پیکربندی امن

Microsoft Exchange 2016

مرکز مدیریت راهبردی افتا

SCMS-Exchange-SER-2016-1.0.0

فروردین 96

فهرست

مقدمه 3
تنظیمات 5
SCMS-1: به‌روزرسانی 5
SCMS-2: سیاست‌های حساب کاربری 5
SCMS-2-2: رعایت حداقل بازه تغییر گذرواژه برای استفاده از گذرواژه‌های تکراری 24
SCMS-2-3: فعال‌سازی الزامات پیچیدگی گذرواژه 25
SCMS-2-4: ذخیره نکردن گذرواژه‌ها با استفاده از رمزگذاری برگشت‌پذیر 25
SCMS-2-5: تنظیم بازه زمانی قفل شدن حساب کاربری 16
پیوست ..... **Error! Bookmark not defined.**

پیش‌گفتار

مرکز مدیریت راهبردی افتا[1] به منظور ساماندهی امنیت تجهیزات در حوزه فاوا[2]، پروژه «پیکربندی امن محصولات IT در کشور» را آغاز نموده است. یکی از گام‌های اساسی در این پروژه ارائه چک‌لیست و راهنمای پیکربندی امن برای محصولات IT می‌باشد. ارائه چک‌لیست برای محصولات داخلی بر عهده تولیدکننده محصول می‌باشد. تولید کننده ملزم است، چک‌لیست خود را در غالب ارائه شده از سمت مرکز افتا ارائه دهد. چک‌لیست‌های ارائه شده، توسط مرکز افتا مورد ارزیابی قرار گرفته و منتشر می‌گردد. سازمان‌های دولتی ملزم به استفاده از چک لیست‌های مذکور برای محصولات در حال استفاده خود هستند. همچنین سازمان‌های دولتی موظفند قبل از استفاده از محصولات IT، آن‌را مطابق چک‌لیست امنیتی مورد تایید مرکز افتا پیکربندی نمایند.

توجه به این نکته حائز اهمیت می‌باشد که چک‌لیست‌های ارائه شده، یک امنیت سطح پایه برای محصول ایجاد می‌نماید و سازمان ها ملزم هستند که برای رسیدن به سطح امنیت مورد نیاز خود، پس از اجرای مدیریت ریسک[3]، الزامات دیگری را نیز به این تنظیمات اضافه و مستند نمایند.

[1] امنیت فضای تولید و تبادل اطلاعات
[2] فناوری اطلاعات و ارتباطات
[3] Risk management

مقدمه

این سند، راهنمایی برای پیکربندی امن Microsoft Exchange 2016 است. در این سند مقادیر و تنظیمات مناسب برای امن سازی سیاست‌ها و پیکربندهای محصول یاد شده ارائه شده است. مدیر سامانه با استفاده از این سند می‌تواند تنظیمات ارائه شده را پیاده سازی نماید.

این سند توسط شرکت "بهین راهکار" و به درخواست و تحت نظارت مرکز مدیریت راهبردی افتا تهیه گردیده است و از تلاش کارشناسان آن شرکت صمیمانه قدردانی می‌گردد. مرکز مدیریت راهبردی افتا ضمن استقبال از نظرات کارشناسان و متخصصان این حوزه برای غنای بیشتر این سند و دیگر اسناد مقاوم سازی، آمادگی دریافت پیشنهادات سازنده از طریق آدرس پست الکترونیکی Hardening@aftasec.ir را اعلام می‌دارد.

در ادامه، تنظیمات مورد نیاز برای پیکربندی امن Microsoft Exchange 2016 آمده است. در این سند هر تنظیم با یک نام لاتین و شماره مختص آن آورده شده است. برای هر الزام دو بخش شرح اجمالی و نحوه پیاده-سازی ارائه شده است. در بخش شرح اجمالی، توضیحی مختصر از ماهیت الزام بیان گردیده و در بخش نحوه پیاده‌سازی نیز، راهنمایی برای پیاده‌سازی الزام توسط مدیر سامانه ارائه شده است.

تنظیمات

SCMS-1: انتقال

SCMS-1-1: تنظیم حداکثر سایز ارسال در سطح Controller با مقدار 10240. (غیر قابل شمارش)

شرح اجمالی:

این تنظیم، مجموع اندازه ی یک پیام را در سطح Connector، محدود می نماید. این شامل هدر پیام، بدنه ی آن و هر آنچه در پیوست پیام است، می باشد. برای جریان پیام داخلی، سرور Exchange از هدر پیام سفارشی برای ذخیره سازی مقدار سایز پیام اصلی استفاده می کند. هر زمانی که پیام با محدودیت های سایز پیام چک می گردد، کمترین مقدار هدر سایز پیام فعلی یا سایز پیام اصلی استفاده می گردد. سایز پیام به دلایلی نظیر تغییر محتوا، رمزنگاری و پردازش عامل می تواند تغییر کند.

نحوه پیاده‌سازی:

برای پیاده سازی حالت توصیه شده، دستور PowerShell زیر را اجرا نمایید:

```
Set-SendConnector "Connection to Contoso.com" -MaxMessageSize 10240KB
```

SCMS-1-2: تنظیم حداکثر سایز دریافت در سطح Organization با مقدار 10240 . (غیر قابل شمارش)

شرح اجمالی:

این محدودیت شامل هدر پیام، بدنه ی آن و هر آنچه در پیوست پیام است، می باشد. برای جریان پیام داخلی، سرور **Exchange** از هدر پیام سفارشی برای ذخیره سازی مقدار سایز پیام اصلی استفاده می کند. هر زمانی که پیام با محدودیت های سایز پیام چک می گردد، کمترین مقدار هدر سایز پیام فعلی یا سایز پیام اصلی استفاده می گردد. سایز پیام به دلایلی نظیر تغییر محتوا، رمزنگاری و پردازش عامل می تواند تغییر کند.

