PowerShell Quick Reference - Security and Compliance Center (v1.0)

Connecting to Security and Compliance Center (SCC)

```
$LiveCred = Get-Credential
$Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri https://ps.compliance.protection.outlook.com/powershell-liveid/ -Credential $LiveCred -Authentication Basic -AllowRedirection
Import-PSSession $Session
```

MFA: Connect-IPPSSession -UserPrincipalName damian@practicalpowershell.com

Cmdlet Changes in 2018

Security and Compliance Center

12.31.2017	158 cmdlets
09.30.2018	190 cmdlets

Listing Cmdlets for the SCC

List all Commands for the Security and Compliance Center

```
$Name = (Get-Module | where {$_.ModuleType -eq 'Script'}).Name
Get-Command | Where {$_.ModuleName -eq $Name}
```

Get-Help

Getting Help

```
Get-Help <command>
Get-Help <command> -Examples
Get-Help <command> -Full
```

Examples

```
Get-Help Set-ComplianceTag
Get-Help Set-ComplianceTag -Examples
Get-Help Set-ComplianceTag -Full
```

Teams Compliance Policy (SCC)

```
Get-TeamsRetentionCompliancePolicy
Get-TeamsRetentionComplianceRule
New-TeamsRetentionCompliancePolicy
New-TeamsRetentionComplianceRule
Remove-TeamsRetentionCompliancePolicy
Remove-TeamsRetentionComplianceRule
Set-TeamsRetentionCompliancePolicy
Set-TeamsRetentionComplianceRule
```

eDiscovery Admin

eDiscovery Admin - *eDiscovery Admins create searches/holds on mailboxes, SharePoint Sites and OneDrive locations. They also manage/create eDiscovery case, content searches and add members to handle these cases.*

List current eDiscovery Admins – There are zero in a greenfield Office 365 Tenant

```
Get-eDiscoveryCaseAdmin
```

New eDiscovery Case Admin

```
Add-eDiscoveryCaseAdmin -User damian@practicalpowershell.com
```

Remove an eDiscovery Admin

```
Remove-eDiscoveryCaseAdmin -User damian@practicalpowershell.com
```

Replace Current eDiscovery Admin

```
Update-eDiscoveryCaseAdmin -Users john@domain.com,jane@domain.com
```

Documentation: https://docs.microsoft.com/en-us/powershell/exchange/office-365-scc/office-365-scc-powershell

Security and Compliance Center Admin Page – https://protection.office.com

Role Groups in the SCC

Role Group Cmdlets:

Get-RoleGroup – User 'Get-RoleGroup | FL' to get a detailed list of accounts in the SCC
New-RoleGroup – Add a custom group, with specific roles in the SCC
Remove-RoleGroup – Remove only custom and not built-in Role Groups
Set-RoleGroup – Modify settings on existing Role Groups

Cmdlet Usage:

```
Get-RoleGroup | Where {$_.Name -like '*admin*'} | Ft
New-RoleGroup 'View-Only Auditor' -Roles 'View-Only Audit Logs' -Members George
Remove-RoleGroup -Name  'View-Only Auditor'
Set-RoleGroup -Name  'View-Only Auditor' -Description "Users with View Only Auditing"

$CSV = Import-CSV "CustomGroupDescriptions.csv"
Foreach ($Group in $CSV) {Set-RoleGroup -Name $Group.Name -Description $Group.Description
}
```

Add User to Role Group

```
Add-RoleGroupMember -Identity Reviewer -Member Damian
Add-RoleGroupMember -Identity ComplianceAdministrator -Member "John Smith"
Add-RoleGroupMember -Identity eDiscoveryManager -Member "Scott Schnoll"
```

Verify Users in Role Group

```
Get-RoleGroupMember -Identity Reviewer
Get-RoleGroupMember -Identity ComplianceAdministrator
Get-RoleGroupMember -Identity eDiscoveryManager
```

