M365 Desired State Configuration

Microsoft 365 DSC is an open source, Microsoft lead, community driven project which allows for extraction, comparison and even remediation of configuration within a Microsoft 365 tenancy or even across multiple tenancies. In this article, I'll detail how it can be used to "snapshot" your tenancy configuration and then compare this snapshot against and updated configuration to detect changes in the environment.

Install the Microsoft 365DSC module

Microsoft 365 DSC comes in the form of a simple PowerShell module. To get started, open up an administrative PowerShell session and run the following command:

Install-Module -Name Microsoft365DSC

This might take a little while as it will need to download a lot of dependencies to allow the DSC module to do its job.

Once complete you should check to see if the latest version is installed by running the following:

Update-M365DSCDependencies

Once this has updated, remove any outdated dependencies:

Uninstall-M365DSCOutdatedDependencies

Creating an account for M365DSC

The account required to execute the export of the tenant configuration requires two attributes similar to a break-glass account (Manage emergency access admin accounts - Azure AD - Microsoft Entra | Microsoft Docs):

- An account with the Global Administrator role assigned
- No MFA is passed to it from Conditional Access or other policies

Due to the legacy nature of some of the modules required for accessing the configuration, any MFA prompt will break the export request as detailed in the Microsoft 365 DSC documentation:

The following table provides an overview of what authentication methods are supported by which workload and what underlying module is being used to authenticate:

Workload	**PowerShell Module**	**Credential**	**Service Principal**		
			Certificate Thumbprint	**Certificate Path**	**Application Secret**

Workload	**PowerShell Module**	**Credential**	**Service Principal**		
*AzureAD**	Microsoft.Graph.Authentication (Connect-MgGraph)	☑	☑	☒	☑
Exchange Online	ExchangeOnlineManagement (Connect-ExchangeOnline)	☑	☑	☑	☒
*Intune**	Microsoft.Graph.Authentication (Connect-MgGraph)	☑	☑	☒	☑
*Office 365**	Microsoft.Graph.Authentication (Connect-MgGraph)	☑	☑	☒	☑
OneDrive	PnP.PowerShell (Connect-PnPOnline)	☑	☑	☑	☑
Power Apps	Microsoft.PowerApps. Administration.PowerShell	☑	☒	☒	☒
*Planner**	Microsoft.Graph.Authentication (Connect-MgGraph)	☒	☑	☒	☑

Workload	PowerShell Module	Credential	Service Principal		
Security & Compliance Center	ExchangeOnlineManagement (Connect-IPPSSession)	✅	❎	❎	❎
SharePoint Online	PnP.PowerShell (Connect-PnPOnline)	✅	✅	✅	✅
Teams	MicrosoftTeams (Connect-MicrosoftTeams)	✅	❎	❎	❎

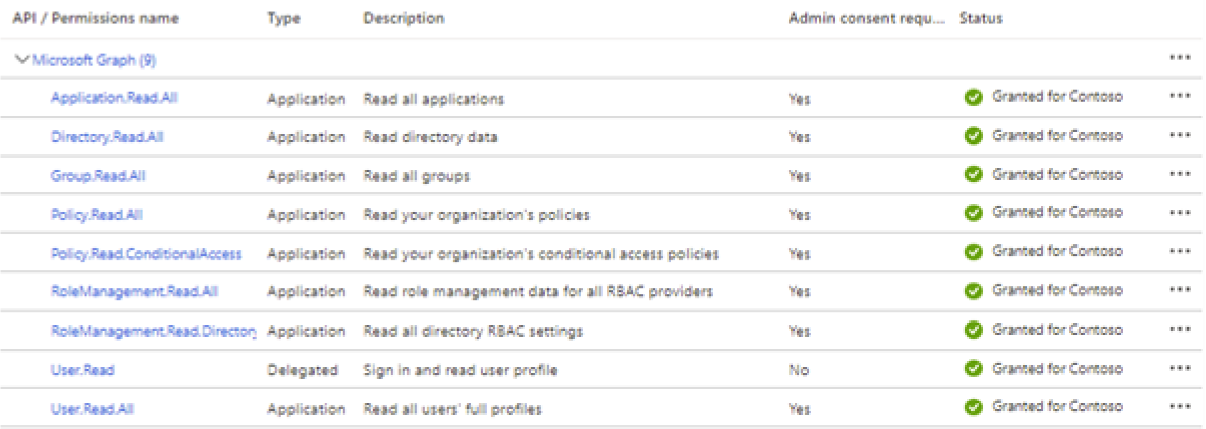
✅ = Supported / ❎ = Not supported

Note: As you can see, while using Credentials is the least preferred option for security reasons, it is the only option that works across **most** supported workloads.

