Configuración del soporte de ISE SCEP para BYOD

Contenido

Introducción

Este documento describe los pasos que se utilizan para configurar correctamente el servicio de inscripción de dispositivos de red (NDES) de Microsoft y el protocolo simple de inscripción de certificados (SCEP) para la iniciativa "Trae tu propio dispositivo" (BYOD) en Cisco Identity Services Engine (ISE).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- ISE versión 1.1.1 o posterior
- Microsoft Windows Server 2008 R2
- Estándar de Microsoft Windows Server 2012
- Infraestructura de clave pública (PKI) y certificados

Componentes Utilizados

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

- ISE versión 1.1.1 o posterior
- Windows Server 2008 R2 SP1 con revisiones KB2483564 y KB2633200 instaladas
- Windows Server 2012 Standard

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

La información relacionada con los servicios de certificados de Microsoft se proporciona como guía específica para Cisco BYOD. Consulte Microsoft TechNet como la fuente definitiva de la verdad para las configuraciones de servidor relacionadas con Microsoft Certification Authority, Network Device Enrollment Service (NDES) y SCEP.

Antecedentes

Una de las ventajas de la implementación de BYOD habilitada para Cisco ISE es la capacidad de los usuarios finales para realizar el registro de dispositivos de autoservicio. Esto elimina la carga administrativa de la TI para distribuir las credenciales de autenticación y habilitar los dispositivos en la red. En el núcleo de la solución BYOD se encuentra el proceso de aprovisionamiento de suplicantes de red, que pretende distribuir los certificados necesarios a los dispositivos propiedad de los empleados. Para cumplir este requisito, se puede configurar una autoridad certificadora de Microsoft (CA) para automatizar el proceso de inscripción de certificados con el SCEP.

SCEP se ha utilizado durante años en entornos de red privada virtual (VPN) para facilitar la inscripción y distribución de certificados a clientes de acceso remoto y routers. La habilitación de la funcionalidad SCEP en un servidor Windows 2008 R2 requiere la instalación de NDES. Durante la instalación de la función NDES, también se instala el servidor Web de Microsoft Internet Information Services (IIS). IIS se utiliza para finalizar las solicitudes de registro HTTP o HTTPS SCEP y las respuestas entre el nodo de políticas de CA e ISE.

La función NDES se puede instalar en una CA actual o en un servidor miembro. En una implementación independiente, el servicio NDES se instala en una CA existente que incluye el servicio Certification Authority y, opcionalmente, el servicio Certification Authority Web Enrollment. En una implementación distribuida, el servicio NDES se instala en un servidor miembro. El servidor NDES distribuido se configura luego para comunicarse con una raíz ascendente o una CA sub-raíz. En esta situación, las modificaciones del Registro descritas en este documento se realizan en el servidor NDES con la plantilla personalizada, donde los certificados residen en la CA ascendente.

Escenarios de implementación de CA/NDES probados

Esta sección proporciona una breve descripción general de los escenarios de implementación de CA/NDES que se han probado en el laboratorio de Cisco. Consulte Microsoft TechNet como la fuente definitiva de la verdad para las configuraciones de servidor relacionadas con Microsoft CA, NDES y SCEP.

