Integre Intune MDM con Identity Services Engine

Contenido

Introducción

Este documento describe cómo integrar la gestión de dispositivos móviles (MDM) de Intune con Cisco Identity Services Engine (ISE).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimientos sobre los servicios de MDM en Cisco ISE
- Conocimiento de Microsoft Azure Intune Services

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Identity Services Engine 3.0
- Aplicación Intune de Microsoft Azure

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

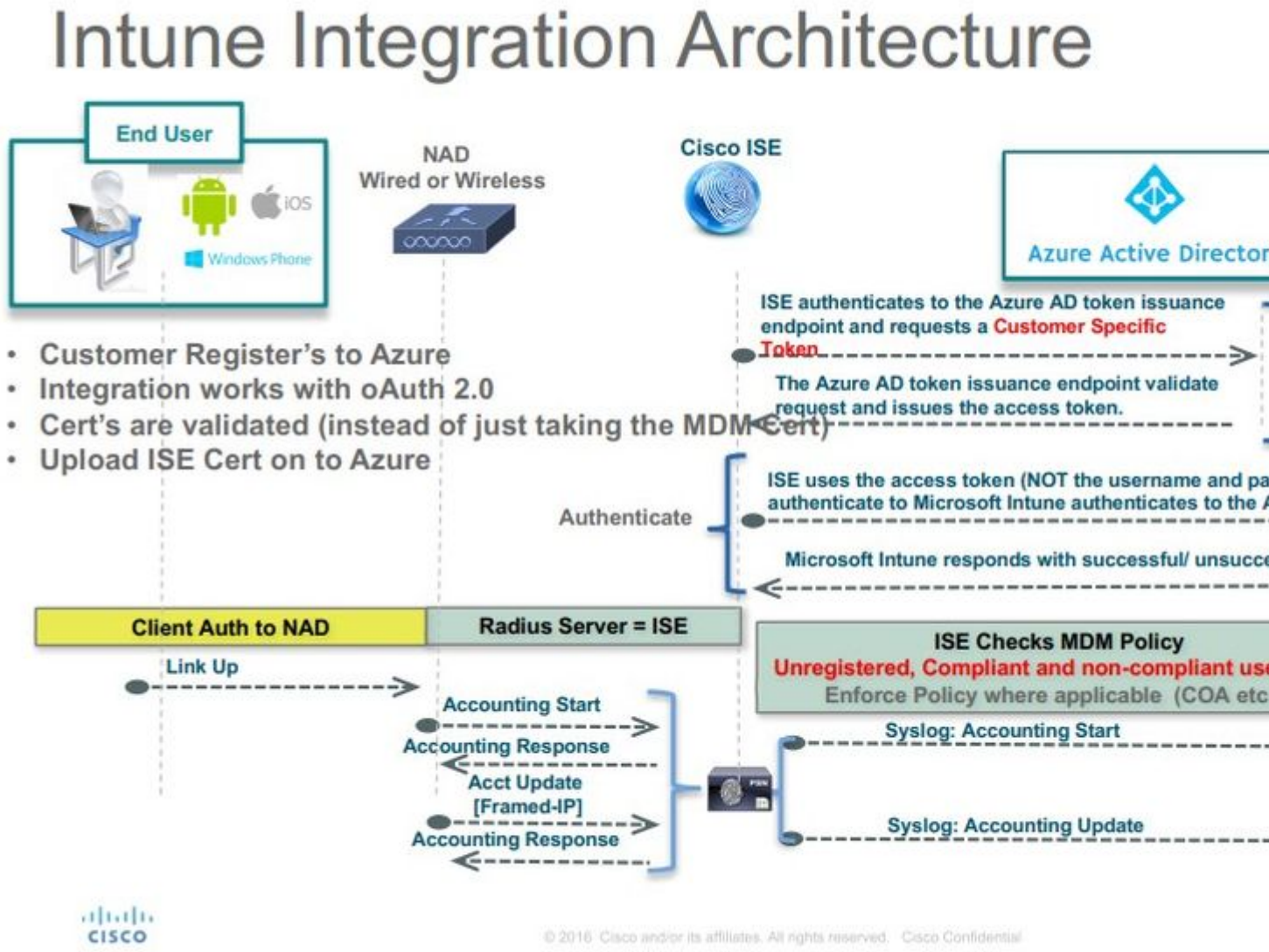
Antecedentes

Los servidores de MDM protegen, supervisan, administran y admiten dispositivos móviles implementados

en operadores móviles, proveedores de servicios y empresas. Estos servidores actúan como el servidor de políticas que controla el uso de algunas aplicaciones en un dispositivo móvil (por ejemplo, una aplicación de correo electrónico) en el entorno implementado. Sin embargo, la red es la única entidad que puede proporcionar acceso granular a los terminales en función de las listas de control de acceso (ACL). ISE consulta a los servidores de MDM los atributos de dispositivo necesarios para crear ACL que proporcionen control de acceso a la red para dichos dispositivos. Cisco ISE se integra con Microsoft Intune MDM Server para ayudar a las organizaciones a proteger los datos corporativos cuando los dispositivos intentan acceder a los recursos en las instalaciones.

Configurar

Diagrama de la red



Configurar Microsoft Intune

Importar los certificados de Intune Portal al almacén de confianza de ISE

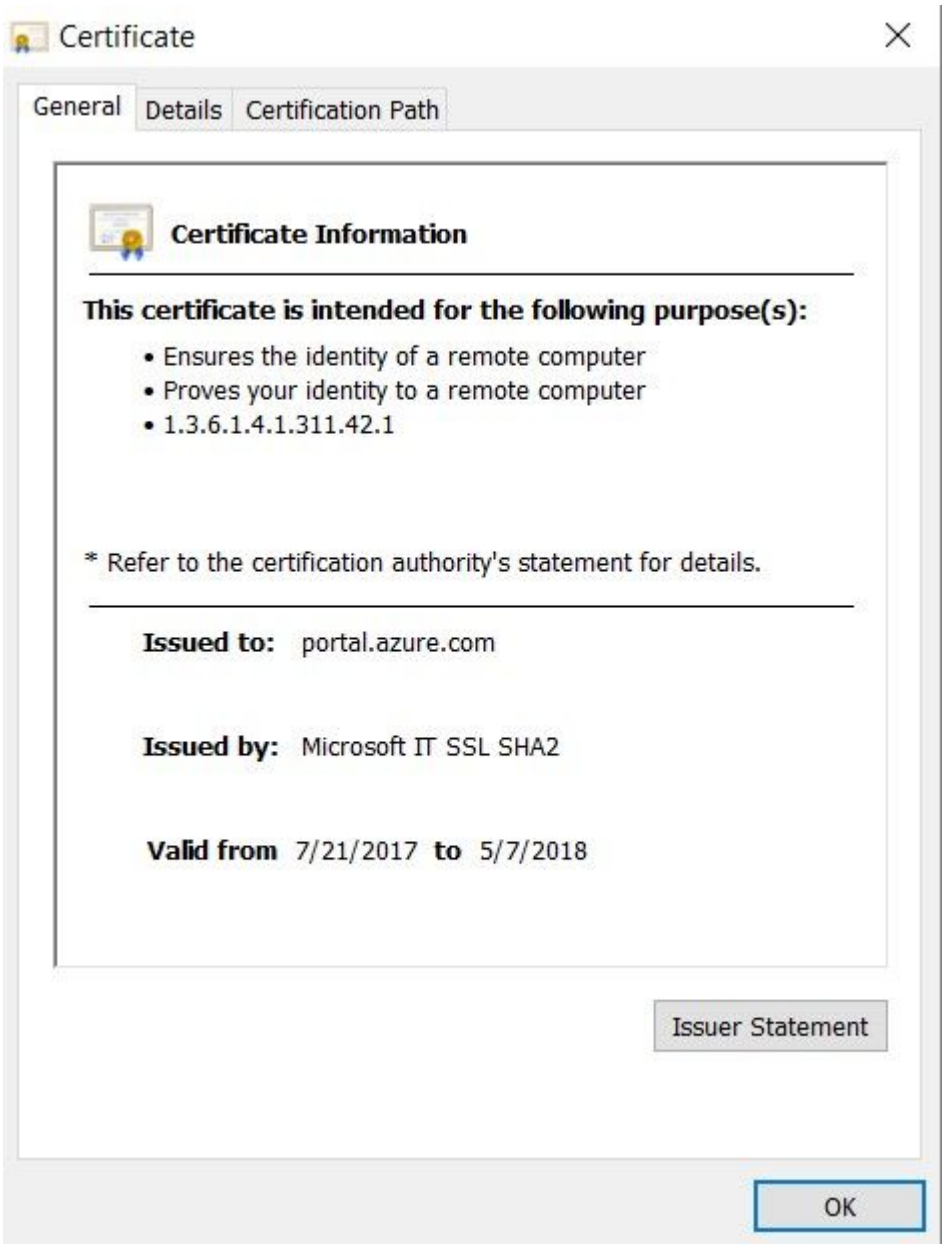
Inicie sesión en la consola de administración de Intune o en la consola de administración de Azure, cualquiera que sea el sitio que tenga su arrendatario. Utilice el navegador para obtener los detalles del