Prepare an Azure AD Application (optional)

To retried the planner configuration you will need register a new Azure AD app. When the app is created take note of the Application ID, Tenant ID (this is the tld which end with .onmicrosoft.com) and your Client Secret.

Next, to grant permissions to the app, add permissions for the Graph API with each resource listed below into the Azure AD registered application:



API / Permissions name	Type	Description	Admin consent requ...	Status	
∨ Microsoft Graph (9)					•••
Application.Read.All	Application	Read all applications	Yes	✓ Granted for Contoso	•••
Directory.Read.All	Application	Read directory data	Yes	✓ Granted for Contoso	•••
Group.Read.All	Application	Read all groups	Yes	✓ Granted for Contoso	•••
Policy.Read.All	Application	Read your organization's policies	Yes	✓ Granted for Contoso	•••
Policy.Read.ConditionalAccess	Application	Read your organization's conditional access policies	Yes	✓ Granted for Contoso	•••
RoleManagement.Read.All	Application	Read role management data for all RBAC providers	Yes	✓ Granted for Contoso	•••
RoleManagement.Read.Director	Application	Read all directory RBAC settings	Yes	✓ Granted for Contoso	•••
User.Read	Delegated	Sign in and read user profile	No	✓ Granted for Contoso	•••
User.Read.All	Application	Read all users' full profiles	Yes	✓ Granted for Contoso	•••

To extract a configuration for planner, run the Export-M365DSCConfiguration cmdlet, passing in the resources you want to extract. For the TenantId, this is the .onmicrosoft.com address, not the object ID, for example ASDA.uk.onmicrosoft.com

Graph API Permissions

To allow access for the M365DSC account credential to use Graph API, the following should be executed in PowerShell to give the appropriate level of permissions require:

Update-M365DSCAllowedGraphScopes -All -Type Read

Running the Planner report collection with an applications

```
# Getting client credential
$Credential = Get-Credential

# Exporting resources using credentials
Export-M365DSCConfiguration -
Components @("PlannerBucket", "PlannerPlan", "PlannerTask") - -
ApplicationId $ApplicationId -ApplicationSecret $ApplicationSecret -
TenantId $TenantId
```

Extract a tenant Configuration with credentials

To extract a configuration, run the Export-M365DSCConfiguration cmdlet, passing in the resources you want to extract.