نحوه پیاده‌سازی:

برای پیاده سازی حالت توصیه شده، دستور PowerShell زیر را اجرا نمایید:

```
Set-TransportConfig -MaxReceiveSize 10240KB
```

SCMS-1-3: تنظیم Enable Sender ID agent با مقدار True (قابل شمارش)

شرح اجمالی:

Sender ID agent یک عامل **antispam** است که روی سرورهای **Exchange** راه اندازی می گردد تا نقش **Edge Transport server** را اجرا نماید. **Sender ID** مشخص می کند که هر پیام ارسالی از دامنه های اینترنت از جایی که ادعا می کنند ارسال شده باشند. این فیلد آدرس سرور ارسال کننده ی پیام را با لیستی از سرورهای مشخص شده در دامنه که امکان ارسال پیام از سمت آن ها وجود دارد، چک می نماید.

نحوه پیاده‌سازی:

برای پیاده سازی حالت توصیه شده، دستور زیر را اجرا نمایید:

```
Set-SenderIDConfig -Enabled $true
```

SCMS-1-4: تنظیم External send connector authentication: DNS Routing با مقدار True. (غیر قابل شمارش)

شرح اجمالی:

از این گزینه برای استفاده از **DNS** جهت مسیریابی ایمیل های بیرونی، استفاده نمایید. اگر این گزینه فعال باشد، اتصال دهنده از **DNS** استفاده می کند تا آدرس **IP** سرور **SMTP** مقصد را بیابد.

نحوه پیاده‌سازی:

برای پیاده سازی حالت توصیه شده، دستور PowerShell زیر را اجرا نمایید:

```
Set-SendConnector "Connection to Contoso.com" -DNSRoutingEnabled $true
```

SCMS-1-5: تنظیم Configure Sender Filtering با مقدار Enable. (قابل شمارش)

شرح اجمالی:

به صورت پیش فرض، این گزینه روی کامپیوتری که نقش سرور **Edge Transport** برای پیام های دریافتی از اینترنت که احراز هویت نشده اند را دارد، فعال است. این پیام ها در دسته پیام های خارجی قرار می گیرند. این

قابلیت را دارید که روی کامپیوتر مد نظرتان و از طریق کنسول مدیریتی **Exchange** و یا محیط **Management Shell** آن، عامل **Sender Filter** را غیر فعال کنید. زمانیکه این گزینه را روی کامپیوتری که **Exchange** را اجرا می کند فعال کنید، عاملِ آن تمام پیام ها از اتصال دهنده ی دریافت روی آن کامپیوتر را فیلتر می کند. فقط پیام های رسیده از منابع خارجی فیلتر می شوند. منابع خارجی به عنوان منابع احراز هویت نشده شناخته می شوند. اینها منابع اینترنتی ناشناس هستند.

نحوه پیاده‌سازی:

برای پیاده سازی حالت توصیه شده، دستور PowerShell زیر را اجرا نمایید:

```
Set-SenderFilterConfig -Enabled $true
```

SCMS-1-6: تنظیم Enable Sender reputation با مقدار True. (قابل شمارش)

شرح اجمالی:

زمانیکه این گزینه روی یک کامپیوتر فعال باشد تمام پیام ها از تمام اتصال دهنده های دریافت توسط این گزینه فیلتر می گردند. فقط پیام های رسیده از منابع خارجی فیلتر می شوند. منابع خارجی به عنوان منابع احراز هویت نشده شناخته می شوند که همانا منابع اینترنتی ناشناس هستند.

نحوه پیاده‌سازی:

برای پیاده سازی حالت توصیه شده، دستور PowerShell زیر را اجرا نمایید:

```
Set-SenderReputationConfig -SenderBlockingEnabled $true -OpenProxyDetectionEnabled $true
```

SCMS-1-7: تنظیم External send connector authentication: DNS Routing با مقدار True. (قابل شمارش)

شرح اجمالی:

از این گزینه برای استفاده از **DNS** جهت مسیریابی ایمیل های بیرونی، استفاده نمایید. اگر این گزینه فعال باشد، اتصال دهنده از **DNS** استفاده می کند تا آدرس **IP** سرور **SMTP** مقصد را بیابد.

نحوه پیاده‌سازی:

برای پیاده سازی حالت توصیه شده، دستور PowerShell زیر را اجرا نمایید:

```
Set-SendConnector "Connection to Contoso.com" -DNSRoutingEnabled $true
```

SCMS-1-8: تنظیم External send connector authentication: Ignore Start TLS با مقدار False. (قابل شمارش)

شرح اجمالی:

اگر این تنظیمات فعال باشد شما دیگر نخواهید توانست احرازهویت کامل(بالغ) **TLS** را پیکر بندی کنید. این نوع احراز هویت **TLS**(کامل)، **External send connector authentication :domain security** نام دارد.