certificado:

Paso 1. Abra el Microsoft Azure portal desde un navegador web.

Paso 2. Haga clic en el símbolo de bloqueo de la barra de herramientas del explorador y, a continuación, haga clic en View Certificates.

Paso 3. En la ventana Certificado, haga clic en el botón Certification Path ficha. Un ejemplo se muestra aquí:

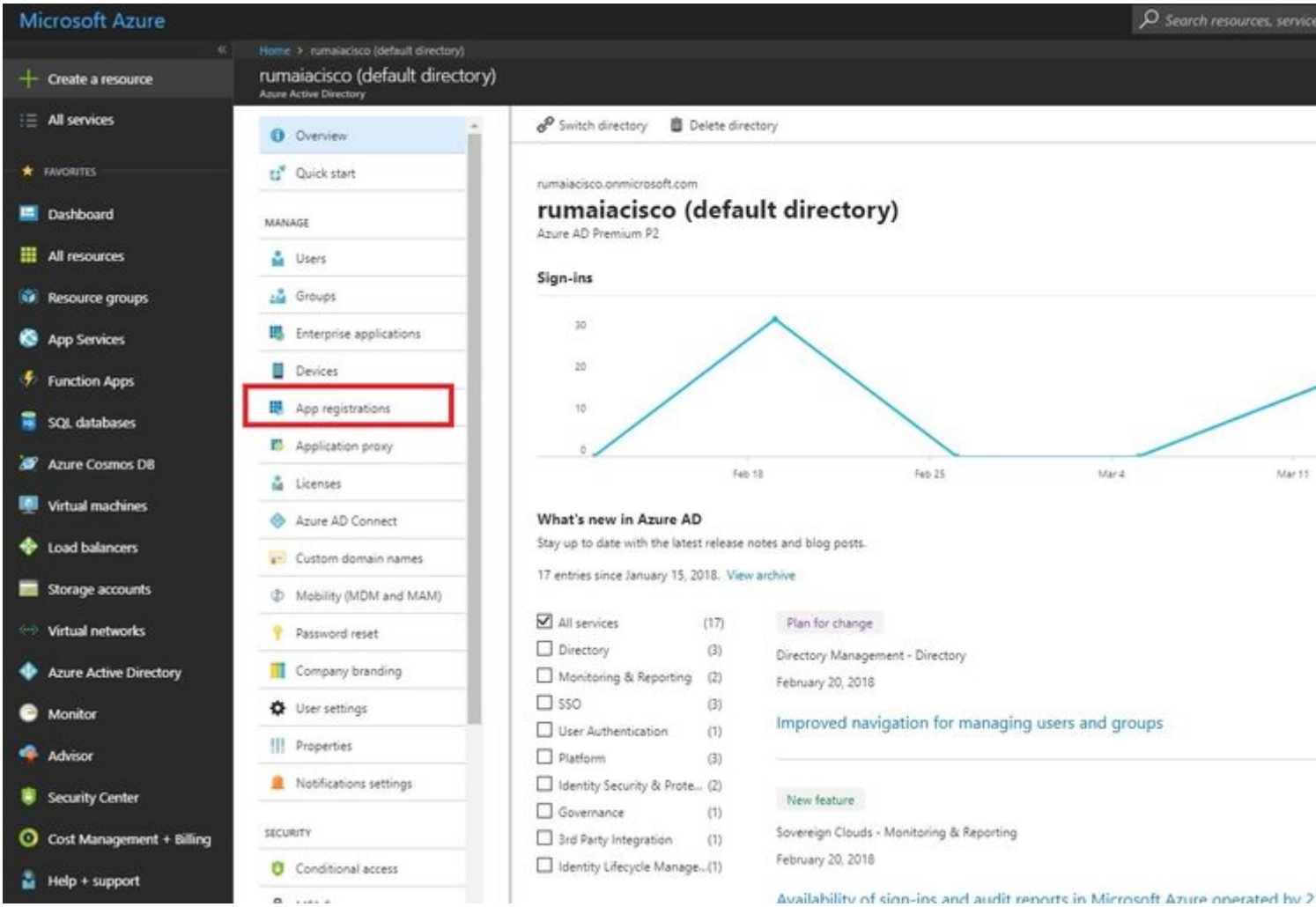


Paso 4. Buscar Baltimore Cyber Trust root, que es la CA raíz habitual. Sin embargo, si hay otra CA raíz distinta, haga clic en ese certificado de CA raíz. En la ficha Detalles de ese certificado de CA raíz, puede copiarlo en el archivo y guardarlo como certificado BASE64.

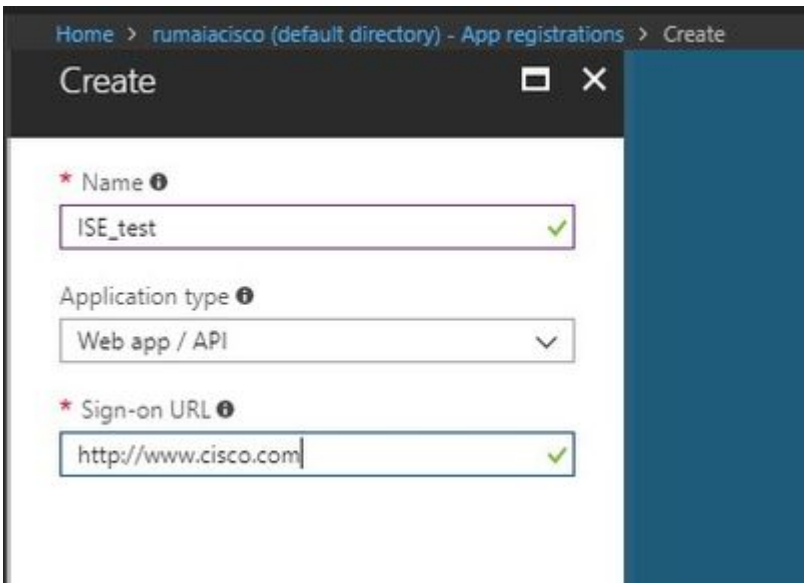
Paso 5. En ISE, vaya a Administration > System > Certificates > Trusted Certificatese importe el certificado raíz que se acaba de guardar. Dé un nombre descriptivo al certificado, como Azure MDM. Repita también el procedimiento para los certificados de CA intermedios.

