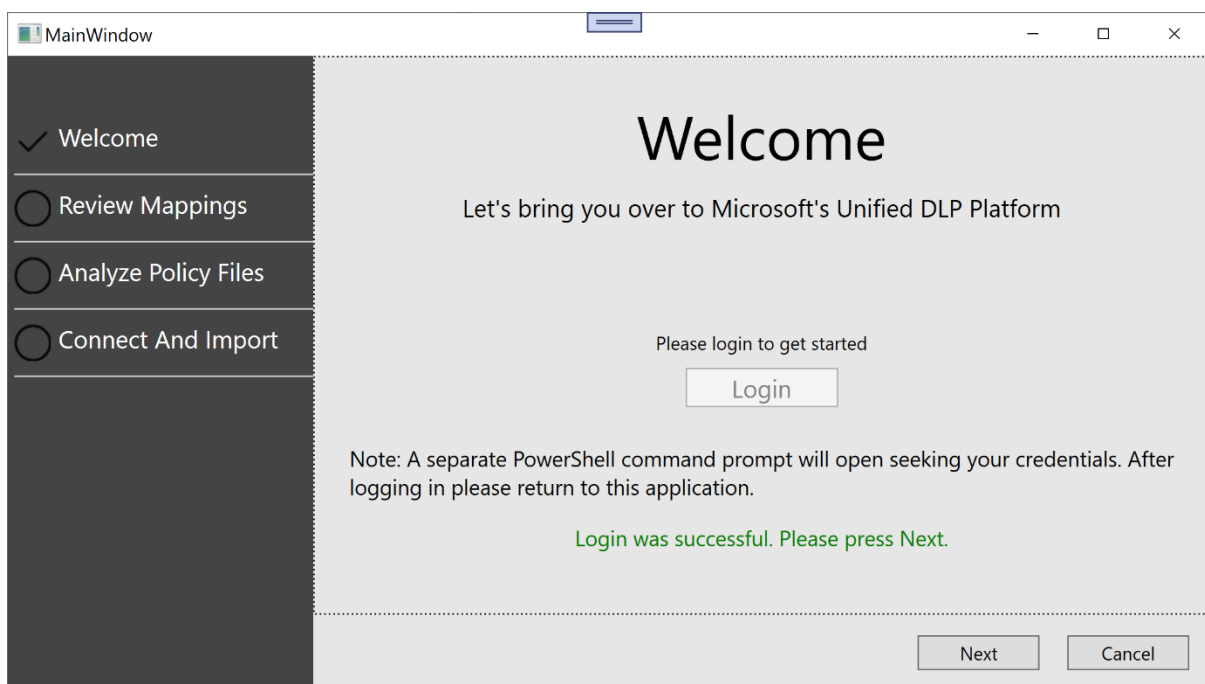
3. You need to wait until your login is validated. Simultaneously, MDMA fetches information that will be required in later stages of the migration process.

All this progress is tracked & logged in a separate PowerShell window like the one below.

```
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
02/02/2021 12:11:25 Connecting to Security & Compliance Center
02/02/2021 12:18:09 Fetching existing Unified DLP Migration Tool Rule Packages
02/02/2021 12:18:56 Existing Unified DLP Migration Tool Rule Packages fetched
02/02/2021 12:18:56 Fetching existing Unified DLP Migration Tool Custom SITS
02/02/2021 12:19:41 Existing Custom SITS fetched
02/02/2021 12:19:41 Fetching existing Keyword Dictionaries
02/02/2021 12:19:42 Existing Keyword Dictionaries fetched
Removed the PSSession ExchangeOnlineInternalSession_1 connected to nam12b.ps.compliance.protection.outlook.com
Disconnected successfully !
02/02/2021 12:19:44 Disconnected Security & Compliance Center successfully. Please go back to the tool to proceed further.
PS C:\Users\karashah\Desktop\WVD\Work\Git\UnifiedDLPMigration\bin\Debug>
```

4. Finally, once your login is validated, you can come back to the MDMA. The next button should now be enabled.

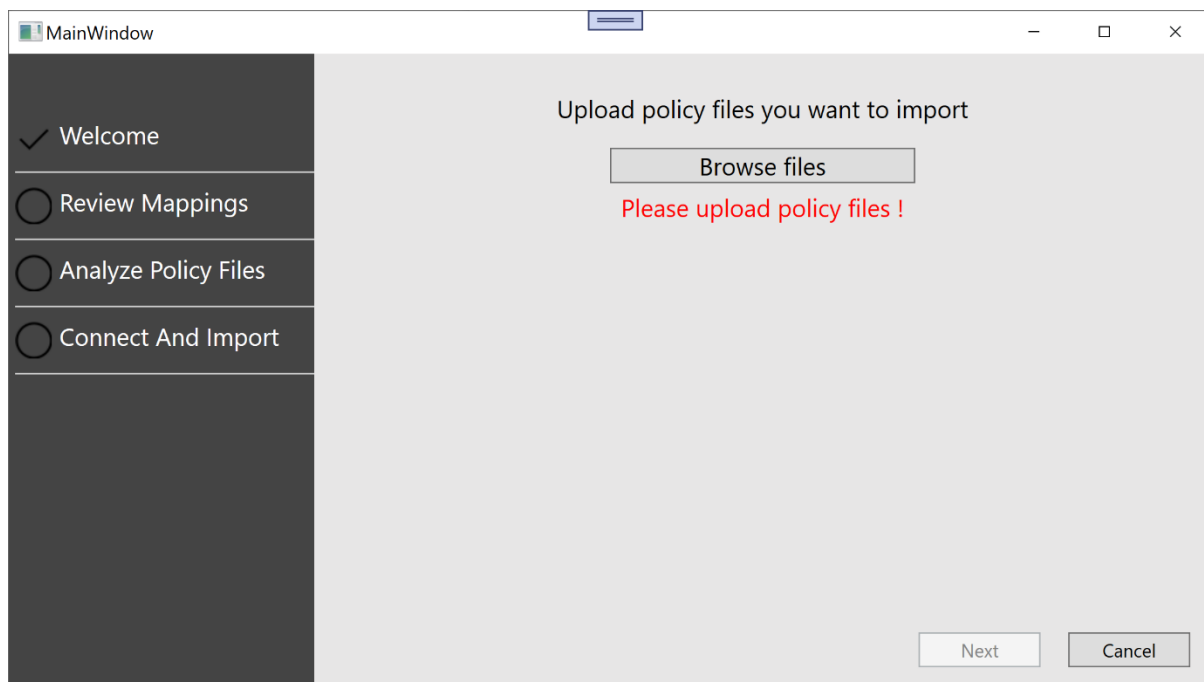
You can click on the Next button and move to the next step in the migration process.