Remove Users from Role Group

```
Remove-RoleGroupMember -IdentityReviewer -Member "Greg Taylor"
Remove-RoleGroupMember -Identity ComplianceAdministrator -Member "Van Hybrid"
Remove-RoleGroupMember -Identity eDiscoveryManager -Member "Jason Sherry"
```

Update Role Group MemberShip

```
Update-RoleGroupMember -Identity Reviewer -Members "Damian","Dave"
```

PowerShell Quick Reference - Security and Compliance Center (v1.0)

DLP CMDLETS

Get-DlpCompliancePolicy
Get-DlpComplianceRule
Get-DlpComplianceRuleV2
Get-DlpDetectionsReport
Get-DlpKeywordDictionary
Get-DlpSensitiveInformationType
Get-DlpSensitiveInformationTypeRulePackage
Get-DlpSiDetectionsReport
Migrate-DlpFingerprint
New-DlpCompliancePolicy
New-DlpComplianceRule
New-DlpComplianceRuleV2
New-DlpFingerprint
New-DlpKeywordDictionary
New-DlpSensitiveInformationType
New-DlpSensitiveInformationTypeRulePackage
Remove-DlpCompliancePolicy
Remove-DlpComplianceRule
Remove-DlpComplianceRuleV2
Remove-DlpKeywordDictionary
Remove-DlpSensitiveInformationType
Remove-DlpSensitiveInformationTypeRulePackage
Set-DlpCompliancePolicy
Set-DlpComplianceRule
Set-DlpComplianceRuleV2
Set-DlpKeywordDictionary
Set-DlpSensitiveInformationType
Set-DlpSensitiveInformationTypeRulePackage

Cmdlet Highlight

Get-SCInsights – provides user totals per workloads – ExO, Archive, SharePoint, OneDrive and more

Device Compliance

To use Device Management cmdlets – Enable MDM for tenant first:
https://support.office.com/en-us/article/overview-of-mobile-device-management-mdm-for-office-365-faa7d8e5-645d-4d59-839c-c8d4c1869e4a

New Device Rule – Tenant Wide, Less Options
New-DeviceTenantRule

New Device Rule – Very Specific Configuration, More Options
New-DeviceConfigurationRule

**** Note** the two cmdlet above have Set, Get and Remove Verbs as well

Device Rules can be used in conjunction with Conditional Access
Get-DeviceConditionalAccessPolicy
Get-DeviceConditionalAccessRule
New-DeviceConditionalAccessPolicy
New-DeviceConditionalAccessRule
Remove-DeviceConditionalAccessPolicy
Remove-DeviceConditionalAccessRule
Set-DeviceConditionalAccessPolicy
Set-DeviceConditionalAccessRule

REGEX Testing / Reference

RegEx Testing

https://regex101.com/
https://regexr.com/
http://osherove.com/tools

Microsoft RegEx Reference

https://docs.microsoft.com/en-us/dotnet/standard/base-types/regular-expression-language-quick-reference

Coming Soon in v1.1

Get-Label
Get-LabelPolicy
Get-LabelPolicyRule
New-Label
New-LabelPolicy
Remove-Label
Remove-LabelPolicy
Remove-RecordLabel
Set-LabelPolicy

Protection Alerting

Get-ProtectionAlert MalwareAlert
New-ProtectionAlert -Category Others -Name MalwareAlert -NotifyUser damian@practicalpowershell.com -ThreatType Malware -Threshold 20 -TimeWindow 61
Remove-ProtectionAlert MalwareAlert
Set-ProtectionAlert MalwareAlert -TimeWindow 90

Created By:

Damian Scoles
Microsoft MVP
Book Author
www.practicalpowershell.com
justaucguy.wordpress.com
@PPowerShell

Helpful Tips

Tab through parameters to see all available
Check for latest module version
Read the latest Microsoft Docs for SCC
Read Teams MVP blogs for more tips
Use MFA for better security
Need Help – 'Get-Help'
Read cmdlet Synopsis for functionality