نحوه پیاده‌سازی:

برای پیاده سازی حالت توصیه شده، دستور PowerShell زیر را اجرا نمایید:

```
set-SendConnector -identity <connector_name> -IgnoreSTARTTLS: $false
```

SCMS-1-9: تنظیم Configure login authentication for POP3 با مقدار SecureLogin. (قابل شمارش)

شرح اجمالی:

پروتکل **POP3** تمام داده شامل اعتبارنامه های کاربر و پیام های حساس را بدون رمزنگاری ارسال می کند. استفاده از این تنظیم و فعال کردن **TLS** این اطمینان خاطر را ایجاد میکند که ترافیک شبکه روی **POP3** به صورت رمز شده می باشد و به کلاینت این امکان را می دهد تا آدرس **IP** سرور را بررسی نمایند.

نحوه پیاده‌سازی:

برای پیاده سازی حالت توصیه شده، دستور PowerShell زیر را اجرا نمایید:

```
Set-PopSettings -LoginType SecureLogin
```

SCMS-1-10: تنظیم Protocol logging روی Receive connector با مقدار Verbose. (قابل شمارش)

شرح اجمالی:

یک **Protocol log** رکوردی از فعالیت های **SMTP** بین سرورهای پیام می باشد. این فعالیت روی **Send connector** ها و **Receive connector** هایی رخ می دهند که روی سرورهای **Hub Transport** و **Edge Transport** تنظیم شده اند. به صورت پیش فرض این گزینه غیر فعال می باشد.

نحوه پیاده‌سازی:

برای پیاده سازی حالت توصیه شده، دستور PowerShell زیر را اجرا نمایید:

```
Set-ReceiveConnector "<IDENTITY>" -ProtocolLoggingLevel Verbose
```

SCMS-1-11: تنظیم Protocol logging روی Send connector با مقدار Verbose (قابل شمارش)

شرح اجمالی:

یک **Protocol log** رکوردی از فعالیت های **SMTP** بین سرورهای پیام می باشد. این فعالیت روی **Send connector** ها و **Receive connector** هایی رخ می دهند که روی سرورهای **Hub Transport** و **Edge Transport** تنظیم شده اند. به صورت پیش فرض این گزینه غیر فعال می باشد.

نحوه پیاده‌سازی:

برای پیاده سازی حالت توصیه شده، دستور PowerShell زیر را اجرا نمایید:

```
Set-SendConnector "IDENTITY" -ProtocolLoggingLevel Verbose
```

SCMS-1-12: تنظیم احراز هویت Send Connector بیرونی (Domain Security) با مقدار True. (قابل شمارش)

شرح اجمالی:

توصیه می گردد از احراز هویت **Exchange** و یا **IPsec** برای **Send Connector** های بیرونی استفاده شود. با این حال در صورتیکه از **Basic authentication** برای فعال سازی **Domain Security** استفاده کردید به شما این امکان را می دهد از اعتبارنامه ها و نیز پیام های ارسالی به سایر سازمان ها محافظت کنید.

اگر فعال باشد، **Send Connector** هنگام ارسال ایمیل تلاش خواهد کرد به ایجاد یک ارتباط **TLS** کامل با سرورهای مقابل. پیش از استفاده **TLS**، می بایستی چند گام تنظیمات انجام پذیرد.

نحوه پیاده‌سازی:

برای پیاده سازی حالت توصیه شده، دستور PowerShell زیر را اجرا نمایید:

```
set-sendconnector -Identity <SendConnectorIdParameter> -DomainSecureEnabled $true
```

SCMS-1-13: تنظیم Message Tracking Logging-Transport با مقدار True. (قابل شمارش)

شرح اجمالی:

لاگ ردیابی پیام، یک لاگ دقیق از تمامی فعالیت های مرتبط به پیام های انتقالی به/از سرورهای **Exchange** را فراهم می کند. به صورت پیش فرض، ردیابی پیام روی سرورهای **Hub Transport**، **Edge Transport** و **Mailbox** در دسترس و فعال می باشد.

نحوه پیاده‌سازی:

برای پیاده سازی حالت توصیه شده، دستور PowerShell زیر را اجرا نمایید:

```
Set-TransportService EXCHANGE1 -MessageTrackingLogEnabled $true
```

SCMS-1-14: تنظیم Message Tracking Logging-Mailbox با مقدار True. (قابل شمارش)

شرح اجمالی:

لاگ ردیابی پیام، یک لاگ دقیق از تمامی فعالیت های مرتبط به پیام های انتقالی به/از سرورهای **Exchange** را فراهم می کند. به صورت پیش فرض، ردیابی پیام روی سرورهای **Hub Transport**، **Edge Transport** و **Mailbox** در دسترس و فعال می باشد.

نحوه پیاده‌سازی:

برای پیاده سازی حالت توصیه شده، دستور PowerShell زیر را اجرا نمایید:

```
Set-TransportService EXCHANGE1 -MessageTrackingLogEnabled $true
```

SCMS-1-15: تنظیم احراز هویت هنگام ورود روی پروتکل IMAP4 با مقدار SecureLogin. (قابل شمارش)

شرح اجمالی:

پروتکل **IMAP4** تمام داده شامل اعتبارنامه های کاربر و پیام های حساس را بدون رمزنگاری ارسال می کند. استفاده از این تنظیم و فعال کردن **SSL** این اطمینان خاطر را ایجاد میکند که ترافیک شبکه روی **IMAP4** به صورت رمز شده می باشد و به کلاینت این امکان را می دهد تا آدرس **IP** سرور را بررسی نمایند.