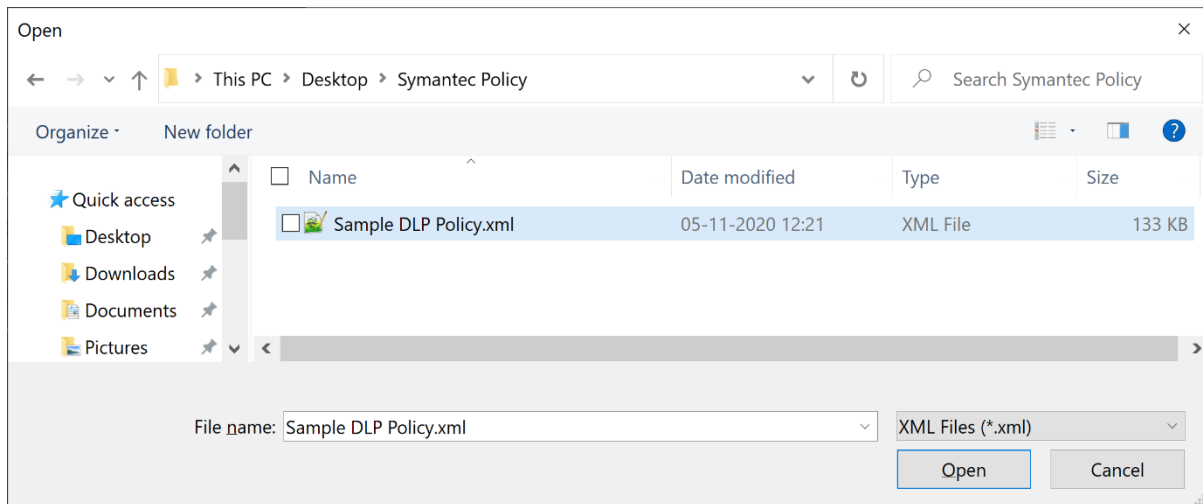
## Step 2: Upload your Symantec policy

Next, you need to upload your Symantec DLP policy exports which will act as an input for MDMA. The policies you upload will be the ones that will be migrated to the Unified DLP platform.

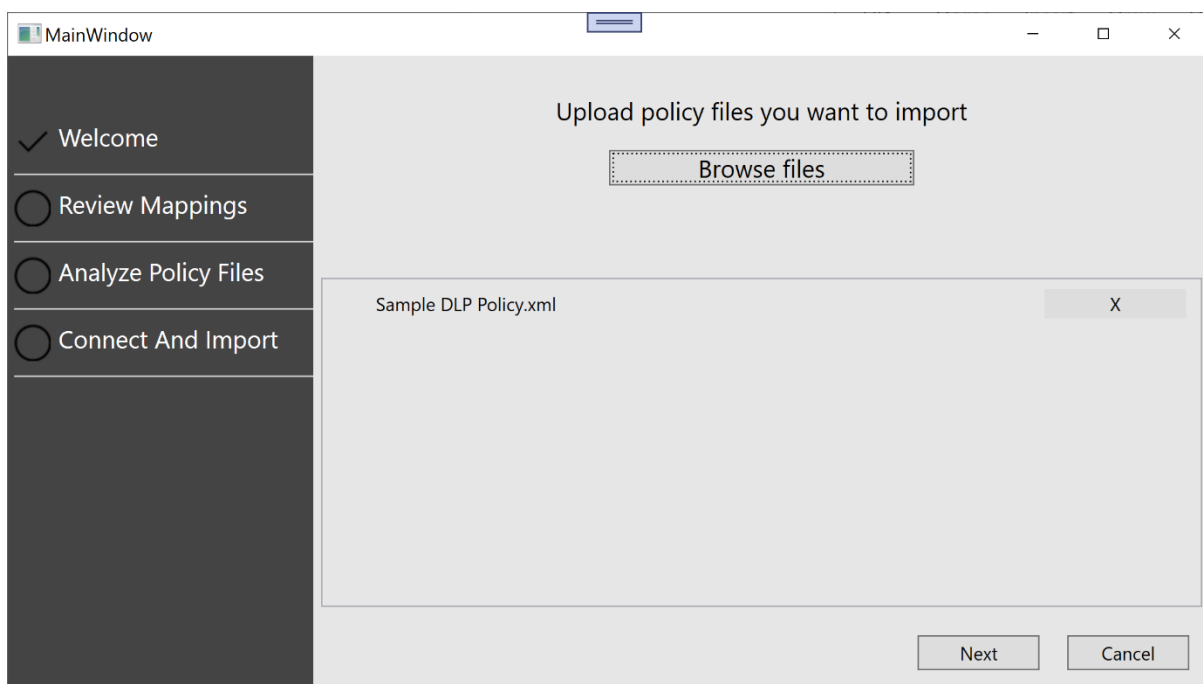
1. To upload the files, you need to click on 'Browse files' button.