Implementaciones independientes

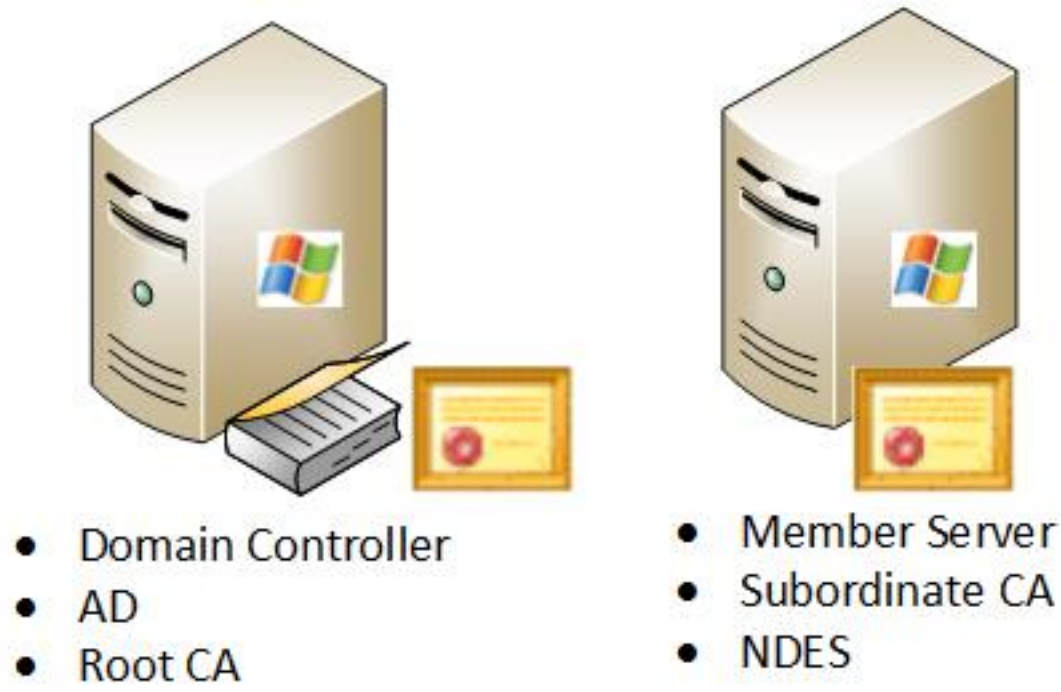
Cuando ISE se utiliza en un escenario de prueba de concepto (PoC), es común implementar un equipo independiente de Windows 2008 o 2012 que actúe como controlador de dominio de Active Directory (AD), CA raíz y servidor NDES:

- Domain Controller
- AD
- Root CA
- NDES

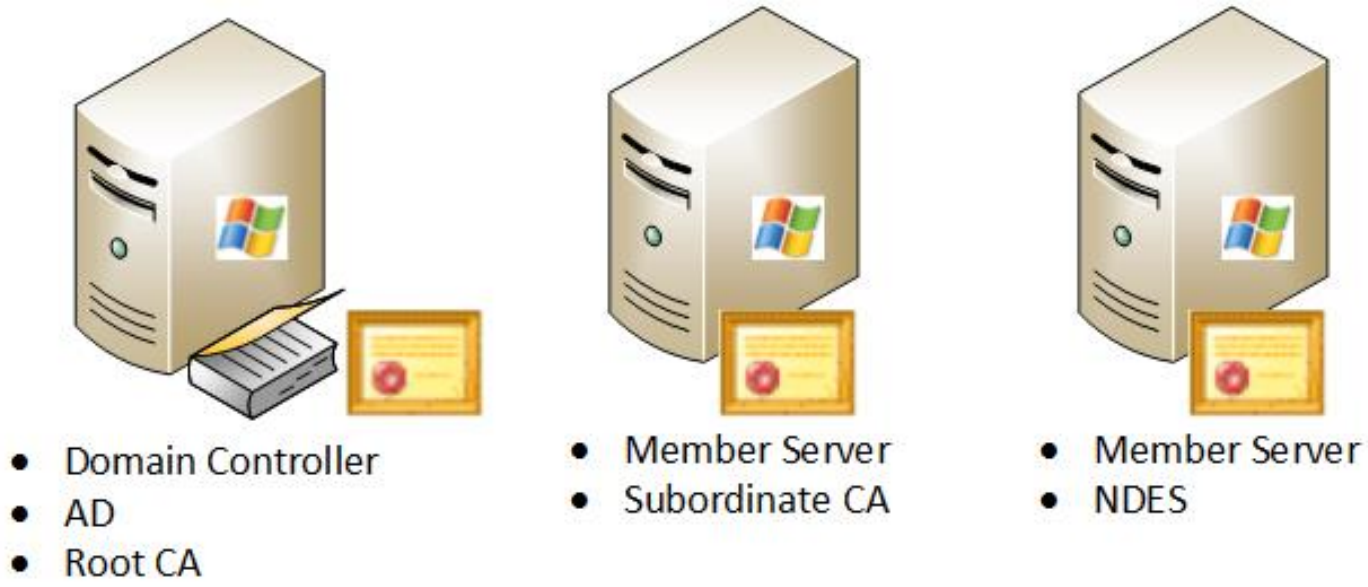
Implementaciones distribuidas

Cuando ISE se integra en un entorno de producción actual de Microsoft AD/PKI, es más común ver servicios distribuidos entre varios servidores Windows 2008 o 2012 distintos. Cisco ha probado dos escenarios para implementaciones distribuidas.