نحوه پیاده‌سازی:

برای پیاده سازی حالت توصیه شده، دستور PowerShell زیر را اجرا نمایید:

```
Set-ImapSettings -LoginType SecureLogin
```

SCMS-1-16: تنظیم Connectivity logging با مقدار True. (قابل شمارش)

شرح اجمالی:

یک لاگ ارتباطی، رکوردی است از فعالیت های ارتباطی **SMTP** مربوط به پیام های خروجی که صف های پیام را به سرورهای **Mailbox** مقصد، میزبان هوشمند یا دامنه تحویل می دهند. **Connectivity logging** روی سرورهای **Hub Transport** و **Edge Transport** وجود دارد که به صورت پیش فرض غیر فعال می باشد.

نحوه پیاده‌سازی:

برای پیاده سازی حالت توصیه شده، دستور PowerShell زیر را اجرا نمایید:

```
Set-TransportService EXCHANGE1 -ConnectivityLogEnabled $true
```

SCMS-1-17: تنظیم Maximum send size - organization level با مقدار 10240. (قابل شمارش)

شرح اجمالی:

این محدودیت شامل هدر پیام، بدنه ی آن و هر آنچه در پیوست پیام است، می باشد. برای جریان پیام داخلی، سرور **Exchange** از هدر پیام سفارشی **(X-MS-Exchange-Organization-OriginalSize)** برای ذخیره

سازی مقدار سایز پیام اصلی رسیده به سرور استفاده می کند. هر زمانی که پیام با محدودیت های سایز پیام چک می گردد، کمترین مقدار هدر سایز پیام فعلی یا سایز پیام اصلی استفاده می گردد. سایز پیام به دلایلی نظیر تغییر محتوا، رمزنگاری و پردازش عامل می تواند تغییر کند.

نحوه پیاده‌سازی:

برای پیاده سازی حالت توصیه شده، دستور PowerShell زیر را اجرا نمایید:

```
Set-TransportConfig -MaxSendSize 10240KB
```

SCMS-1-18: تنظیم Maximum receive size - Connector level با مقدار 10240. (قابل شمارش)

شرح اجمالی:

از این گزینه می توانید برای محدود سازی مجموع سایز پیام در سطح **Connector** استفاده نمایید. این شامل هدر پیام، بدنه ی آن و هر آنچه در پیوست پیام است، می باشد. برای جریان پیام داخلی، سرور **Exchange** از هدر پیام سفارشی(**X-MS-Exchange-Organization-OriginalSize**) برای ذخیره سازی مقدار سایز پیام اصلی رسیده به سرور استفاده می کند. هر زمانی که پیام با محدودیت های سایز پیام چک می گردد، کمترین مقدار هدر سایز پیام فعلی یا سایز پیام اصلی استفاده می گردد. سایز پیام به دلایلی نظیر تغییر محتوا، رمزنگاری و پردازش عامل می تواند تغییر کند.

نحوه پیاده‌سازی:

برای پیاده سازی حالت توصیه شده، دستور PowerShell زیر را اجرا نمایید:

```
Set-ReceiveConnector "Connection from Contoso.com" -MaxMessageSize 10240KB
```

SCMS-2: صندوق پست

SCMS-2-1: تعیین حجم صندوق پستی: پیغام اخطار را روی 1991680 قرار دهید. (غیر قابل شمارش)

شرح اجمالی:

می توانید تنظیمات این بخش را طوری انجام دهید که اگر حجم صندوق پستی به میزان تعیین شده توسط شما رسید به صورت اتوماتیک یک پیام اخطار برای کاربر صادر شود. برای تعیین محدودیت بر روی صندوق پستی گزینه مربوط به ظرفیت را انتخاب و سپس اندازه آنرا به کیلو بایت وارد می کنیم که با این کار قبل از اینکه حجم صندوق پستی کاربر به اتمام برسد یک پیغام اخطار مبنی بر پر شدن حجم صندوق پستی به صندوق پستی کاربر ارسال می شود. عدد وارد شده برای تعیین حجم صندوق پستی می تواند عددی بین 0 تا 2149483647 کیلو بایت و یا 2.1 ترابایت باشد.

نحوه پیاده‌سازی:

به منظور اجرای پیشنهاد اریه شده، دستور زیر را در محیط متنی اجرای دستورات وارد کنید:

```
Set-MailboxDatabase "EXCHANGE01\Mailbox Database" -IssueWarningQuota 1991680KB
```

SCMS-2-2: تعیین میزان حجم صندوق پستی: جلوگیری از ارسال و دریافت ایمیل در حجم 2411520. (غیر قابل شمارش)

شرح اجمالی:

تنظیمات این قسمت باعث می شود از ارسال و دریافت ایمیل توسط کاربر در هنگامی که حجم صندوق پستی او به میزان تعیین شده رسید جلوگیری شود. برای تعیین این محدودیت قسمت مربوطه را انتخاب و سپس میزان حجم صندوق پستی را به کیلو بایت وارد کنید که این عمل باعث می شود یک نامه به صندوق پستی کاربر ارسال شود و او را از این که نمی تواند نامه ای ارسال و دریافت کند مطلع کند. عدد وارد شده بین 0 تا 2147483647 کیلو بایت و یا 2.1 ترابایت باشد.