2. Please select the required policy files in the File Explorer pop-up window and click 'Open'.
  - a. You can select more than one XML file to migrate multiple policies at a time. Based on our initial engagement with some customers, we have learned that it is best to migrate anywhere from one to three policies at a time to avoid confusion during later stages of the migration process.
  - b. Ensure that the XML files you upload are Symantec DLP policy exports only and no other kind of XML. In such a scenario, the migration process will fail, and you will have to restart it from Step 1.



3. The tool will show you a list of your selected input policy files.
  - a. If you wish to deselect a previously selected policy file, you can click the cross icon corresponding to that policy.



4. Once you have completed selection of the policy files you wish to migrate, you can click 'Next' and move to the next step.



### Step 3: Review policy mapping

---

Once you input the policies you want to migrate, MDMA will process those files to identify what sensitive information you are trying to protect in your policies and what actions are being performed when the policies are triggered.

#### *Sensitive Information Types*

There are certain nuances in how Symantec DLP and MIP differ in allowing users to define sensitive information that needs to be protected.

MIP allows users to define sensitive information that needs to be protected as Sensitive Information Types (SIT). Microsoft ships many commonly used SITs like Credit Card Number out-of-box, often called out-of-box SITs or OOB SITs. Alternatively, it allows users to also create their own custom SITs.

The most common ways in which Symantec users specify what kind of sensitive information needs to be protected are:

- Use out-of-box (OOB) Data Identifiers
- Customize OOB Data Identifiers
- Define regular expressions and/or keywords in DLP rules

MDMA takes care of each of the above scenarios in one of two ways:

- **Map to an existing OOB SIT:**

For all sensitive data types for which there exists an equivalent SIT in MIP, MDMA will try to map it the same.

It automatically maps OOB Symantec Data Identifiers to OOB Sensitive Information Type (SITs) if an equivalent SIT is available.

We do the same for customized OOB Symantec Data Identifiers because we believe strongly in the effectiveness of our OOB SITs. If you wish to still bring it over 'as-is' then you can choose to create a new SIT as described in next step (Step 3-2).

- **Migrate as a new Custom SIT:**

For all sensitive data types for which there is not an equivalent SIT available in MIP, MDMA will automatically opt to create a new SIT.

It will automatically opt to create a new SIT for all OOB Symantec Data Identifiers for which no equivalent SIT in MIP is available.

Similarly, any regular expression(s) or keyword(s) defined directly in rules will be brought over as a new Custom SIT.

**Note:** Regular expressions and/or keywords defined directly at the rule-level in Symantec policies will take up names of the rule itself and show in the Source column. In case of multiple such regexes and/or keywords, it will take up the name of the rule name followed by roman numerals.

Each of these will be migrated separately as a Custom SIT. Understandably, this may lead to confusion later and we recommend you review and rename these SITs at the earliest.

You cannot edit the name of these SITs within MDMA. You can edit the names of these Custom SITs from Compliance Center or via PowerShell after the policy migration has been completed.

### *Actions*

The current version of MDMA brings over policies with 'Generate Incident Report' as a default action. Also, DLP policies in MIP automatically log events in Unified Audit Log and do not need to have a separate action equivalent to 'Syslog' in Symantec DLP.

For a complete list of all supported actions, please see this [section](#).

All other response rules in Symantec are currently not supported by MDMA and thus not migrated along with other policy elements. However, you can manually add (or remove) actions to the policies using Compliance Center after MDMA has successfully migrated the policies.

1. You will be able to see a list of all the sensitive data types (or sensitive information types) as well as response rules (or actions).

These lists are represented as a table with two columns, namely 'Source' and 'Target'.

As the name suggests, the Source column refers to the input policies from Symantec, whereas the Target column refers to the output policies that will be created in MIP.

MainWindow

Symantec

☐ Welcome

☒ Review Mappings

☐ Analyze Policy Files

☐ Connect And Import

^ Sensitive Data Types

Source	Target
Swift Code	SWIFT Code
Brazil Bank Account	New SIT
Turkish Tax Identification Number	Turkish Tax Identification Number

^ Action / Response rules

Source	Target
Generate DLP Incident	GenerateIncidentReport

Enter comma(,) separated email address(es).