Reporting Cmdlets

Get-DataRetentionReport
Get-DeviceComplianceDetailsReport
Get-DeviceComplianceDetailsReportFilter
Get-DeviceComplianceReportDate
Get-DeviceComplianceSummaryReport
Get-DeviceComplianceUserReport
Get-DlpDetectionsReport
Get-DlpSiDetectionsReport
Get-MailFilterListReport
Get-SupervisoryReviewPolicyReport
Get-SupervisoryReviewReport

More On PowerShell

Windows PowerShell Blog
blogs.msdn.com/b/powershell
Script Center
technet.microsoft.com/scriptcenter
PowerShell Tips of the Week
www.practicalpowershell.com/blog
PowerShell Team – GitHub
https://github.com/powershell

PowerShell Quick Reference - Security and Compliance Center (v1.0)

DLP Sensitive Information Types

Find existing Sensitive Information Types:

```
Get-DlpSensitiveInformationType
```

Create new Sensitive Information Type with Fingerprints:

```
$Content01 = Get-Content "\\File01\HR\EmployeeInfo.docx" -Encoding byte
$FingerPrint01 = New-DlpFingerprint -FileData $Content01 -Description "Confidential Employee Information"
New-DlpSensitiveInformationType -Name "Confidential Employee Information" -Fingerprints  $FingerPrint01 -Description "Sensitive Employee Information - HR"
```

Remove old unused Sensitive Information Types:

```
Remove-DlpSensitiveInformationType – Name "Confidential Employee Information"
```

Change an existing Sensitive Information Type:

```
Set-DlpSensitiveInformationType – Name "Confidential Employee Information"
```

Working with Compliance Cases

Create New Case

```
New-ComplianceCase -Name “Case # 4302-1” -Description “Legal Case – R&D – 10-2018”
```

Add Compliance Case Members

```
Add-ComplianceCaseMember -Case “Case # 4302-1” -Member damian@practicalpowershell.com
Add-ComplianceCaseMember -Case “Case # 4302-1” -Member dave@practicalpowershell.com
```

Add Searches and Holds to the Case

```
New-CaseHoldPolicy -Name "Hold - Damian" -Case "Case # 4302-1" -ExchangeLocation "John”
New-ComplianceSearch -Name “Secret Meetings” -ExchangeLocation Damian -ContentMatchQuery "subject:Secret Meettings"
```

Start the Search and apply a Search Action

```
Start-ComplianceSearch -Identity “Secret Meetings”
New-ComplianceSearchAction -SearchName “Secret Meetings” -Export
```

View Existing Compliance Cases

```
Get-ComplianceCase
```

Compliance Holds and Tags

Create a new compliance tag:

```
New-ComplianceTag -Name "R&D" -RetentionAction Delete -RetentionDuration 365 -RetentionType TaggedAgeInDays
```

List all current Compliance Tags

```
Get-ComplianceTag
```

Removing and existing Compliance Tag

```
Remove-ComplianceTag-Name "R&D"
```

Modifying an existing tag by adding a reviewer

```
Set-ComplianceTag -Name "R&D" -Reviewer damian@practicapowerhsell.com
```

Security, Privacy and Compliance Blog

https://techcommunity.microsoft.com/t5/Security-Privacy-and-Compliance/bg-p/securityprivacycompliance

Permissions in Security and Compliance Center

https://docs.microsoft.com/en-us/office365/securitycompliance/permissions-in-the-security-and-compliance-center

First, create a Hold Compliance Policy

```
New-HoldCompliancePolicy -Name “Case 5412-10” -ExchangeLocation john@standard.net
```

Then create one or more Hold Compliance Rules

```
New-HoldComplianceRule -Policy “Case 5412-10” -Name “Hold 2017” -ContentDateFrom “01/01/2017” -ContentDateTo “12/31/17”
```