I have listed the command below which should be run against your environment:

```
# Getting client credential
$Credential = Get-Credential

# Exporting resources using credentials
Export-M365DSCConfiguration -
Components @("AADApplication", "AADAuthorizationPolicy", "AADConditionalAccess
Policy", "AADGroup", "AADGroupLifecyclePolicy", "AADGroupsNamingPolicy", "AADG
roupsSettings", "AADNamedLocationPolicy", "AADRoleDefinition", "AADSecurityDef
aults", "AADServicePrincipal", "AADTenantDetails", "AADTokenLifetimePolicy", "
EXOAcceptedDomain", "EXOActiveSyncDeviceAccessRule", "EXOAddressBookPolicy", "
EXOAddressList", "EXOAntiPhishPolicy", "EXOAntiPhishRule", "EXOApplicationAcce
ssPolicy", "EXOAtpPolicyForO365", "EXOAuthenticationPolicy", "EXOAuthenticatio
nPolicyAssignment", "EXOAvailabilityAddressSpace", "EXOAvailabilityConfig", "E
XOCASMailboxPlan", "EXOCASMailboxSettings", "EXOClientAccessRule", "EXODataCla
ssification", "EXODataEncryptionPolicy", "EXODistributionGroup", "EXODkimSigni
ngConfig", "EXOEmailAddressPolicy", "EXOGlobalAddressList", "EXOHostedConnecti
onFilterPolicy", "EXOHostedContentFilterPolicy", "EXOHostedContentFilterRule",
 "EXOHostedOutboundSpamFilterPolicy", "EXOHostedOutboundSpamFilterRule", "EXOI
nboundConnector", "EXOIntraOrganizationConnector", "EXOIRMConfiguration", "EXO
JournalRule", "EXOMailboxPlan", "EXOMailboxSettings", "EXOMailTips", "EXOMalwa
reFilterPolicy", "EXOMalwareFilterRule", "EXOManagementRole", "EXOMessageClass
ification", "EXOMobileDeviceMailboxPolicy", "EXOOfflineAddressBook", "EXOOMECo
nfiguration", "EXOOnPremisesOrganization", "EXOOrganizationConfig", "EXOOrgani
zationRelationship", "EXOOutboundConnector", "EXOOwaMailboxPolicy", "EXOPartne
rApplication", "EXOPerimeterConfiguration", "EXOPolicyTipConfig", "EXOQuaranti
nePolicy", "EXORemoteDomain", "EXOResourceConfiguration", "EXORoleAssignmentPo
licy", "EXOSafeAttachmentPolicy", "EXOSafeAttachmentRule", "EXOSafeLinksPolicy
", "EXOSafeLinksRule", "EXOSharedMailbox", "EXOSharingPolicy", "EXOTransportCo
nfig", "EXOTransportRule", "IntuneAntivirusPolicyWindows10SettingCatalog", "In
tuneAppConfigurationPolicy", "IntuneApplicationControlPolicyWindows10", "Intun
eAppProtectionPolicyAndroid", "IntuneAppProtectionPolicyiOS", "IntuneASRRulesP
olicyWindows10", "IntuneAttackSurfaceReductionRulesPolicyWindows10ConfigManage
r", "IntuneDeviceAndAppManagementAssignmentFilter", "IntuneDeviceCategory", "I
ntuneDeviceCompliancePolicyAndroid", "IntuneDeviceCompliancePolicyAndroidDevic
eOwner", "IntuneDeviceCompliancePolicyAndroidWorkProfile", "IntuneDeviceCompli
ancePolicyiOs", "IntuneDeviceCompliancePolicyMacOS", "IntuneDeviceCompliancePo
licyWindows10", "IntuneDeviceConfigurationPolicyAndroidDeviceOwner", "IntuneDe
viceConfigurationPolicyAndroidWorkProfile", "IntuneDeviceConfigurationPolicyiO
S", "IntuneDeviceConfigurationPolicyWindows10", "IntuneDeviceEnrollmentLimitRe
striction", "IntuneDeviceEnrollmentPlatformRestriction", "IntuneExploitProtect
ionPolicyWindows10SettingCatalog", "IntuneSettingCatalogASRRulesPolicyWindows1
0", "O365AdminAuditLogConfig", "O365Group", "O365OrgCustomizationSetting", "O3
65User", "ODSettings", "PPPowerAppsEnvironment", "PPTenantIsolationSettings",
"PPTenantSettings", "SCAuditConfigurationPolicy", "SCCaseHoldPolicy", "SCCaseH
oldRule", "SCComplianceCase", "SCComplianceSearch", "SCComplianceSearchAction"
, "SCComplianceTag", "SCDeviceConditionalAccessPolicy", "SCDeviceConfiguration
Policy", "SCDLPCompliancePolicy", "SCDLPComplianceRule", "SCFilePlanPropertyAu
thority", "SCFilePlanPropertyCategory", "SCFilePlanPropertyCitation", "SCFileP
lanPropertyDepartment", "SCFilePlanPropertyReferenceId", "SCFilePlanPropertySu
bCategory", "SCLabelPolicy", "SCRetentionCompliancePolicy", "SCRetentionCompli
anceRule", "SCRetentionEventType", "SCSensitivityLabel", "SCSupervisoryReviewP
olicy", "SCSupervisoryReviewRule", "SPOAccessControlSettings", "SPOApp", "SPOB
rowserIdleSignout", "SPOHomeSite", "SPOHubSite", "SPOOrgAssetsLibrary", "SPOPr
opertyBag", "SPOSearchManagedProperty", "SPOSearchResultSource", "SPOSharingSe
ttings", "SPOSite", "SPOSiteAuditSettings", "SPOSiteDesign", "SPOSiteDesignRig
hts", "SPOSiteGroup", "SPOSiteScript", "SPOStorageEntity", "SPOTenantCdnEnable
d", "SPOTenantCdnPolicy", "SPOTenantSettings", "SPOTheme", "SPOUserProfileProp
erty", "TeamsCallingPolicy", "TeamsChannel", "TeamsChannelsPolicy", "TeamsChan
nelTab", "TeamsClientConfiguration", "TeamsEmergencyCallingPolicy", "TeamsEmer
gencyCallRoutingPolicy", "TeamsFederationConfiguration", "TeamsGuestCallingCon
figuration", "TeamsGuestMeetingConfiguration", "TeamsGuestMessagingConfigurati
on", "TeamsMeetingBroadcastConfiguration", "TeamsMeetingBroadcastPolicy", "Tea
msMeetingConfiguration", "TeamsMeetingPolicy", "TeamsMessagingPolicy", "TeamsP
stnUsage", "TeamsTeam", "TeamsTenantDialPlan", "TeamsUpdateManagementPolicy",
"TeamsUpgradeConfiguration", "TeamsUpgradePolicy", "TeamsUser", "TeamsVoiceRou
te", "TeamsVoiceRoutingPolicy") -Credential $Credential
```