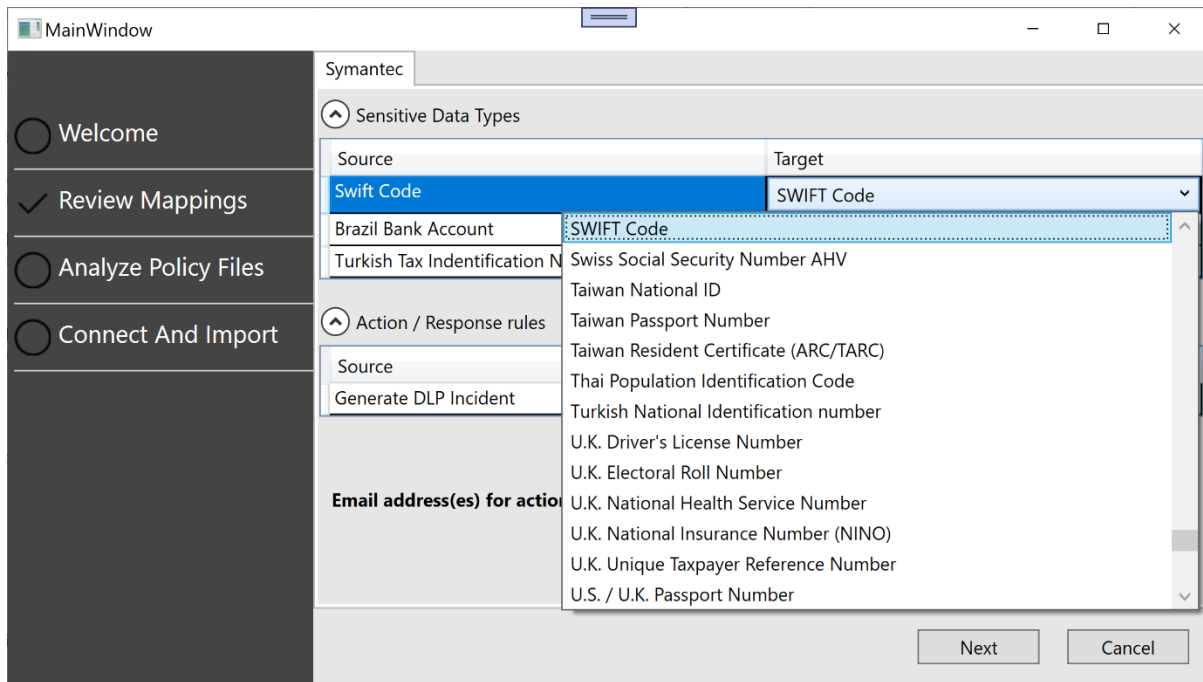
**Email address(es) for actions**

Next Cancel

2. You need to review the automated mapping between Source (Symantec) and Target (MIP) that MDMA does for you.
  - a. MDMA performs this automated mapping based on the Data Identifier class name in Symantec and based on identical SIT names for any previously created custom SIT.
3. You can manually change any of the mapping if you wish to by clicking on the corresponding row in the 'Target' column.

This will open a drop-down list with all the out-of-box SITs (OOB SITs) and all the custom SITs (if any) that you may have previously created. You can choose the option to which you wish to map to the 'Source' row item.

Alternatively, you can also choose the option 'New SIT' from the drop-down and MDMA will bring over the Source SIT as a new Custom SIT.



**Recommendation:** We highly recommend you spend a little extra to review this mapping and choose an existing OOB or Custom SIT for as many instances as possible. This will help reduce the number of new duplicate SITs created. Learn more about [sensitive information type entity definitions](#).

We try to *automatically* map only for OOB Symantec Data Identifiers (customized or not) as these are standard across all Symantec customers.

We refrain from making *automatic* matches for any other sensitive information as doing so can critically impact the output policy generated and thus recommend you perform this step carefully.

**Warning:** MIP platform has a threshold for up to 10 rule packages per tenant. This limit is enough for most customers, but the creation of many duplicate Custom SITs may quickly lead you to hitting this threshold without the ability to create any new Custom SITs.

4. You will have to enter the email IDs of all users to whom you wish to send generated incident reports. Typically, for most organizations, these are the admins.

These details can be edited later using Compliance Center after the policy is migrated.

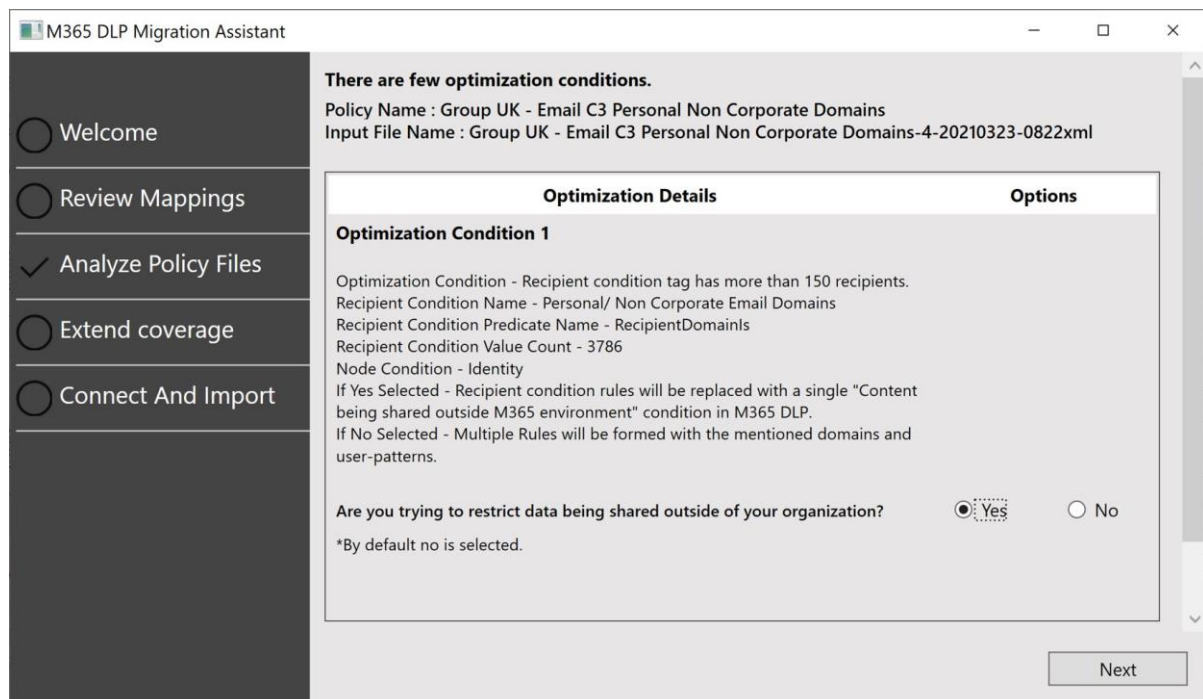
5. After you have reviewed the Sensitive Data Types and completed above steps, you can click 'Next' and move to next step.