نحوه پیاده‌سازی:

به منظور اجرای پیشنهاد ارایه شده، دستور زیر را در محیط متنی اجرای دستورات وارد کنید:

```
Set-MailboxDatabase "EXCHANGE01\Mailbox Database" -ProhibitSendReceiveQuota 2411520 KB
```

SCMS-2-3: تعیین میزان حجم صندوق پستی: جلوگیری از ارسال ایمیل در حجم 2097152. (غیر قابل شمارش)

شرح اجمالی:

تنظیمات این قسمت باعث می شود از ارسال ایمیل توسط کاربر در هنگامی که حجم صندوق پستی او به میزان تعیین شده رسید جلوگیری شود. برای تعیین این محدودیت قسمت مربوطه را انتخاب و سپس میزان حجم صندوق پستی را به کیلو بایت وارد کنید که این عمل باعث می شود یک نامه به صندوق پستی کاربر ارسال شود و او را از این که نمی تواند نامه ای ارسال کند مطلع کند. عدد وارد شده بین 0 تا 2147483647 کیلو بایت و یا 2.1 ترابایت باشد.

نحوه پیاده‌سازی:

به منظور اجرای پیشنهاد ارایه شده، دستور زیر را در محیط متنی اجرای دستورات وارد کنید:

```
Set-MailboxDatabase "EXCHANGE01\Mailbox Database" -ProhibitSendQuota 2097152KB
```

SCMS-2-4: تنظیم مربوط به نگهداری صندوق‌های پستی حذف شده به مدت 30 روز. (قابل شمارش)

شرح اجمالی:

از این تنظیم برای مشخص کردن زمان نگهداری صندوق‌های پستی حذف شده، قبل از این که به طور دایم حذف شوند استفاده می شود. تعیین یک بازه زمانی نگهداری صندوق های پستی که به طور تصادفی حذف شده اند، بازگرداندن آن ها را تسهیل می کند.

نحوه پیاده‌سازی:

به منظور اجرای پیشنهاد ارایه شده، دستور زیر را در محیط متنی اجرای دستورات وارد کنید:

```
Set-Mailboxdatabase "EXCHANGE01\Mailbox Database" -MailboxRetention 30.00:00:00
```

SCMS-2-5: انجام تنظیمات طوری که تا زمان تهیه نسخه پشتیبان از پایگاه داده هیچ چیزی به طور دائم حذف نشود. (قابل شمارش)

شرح اجمالی:

این تنظیم باعث می شود تا زمانی که از پایگاه داده نسخه پشتیبان تهیه نشود هیچ موردی از دیتابیس حذف نگردد.

نحوه پیاده‌سازی:

به منظور اجرای پیشنهاد ارایه شده، دستور زیر را در محیط متنی اجرای دستورات وارد کنید:

```
Set-MailboxDatabase <Mailbox Database Name> -RetainDeletedItemsUntilBackup $true
```

SCMS-2-6: اجازه ورود پسورد ساده را بر روی گزینه False قرار دهید. (قابل شمارش)

شرح اجمالی:

قبل از اینکه دستگاه‌های موبایل بتوانند با استفاده از پروتکل **ActiveSync** به سرور **Exchange** متصل شوند تنظیمات مربوط به قرار دادن پسورد پیچیده را بر روی سرور اعمال کنید. **(قابل شمارش)**

نحوه پیاده‌سازی:

به منظور اجرای پیشنهاد ارایه شده، دستور زیر را در محیط متنی اجرای دستورات وارد کنید:

```
Set-MobileDeviceMailboxPolicy <Profile> -AllowSimplePassword $false
```

SCMS-2-7: تاریخچه نگهداری پسورد را روی 4 یا بیشتر قرار دهید. (قابل شمارش)

شرح اجمالی:

نگهداری پسورد های قدیمی این تضمین را به ما می دهد که آن‌ها دیگر در یک بازه زمانی مشخص نمی توانند مورد استفاده مجدد قرار بگیرند.

نحوه پیاده‌سازی:

به منظور اجرای پیشنهاد ارایه شده، دستور زیر را در محیط متنی اجرای دستورات وارد کنید:

```
Set-MobileDeviceMailboxPolicy <Profile> -PasswordHistory 4
```

SCMS-2-8: تنظیم مربوط به زمان انقضای کلمه عبور را روی 90 روز یا کمتر قرار دهید. (قابل شمارش)

شرح اجمالی:

با انجام این تنظیم مشخص می کنید چه زمانی پسورد منقضی شود و کاربر باید پسورد خود را تغییر دهد.

نحوه پیاده‌سازی:

به منظور اجرای پیشنهاد ارایه شده، دستور زیر را در محیط متنی اجرای دستورات وارد کنید:

```
Set-MobileDeviceMailboxPolicy default -PasswordExpiration 90
```

SCMS-2-9: تنظیم مربوط به حداقل طول پسورد روی عدد 4 یا بیشتر. (قابل شمارش)

شرح اجمالی:

می‌توانید با انجام این تنظیم طول حداقل کلمات عبور برای پسورد دستگاه‌ها را تعیین کنید. کلمات عبور طولانی می تواند سطح امنیت بالایی را تضمین کند. در ضمن کلمات عبور طولانی باعث کاهش قابلیت استفاده آن دستگاه می شود.

نحوه پیاده‌سازی:

به منظور اجرای پیشنهاد ارایه شده، دستور زیر را در محیط متنی اجرای دستورات وارد کنید:

```
Set-MobileDeviceMailboxPolicy default -MinPasswordLength 4
```

SCMS-2-10: تنظیم مربوط به حالت Startup Mode را روی حالت TLS قرار دهید. (قابل شمارش)

شرح اجمالی:

از این تنظیم برای قرار دادن سرور **Unified Messaging** بر روی حالت امن استفاده می شود. این تنظیم تمامی تماس های صوتی را مجبور به استفاده از **TLS** می کند.

