1 Transport:

Set-SendConnector
Set-SenderFilterConfig
Set-SenderReputationConfig
Set-ReceiveConnector
Set-TransportServer
Set-TransportService
Set-TransportConfig
Set-PopSettings
Set-ImapSettings
SEND/RECEIVE CONNECTORs!!

- 1.1 **Set 'Maximum send size - connector level'** to '10240' (Not Scored)
  ***Audit**:*
  Execute the following cmdlet and ensure MaxMessageSize is set to '10240':
  Get-SendConnector "Connection to Contoso.com" | fl -property MaxMessageSize
  ***Remediation**:*
  To implement the recommended state, execute the following PowerShell cmdlet:
  Set-SendConnector "Connection to Contoso.com" -MaxMessageSize 10240KB
- 1.2 **Set 'Maximum receive size - organization level'** to '10240' (Not Scored)
  ***Audit**:*
  Execute the following cmdlet and ensure MaxReceiveSize is set to '10240 ':
  Get-TransportConfig | fl -property MaxReceiveSize
  ***Remediation**:*
  To implement the recommended state, execute the following PowerShell cmdlet:
  Set-TransportConfig -MaxReceiveSize 10240KB
- 1.3 **Set 'Enable Sender ID agent'** to 'True' (Scored)
  ***Audit**:*
  Execute the following cmdlet and ensure InternalSMTPServers is set to 'True':
  Set-SenderIDConfig | fl -property Enabled
  ***Remediation**:*
  To remediate this settings, execute the following cmdlet:
  Set-SenderIDConfig -Enabled $true
- 1.4 **Set 'External send connector authentication: DNS Routing'** to 'True' (Not Scored)
  ***Audit**:*
  Execute the following cmdlet and ensure DNSRoutingEnabled is set to 'True':
  Get-SendConnector "Connection to Contoso.com" | fl -property DNSRoutingEnabled
  ***Remediation**:*
  To implement the recommended state, execute the following PowerShell cmdlet:
  Set-SendConnector "Connection to Contoso.com" -DNSRoutingEnabled $true
- 1.5 **Set 'Configure Sender Filtering'** to 'Enabled' (Scored)
  ***Audit**:*
  Execute the following cmdlet and ensure Enabled is set to 'True':
  Get-SenderFilterConfig | fl -property Enabled
  Remediation:

To implement the recommended state, execute the following PowerShell cmdlet:
Set-SenderFilterConfig -Enabled $true

- 1.6 **Set 'Enable Sender reputation'** to 'True' (Scored)
  ***Audit**:*
  Execute the following cmdlet and ensure SenderBlockingEnabled and OpenProxyDetectionEnabled are set to 'True':
  Get-SenderReputationConfig | fl -property SenderBlockingEnabled
  ***Remediation**:*
  To implement the recommended state, execute the following PowerShell cmdlet:
  Set-SenderReputationConfig -SenderBlockingEnabled $true -OpenProxyDetectionEnabled $true
- 1.7 **Set 'Maximum number of recipients - organization level'** to '5000' (Scored)
  ***Audit**:*
  Execute the following cmdlet and ensure PickupDirectoryMaxRecipientsPerMessage is set to '5000':
  Get-TransportService -Identity "Server01" | fl -property PickupDirectoryMaxRecipientsPerMessage
  Remediation:
  To implement the recommended state, execute the following PowerShell cmdlet:
  Set-TransportService -Identity "Server01" -PickupDirectoryMaxRecipientsPerMessage 5000
- 1.8 **Set 'External send connector authentication: Ignore Start TLS'** to 'False' (Scored)
  ***Audit**:*
  Execute the following cmdlet and ensure IgnoreSTARTTLS is set to 'False':
  Get-SendConnector -identity <connector_name> | fl -property IgnoreSTARTTLS
  ***Remediation**:*
  To implement the recommended state, execute the following PowerShell cmdlet:
  set-SendConnector -identity <connector_name> -IgnoreSTARTTLS: $false
- 1.9 **Set 'Configure login authentication for POP3'** to 'SecureLogin' (Scored)
  ***Audit**:*
  Execute the following cmdlet and ensure SecureLogin is set to 'SecureLogin':
  Get-PopSettings | fl -property LoginType
  ***Remediation**:*
  To implement the recommended state, execute the following PowerShell cmdlet:
  Set-PopSettings -LoginType SecureLogin
- 1.10 **Set receive connector 'Configure Protocol logging'** to 'Verbose' (Scored)
  Audit:
  Execute the following cmdlet and ensure ProtocolLoggingLevel is set to 'Verbose':
  Get-ReceiveConnector "<IDENTITY>" | fl -property ProtocolLoggingLevel
  ***Remediation**:*
  To implement the recommended state, execute the following PowerShell cmdlet:
  Set-ReceiveConnector "<IDENTITY>" -ProtocolLoggingLevel Verbose
- 1.11 **Set send connector 'Configure Protocol logging'** to 'Verbose' (Scored)
  ***Audit**:*
  Execute the following cmdlet and ensure ProtocolLogginglevel is set to 'Verbose':
  Get-SendConnector "IDENTITY" | fl -property ProtocolLoggingLevel