## Step 4: Optimize & Fix validation errors (if any)

Next, MDMA checks all elements within the source policy to check if it is in accordance with Microsoft's Unified DLP platform thresholds. We would provide options to optimize your policy and/or fix validation errors.

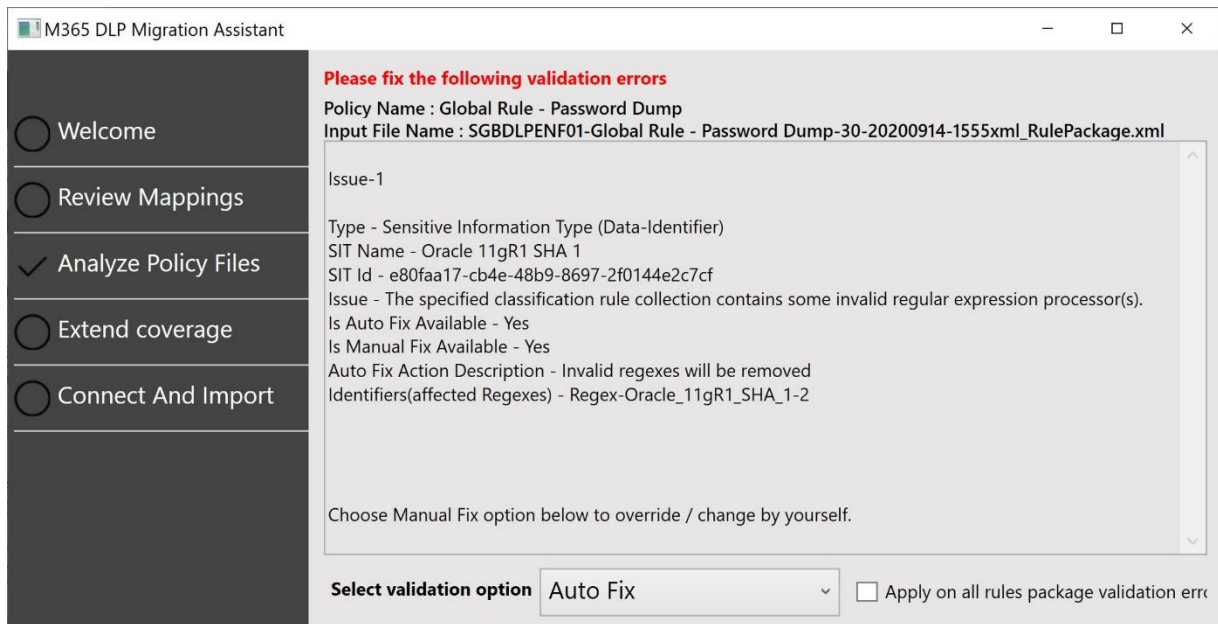
### *Optimization Recommendations*

If MDMA detects conditions in your policy that could be optimized as you bring it into 365 DLP, then it will recommend the same.



A few of the checks (but not limited to) that MDMA performs at this stage are:

- Does any keyword exceed more than 50 characters?
- Does any SIT have more than 20 regex patterns?
- Does any of the policies have unsupported characters?



MDMA will highlight all validation checks that did not pass and ask you to remediate the same.

It will give you two options:

- **Manual Fix:** MDMA will open a temporary text file where you will have to review and manually fix the error.
- **Auto Fix:** MDMA will automatically remediate the validation error. Please use this feature with caution as it may lead to some scenario loss.

## Step 5: Extend Coverage

In this step, you can choose if you want to extend the coverage of your current policy to other Microsoft or non-Microsoft workloads.

1. By default, MDMA will have Exchange workload selected. If you wish to extend the current policy to other workloads, then select the check box for the same.

Policy Na	Exchange	SharePoint	OneDrive	Teams	Endpoint	MCAS
Global Rule - Password Dump	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**Warning:** Select only the workloads that are part of your M365 subscription license. In case you choose a workload that is not part of your license then the policy creation will fail in the final step.