Implementar ISE como una aplicación en el portal de Azure

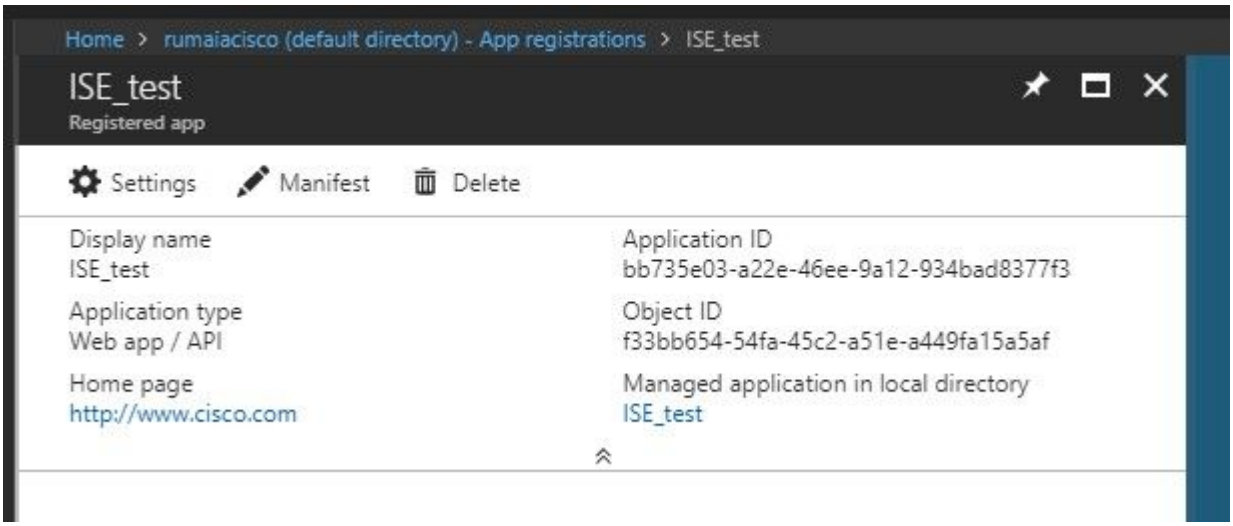
Paso 1. Desplácese hasta el Azure Active Directory y elija App registrations.



Paso 2. En el App registrations, cree un nuevo registro de aplicación con el nombre de ISE. Haga clic en Create como se muestra en esta imagen.



Paso 3. Elegir Settings para editar la aplicación y agregar los componentes requeridos.



Paso 4. Debajo Settings, elija los permisos necesarios y aplique estas opciones:

1. Microsoft Graph
    - Permisos de aplicación
        - Leer datos de directorio
    - Permisos delegados
        - Leer configuración y directivas de dispositivos de Microsoft Intune
        - Leer configuración de Microsoft Intune
        - Iniciar sesión como usuarios
        - Acceder a los datos del usuario en cualquier momento

2. API de Microsoft Intune
    - Permisos de aplicación
        - Obtener información sobre el estado y el cumplimiento del dispositivo de Microsoft Intune

3. Windows Azure Active Directory
    - Permisos de aplicación
        - Leer datos de directorio

    - Permisos delegados
        - Leer datos de directorio
        - Inicie sesión y lea el perfil de usuario

El resultado de la configuración es similar a lo que se muestra aquí :

+ Add a permission ✓ Grant admin consent for pavagupt-tme

API / Permissions name	Type	Description	Admin consent requ...	Status
Azure Active Directory Graph (3)				
Directory.Read.All	Delegated	Read directory data	Yes	Gra
Directory.Read.All	Application	Read directory data	Yes	Gra
User.Read.All	Delegated	Read all users' full profiles	Yes	Gra
Intune (1)				
get_device_compliance	Application	Get device state and compliance information from Micros...	Yes	Gra
Microsoft Graph (7)				
Directory.Read.All	Delegated	Read directory data	Yes	Gra
Directory.Read.All	Application	Read directory data	Yes	Gra
offline_access	Delegated	Maintain access to data you have given it access to	No	Gra
openid	Delegated	Sign users in	No	Gra
User.Read	Delegated	Sign in and read user profile	No	Gra
User.Read.All	Delegated	Read all users' full profiles	Yes	Gra
User.Read.All	Application	Read all users' full profiles	Yes	Gra

Settings

Filter settings

GENERAL

- Properties
- Reply URLs
- Owners

API ACCESS

- Required permissions
- Keys

TROUBLESHOOTING + SUPPORT

- Troubleshoot
- New support request

Required permissions

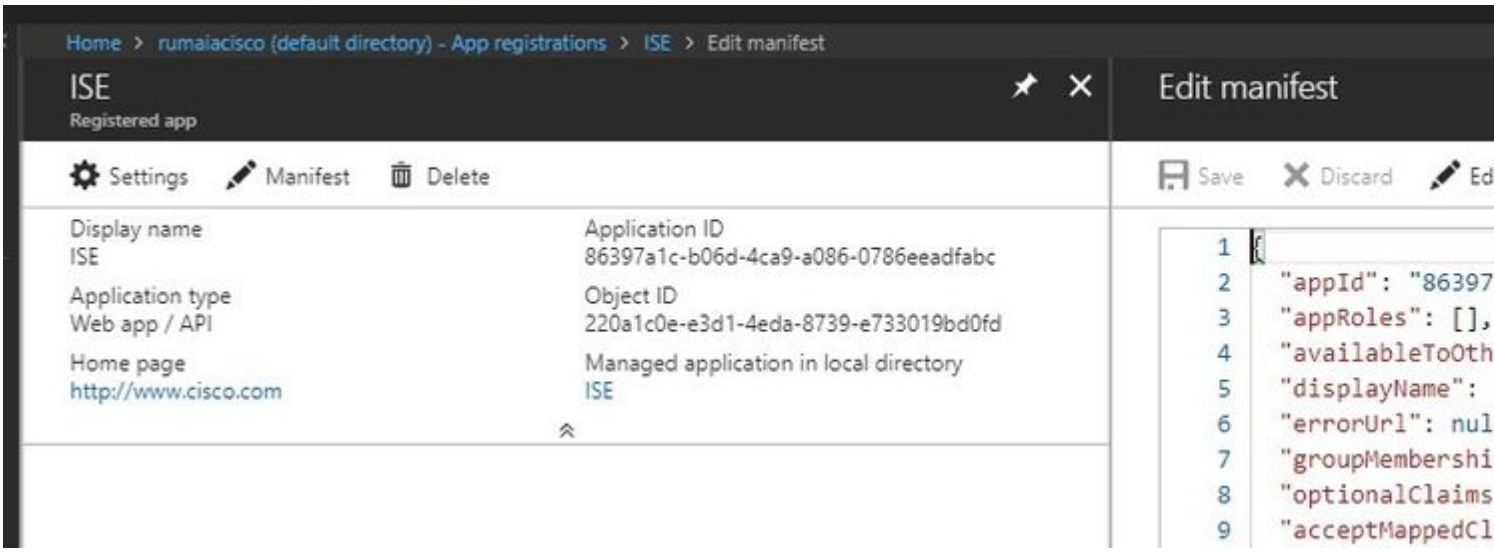
+ Add Grant Permissions

API	APPLICATION PERMI
Microsoft Graph	1
Microsoft Intune API	1
Windows Azure Active Directory	1

Paso 5. Haga clic en Grant Permissions para confirmar todos los permisos de la aplicación. Este proceso tarda de 5 a 10 minutos en surtir efecto. Edite el Azure Manifest para la aplicación creada para importar certificados de CA de ISE internos.