Esta imagen ilustra el primer escenario probado para implementaciones distribuidas:



Esta imagen ilustra el segundo escenario probado para implementaciones distribuidas:



Importantes revisiones de Microsoft

Antes de configurar el soporte SCEP para BYOD, asegúrese de que el servidor Windows 2008 R2 NDES tenga instaladas estas revisiones de Microsoft:

- La solicitud de renovación de un certificado SCEP falla en Windows Server 2008 R2 si el certificado se administra mediante NDES - Este problema ocurre porque NDES no soporta la operación **GetCACaps**.

- NDES no envía solicitudes de certificado después de reiniciar la CA empresarial en Windows Server 2008 R2 - Este mensaje aparece en el **Visor de eventos**: "*El Servicio de inscripción de dispositivos de red no puede enviar la solicitud de certificado (0x800706ba). El servidor RPC no está disponible*".

Advertencia: Al configurar la CA de Microsoft, es importante comprender que ISE no admite el algoritmo de firma RSASSA-PSS. Cisco recomienda que configure la política de CA para que utilice sha1WithRSAEncryption o sha256WithRSAEncryption en su lugar.

Puertos y protocolos BYOD importantes

A continuación se incluye una lista de los protocolos y puertos BYOD más importantes:

- TCP: 8909 Aprovisionamiento: Instalación del asistente desde Cisco ISE (sistemas operativos Windows y Macintosh (OS)))
- TCP: 443 Aprovisionamiento: Instalación del asistente desde Google Play (Android)
- TCP: 8905 Aprovisionamiento: Proceso de aprovisionamiento de suplicante
- TCP: 80 o TCP: 443 Proxy SCEP para CA (basado en la configuración de URL SCEP RA)

Nota: Para obtener la última lista de puertos y protocolos requeridos, refiérase a la Guía de Instalación de Hardware de ISE 1.2.

Configurar

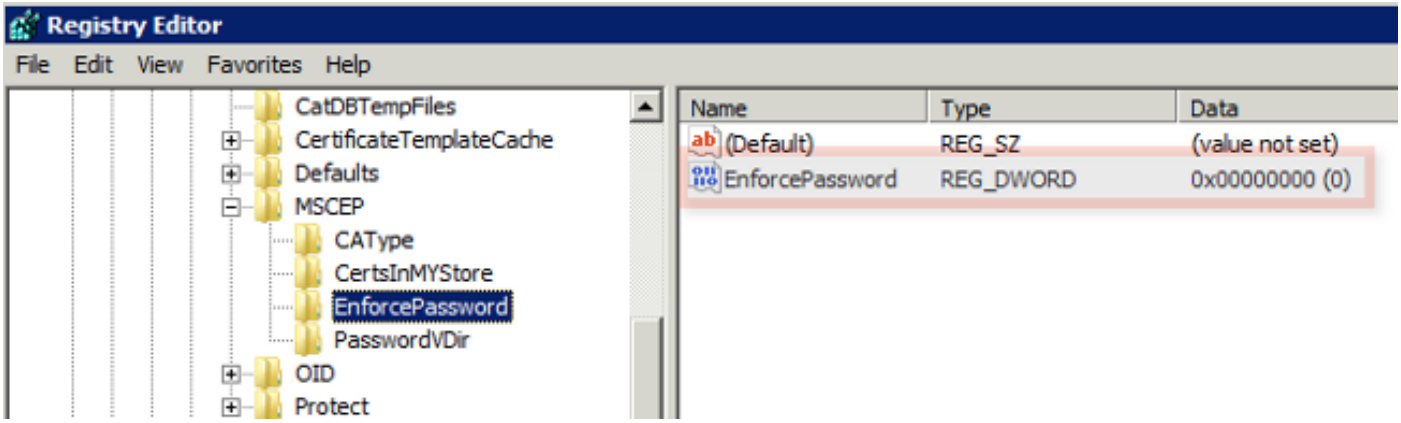
Utilice esta sección para configurar la compatibilidad con NDES y SCEP para BYOD en ISE.