***Remediation**:*
To implement the recommended state, execute the following PowerShell cmdlet:
Set-SendConnector "IDENTITY" -ProtocolLoggingLevel Verbose

- 1.12 **Set 'External send connector authentication: Domain Security'** to 'True' (Scored)
  ***Audit**:*
  Execute the following cmdlet and ensure DomainSecureEnabled is set to 'True':
  get-sendconnector -Identity <SendConnectorIdParameter> | fl DomainSecureEnabled
  Remediation:
  To implement the recommended state, execute the following PowerShell cmdlet:
  set-sendconnector -Identity <SendConnectorIdParameter> -DomainSecureEnabled $true
- 1.13 **Set 'Message tracking logging - Transport'** to 'True' (Scored)
  ***Audit**:*
  Execute the following cmdlet and ensure MessageTrackingLogEnabled is set to 'True':
  Get-TransportService EXCHANGE1 | fl -property MessageTrackingLogEnabled
  ***Remediation**:*
  To implement the recommended state, execute the following PowerShell cmdlet:
  Set-TransportService EXCHANGE1 -MessageTrackingLogEnabled $true
- 1.14 **Set 'Message tracking logging - Mailbox'** to 'True' (Scored)
  ***Audit**:*
  Execute the following cmdlet and ensure MessageTrackingLogEnabled is set to 'True':
  Get-TransportService EXCHANGE1 | fl -property -MessageTrackingLogEnabled
  ***Remediation**:*
  To implement the recommended state, execute the following PowerShell cmdlet:
  Set-TransportService EXCHANGE1 -MessageTrackingLogEnabled $true
- 1.15 **Set 'Configure login authentication for IMAP4'** to 'SecureLogin' (Scored)
  ***Audit**:*
  Execute the following cmdlet and ensure LoginType is set to 'SecureLogin':
  Get-ImapSettings | fl -property LoginType
  Remediation:
  To implement the recommended state, execute the following PowerShell cmdlet:
  Set-ImapSettings -LoginType SecureLogin
- 1.16 **Set 'Turn on Connectivity logging'** to 'True' (Scored)
  ***Audit**:*
  Execute the following cmdlet and ensure ConnectivityLogEnabled is set to 'True':
  Get-TransportService EXCHANGE1 | fl -property ConnectivityLogEnabled
  ***Remediation**:*
  To implement the recommended state, execute the following PowerShell cmdlet:
  Set-TransportService EXCHANGE1 -ConnectivityLogEnabled $true
- 1.17 **Set 'Maximum send size - organization level'** to '10240' (Scored)
  ***Audit**:*
  Execute the following cmdlet and ensure MaxSendSize is set to '10240':
  Get-TransportConfig | fl -property MaxSendSize
  ***Remediation**:*
  To implement the recommended state, execute the following PowerShell cmdlet:

Set-TransportConfig -MaxSendSize 10240KB

- 1.18 **Set 'Maximum receive size - connector level'** to '10240' (Scored)
  ***Audit**:*
  Execute the following cmdlet and ensure MaxMessageSize is set to '10240KB':
  Get-ReceiveConnector "Connection from Contoso.com" | fl -property MaxMessageSize
  ***Remediation**:*
  To implement the recommended state, execute the following PowerShell cmdlet:
  Set-ReceiveConnector "Connection from Contoso.com" -MaxMessageSize 10240KB

2 Mailbox:

Set-MailboxDatabase

Set-ActiveSyncMailboxPolicy

Set-UMService

Set-UMMailboxPolicy

Set-UMDialPlan

Set-CASMailbox

- 2.1 **Set 'Mailbox quotas: Issue warning at'** to '1991680' (Not Scored)
  ***Audit**:*
  Execute the following cmdlet and ensure IssueWarningQuota is set to '1991680KB':
  Get-MailboxDatabase "EXCHANGE01\Mailbox Database" | fl -property IssueWarningQuota
  Remediation:
  To implement the recommended state, execute the following PowerShell cmdlet:
  Set-MailboxDatabase "EXCHANGE01\Mailbox Database" -IssueWarningQuota 1991680KB
- 2.2 **Set 'Mailbox quotas: Prohibit send and receive at'** to '2411520' (Not Scored)
  ***Audit**:*
  Execute the following cmdlet and ensure ProhibitSendReceiveQuota is set to '2411520KB':
  Get-MailboxDatabase "EXCHANGE01\Mailbox Database" | fl -property ProhibitSendReceiveQuota
  ***Remediation**:*
  To implement the recommended state, execute the following PowerShell cmdlet:
  Set-MailboxDatabase "EXCHANGE01\Mailbox Database" -ProhibitSendReceiveQuota 2411520KB
- 2.3 **Set 'Mailbox quotas: Prohibit send at'** to '2097152' (Not Scored)
  ***Audit**:*
  Execute the following cmdlet and ensure ProhibitSendQuota is set to '2097152KB':
  Get-MailboxDatabase "EXCHANGE01\Mailbox Database" | fl -property ProhibitSendQuota
  ***Remediation**:*
  To implement the recommended state, execute the following PowerShell cmdlet:
  Set-MailboxDatabase "EXCHANGE01\Mailbox Database" -ProhibitSendQuota 2097152KB

- 2.4 **Set 'Keep deleted mailboxes for the specified number of days'** to '30' (Scored)
  Audit:
  Execute the following cmdlet and ensure MailboxRetention is set to '30.00:00:00':
  Get-Mailboxdatabase "EXCHANGE01\Mailbox Database" | fl -property MailboxRetention
  Remediation:
  To implement the recommended state, execute the following PowerShell cmdlet:
  Set-Mailboxdatabase "EXCHANGE01\Mailbox Database" -MailboxRetention 30.00:00:00
- 2.5 Set **'Do not permanently delete items until the database has been backed up'** to 'True' (Scored)
  Audit*:*
  Execute the following cmdlet and ensure RetainDeletedItemsUntilBackup is set to 'True':
  Get-MailboxDatabase <Mailbox Database Name> | fl -property RetainDeletedItemsUntilBackup
  Remediation:
  To implement the recommended state, execute the following PowerShell cmdlet:
  Set-MailboxDatabase <Mailbox Database Name> -RetainDeletedItemsUntilBackup $true
- 2.6 **Set 'Allow simple passwords'** to 'False' (Scored)
  Audit*:*
  Execute the following cmdlet and ensure AllowSimpleDevicePassword is set to 'False':
  Get-MobileDeviceMailboxPolicy | fl -property AllowSimplePassword
  Remediation*:*
  To implement the recommended state, execute the following PowerShell cmdlet:
  Set-MobileDeviceMailboxPolicy <Profile> -AllowSimplePassword $false
- 2.7 **Set 'Enforce Password History'** to '4' or greater (Scored)
  Audit*:*
  Execute the following cmdlet and ensure DevicePasswordHistory is set to '4' or greater:
  Get-MobileDeviceMailboxPolicy | fl -property PasswordHistory
  Remediation*:*
  To implement the recommended state, execute the following PowerShell cmdlet:
  Set-MobileDeviceMailboxPolicy <Profile> -PasswordHistory 4
- 2.8 **Set 'Password Expiration'** to '90' or less (Scored)
  Audit:
  Execute the following cmdlet and ensure DevicePasswordExpiration is set to '90' or less:
  Get-MobileDeviceMailboxPolicy | fl -property PasswordExpiration
  Remediation*:*
  To implement the recommended state, execute the following PowerShell cmdlet:
  Set-MobileDeviceMailboxPolicy default -PasswordExpiration 90
- 2.9 **Set 'Minimum password length'** to '4' or greater (Scored)
  Audit*:*
  Execute the following cmdlet and ensure MinDevicePasswordLength is set to '4' or greater:
  Get-MobileDeviceMailboxPolicy | fl -property MinPasswordLength
  Remediation*:*
  To implement the recommended state, execute the following PowerShell cmdlet:
  Set-MobileDeviceMailboxPolicy default -MinPasswordLength 4