Importar certificados de ISE a la aplicación en Azure

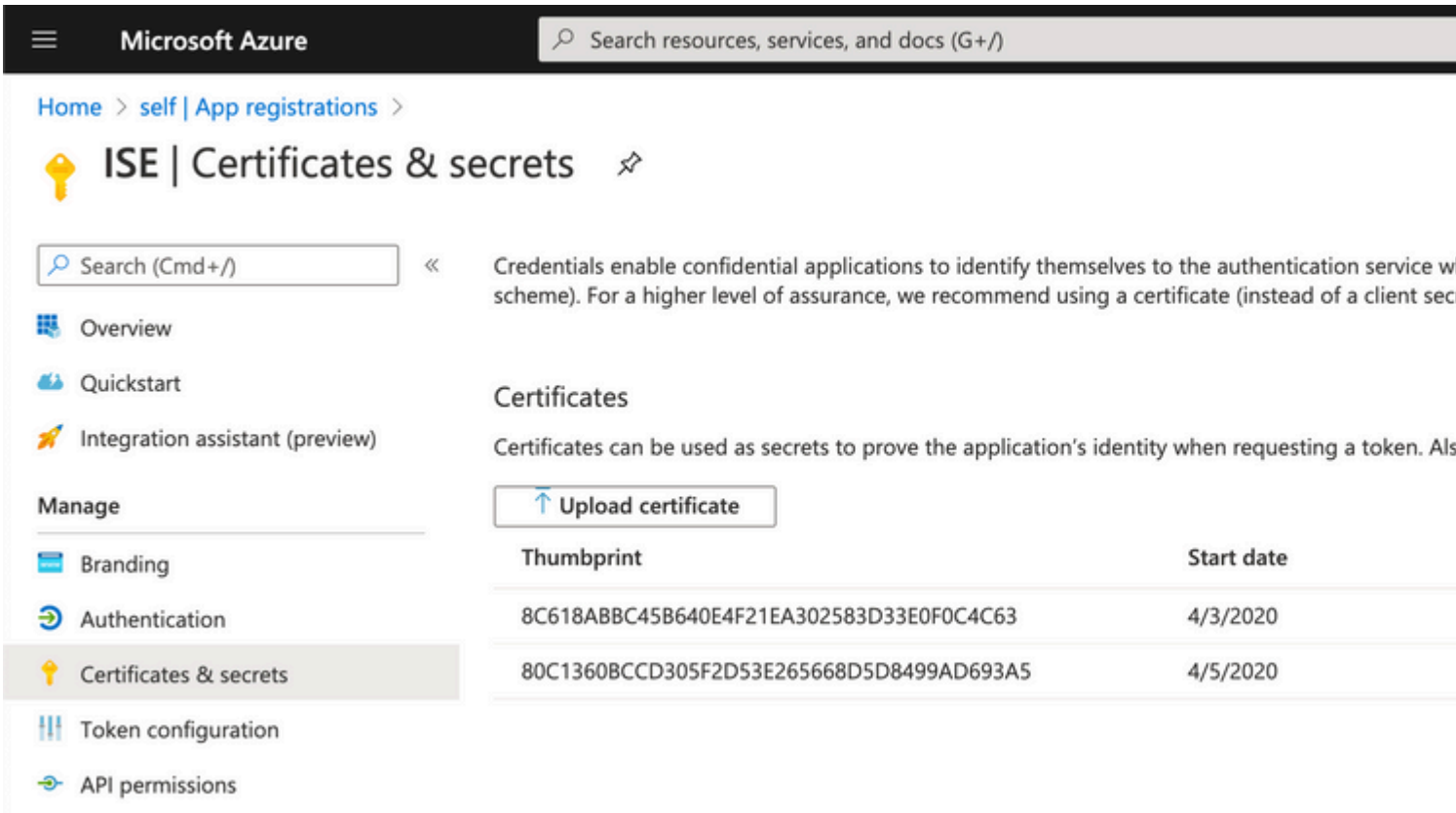
Paso 1. Descargue el archivo de manifiesto de la aplicación.



> **Nota**: Es un archivo con una extensión JSON. No edite el nombre de archivo o la extensión; de lo contrario, no se podrá editar.

Paso 2. Exporte el certificado del sistema ISE desde todos los nodos. En el panel, desplácese hasta Administration > System > Certificates > System Certificates, elija el certificado de servidor autofirmado predeterminado y haga clic en Export. Elegir Export Certificate Only (valor predeterminado) y elija un lugar para guardarlo. Elimine las etiquetas BEGIN y END del certificado y copie el resto del texto como una sola línea. Esto se aplica a las versiones anteriores a junio de 2020 descritas en la sección Legacy Option (Opción heredada).

Desde junio de 2020, el portal le permite cargar certificados directamente.



Opción heredada:

Paso 1. Ejecute un procedimiento de PowerShell para convertir el certificado a BASE64 e importarlo correctamente al archivo de manifiesto JSON de Azure. Utilice la aplicación ISE de Windows PowerShell o Windows PowerShell desde Windows. Use estos comandos:

```
$cer = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2
$cer.Import(â€œmycer.cerâ€)
$bin = $cer.GetRawCertData()
$base64Value = [System.Convert]::ToBase64String($bin)

$bin = $cer.GetCertHash()
$base64Thumbprint = [System.Convert]::ToBase64String($bin)

$keyid = [System.Guid]::NewGuid().ToString()
```

Paso 2. Mantener los valores para $base64Thumbprint, $base64Value,y $keyid, que se utilizan en el paso siguiente. Todos estos valores se agregan al campo JSON keyCredentials dado que, de forma predeterminada, tiene el siguiente aspecto:

```
15  "identifierUris": [
16    "https://rumaiacisco.onmicrosoft.com/239c7d6d-12d6-453c-8d3e-acfa701dc063"
17  ],
18  "keyCredentials": [],
19  "knownClientApplications": [],
```

Para ello, asegúrese de utilizar los valores en este orden:

```
"keyCredentials": [

  {

  â€œcustomKeyIdentifierâ€œ: â€œ$base64Thumbprint_from_powerShell_for_PPANâ€,

  â€œkeyIdâ€œ: â€œ$keyid_from_above_PPANâ€œ,

  "type": "AsymmetricX509Cert",

  "usage": "Verify",

  "value": "Base64 Encoded String of ISE PPAN cert"

  },

  {

  â€œcustomKeyIdentifierâ€œ: â€œ$base64Thumbprint_from_powerShell_for_SPANâ€,

  â€œkeyIdâ€œ: â€œ$keyid_from_above_SPANâ€œ,

  "type": "AsymmetricX509Cert",

  "usage": "Verify",
```

```
  "value": "Base64 Encoded String of ISE SPAN cert"

  }
],
```