Desactivar el requisito de contraseña de desafío de inscripción SCEP

De forma predeterminada, la implementación de Microsoft SCEP (MSCEP) utiliza una contraseña de desafío dinámico para autenticar clientes y terminales durante todo el proceso de inscripción de certificados. Con este requisito de configuración implementado, debe navegar a la GUI web del administrador de MSCEP en el servidor NDES para generar una contraseña a demanda. Debe incluir esta contraseña como parte de la solicitud de registro.

En una implementación de BYOD, el requisito de una contraseña de impugnación es contrario al objetivo de una solución de autoservicio para el usuario. Para eliminar este requisito, debe modificar esta clave de registro en el servidor NDES:

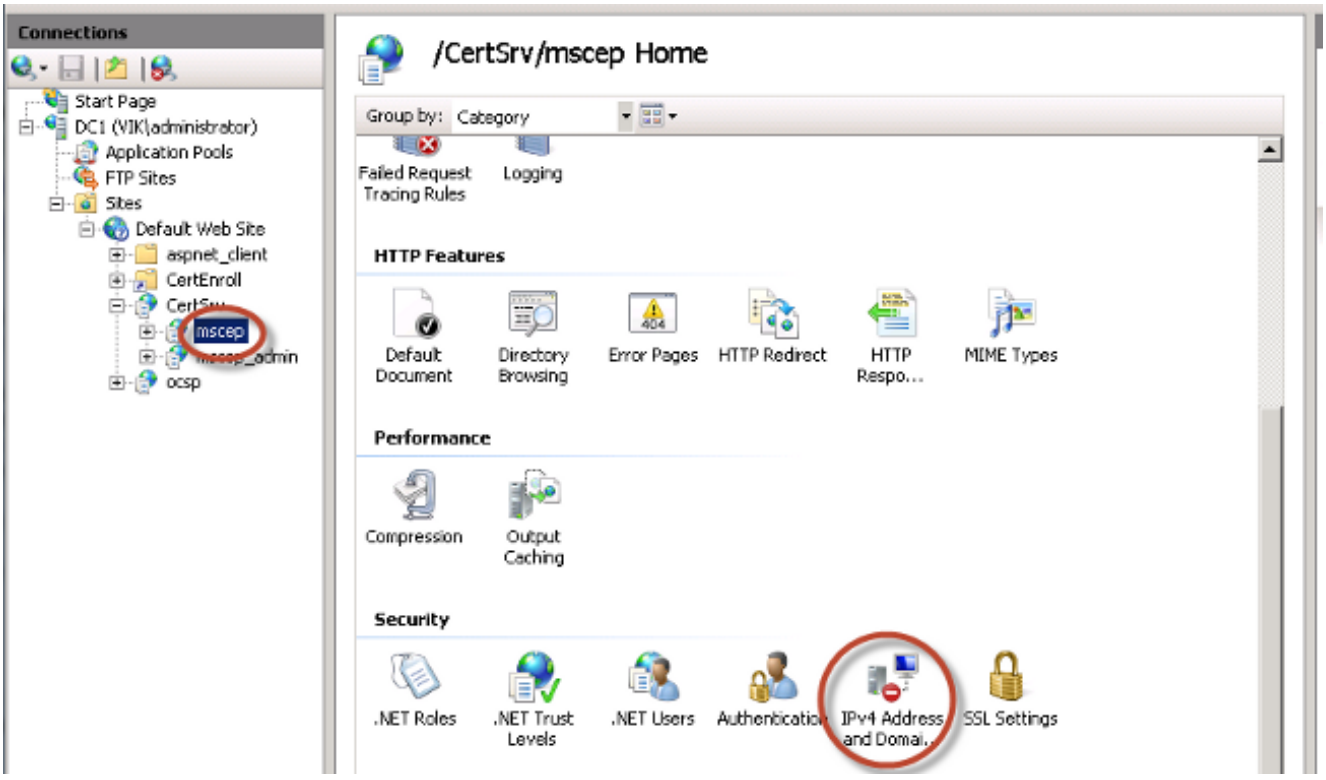
1. Haga clic en **Inicio** e introduzca **regedit** en la barra de búsqueda.
2. Vaya a Computer > HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Cryptography > MSCEP > EnforcePassword.
3. Asegúrese de que el valor **EnforcePassword** esté establecido en **0** (el valor predeterminado es **1**).