Removing policies or rules

```
Remove-HoldCompliancePolicy “Case 5412-10”
Remove-HoldComplianceRule “Hold 2017”
```

Modify existing rules or policies:

```
Set-HoldCompliancePolicy -Name “Case 5412-10” -SharePointLocation "http://standard.sharepoint.com/sites/Teams/R&D"
Set-HoldComplianceRule -Name “Hold 2017”  -ContentDateFrom “07/01/17"
```

List policies or rules that were created previously

```
Get-HoldCompliancePolicy
Get-HoldComplianceRule -Name “Hold 2017”
```

PowerShell Quick Reference - Security and Compliance Center (v1.0)

Admin Audit Log

View Default Admin Audit Log Settings

```
Get-AdminAuditLogConfig
```

Search the Admin Audit Log and send Email of results

```
New-AdminAuditLogSearch -StartDate 8/1/18 -EndDate 8/15/18 -StatusMailRecipients damian@practicalpowershell.com
```

Disable/Enable Office 365 Admin Audit logs

```
Set-AdminAuditLogConfig -UnifiedAuditLogIngestionEnabled $False
Set-AdminAuditLogConfig -UnifiedAuditLogIngestionEnabled $True
```

*** Note – Changes (using Set) need to be performed in Exchange Online PowerShell*

New Unified Log Search – Exchange, SharePoint, OneDrive, Intune, AzureAD and more!

```
Search-UnifiedAuditLog -StartDate 10/1/2018 -EndDate 10/24/18
```

Or SharePoint Only - Search-UnifiedAuditLog -StartDate 10/1/2018 -EndDate 10/24/18 -RecordType SharePoint

Create Custom XML for DLP

https://justaucguy.wordpress.com/2014/11/21/adventures-in-custom-dlp-rules-part-one/

DLP Keyword Dictionary

Create a list of keywords to be used by DLP to protect information in your tenant

Check settings on Existing Dictionary:

```
Get-DlpKeywordDictionary -Name "Technical Docs"
```

Create New DLP Keywords Dictionary

```
$DLPKeywords = "Technical Specifications, Research Grant, Development Methodologies"
$EncodedDLPKeywords = [system.Text.Encoding]::UTF8.GetBytes($DLPKeywords);
New-DlpKeywordDictionary -Name "Technical Docs" -Description "Keywords appearing in internal docs" -FileData $EncodedDLPKeywords
```

Remove an unneeded dictionary

```
Remove-DlpKeywordDictionary -Name "Technical Docs"
```

Modify an Existing Dictionary (removing keywords in this case)

```
$DLPKeywords = "Technical Specifications, Development Methodologies"
$EncodedDLPKeywords = [system.Text.Encoding]::UTF8.GetBytes($DLPKeywords);
Set-DlpKeywordDictionary -Name "Technical Docs" -FileData $EncodedDLPKeywords
```

Auditing

Change Audit Config

```
Set-AuditConfig -Workload Exchange,SharePoint,OneDriveForBusiness,Intune
```

Audit all operations for a workload:

```
New-AuditConfigurationPolicy -Workload SharePoint
```

Remove existing Audit Configuration Policy

```
Remove-AuditConfigurationPolicy 91f20f6f-7ef9-4561-9a38-d771452d5e45
```

Audit specific operations in a workload

```
New-AuditConfigurationRule -Workload Exchange,SharePoint -AuditOperation Delete
```

Modify existing Audit Configuration Rule

```
Set-AuditConfigurationRule
```

Remove existing Audit Configuration Rule

```
New-AuditConfigurationRule -Identity <GUID of Rule>
```

Current Configutation:

```
Get-AuditConfig
Get-AuditConfigurationPolicy
Get-AuditConfigurationRule
```

Supervisory Review

First we need to create a Supervisory Policy as none exist by default:

```
New-SupervisoryReviewPolicyV2 -Name "R&D" -Reviewers george@cooltoys.com -Comment "Monitory R&D emails"
```

