如何配置天蓝色AD和办公室365邮箱设置ESA的

目录

简介

本文为注册在Windows天蓝色的新应用和获取需要的值提供一逐步" how-to "，为了办公室365邮箱设置的完整的配置在思科电子邮件安全工具(ESA)。 这要求，当ESA管理员配置邮箱自动修正(3月)时先进的恶意软件保护的(安培)在ESA的邮件策略设置。

先决条件

相关产品

本文适用于以下：

- 所有ESA、硬件和虚拟运行的10.x和更新
- 所有Cloud电子邮件安全(CES) ESA，运行10.x和更新

要求

本文要求以下：

- 办公室365帐户订阅(请确保您的办公室365帐户订阅包括访问发电子邮件，例如企业E3或企业E5帐户。)
- Microsoft天蓝色帐户
- 办公室365和Microsoft天蓝色的AD帐户适当地附加对一个活动*user@domain.com*电子邮件地址，并且您能通过该域和帐户发送和收到电子邮件。
- 访问对Windows PowerShell，通常管理从Windows主机或服务器。
- 域活动公共/Private证书和专用密钥曾经签署证书，或者能力创建一公共/Private证书和能力保存专用密钥曾经签署证书。

您创建以下四个值为了配置ESA邮箱连接器回到天蓝色AD ：

1. 客户端ID
2. 承租人ID
3. Thumbprint
4. 在.pem格式的证书专用密钥

为了建立这些需要的值，您将需要完成在本文的步骤。 在开始之前，您将需要通过Windows Powershell运行以下：

1. **$cer =新对象System.Security.Cryptography.X509Certificates.X509Certificate2**
2. **$cer. 导入('C:\path _to_cert \ PEM_certificate.crt')**
3. **$bin = $cer.GetRawCertData()**
4. **$base64Value = [System.Convert]::ToBase64String($bin)**
5. **$bin = $cer.GetCertHash()**
6. **$base64Thumbprint = [System.Convert]::ToBase64String($bin)**
7. **$keyid = [System.Guid] ： ：NewGuid().ToString()**
8. **响应$base64Value**
9. **响应$base64Thumbprint**
10. **响应$keyid**

    注意：对于#2，请用路径替换**'C:\path _to_cert \ PEM_certificate.crt'**对您的证书。

$base64Thumbprint = *Thumbprint*。 添加此值到需要的值您的前提条件列表。

> **提示**： 因为他们将是要求的以后在配置步骤，请把输出保存本地为*$base64Value*、*$base64Thumbprint*和*$keyid*。 此时，您用证书的.crt完成。 请有您的证书相关的.pem在联机，在您的计算机的本地文件夹。

背景信息

Microsoft允许对天蓝色的门户的两个版本的访问：

- https://manage.windowsazure.com (经典门户)
- https://portal.azure.com (新建的门户)

您能由左手工具栏访问"经典门户"从新的门户，选择"Azure Active Directory" >经典门户

为本文，应用程序的注册和配置在新的门户被执行。 对使用"经典门户的"步骤包括在本文结束时。

(Microsoft可能选择在某时禁用经典天蓝色的门户。)

如何配置天蓝色AD和办公室365邮箱设置ESA的

注册在天蓝色的新应用

1. 访问天蓝色的用户界面：https://portal.azure.com/
2. 左边菜单栏，点击**更多Services>安全+标识： App注册**
3. 从App注册窗格，请点击**+Add**
4. 创建一名称对于您的app
5. 对于应用类型，请离开作为**Web app/API**
6. 对于登录URL，请使用以下格式： https:// *<company_domain.com>/ManualRegistration***注意**： *<company_domain.com>*是域用户能签到和访问您的O365域您的O365的域。
7. 单击**创建**

设置应用程序的需要的权限

1. 点击为您注册的app'关联的'显示名称
2. 在设置窗格中， API访问的，请点击**需要的权限**
3. 点击**+Add**
4. 在"请添加API访问"窗格中，点击**精选API**
5. 在"请选择，并且API"窗格中，请点击**办公室365联机的Exchange (Microsoft Exchange)**
6. 在**精选**页的单击的底部
7. 对于应用程序权限请选择：
   •以对所有邮箱的完全权限使用Exchange网站服务
   •发送邮件作为所有用户
   •读并且写入在所有邮箱的邮件
8. 对于Delegated权限请选择：
   •发送邮件作为用户
   •读并且写入用户邮件
   •读用户邮件
   •访问邮箱作为签署在用户通过Exchange网站服务
9. 单击**精选**在页底端，这将关闭"选择API"窗格
10. 单击**完成**在页底端，这将关闭"添加API访问"窗格
11. 点击**格兰特权限**
12. 当提示"您要为所有帐户的myESA同意下面权限在当前目录？此操作将更新此应用程序必须已经匹配的所有现有权限什么下面是列出的。"，请点击**是**