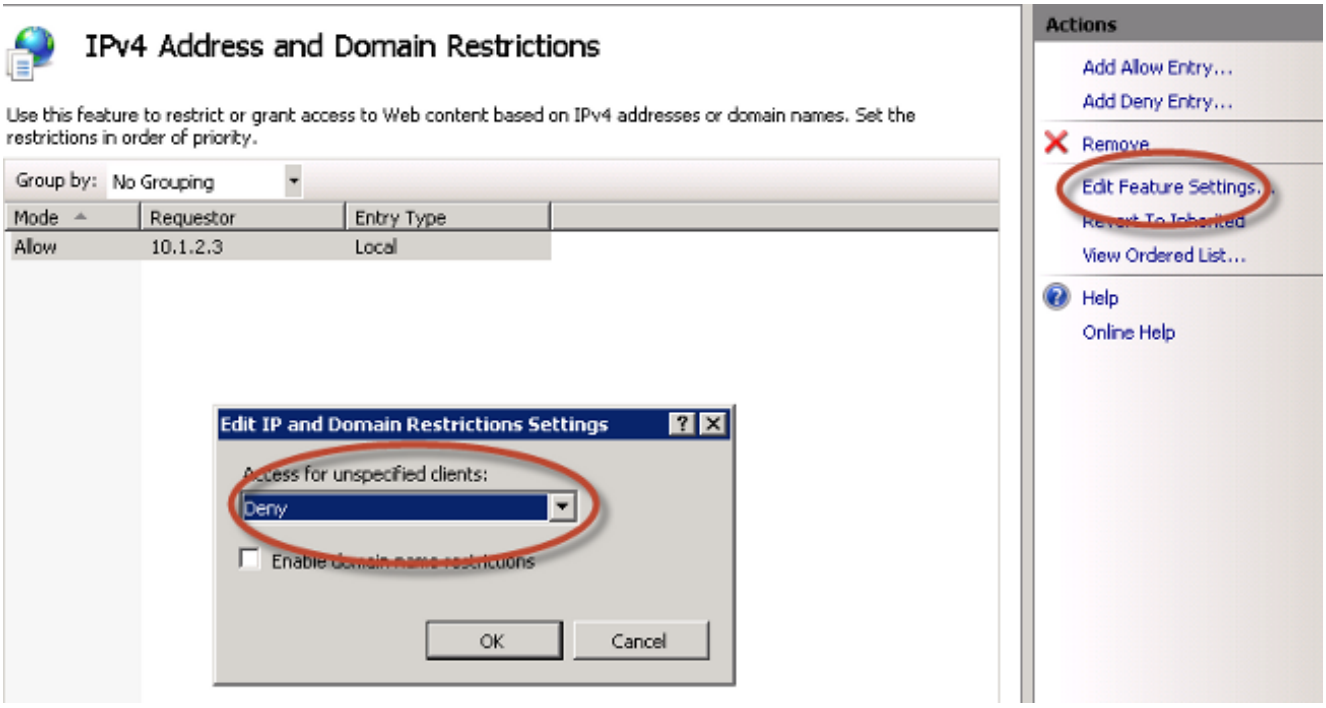
Restringir la inscripción SCEP a nodos ISE conocidos

En algunos escenarios de implementación, podría ser preferible restringir las comunicaciones SCEP a una lista seleccionada de nodos ISE conocidos. Esto se puede lograr con la característica de Restricciones de Dominio y Dirección IPv4 en IIS:

1. Abra IIS y navegue hasta el sitio web **/CertSrv/mscep**.



2. Haga doble clic en **Security > IPv4 Address and Domain Restrictions . Utilice las acciones Add Allow Entry** y **Add Deny Entry** para permitir o restringir el acceso al contenido web en función de las direcciones IPv4 o los nombres de dominio del nodo ISE. Utilice la acción **Editar configuración de funciones** para definir una regla de acceso predeterminada para clientes no especificados.