نحوه پیاده‌سازی:

به منظور اجرای پیشنهاد ارایه شده، دستور زیر را در محیط متنی اجرای دستورات وارد کنید:

```
Set-UMService -Identity Exchange1 -UMStartUpMode TLS
```

SCMS-2-11: حالت Refresh Interval را بر روی عدد 1 تنظیم کنید. (قابل شمارش)

شرح اجمالی:

با استفاده از این تنظیم می توانید مشخص کنید، در چه بازه‌های زمانی تنظیمات مربوط به سیاست های تعریف شده بر روی دستگاه‌ها اعمال شود.

نحوه پیاده‌سازی:

به منظور اجرای پیشنهاد ارایه شده، دستور زیر را در محیط متنی اجرای دستورات وارد کنید:

```
Set-MobileDeviceMailboxPolicy -Identity default -DevicePolicyRefreshInterval '1:00:00'
```

SCMS-2-12: حالت Configure Dial Plan Security را روی Secured قرار دهید. (قابل شمارش)

شرح اجمالی:

در صورتی که سرور **Unified Messaging** قادر به برقراری تماس صوتی در حالت **TLS** نباشد برای محافظت از برخی صندوق های پستی خاص می توان از این تنظیم استفاده کرد. برای استفاده از این ابزار سرور **UM** باید در حالت **DUAL Mode** قرار بگیرد.

نحوه پیاده‌سازی:

به منظور اجرای پیشنهاد ارایه شده، دستور زیر را در محیط متنی اجرای دستورات وارد کنید:

```
Set-UMDialPlan -identity MySecureDialPlan -VoIPSecurity Secured
```

SCMS-2-13: حالت دسترسی به Voice Mail بدون وارد نمودن PIN را در حالت False قرار دهید. (قابل شمارش)

شرح اجمالی:

از این تنظیم برای دسترسی به **Mailbox** با استفاده از **PIN** استفاده کنید

نحوه پیاده‌سازی:

به منظور اجرای پیشنهاد ارایه شده، دستور زیر را در محیط متنی اجرای دستورات وارد کنید:

```
Set-UMMailboxPolicy -id MyUMMailboxPolicy -AllowPinlessVoiceMailAccess $false
```

SCMS-2-14: تنظیم مربوط به نگهداری موارد حذف شده را بر روی 14 روز قرار دهید. (قابل شمارش)

شرح اجمالی:

از این تنظیم می توانید برای تعیین اینکه پیام‌های حذف شده تا چه زمانی قبل از اینکه به طور دایم از دیتا بیس حذف شوند نگهداری شوند استفاده کنید. قرار دادن یک بازه زمانی معقول برای بازگرداندن پیام هایی که به صورت ناخواسته حذف می شوند کار بازگردانی را تسهیل خواهد کرد.

نحوه پیاده‌سازی:

به منظور اجرای پیشنهاد ارایه شده، دستور زیر را در محیط متنی اجرای دستورات وارد کنید:

```
Set-MailboxDatabase -Identity MDB2 -DeletedItemRetention 14
```

SCMS-2-15: تنظیم مربوط به Allow Unmanaged Devices را روی گزینه False قرار دهید. (قابل شمارش)

شرح اجمالی:

با این تنظیم می توانید مشخص کنید دستگاه‌هایی که سیاست‌های امنیتی سرویس **Exchange** را ندارند چه رفتاری در قبال آن‌ها انجام شود.

نحوه پیاده‌سازی:

به منظور اجرای پیشنهاد ارایه شده، دستور زیر را در محیط متنی اجرای دستورات وارد کنید:

```
Set-MobileDeviceMailboxPolicy -Identity default -AllowNonProvisionableDevices $false
```

SCMS-2-16: تنظیم مربوط به Required encryption on devices را روی حالت True قرار دهید. (قابل شمارش)

شرح اجمالی:

این تنظیم برای مواقعی است که بخواهیم موبایل‌ها از رمز نگاری برای ارتباطات استفاده کنند. استفاده از این تنظیم باعث بالا رفتن سطح امنیت به وسیله رمز نگاری تمام اطلاعات روی کارت‌های ذخیره سازی موبایل‌ها می شود.

نحوه پیاده‌سازی:

به منظور اجرای پیشنهاد ارایه شده، دستور زیر را در محیط متنی اجرای دستورات وارد کنید:

```
Set-MobileDeviceMailboxPolicy -Identity default -RequireDeviceEncryption $true
```

SCMS-2-17: تنظیم حالت Time without user input before password must be re-entered را روی عدد 15 قرار دهید. (قابل شمارش)

شرح اجمالی:

با استفاده از این تنظیم می توانید مشخص کنید، بعد از چند دقیقه که کاربر در حالت غیر فعال بود دوباره درخواست رمز عبور از کاربر شود. اگر این تنظیم را روی 15 دقیقه قرار دهیدکاربر را مجبور به وارد نمودن رمز عبور بعد از اینکه 15 دقیقه در حالت بیکار بود می کنید و اگر کاربر کمتز از 15 دقیقه بیکار باشد نیاز به وارد نمودن دوباره رمز عبور نمی‌باشد.