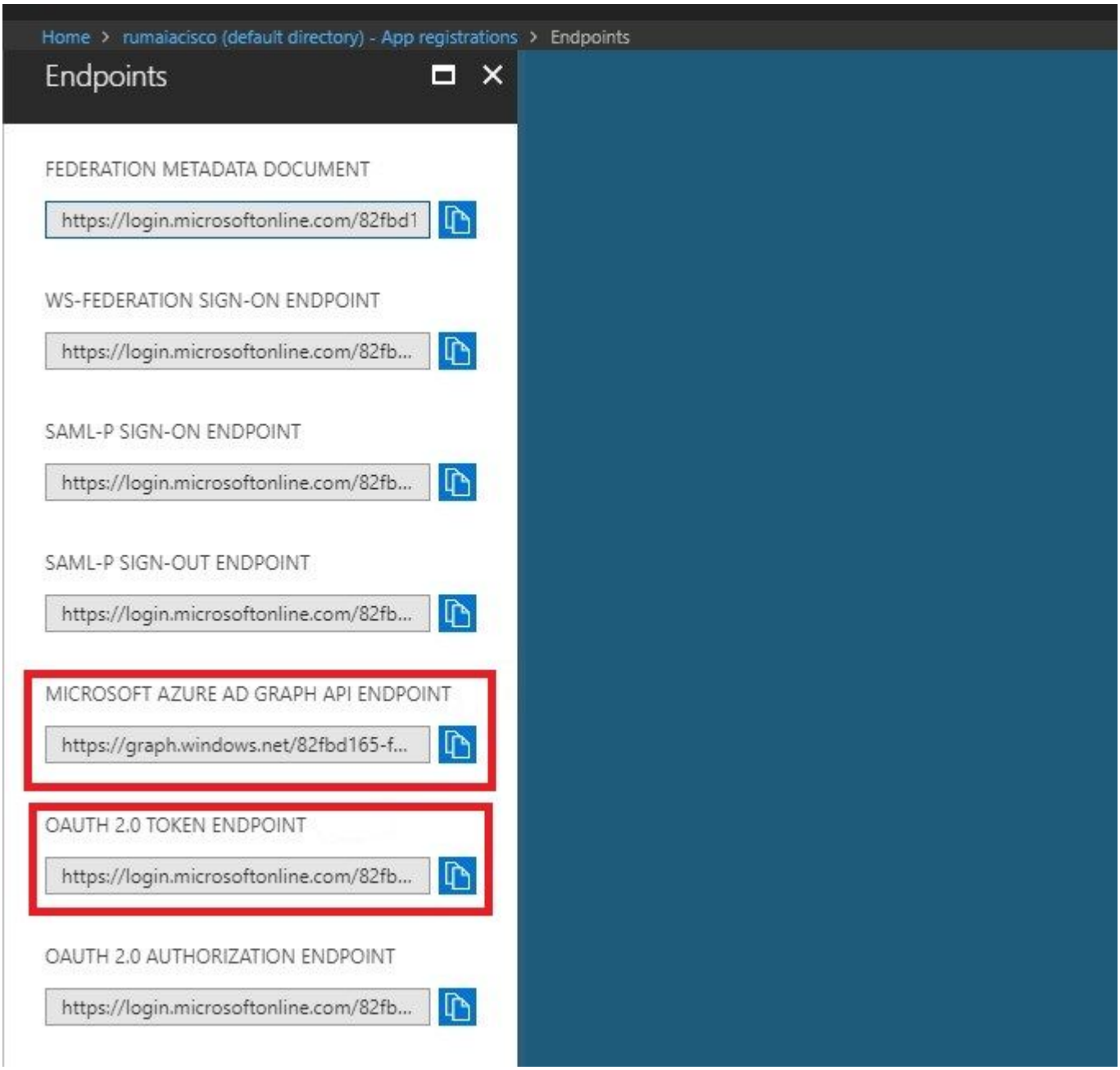
Paso 3. Cargar el archivo editado JSON a Azure Portal para validar la keyCredentials de los certificados utilizados en ISE.

Debe tener un aspecto similar al siguiente:

```
"keyCredentials": [
  {
    "customKeyIdentifier": "wteOPVePuM0wUeFNB9s22fkDYZE=",
    "endDate": "2019-01-22T11:41:01Z",
    "keyId": "eb7b1833-3240-4203-98a6-c3ccc6790d9d",
    "startDate": "2018-01-22T11:41:01Z",
    "type": "AsymmetricX509Cert",
    "usage": "Verify",
    "value": null
  },
  {
    "customKeyIdentifier": "B5Zz60fZKHGN6qAMvt43swIZQko=",
    "endDate": "2019-01-05T14:32:30Z",
    "keyId": "86462728-544b-423d-8e5e-22adf3521d23",
    "startDate": "2018-01-05T14:32:30Z",
    "type": "AsymmetricX509Cert",
    "usage": "Verify",
    "value": null
  },
  {
    "customKeyIdentifier": "GMlDp/1DYiNknFIJkgjnTbjo9nk=",
    "endDate": "2018-12-06T10:46:32Z",
    "keyId": "2ed5b262-ced6-4c1a-8a1a-c0abb82ae3c1",
    "startDate": "2017-12-06T10:46:32Z",
    "type": "AsymmetricX509Cert",
    "usage": "Verify",
    "value": null
  },
```

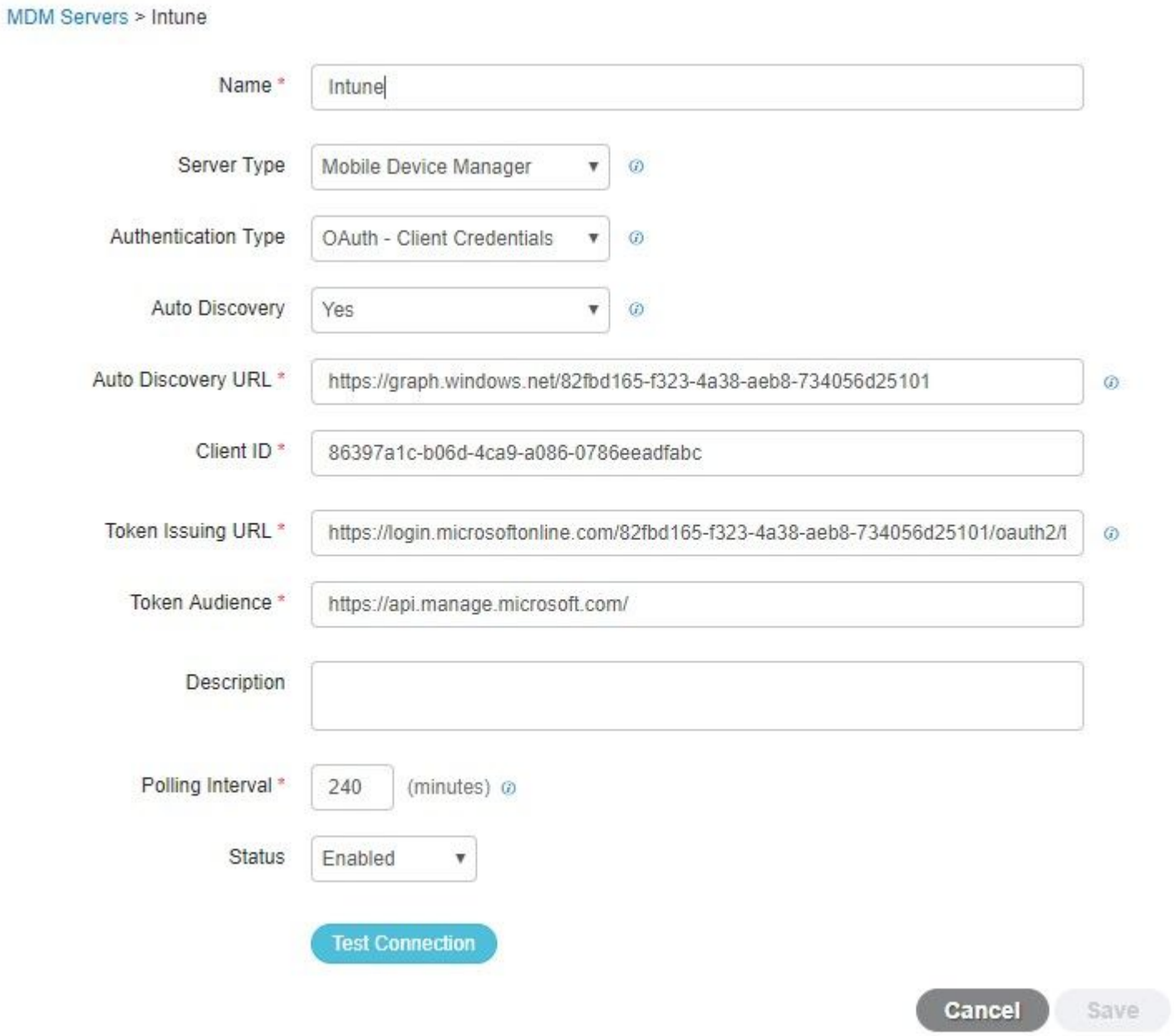
Paso 4. Tenga en cuenta que, después de la carga, el value campo debajo de keyCredentials espectáculos null ya que esto es forzado por el lado de Microsoft para no permitir que estos valores sean vistos después de la primera carga.