Then create one or more Supervisory Rules:

```
New-SupervisoryReviewRule -SamplingRate 50 -Policy "R&D" -Condition (Reviewee:damian@cooltoys.com)
```

Grab reports or information on the rules / policies created:

```
Get-SupervisoryReviewPolicyReport,  Get-SupervisoryReviewPolicyV2
Get-SupervisoryReviewReport, Get-SupervisoryReviewRule
```

Remove a policy (No cmdlet for removing a rule):**

```
Remove-SupervisoryReviewPolicyV2
```

Modify existing rules/policies

```
Set-SupervisoryReviewPolicyV2 -Name "R&D"  -Reviewers “greg@cooltoys.com”
Set-SupervisoryReviewRule -SamplingRate 25 -Policy "R&D"
```

Security and Compliance Center (v1.0) – Complete Cmdlet List

Add-ComplianceCaseMember
Add-eDiscoveryCaseAdmin
Add-RoleGroupMember
Enable-ComplianceTagStorage
Get-ActivityAlert
Get-AdminAuditLogConfig
Get-AuditConfig
Get-AuditConfigurationPolicy
Get-AuditConfigurationRule
Get-CaseHoldPolicy
Get-CaseHoldRule
Get-ComplianceCase
Get-ComplianceCaseMember
Get-ComplianceCaseStatistics
Get-ComplianceRetentionEvent
Get-ComplianceRetentionEventType
Get-ComplianceSearch
Get-ComplianceSearchAction
Get-ComplianceSecurityFilter
Get-ComplianceTag
Get-ComplianceTagStorage
Get-DataRetentionReport
Get-DeviceComplianceDetailsReport
Get-DeviceComplianceDetailsReportFilter
Get-DeviceCompliancePolicyInventory
Get-DeviceComplianceReportDate
Get-DeviceComplianceSummaryReport
Get-DeviceComplianceUserInventory
Get-DeviceComplianceUserReport
Get-DeviceConditionalAccessPolicy
Get-DeviceConditionalAccessRule
Get-DeviceConfigurationPolicy
Get-DeviceConfigurationRule
Get-DevicePolicy
Get-DeviceTenantPolicy
Get-DeviceTenantRule
Get-DlpCompliancePolicy
Get-DlpComplianceRule
Get-DlpComplianceRuleV2
Get-DlpDetectionsReport
Get-DlpKeywordDictionary
Get-DlpSensitiveInformationType
Get-DlpSensitiveInformationTypeRulePackage
Get-DlpSiDetectionsReport
Get-eDiscoveryCaseAdmin
Get-Group
Get-HoldCompliancePolicy
Get-HoldComplianceRule
Get-Label

Get-LabelPolicy
Get-LabelPolicyRule
Get-MailFilterListReport
Get-ManagementRole
Get-ProtectionAlert
Get-Recipient
Get-RetentionCompliancePolicy
Get-RetentionComplianceRule
Get-RoleGroup
Get-RoleGroupMember
Get-SCInsights
Get-SecurityPrincipal
Get-SupervisoryReviewPolicyReport
Get-SupervisoryReviewPolicyV2
Get-SupervisoryReviewReport
Get-SupervisoryReviewRule
Get-TeamsRetentionCompliancePolicy
Get-TeamsRetentionComplianceRule
Get-User
Install-UnifiedCompliancePrerequisite
Migrate-DlpFingerprint
New-ActivityAlert
New-AdminAuditLogSearch
New-AuditConfigurationPolicy
New-AuditConfigurationRule
New-CaseHoldPolicy
New-CaseHoldRule
New-ComplianceCase
New-ComplianceRetentionEvent
New-ComplianceRetentionEventType
New-ComplianceSearch
New-ComplianceSearchAction
New-ComplianceSecurityFilter
New-ComplianceTag
New-DeviceConditionalAccessPolicy
New-DeviceConditionalAccessRule
New-DeviceConfigurationPolicy
New-DeviceConfigurationRule
New-DeviceTenantPolicy
New-DeviceTenantRule
New-DlpCompliancePolicy
New-DlpComplianceRule
New-DlpComplianceRuleV2
New-DlpFingerprint
New-DlpKeywordDictionary
New-DlpSensitiveInformationType
New-DlpSensitiveInformationTypeRulePackage
New-HoldCompliancePolicy