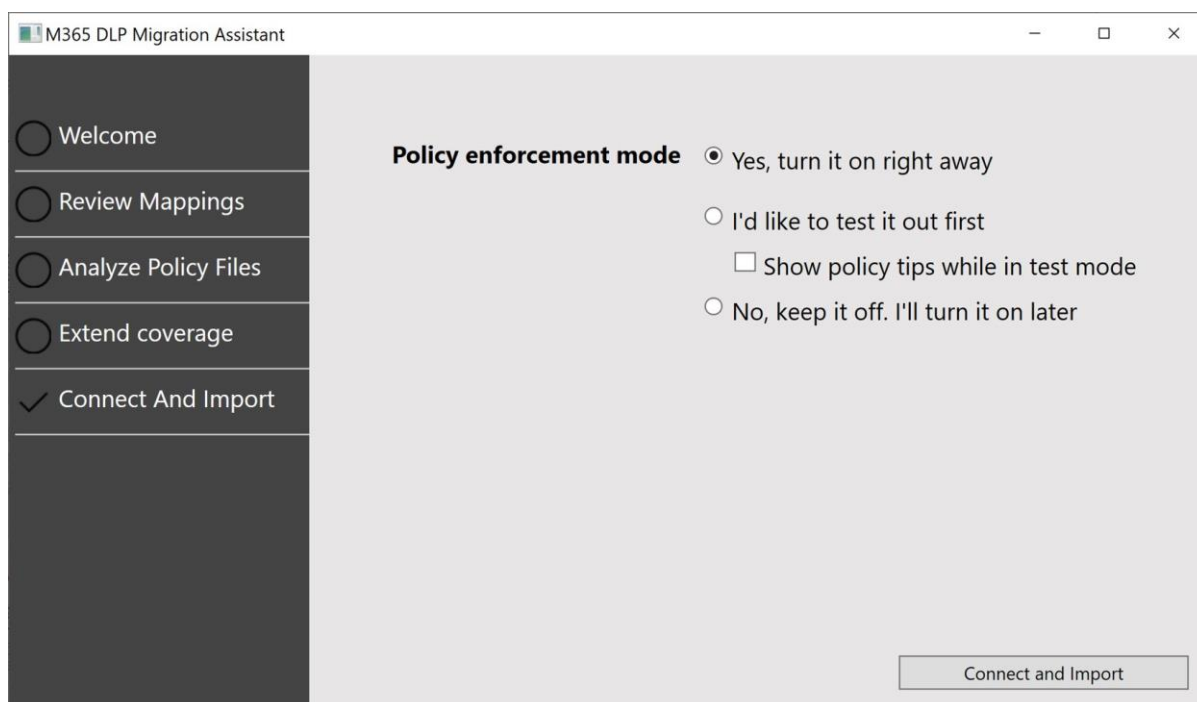
This is currently a limited feature; and for all the other workloads you select (apart from Exchange), MDMA will create a simple DLP policy with the condition 'Content contains' scoped to the entire organization. You can customize this policy further post migration.

In future releases, we will also add support more cross-workload conditions and response rules so extending policy coverage for maximum workloads within your organization.

## Step 6: Connect & import policy

Finally, after you completed all the previous steps, your Symantec DLP policy is ready to be imported to Microsoft's Unified DLP platform.

1. The last thing that you need to do before the policies are imported is to choose whether to turn on or off the imported policies.



There are three options you can choose from:

- Turn on policy immediately.
- Turn on policy in test mode first. Remove from test mode later manually.
- Turn off policy. Turn on later manually.

**Recommendation:** We recommend that you choose to bring over policies first in test mode. You can monitor the alerts that the policy generates and finetune it as required by your organization.

Once your policy is finetuned, you can turn it on or in other words put it into production.

2. Next, click 'Connect and Import' to import your policy. A new PowerShell window will open asking you to login again.

After you login, PowerShell scripts will get executed to create new policies in Microsoft's Unified DLP platform with all the data in the input policy files and any additional settings you made during previous MDMA steps.

Please wait until the script completes execution with a Success/Failure message. Thereafter, new SITs and policies will start showing up in Compliance Center as well.



## View your migration report!

Once your policies are imported and the migration process is complete then you can view the migration report.

For each session, a separate report is generated. We define a session from when the user launches the app, and the session ends when migration process is completed, or user exits the app.

It is an Excel-based report that is divided into three different sheets:

- Overview
- Policy Details
- SIT Details

### Overview Sheet

As the name suggests, it provides an overview of the migration session.