Los valores necesarios para agregar el servidor MDM en ISE se pueden copiar desde Microsoft Azure AD Graph API Endpoint y OAUTH 2.0 Token Endpoint.

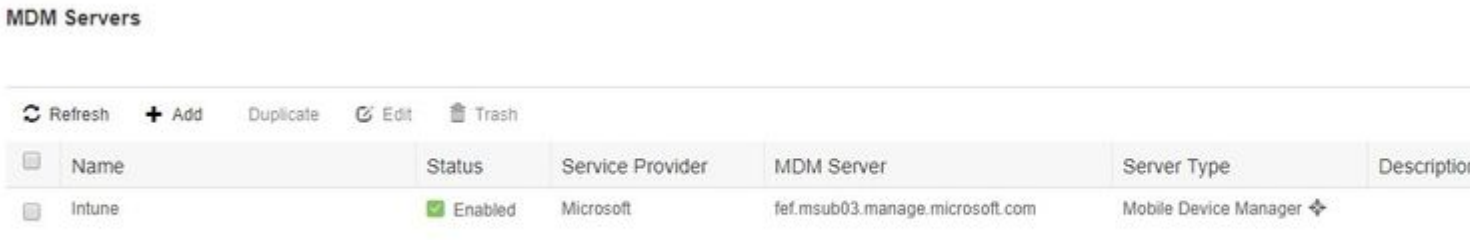


Estos valores deben introducirse en la GUI de ISE. Desplácese hasta Administration > Network Resources > External MDM y agregue un nuevo servidor:

ISE	Intune
URL de detección automática	Terminales > Extremo API de Microsoft Azure AD Graph
ID del cliente	{Registered-App-Name} > ID de aplicación
URL de emisión de token	Terminales > Terminal Token de OAuth 2.0

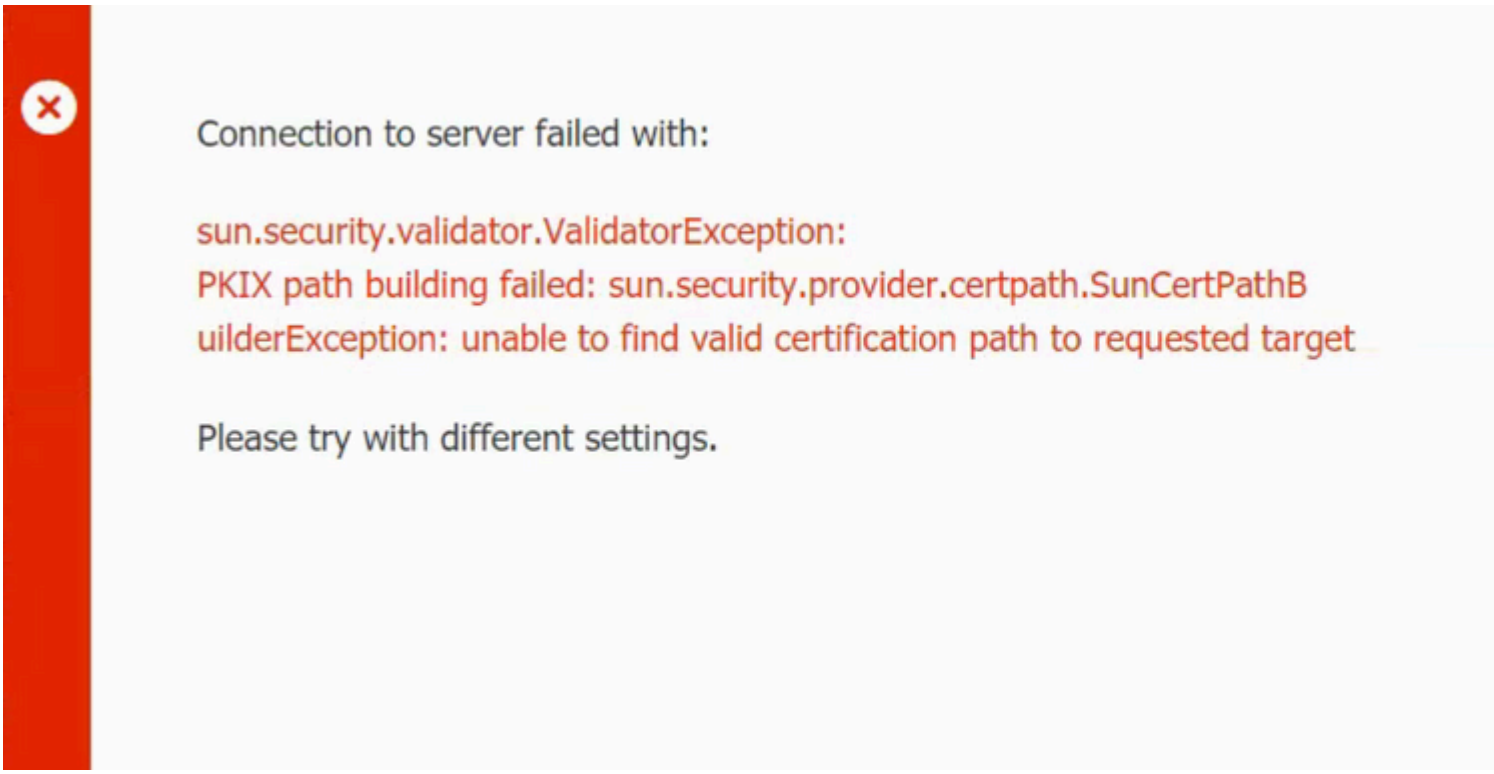


Una vez completada la configuración, el estado muestra habilitado.



Verificación y resolución de problemas

"Error de conexión al servidor" basado en sun.security.validatorException



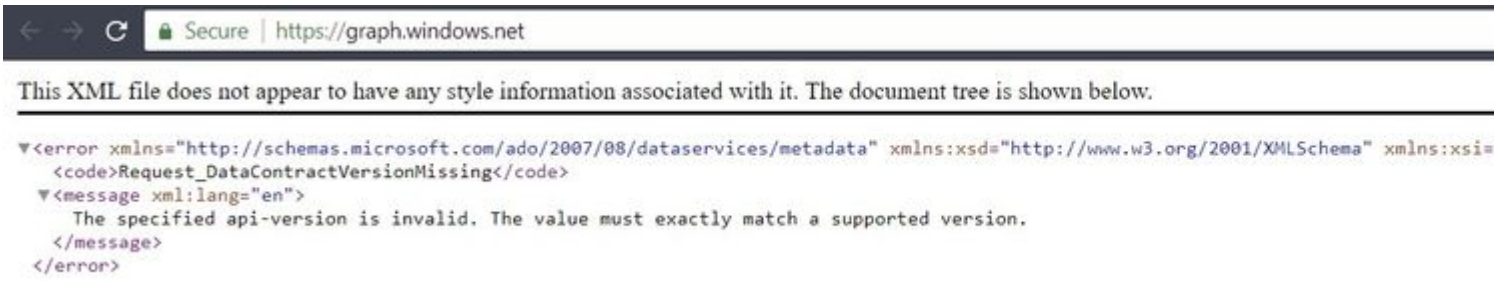
Paso 1. Recopile el paquete de soporte con estos registros en el nivel TRACE:

- portal (guest.log)
- mdmportal (ise-psc.log)
- external-mdm (ise-psc.log)