您应该当前有两个API列出的， "Windows天蓝色的活动目录"和"办公室365联机的Exchange"。

您将需要回来到已注册app窗格继续进行下一部分：

1. 点击"X"关闭"要求权限"窗格
2. 点击"X关闭"设置"窗格

您当前是回到在已注册app窗格。

准备明显应用程序的

编辑明显

1. 从已注册app窗格，请点击明显在工具栏
2. 在编辑器提交您完整表明。 线路12应该是“keyCredentials”。您替换有以下的仅线路12 ：

```
"keyCredentials": [
{
"customKeyIdentifier": "$base64Thumbprint",
"keyId": "$keyid",
"type": "AsymmetricX509Cert",
"usage": "Verify",
"value": "$base64Value"
}
],
```

3. 您将需要用您的值替换$base64Thumbprint、$keyid和$base64Value 在所有值附近留下报价单(“”)，如显示给予特别注意每个值是ONLY1线路，包括$base64Thumbprint
4. 点击**“Save”**更新您的应用程序。您应该看到“顺利地更新的应用程序”公告在工具栏区域。

您将需要回来到已注册app窗格继续进行下一部分：

点击"X"结束“编辑明显”窗格。

(可选)请下载明显

> **提示**：如果顺利地能使用天蓝色编辑器明显，您可以跳过明显的下载和上传明显。 否则，并且您需要手工编辑明显，请继续。

1. 从已注册app窗格，请点击明显在工具栏
2. 在编辑明显菜单请点击**下载**
3. 保存明显对包含您的证书的目录。 这将保存明显在.json格式本地到您的计算机。
4. 使用一台本地编辑器(Wordpad++、原子等等)，从的完整步骤2和3 “编辑本文的明显”部分
5. 保存明显.json文件本地

(可选)请上传明显

如果选择下载并且手工编辑明显，您将需要上传编辑的明显：

1. 返回到您的浏览器和天蓝色门户
2. 点击从的**加载**“编辑明显”窗格

您将需要回来到已注册app窗格继续进行下一部分：

点击"X"结束“编辑明显”窗格。

获得应用程序的客户端ID

1. 从已注册app请查找“申请ID”
2. 复制申请ID (申请ID =*客户端ID*)
3. 添加此值到需要的值您的前提条件列表。

获得应用程序的承租人ID值

1. 从“App注册”窗格，请点击“终端”并且选择联邦元数据文档的第一行
2. 复制和插入线路到一台外部编辑器
3. 您将要获取*承租人ID*，是ID串在“https://login.windows.net/以后”
4. 添加此值到需要的值您的前提条件列表。

示例：

```
"keyCredentials": [
{
"customKeyIdentifier": "$base64Thumbprint",
"keyId": "$keyid",
"type": "AsymmetricX509Cert",
"usage": "Verify",
"value": "$base64Value"
}
],
```

对于此示例，承租人ID将是"ed437e13-ba50-479e-b40d-8affa4f7e1d7"。

验证需要的值

您的值当前完成。您应该能填写以下值：

- 客户端ID
- 承租人ID
- Thumbprint (请参阅前提条件)
- 在.pem格式的证书专用密钥(请参阅前提条件)

您准备通过配置在ESA的这些值完成办公室365邮箱设置。

配置ESA

1. 在ESA GUI ：**系统管理>邮箱设置> Edit设置…**
2. 回车按您的从前面部分(客户端ID的值，承租人ID， Thumbprint)
3. 装载已保存证书(.pem)
4. 单击 **Submit**
5. 您看到“设置顺利地配置。您必须确认更改和测试连接”。
6. 从右上角，请在所有测试之前单击**进行更改**
7. 点击"Check Connection…"并且在已知好的回车，工作电子邮件地址关联与您的O365域
8. 点击"Test Connection"

您应该接收成功导致连接状态：

```
"keyCredentials": [
{
"customKeyIdentifier": "$base64Thumbprint",
"keyId": "$keyid",
"type": "AsymmetricX509Cert",
"usage": "Verify",
"value": "$base64Value"
}
],
```

排除故障ESA

如果看不到连接状态的成功的结果测试，您可以希望查看从天蓝色AD进行的应用程序注册。

从ESA，设置3月日志为跟踪级别并且再测试连接。

对于不成功连接，日志可能显示类似于：

```
"keyCredentials": [
{
"customKeyIdentifier": "$base64Thumbprint",
"keyId": "$keyid",
"type": "AsymmetricX509Cert",
"usage": "Verify",
"value": "$base64Value"
}
],
```