AutoSave

MDMA\_2021\_05\_06-123407.xlsx

Search

Karan Shah

File

Home

Insert

Draw

Page Layout

Formulas

Data

Review

View

Help

Team

Redirection

Share

Comments

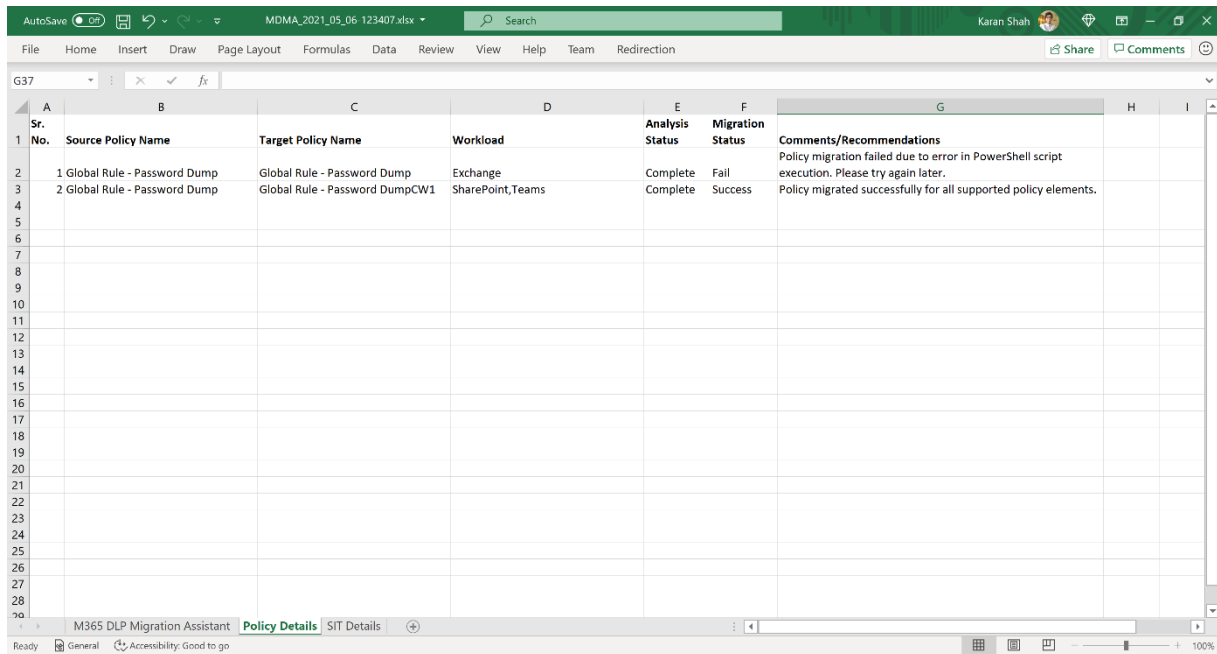
F32

It provides the following information:

- Your tenant's name.
- Date of session.
- Overall summary stats for that session.
- Input policy level details, migration status and comments/recommendations

## Policy Details

This sheet provides a more detailed view of each migrated (or output) policy created or not created.



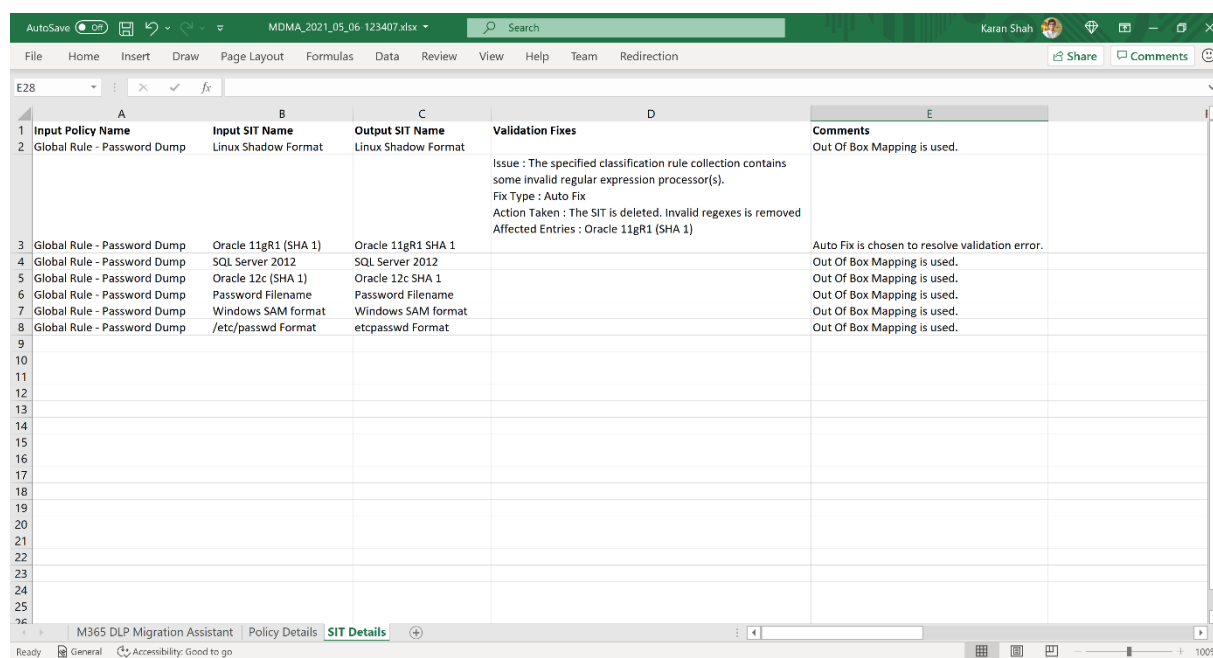
Sr. No.	Source Policy Name	Target Policy Name	Workload	Analysis Status	Migration Status	Comments/Recommendations
1	Global Rule - Password Dump	Global Rule - Password Dump	Exchange	Complete	Fail	Policy migration failed due to error in PowerShell script execution. Please try again later.
2	Global Rule - Password Dump	Global Rule - Password DumpCW1	SharePoint, Teams	Complete	Success	Policy migrated successfully for all supported policy elements.