نحوه پیاده‌سازی:

به منظور اجرای پیشنهاد ارایه شده، دستور زیر را در محیط متنی اجرای دستورات وارد کنید:

```
Set-MobileDeviceMailboxPolicy -Identity Default -MaxInactivityTimeLock 00:15:00
```

SCMS-2-18: تنظیم مربوط به Require alphanumeric password را روی حالت True قرار دهید. (قابل شمارش)

شرح اجمالی:

کاربران را مجبور به استفاده از کلمات و علایم در رمز عبورشان کنید که این کار باعث افزایش امنیت رمز عبور در سازمان شما می شود.

نحوه پیاده‌سازی:

به منظور اجرای پیشنهاد ارایه شده، دستور زیر را در محیط متنی اجرای دستورات وارد کنید:

```
Set-MobileDeviceMailboxPolicy -Identity Default -AlphanumericPasswordRequired $true
```

SCMS-2-19: تنظیم مربوط به Require client MAPI encryption را روی حالت True قرار دهید. (قابل شمارش)

شرح اجمالی:

گواهینامه‌های امنیتی می توانند در قسمت Certificate Store دستگاه‌های قابل حمل یا دستگاه‌های **smart card** قرار بگیرند. یکی از روش‌هایی که گواهینامه احراز هویت از آن استفاده می کند، استفاده از پروتکل احراز هویت و پروتکل امنیت لایه انتقال می باشد. با استفاده از این نوع گواهینامه احراز هویت که ترکیبی از هر دو پروتکل می باشد کلاینت و سرور از هویت همدیگر اطمینان پیدا می کنند. برای مثال زمانی که یک ارتباط از طریق تلفن همراه شکل می گیرد گواهینامه کاربر آن دستگاه به سرور دسترسی کلاینت ارایه می شود و سپس سرور دسترسی کلاینت گواهینامه رایانه خودش را به دستگاه‌های سیار برای تامین کردن یک ارتباط دوطرفه ارایه می کند.

نحوه پیاده‌سازی:

به منظور اجرای پیشنهاد ارایه شده، دستور زیر را در محیط متنی اجرای دستورات وارد کنید:

```
Set-RpcClientAccess -Server CAS01 -EncryptionRequired $true
```

SCMS-2-20: تنظیم مربوط به Number of attempts allowed را روی عدد 10 قرار دهید. (قابل شمارش)

شرح اجمالی:

از این تنظیم برای محدود نمودن تعداد دفعات سعی در ورود استفاده می شود.

نحوه پیاده‌سازی:

به منظور اجرای پیشنهاد ارایه شده، دستور زیر را در محیط متنی اجرای دستورات وارد کنید:

```
Set-MobileDeviceMailboxPolicy -Identity Default -MaxPasswordFailedAttempts 10
```

SCMS-2-21: تنظیم مربوط به Required Password را روی True قرار دهید. (قابل شمارش)

شرح اجمالی:

رمز عبور برای باز کردن قفل دستگاه‌های سیار ضروری می باشد و برای تامین امنیت اطلاعات حساس ذخیره شده روی دستگاه‌ها در صورت از دست رفتن یا به سرقت رفتن ما را کمک می کند.

نحوه پیاده‌سازی:

به منظور اجرای پیشنهاد ارایه شده، دستور زیر را در محیط متنی اجرای دستورات وارد کنید:

```
Set-MobileDeviceMailboxPolicy -Identity Default -PasswordEnabled $true
```

SCMS-3: سایر

SCMS-3-1: فعال کردن لاگ ممیزی مدیریتی. (قابل شمارش)

شرح اجمالی:

لاگ ممیزی مدیریتی، لاگی را از تغییرات تنظیمات که توسط مدیر سیستم رخ داده است را ایجاد می کند. این تنظیم به صورت پیش فرض فعال است تا بتوان تنظیمات مرتبط به شکاف های امنیتی را بررسی نمود.

نحوه پیاده‌سازی:

برای پیاده سازی حالت توصیه شده، دستور PowerShell زیر را اجرا نمایید:

```
Set-AdminAuditLogConfig -AdminAuditLogCmdlets *
```

SCMS-3-2: تنظیم Require Client Certificates با مقدار Required (غیر قابل شمارش)

شرح اجمالی:

گواهی ها می توانند روی دستگاه های سیار و کارت های هوشمند قرار داده شوند. یک روش احراز هویت گواهی از پروتکل های **EAP** و **TLS** استفاده می نماید. طی این احراز هویت، کلاینت و سرور هویتشان را برای یکدیگر ثابت می کنند. به طور مثال یک کلاینت که از **ActiveSync** برای ارتباط با **Exchange** استفاد می کند، گواهی کاربری خود را به سرور **CAS** ارائه می کند و در مقابل نیز سرور **CAS** گواهی ماشین خود را برای دستگاه سیار ارائه نموده تا احراز هویت کامل صورت گیرد.

نحوه پیاده‌سازی:

به منظور اجرای این سیاست، به آدرس زیر مراجعه فرمایید.

```
http://technet.microsoft.com/en-us/library/bb266938%28v=exchg.141%29.aspx
```

SCMS-3-3: تنظیم Turn on script execution با مقدار RemoteSigned. (قابل شمارش)

شرح اجمالی:

با این گزینه می توان سیاست های اجرای فرامین را به گونه ای تنظیم نمود که بتوان نوع فرامین اجرایی توسط کاربر را کنترل کرد.