确认申请ID、是相同的象承租人ID)的目录ID (或者从日志的其他相关的标识与您的在天蓝色AD的应用程序。 如果对值是不确定的，请删除从门户天蓝色的AD的应用程序并且开始。

对于成功的连接，日志应该类似于：

```
"keyCredentials": [
{
"customKeyIdentifier": "$base64Thumbprint",
"keyId": "$keyid",
"type": "AsymmetricX509Cert",
"usage": "Verify",
"value": "$base64Value"
}
],
```

排除故障天蓝色AD

> **注意**： 没有资格Cisco TAC和Cisco支持排除故障与Microsoft Exchange的用户方面问题，Microsoft天蓝色AD或者办公室365。

对于与Microsoft天蓝色AD的用户方面问题，您将需要从事Microsoft支持。 请参阅从您的Microsoft天蓝色控制板的“帮助+支持”选项。 您可以能打开直接支持请求到从控制板的Microsoft支持。

(可选)使用经典门户，如何创建和配置在天蓝色的应用程序

> **注意**：您不需要完成此，如果顺利地能通过访问https://portal.azure.com使用天蓝色门户(新建的门户)。 这为选择仍然使用“经典门户”的天蓝色的管理员只被参考。 如果希望使用天蓝色AD门户的此版本，请找出完成的需要的值以下逐步指导：

添加应用程序

1. 登陆对Microsoft天蓝色。
2. 从左边菜单栏，请导航对**所有ITEM**
3. 点击资源名称对于您的域
4. 从在您的资源名称下的工具选项卡，请选择**应用程序**
5. 从底下工具栏区域，请单击**添加**

6. 提交*“什么时候要执行什么？”*，请选择**添加我的组织开发的应用程序**
7. 完成*“告诉我们关于您的应用程序”*信息： 创建一名称对于您的app对于应用类型，请离开作为**Web应用程序和Web API**点击箭头继续
8. 完成App属性： 对于登录URL，请使用以下格式： https://*<company_domain.com>/ManualRegistration***注意**： *<company_domain.com>是*域用户能签到和访问您的O365域您的O365的域。对于APP ID URI，请使用以下格式：https:// <company_domain.com>点击复选标记完成

配置您的应用程序

1. 一旦自定义Web应用程序创建，您自动地导航到自定义Web应用程序。 从这里，在工具选项卡，精选请**配置**
2. **客户端ID**在此屏幕列出。 复制并且添加此值到需要的值您的前提条件列表。
3. 移动到底部的屏幕发现“对其他应用程序的权限”。
4. 单击**添加应用程序** 选择**办公室365联机的Exchange**并且点击检查继续**应用程序权限**，精选：**读并且写入在所有邮箱的邮件发送邮件作为所有用户以完全权限使用Exchange网站服务**…Delegated权限，精选： **发送邮件作为用户读并且写入用户邮件读用户邮件访问邮箱作为签署在用户通过Exchange**
5. 点击从底下工具栏的**“Save”**保存所有工作和配置自定义Web应用程序的

管理明显

1. 一旦自定义Web应用程序完成保存和更新，请单击**管理明显>下载明显**从底下工具栏
2. 通过答复导航，并且保存Web应用程序明显在.json格式对您的本地计算机。
3. 本地，请查找.json文件并且打开与文本编辑。 (更可取的Notepad++、原子等等)
4. 搜索并且查找“keyCredentials”线路
5. 替换此单个线路用以下多条线路，定制通过使用*$base64Thumbprint*、*$keyid*和*$base64Value*

```
： "keyCredentials": [
{
"customKeyIdentifier": "$base64Thumbprint",
"keyId": "$keyid",
"type": "AsymmetricX509Cert",
"usage": "Verify",
"value": "$base64Value"
}
],
```

6. 当输入*$base64Value时*，这要求编辑到单个线路值
7. 保存.json文件本地
8. 返回到您的浏览器和Microsoft天蓝色的门户
9. 单击**管理明显>明显的加载**
10. 浏览并且查找编辑的.json文件
11. 选择复选标记完成加载

查找承租人ID

1. 从底下工具栏，请点击**视图终端**查看在Microsoft天蓝色AD集成的终端
2. 选择联邦元数据文档的第一行
3. 复制和插入线路到一台外部编辑器
4. 您将要获取*承租人ID*，是ID串在“https://login.windows.net/以后”

5. 添加此值到需要的值您的前提条件列表

示例：

```
"keyCredentials": [
{
"customKeyIdentifier": "$base64Thumbprint",
"keyId": "$keyid",
"type": "AsymmetricX509Cert",
"usage": "Verify",
"value": "$base64Value"
}
],
```

对于此示例，承租人ID将是"ed437e13-ba50-479e-b40d-8affa4f7e1d7"。

相关信息

- 在办公室365邮箱的自动Remediating消息