- 2.10 **Set 'Configure startup mode'** to 'TLS' (Scored)
  ***Audit**:*
  Execute the following cmdlet and ensure UMStartUpMode is set to 'TCP':
  Get-UMService -Identity Exchange1| fl -property UMStartUpMode
  ***Remediation**:*
  To implement the recommended state, execute the following PowerShell cmdlet:
  Set-UMService -Identity Exchange1 -UMStartUpMode TLS
- 2.11 **Set 'Refresh interval'** to '1' (Scored)
  Audit:
  Execute the following PowerShell script and ensure DevicePolicyRefreshInterval is set to '1:00:00'.
  Get-MobileDeviceMailboxPolicy -Identity default| fl -property -DevicePolicyRefreshInterval
  ***Remediation**:*
  To implement the recommended state, execute the following PowerShell cmdlet:
  Set-MobileDeviceMailboxPolicy -Identity default -DevicePolicyRefreshInterval '1:00:00'
- 2.12 **Set 'Configure dial plan security'** to 'Secured' (Scored)
  ***Audit**:*
  Execute the following cmdlet and ensure VoIPSecurity is set to 'Secured':
  Get-UMDialPlan -identity MySecureDialPlan | fl -property VoIPSecurity
  ***Remediation**:*
  To implement the recommended state, execute the following PowerShell cmdlet:
  Set-UMDialPlan -identity MySecureDialPlan -VoIPSecurity Secured
- 2.13 **Set 'Allow access to voicemail without requiring a PIN'** to 'False' (Scored)
  ***Audit**:*
  Execute the following PowerShell cmdlet and ensure AllowPinlessVoiceMailAccess is set to 'False':
  Get-UMMailboxPolicy -id MyUMMailboxPolicy | fl -property AllowPinlessVoiceMailAccess
  ***Remediation**:*
  To implement the recommended state, execute the following PowerShell cmdlet:
  Set-UMMailboxPolicy -id MyUMMailboxPolicy -AllowPinlessVoiceMailAccess $false
- 2.14 **Set 'Retain deleted items for the specified number of days'** to '14' (Scored)
  Audit:
  Execute the following PowerShell cmdlet and ensure DeletedItemRetention is set to '14':
  Get-MailboxDatabase -Identity MDB2 | fl -property DeletedItemRetention
  ***Remediation**:*
  To implement the recommended state, execute the following PowerShell cmdlet:
  Set-MailboxDatabase -Identity MDB2 -DeletedItemRetention 14
- 2.15 **Set 'Allow unmanaged devices'** to 'False' (Scored)
  ***Audit**:*
  Execute the following PowerShell cmdlet and ensure AllowNonProvisionableDevices is set to "False':
  Get-MobileDeviceMailboxPolicy -Identity default | fl -property AllowNonProvisionableDevices
  Remediation:
  To implement the recommended state, execute the following PowerShell cmdlet:
  Set-MobileDeviceMailboxPolicy -Identity default -AllowNonProvisionableDevices $false