New-HoldComplianceRule
New-Label
New-LabelPolicy
New-ProtectionAlert
New-RetentionCompliancePolicy
New-RetentionComplianceRule
New-RoleGroup
New-SupervisoryReviewPolicyV2
New-SupervisoryReviewRule
New-TeamsRetentionCompliancePolicy
New-TeamsRetentionComplianceRule
Remove-ActivityAlert
Remove-AuditConfigurationPolicy
Remove-AuditConfigurationRule
Remove-CaseHoldPolicy
Remove-CaseHoldRule
Remove-ComplianceCase
Remove-ComplianceCaseMember
Remove-ComplianceRetentionEvent
Remove-ComplianceRetentionEventType
Remove-ComplianceSearch
Remove-ComplianceSearchAction
Remove-ComplianceSecurityFilter
Remove-ComplianceTag
Remove-DeviceConditionalAccessPolicy
Remove-DeviceConditionalAccessRule
Remove-DeviceConfigurationPolicy
Remove-DeviceConfigurationRule
Remove-DeviceTenantPolicy
Remove-DeviceTenantRule
Remove-DlpCompliancePolicy
Remove-DlpComplianceRule
Remove-DlpComplianceRuleV2
Remove-DlpKeywordDictionary
Remove-DlpSensitiveInformationType
Remove-DlpSensitiveInformationTypeRulePackage
Remove-eDiscoveryCaseAdmin
Remove-HoldCompliancePolicy
Remove-HoldComplianceRule
Remove-Label
Remove-LabelPolicy
Remove-ProtectionAlert
Remove-RecordLabel
Remove-RetentionCompliancePolicy
Remove-RetentionComplianceRule
Remove-RoleGroup
Remove-RoleGroupMember
Remove-SupervisoryReviewPolicyV2

Remove-TeamsRetentionCompliancePolicy
Remove-TeamsRetentionComplianceRule
Search-AdminAuditLog
Set-ActivityAlert
Set-AuditConfig
Set-AuditConfigurationRule
Set-CaseHoldPolicy
Set-CaseHoldRule
Set-ComplianceCase
Set-ComplianceRetentionEvent
Set-ComplianceRetentionEventType
Set-ComplianceSearch
Set-ComplianceSearchAction
Set-ComplianceSecurityFilter
Set-ComplianceTag
Set-DeviceConditionalAccessPolicy
Set-DeviceConditionalAccessRule
Set-DeviceConfigurationPolicy
Set-DeviceConfigurationRule
Set-DeviceTenantPolicy
Set-DeviceTenantRule
Set-DlpCompliancePolicy
Set-DlpComplianceRule
Set-DlpComplianceRuleV2
Set-DlpKeywordDictionary
Set-DlpSensitiveInformationType
Set-DlpSensitiveInformationTypeRulePackage
Set-HoldCompliancePolicy
Set-HoldComplianceRule
Set-LabelPolicy
Set-ProtectionAlert
Set-RetentionCompliancePolicy
Set-RetentionComplianceRule
Set-RoleGroup
Set-SupervisoryReviewPolicyV2
Set-SupervisoryReviewRule
Set-TeamsRetentionCompliancePolicy
Set-TeamsRetentionComplianceRule
Start-ComplianceSearch
Stop-ComplianceSearch
Test-DataClassification
Update-ComplianceCaseMember
Update-eDiscoveryCaseAdmin
Update-RoleGroupMember
Validate-RetentionRuleQuery