نحوه پیاده‌سازی:

برای پیاده سازی حالت توصیه شده، دستور PowerShell زیر را اجرا نمایید:

```
Set-ExecutionPolicy RemoteSigned
```

SCMS-3-4: فعال کردن لاگ ممیزی مدیریتی. (قابل شمارش)

شرح اجمالی:

لاگ ممیزی مدیریتی، لاگی را از تغییرات تنظیمات که توسط مدیر سیستم رخ داده است را ایجاد می کند. این تنظیم به صورت پیش فرض فعال است تا بتوان تنظیمات مرتبط به شکاف های امنیتی را بررسی نمود.

نحوه پیاده‌سازی:

برای پیاده سازی حالت توصیه شده، دستور PowerShell زیر را اجرا نمایید:

```
Set-AdminAuditLogConfig -AdminAuditLogEnabled $True
```

SCMS-3-5: تنظیم مربوط بـه Enable automatic replies to remote domains را روی حالـت False قـرار دهید. (قابل شمارش)

شرح اجمالی:

با استفاده از تنظمیات این قسمت می توانید تعیین کنید که سرویس **Exchange** به صورت اتوماتیک به دامنه-های متصل به دامین ما پیام های بازگشت ارسال کند یا خیر.

نحوه پیاده‌سازی:

به منظور اجرای پیشنهاد ارایه شده، دستور زیر را در محیط متنی اجرای دستورات وارد کنید:

```
Set-RemoteDomain -Identity Default -AutoReplyEnabled $false
```

SCMS-3-6: تنظیم مربوط به Allow Basic authentication را روی حالت False قرار دهید. (قابل شمارش)

شرح اجمالی:

از تنظیمات این بخش برای این که تعیین کنیم آیا می خواهید به کلاینت‌ها اجازه استفاده از **Basic Authentication** را بدهید یا خیر استفاده می کنیم.

نحوه پیاده‌سازی:

به منظور اجرای پیشنهاد ارایه شده، دستور زیر را در محیط متنی اجرای دستورات وارد کنید:

```
Set-OwaVirtualDirectory -Identity "owa (Default Web Site)" -BasicAuthentication $false
```

SCMS-3-7: تنظیم مربوط به Enable non-delivery reports to remote domains را روی حالت False قرار دهید. (قابل شمارش)

شرح اجمالی:

از این تنظیم برای این استفاده می شود که تعیین کنیم آیا می خواهیم گزارش تحویل را برای دامنه‌های متصل به دامنه ما ارسال کنیم یا خیر.

نحوه پیاده‌سازی:

به منظور اجرای پیشنهاد ارایه شده، دستور زیر را در محیط متنی اجرای دستورات وارد کنید:

```
Set-RemoteDomain -Identity Contoso -NDREnabled $false
```

SCMS-3-8: تنظیم مربوط به Enable OOF messages to remote domains را روی حالت None قرار دهید.

(قابل شمارش)

شرح اجمالی:

از این تنظیم برای این استفاده می شود که تعیین کنیم آیا می خواهیم به صورت اتوماتیک پیام‌هایی که شامل **out-of-office** هستند برای دامنه‌های متصل به دامنه ما ارسال شود یا خیر.

نحوه پیاده‌سازی:

به منظور اجرای پیشنهاد ارایه شده، دستور زیر را در محیط متنی اجرای دستورات وارد کنید:

```
Set-RemoteDomain "RemoteDomain" -AllowedOOFType None
```

SCMS-3-9: تنظیم مربوط به Enable automatic forwards to remote domains را روی حالت False قرار دهید. (قابل شمارش)

شرح اجمالی:

با استفاده از این تنظیم می توانید مشخص کنید که آیا می خواهید سرور پیام‌ها را به صورت اتوماتیک به دامنه-های دیگر ارسال کند یا خیر.

نحوه پیاده‌سازی:

به منظور اجرای پیشنهاد ارایه شده، دستور زیر را در محیط متنی اجرای دستورات وارد کنید:

```
Set-RemoteDomain -Identity Contoso -AutoForwardEnabled $false
```

SCMS-3-10: تنظیم مربوط به Enable S/MIME for OWA 2010 را روی حالت True قرار دهید.

(قابل شمارش)

شرح اجمالی:

با فعال کردن این امکان به کاربران این امکان را می دهید تا بتوانند کنترل مربوط به **S/MIME** را دانلود کنند تا با استفاده از آن بتوانند پیام‌های امضا شده رمزنگاری شده را بخوانند و همچنین بتوانند این نوع پیام‌ها را بسازند.

نحوه پیاده‌سازی:

به منظور اجرای پیشنهاد ارایه شده، دستور زیر را در محیط متنی اجرای دستورات وارد کنید:

```
Set-OWAVirtualDirectory -identity "owa (Default Web Site)" -SMimeEnabled $true
```

SCMS-3-11: تنظیم مربوط به Turn on Administrator Audit Logging را روی حالت True قرار دهید.

(قابل شمارش)

شرح اجمالی:

لاگ‌های ردیابی سطح مدیریت برای آگاهی از تغییرات صورت گرفته توسط مدیران استفاده می شود. به صورت پیش فرض این تنظیم بر روی حالت فعال قرار دارد تا با استفاده از آن بتوان رخنه‌های امنیتی مربوط به پیکر بندی را تشخصی داد.

نحوه پیاده‌سازی:

به منظور اجرای پیشنهاد ارایه شده، دستور زیر را در محیط متنی اجرای دستورات وارد کنید:

```
Set-AdminAuditLogConfig -AdminAuditLogEnabled $true
```