- 2.16 **Set 'Require encryption on device'** to 'True' (Scored)
  ***Audit**:*
  Execute the following PowerShell cmdlet and ensure RequireDeviceEncryption is set to 'True':
  Get-MobileDeviceMailboxPolicy -Identity default | fl -property RequireDeviceEncryption
  ***Remediation**:*
  To implement the recommended state, execute the following PowerShell cmdlet:
  Set-MobileDeviceMailboxPolicy -Identity default -RequireDeviceEncryption $true
- 2.17 **Set 'Time without user input before password must be re-entered'** to '15' (Scored)
  ***Audit**:*
  Execute the following PowerShell cmdlet and ensure MaxInactivityTimeLock is set to '15':
  Get-MobileDeviceMailboxPolicy -Identity Default | fl -property MaxInactivityTimeLock
  ***Remediation**:*
  To implement the recommended state, execute the following PowerShell cmdlet:
  Set-MobileDeviceMailboxPolicy -Identity Default -MaxInactivityTimeLock 00:15:00
- 2.18 **Set 'Require alphanumeric password'** to 'True' (Scored)
  ***Audit**:*
  Execute the following PowerShell cmdlet and ensure AlphanumericPasswordRequired is set to 'True':
  Get-MobileDeviceMailboxPolicy -Identity Default | fl -property AlphanumericPasswordRequired
  ***Remediation**:*
  To implement the recommended state, execute the following PowerShell cmdlet:
  Set-MobileDeviceMailboxPolicy -Identity Default -AlphanumericPasswordRequired $true
- 2.19 **Set 'Require client MAPI encryption'** to 'True' (Scored)
  ***Audit**:*
  Execute the following PowerShell cmdlet and ensure EncryptionRequired is set to 'True'
  Get-RpcClientAccess | fl -property EncryptionRequired
  ***Remediation**:*
  To implement the recommended state, execute the following PowerShell cmdlet:
  Set-RpcClientAccess -Server CAS01 EncryptionRequired $true
- 2.20 **Set 'Number of attempts allowed'** to '10' (Scored)
  ***Audit**:*
  Execute the following PowerShell cmdlet and ensure MaxPasswordFailedAttempts is set to '10' or less:
  Get-MobileDeviceMailboxPolicy -Identity Default | fl -property MaxPasswordFailedAttempts
  ***Remediation**:*
  To implement the recommended state, execute the following PowerShell cmdlet:
  Set-MobileDeviceMailboxPolicy -Identity Default -MaxPasswordFailedAttempts 10
- 2.21 **Set 'Require password'** to 'True' (Scored)
  ***Audit**:*
  Execute the following PowerShell cmdlet and ensure PasswordEnabled is set to 'True':
  Get-MobileDeviceMailboxPolicy -Identity Default | fl -property PasswordEnabled
  ***Remediation**:*
  To implement the recommended state, execute the following PowerShell cmdlet:
  Set-MobileDeviceMailboxPolicy -Identity Default -PasswordEnabled $true

3 Other:

Set-ExecutionPolicy
Set-RemoteDomain
Set-OwaVirtualDirectory
Set-AdminAuditLogConfig

- 3.1 **Set cmdlets 'Turn on Administrator Audit Logging'** to 'True' (Scored)
  ***Audit**:*
  Execute the following cmdlet and ensure AdminAuditLogCmdlets is set to '':*
  Get-AdminAuditLogConfig | fl -property AdminAuditLogCmdlets
  ***Remediation**:*
  To implement the recommended state, execute the following PowerShell cmdlet:
  *Set-AdminAuditLogConfig -AdminAuditLogCmdlets **
- 3.2 **Set 'Require Client Certificates'** to 'Required' (Not Scored)