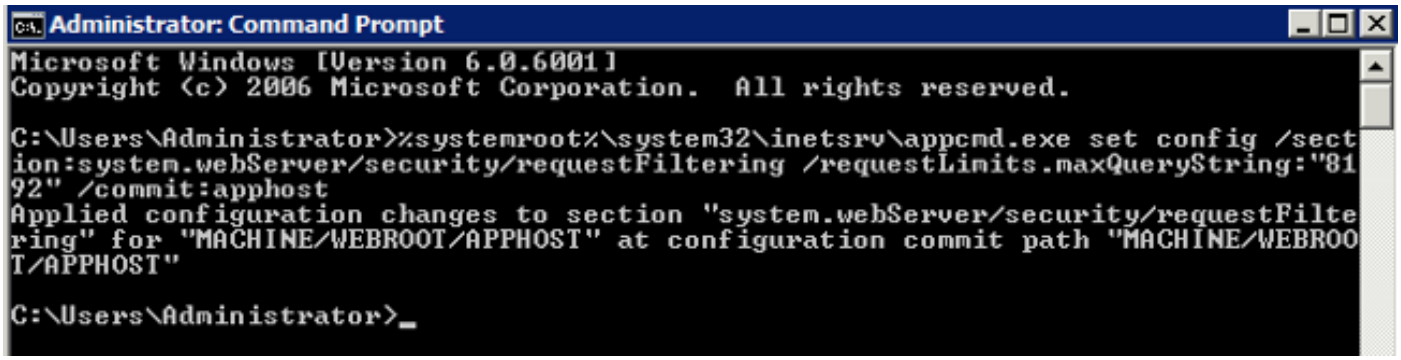


Extender la longitud de la URL en IIS

Es posible que ISE genere URL que son demasiado largas para el servidor Web IIS. Para evitar este problema, la configuración de IIS predeterminada se puede modificar para permitir URL más largas. Ingrese este comando desde la CLI del servidor NDES:

```
%systemroot%\system32\inetsrv\appcmd.exe set config /section:system.webServer/
 security/requestFiltering /requestLimits.maxQueryString:"8192" /commit:apphost
```

> **Nota:** El tamaño de la cadena de consulta puede variar en función del ISE y la configuración del terminal. Ingrese este comando desde la CLI del servidor NDES con privilegios administrativos.