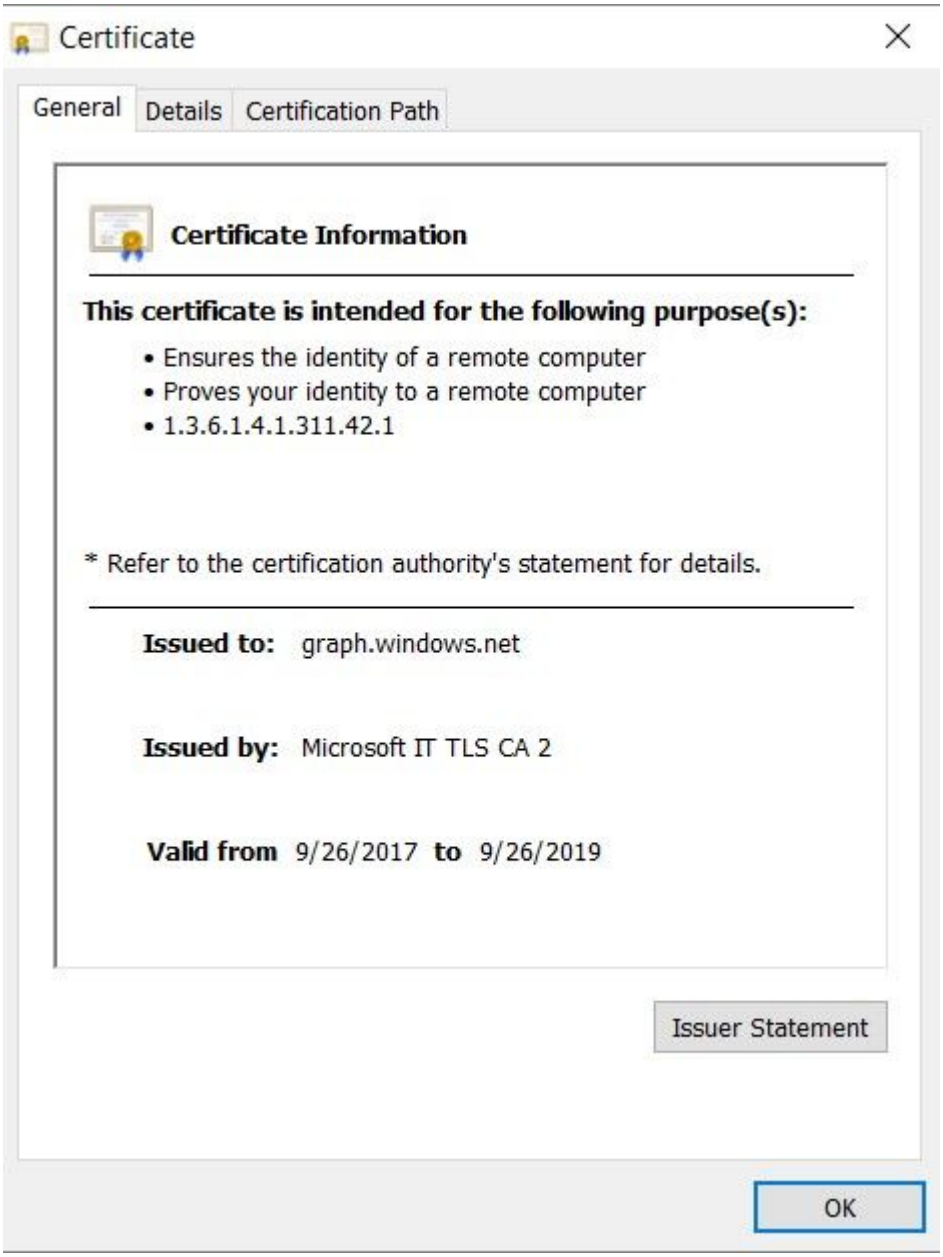
Paso 2. Cheque ise-psc.log para estos registros:

- 2016-10-17 12:45:52,158 DEBUG [admin-http-pool9300][] cisco.cpm.mdm.authtoken.MdmAzureActiveDirectoryClient -::::- ClientId - a46a6fd7-4a31-4471-9078-59cb2bb6a5ab, Token issuance endpoint - https://login
- microsoftonline.com/273106dc-2878-42eb-b7c8-069dcf334687/oauth2/token, ResourceId/App Id uri - https://graph.windows.net
- 2016-10-17 12:45:52,329 DEBUG [admin-http-pool9300][] cisco.cpm.mdm.authtoken.MdmCertAndKeyUtil -::::- Certificate Friendly Name -USMEM-AM01-ISE.Sncorp.smith-nephew.com#USMEM-AM01-ISE.Sncorp.smith-nephew.c
- om#00003
- **2016-10-17 12:45:52,354 DEBUG [admin-http-pool9300][] cisco.cpm.mdm.authtoken.MdmCertAndKeyUtil -::::- Result of command invocation**
- 2016-10-17 12:45:52,363 DEBUG [admin-http-pool9300][] cisco.cpm.mdm.authtoken.MdmCertAndKeyUtil -::::- Result of command invocation
- **2016-10-17 12:45:52,364 DEBUG [admin-http-pool9300][] cisco.cpm.mdm.authtoken.MdmCertAndKeyUtil -::::- Successfuly decrypted private key**
- 2016-10-17 12:45:52,794 ERROR [admin-http-pool9300][] cisco.cpm.mdm.authtoken.MdmAzureActiveDirectoryClient -::::- There is a problem with the Azure certificates or ISE trust store. sun.security.validator
- .ValidatorException: PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target
- 2016-10-17 12:45:52,794 ERROR [admin-http-pool9300][] cisco.cpm.mdm.authtoken.MdmAzureActiveDirectoryClient -::::- Unable to acquire access token from Azure
- **java.util.concurrent.ExecutionException: javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException: PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException**
- : unable to find valid certification path to requested target

Esto indica que es necesario importar el archivo graph.microsoft.com presente en esta página.