It provides the following information:

- Mapping of source policy and target policy(s) created.
- List of workloads each policy is applied to.
- Analysis status for each policy highlights if MDMA can migrate the policy completely, partially or cannot migrate.
  - For workloads other than Exchange, this would typically show as 'Complete' since we create a simple policy with the 'Content contains' condition which is supported across all workloads.
- Migration status for each policy will tell you if the policy was migration was a success or failure.
- Comments/recommendations column will provide you with more details related to that policy.

## SIT Details

This sheet provides information about all the Sensitive Information Types that were migrated.



Input Policy Name	Input SIT Name	Output SIT Name	Validation Fixes	Comments
Global Rule - Password Dump	Linux Shadow Format	Linux Shadow Format	Issue : The specified classification rule collection contains some invalid regular expression processor(s). Fix Type : Auto Fix Action Taken : The SIT is deleted. Invalid regexes is removed Affected Entries : Oracle 11gR1 (SHA 1)	Out Of Box Mapping is used.
Global Rule - Password Dump	Oracle 11gR1 (SHA 1)	Oracle 11gR1 SHA 1		Auto Fix is chosen to resolve validation error.
Global Rule - Password Dump	SQL Server 2012	SQL Server 2012		Out Of Box Mapping is used.
Global Rule - Password Dump	Oracle 12c (SHA 1)	Oracle 12c SHA 1		Out Of Box Mapping is used.
Global Rule - Password Dump	Password Filename	Password Filename		Out Of Box Mapping is used.
Global Rule - Password Dump	Windows SAM format	Windows SAM format		Out Of Box Mapping is used.
Global Rule - Password Dump	/etc/passwd Format	etcpasswd Format		Out Of Box Mapping is used.

It provides the following information:

- Policy-wise mapping of input & output SIT created.
- Validation fixes column will provide information about validation errors that occurred during the migration process (if any)
- Comments column tells you about SIT auto-mapping, remediation steps, etc.

## Output PowerShell scripts & rule package XMLs

The final PowerShell scripts and rule packages XMLs used for migration are stored on the local machine at the following directory by default:

```
C:\Users\<username>\AppData\Local\Temp\M365DLPMigrationAssistant\output\Symantec
```

Separate folders are created for each session. These files may contain sensitive data related to your organization and its DLP policies.

## Next Steps: After policy import

---

After the migration process is complete, you should visit Compliance Center, validate if the policies were migrated successfully and test the efficacy of the same.

**Recommendation:** We recommend you visit Compliance Center after each MDMA session ends and perform these checks for all the policies that were migrated in that session.

### *Check Sensitive Information Types*

1. **Validate SITs are created:** Choose 'Data Classification' from left panel and navigate to 'Sensitive Information Type' tab and check if new SITs are created.

To make this easier, you can sort the list on 'Publisher' and check for SITs with publisher name as "DLP Migration Tool".

2. **Rename SITs:** For many SITs, you may notice there are similar names often followed by roman numerals. To avoid confusion as well as duplication post-migration, we recommend you rename these SITs at the earliest.

This is especially true in cases where your regular expressions and keywords are defined directly in rules within your input Symantec DLP policies.

3. **Test and finetune SITs:** We also recommend you test the migrated SITs by yourself. Further, we also urge you to finetune it to achieve the performance you desire for your organization.

MDMA creates new SITs with a few standard settings which may not or may not be optimal for your tenant. A few things to look for:

- a. Regular expressions
  - i. Unsupported or delete regexes (during migration)
- b. Keywords
  - i. Case sensitive vs insensitive keywords
  - ii. String vs word match
  - iii. Proximity
- c. Optional validators

### *Check DLP Policies*

1. **Validate DLP policies are created:** Choose 'Data Loss Prevention' from left panel and check if new policies are created.
2. **Add missing policy elements:** While most of your input Symantec DLP policy elements (like conditions, exclusions, or actions) will get migrated, often few elements from your input Symantec DLP policy may get dropped during the migration process owing to some limitations of MDMA.

In many of these scenarios, these elements are supported by the M365 DLP platform and you will have to manually add these elements to the policy.

3. **Test and finetune policy:** Once your policy is properly configured with all requisite elements, you should test the policy and finetune it as per the needs of your organization.
4. **Turn on policy:** Once your policy is tested and finetuned as per the needs of your organization, you can go ahead and 'Turn on' this policy. In other words, put the policy in production mode.
5. **Bring over remaining policies:** Once you have completed the above checks, you can go back to bringing over the next policy or next batch policies using MDMA.

## Reporting Errors & Providing Feedback

---

Please share feedback with us using this [feedback form](#).

To report errors & any feature requests with us by opening a new issue in this Github repository. Alternatively, you can reach out to us at [cxe-help@microsoft.com](mailto:cxe-help@microsoft.com) or via your CXE / Fasttrack / Microsoft partner to share your feedback and suggestions.

## Telemetry Notice

---

**Data Collection:** This software may collect information about you and your use of the software and send it to Microsoft. Microsoft may use this information to provide services and improve our products and services. If you wish to turn off telemetry, please reach out to us and we will provide you with a separate version of tool with telemetry turned off. There are also some features in the software that may enable you and Microsoft to collect data from users of your applications. If you use these features, you must comply with applicable law, including providing appropriate notices to users of your applications together with a copy of Microsoft's privacy statement. Our privacy statement is located at <https://go.microsoft.com/fwlink/?LinkID=824704>. You can learn more about data collection and use in the help documentation and our privacy statement. Your use of the software operates as your consent to these practices.