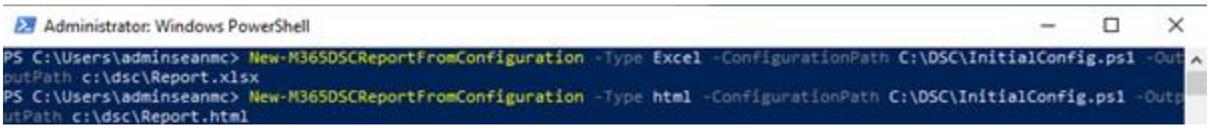
Create a configuration report

The PS1 Configuration file exported by DSC isn't a very user friendly way of reviewing the tenant config. The configuration can be exported to Excel or HTML format by using the New-M365DSCReportFromConfiguration cmdlet.

Ensure you are in the working directory used for the output of the configuration data and then run the following:

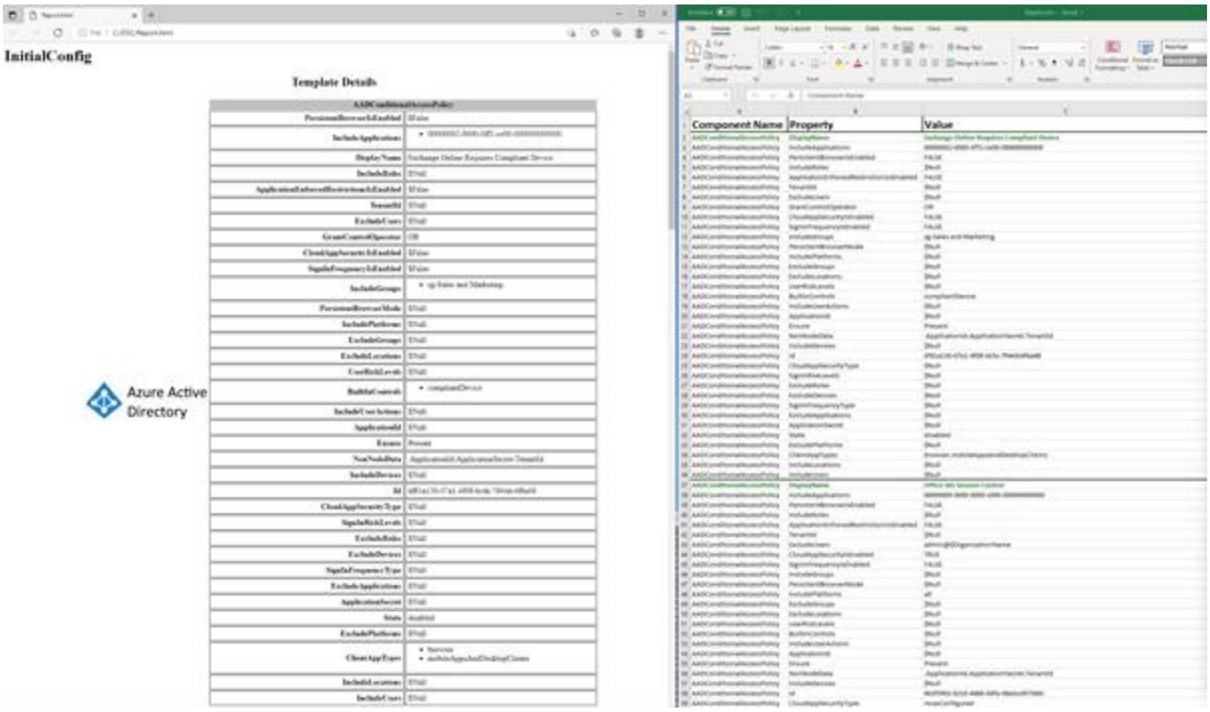
New-M365DSCReportFromConfiguration -type html -ConfigurationPath .\M365TenantConfig.ps1 -OutputPath .\Report.html

New-M365DSCReportFromConfiguration -type Excel -ConfigurationPath .\M365TenantConfig.ps1 -OutputPath .\Report.xlsx



```
PS C:\Users\adminseanmc> New-M365DSCReportFromConfiguration -Type Excel -ConfigurationPath C:\DSC\InitialConfig.ps1 -Out
putPath c:\dsc\Report.xlsx
PS C:\Users\adminseanmc> New-M365DSCReportFromConfiguration -Type html -ConfigurationPath C:\DSC\InitialConfig.ps1 -Outp
utPath c:\dsc\Report.html
```

The exported configuration will be exported in a much easier to read format.



Once you have this report generated, can you send over all of the exported files and the report itself, SPO or ODFB is probably the best way to transfer this.

If you run into any issues that aren't covered in the official documentation, drop me an email and we can jump on a call.