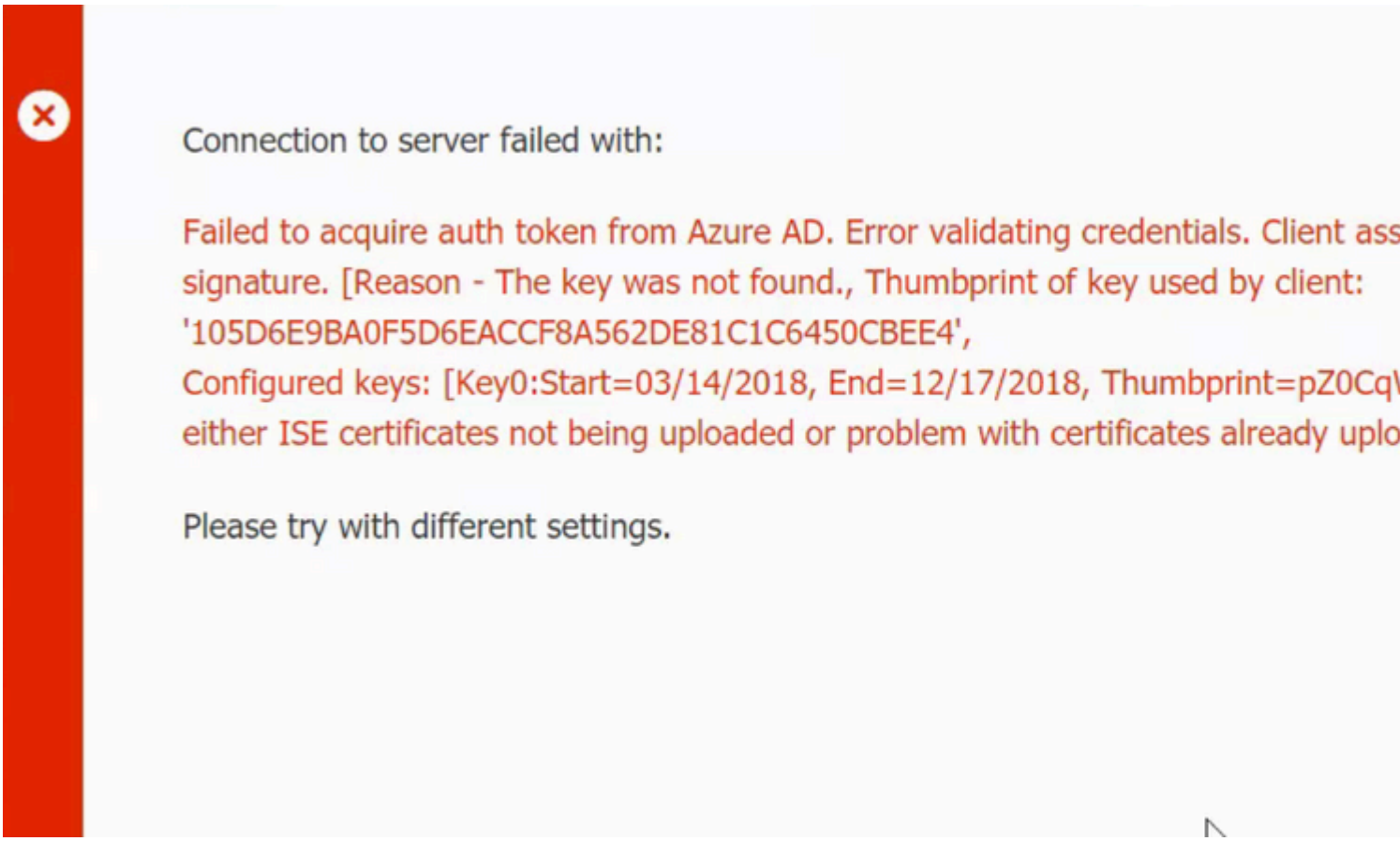


Paso 3. Haga clic en el locker y compruebe los detalles del certificado.



Paso 4. Guárdelo en un archivo en formato BASE64 e impórtelo a ISE Trusted Store. Asegúrese de importar la cadena de certificados completa. Después de esto, vuelva a probar la conexión con el servidor MDM.

Error al adquirir token de autenticación de Azure AD



Normalmente, este error se produce cuando el manifiesto JSON contiene la cadena de certificados ISE incorrecta. Antes de cargar el archivo de manifiesto en Azure, verifique si al menos esta configuración está presente:

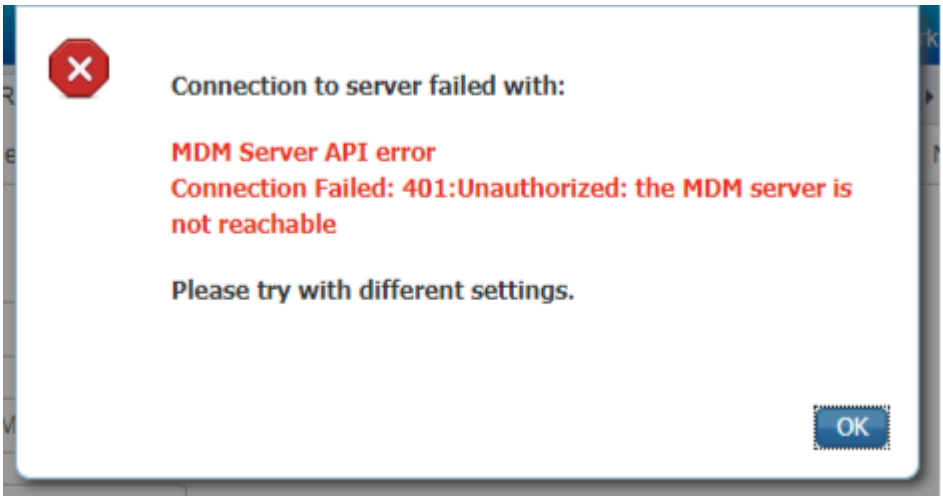
```
"keyCredentials": [
  {
  â€œcustomKeyIdentifierâ€œ: â€œ$base64Thumbprint_from_powerShell_for_PPANâ€ï¿½,
  â€œkeyIdâ€œ: â€œ$keyid_from_above_PPANâ€œ,
  "type": "AsymmetricX509Cert",
  "usage": "Verify",
  "value": "Base64 Encoded String of ISE PPAN cert"
  },
  {
  â€œcustomKeyIdentifierâ€œ: â€œ$base64Thumbprint_from_powerShell_for_SPANâ€ï¿½,
  â€œkeyIdâ€œ: â€œ$keyid_from_above_SPANâ€œ,
  "type": "AsymmetricX509Cert",
  "usage": "Verify",
  "value": "Base64 Encoded String of ISE SPAN cert"
  }
}
],
```

El ejemplo anterior se basa en un escenario en el que hay una PAN y una SAN. Ejecute de nuevo los scripts desde PowerShell e importe los valores BASE64 adecuados. Intente cargar el archivo de manifiesto y no debe enfrentarse a ningún error.

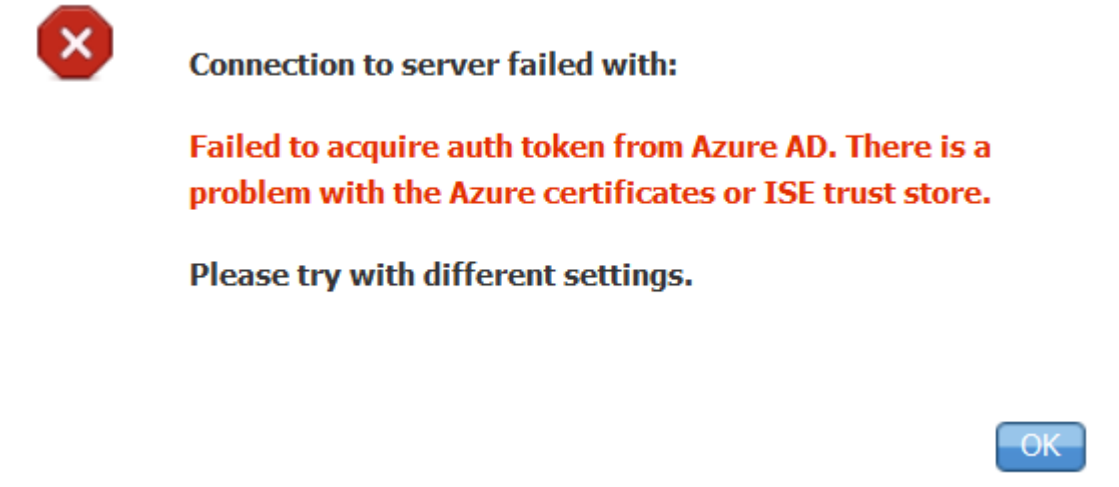
```
$cer = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2
$cer.Import(â€œmycer.crtâ€)
$bin = $cer.GetRawCertData()
$base64Value = [System.Convert]::ToBase64String($bin)

$bin = $cer.GetCertHash()
$base64Thumbprint = [System.Convert]::ToBase64String($bin)

$keyid = [System.Guid]::NewGuid().ToString()
```

Recuerde aplicar los valores para $base64Thumbprint, $base64Value y $keyid como se menciona en los pasos de la sección Configurar.

Error al adquirir token de autenticación de Azure AD



A menudo, este error se produce cuando no se conceden los permisos adecuados a la aplicación de Azure en portal.azure.com. Compruebe que la aplicación tiene los atributos correctos y asegúrese de que hace clic en Grant Permissions cada cambio.



Este mensaje aparece cuando ISE intenta acceder a la URL de emisión de token y devuelve un certificado que ISE no envía. Asegúrese de que la cadena completa de CA esté en el almacén de confianza de ISE. Si el problema continúa después de instalar el certificado correcto en el almacén de confianza de ISE, realice capturas de paquetes y pruebe la conectividad para ver qué se envía.

Información Relacionada

- Llamadas de servicio a servicio mediante credenciales de cliente
- Azure - Autenticación vs. autorización
- Azure - Quickstart: Registrar una aplicación con la plataforma de identidad de Microsoft
- Azure Active Directory app manifest
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).