- 3.3 **Set 'Turn on script execution'** to 'RemoteSigned' (Scored)
  ***Audit**:*
  Execute the following cmdlet and ensure RemoteSigned is set to 'RemoteSigned':
  Get-ExecutionPolicy | fl -property RemoteSigned
  ***Remediation**:*
  To implement the recommended state, execute the following PowerShell cmdlet:
  Set-ExecutionPolicy RemoteSigned
- 3.4 **Set 'Turn on Administrator Audit Logging'** to 'True' (Scored)
  ***Audit**:*
  Execute the following cmdlet and ensure AdminAuditLogEnabled is set to 'true':
  Get-AdminAuditLogConfig | fl -property AdminAuditLogEnabled
  ***Remediation**:*
  To implement the recommended state, execute the following PowerShell cmdlet:
  Set-AdminAuditLogConfig -AdminAuditLogEnabled $True
- 3.5 **Set 'Enable automatic replies to remote domains'** to 'False' (Scored)
  Audit:
  Execute the following cmdlet and ensure AutoReplyEnabled is set to 'False':
  Get-RemoteDomain -Identity Contoso | fl -property AutoReplyEnabled
  ***Remediation**:*
  To implement the recommended state, execute the following PowerShell cmdlet:
  Set-RemoteDomain -Identity Contoso -AutoReplyEnabled $false
- 3.6 **Set 'Allow basic authentication'** to 'False' (Scored)
  ***Audit**:*
  Execute the following cmdlet and ensure BasicAuthentication is set to 'True':
  Get-OwaVirtualDirectory -Identity "owa (Default Web Site)" | fl -property BasicAuthentication
  ***Remediation**:*
  To implement the recommended state, execute the following PowerShell cmdlet:
  Set-OwaVirtualDirectory -Identity "owa (Default Web Site)" -BasicAuthentication $false

- 3.7 **Set 'Enable non-delivery reports to remote domains'** to 'False' (Scored)
  ***Audit**:*
  Execute the following cmdlet and ensure NDREnabled is set to 'True':
  Get-RemoteDomain -Identity Contoso | fl -property NDREnabled
  ***Remediation**:*
  To implement the recommended state, execute the following PowerShell cmdlet:
  Set-RemoteDomain -Identity Contoso -NDREnabled $false
- 3.8 **Set 'Enable OOF messages to remote domains'** to 'None' (Scored)
  ***Audit**:*
  Execute the following cmdlet and ensure AllowedOOFType is set to 'External':
  Get-RemoteDomain "RemoteDomain" | fl -property AllowedOOFType
  ***Remediation**:*
  To implement the recommended state, execute the following PowerShell cmdlet:
  Set-RemoteDomain "RemoteDomain" -AllowedOOFType None
- 3.9 **Set 'Enable automatic forwards to remote domains'** to 'False' (Scored)
  ***Audit**:*
  Execute the following cmdlet and ensure AutoForwardEnabled is set to 'False':
  Get-RemoteDomain -Identity Contoso | fl -property AutoForwardEnabled
  ***Remediation**:*
  To implement the recommended state, execute the following PowerShell cmdlet:
  Set-RemoteDomain -Identity Contoso -AutoForwardEnabled $false
- 3.10 **Set 'Enable S/MIME for OWA 2010'** to 'True' (Scored)
  ***Audit**:*
  Execute the following cmdlet and ensure SMimeEnabled is set to 'True':
  Get-OWAVirtualDirectory -identity "owa (Default Web Site)" | fl -property SMimeEnabled
  ***Remediation**:*
  To implement the recommended state, execute the following PowerShell cmdlet:
  Set-OWAVirtualDirectory -identity "owa (Default Web Site)" -SMimeEnabled $true
- 3.11 **Set mailbox 'Turn on Administrator Audit Logging'** to 'True' (Scored)
  ***Audit**:*
  Execute the following cmdlet and ensure AdminAuditLogEnabled is set to 'True':
  Get-AdminAuditLogConfig | fl -property AdminAuditLogEnabled
  Remediation:
  To implement the recommended state, execute the following PowerShell cmdlet:
  Set-AdminAuditLogConfig -AdminAuditLogEnabled $true