Descripción general de la plantilla de certificado

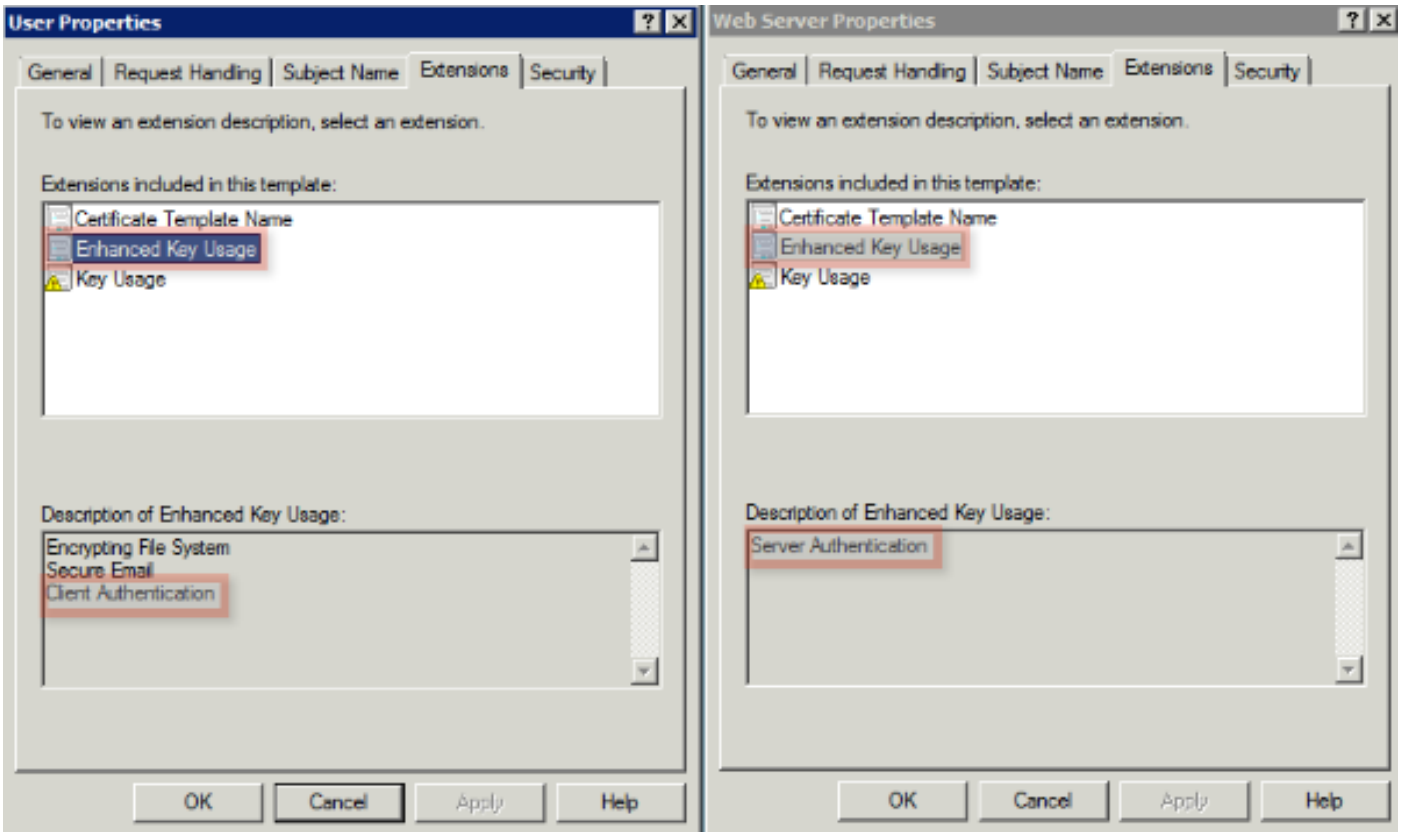
Los administradores de una CA de Microsoft pueden configurar una o más plantillas que se utilizan para aplicar políticas de aplicación a un conjunto común de certificados. Estas políticas ayudan a identificar para qué función se utilizan el certificado y las claves asociadas. Los valores de las políticas de aplicación se incluyen en el campo Uso de clave extendido (EKU) del certificado. El autenticador analiza los valores en el campo EKU para asegurarse de que el certificado presentado por el cliente pueda ser utilizado para la función deseada. Algunos de los usos más comunes incluyen autenticación de servidor, autenticación de cliente, VPN IPSec y

correo electrónico. En términos de ISE, los valores EKU más utilizados incluyen la autenticación de servidor y/o cliente.

Por ejemplo, al navegar a un sitio web de banco seguro, el servidor web que procesa la solicitud se configura con un certificado que tiene una política de aplicación de autenticación del servidor. Cuando el servidor recibe una solicitud HTTPS, envía un certificado de autenticación del servidor al explorador web conectado para la autenticación. El punto importante aquí es que este es un intercambio unidireccional del servidor al cliente. En lo que se refiere a ISE, un uso común para un certificado de autenticación de servidor es el acceso GUI de administración. ISE envía el certificado configurado al explorador conectado y no espera recibir un certificado de vuelta del cliente.

Cuando se trata de servicios como BYOD que utilizan EAP-TLS, se prefiere la autenticación mutua. Para habilitar este intercambio de certificados bidireccional, la plantilla utilizada para generar el certificado de identidad ISE debe poseer una política de aplicación mínima de autenticación del servidor. La plantilla de certificado de servidor Web cumple este requisito. La plantilla de certificado que genera los certificados de terminal debe contener una política de aplicación mínima de autenticación de cliente. La plantilla de certificado de usuario cumple este requisito. Si configura ISE para servicios como el Punto de aplicación de políticas en línea (iPEP), la plantilla utilizada para generar el certificado de identidad del servidor ISE debe contener tanto atributos de autenticación de cliente como de servidor si utiliza ISE versión 1.1.x o anterior. Esto permite que los nodos admin y en línea se autentiquen mutuamente. La validación de EKU para iPEP se eliminó en ISE versión 1.2, lo que hace que este requisito sea menos relevante.

Puede reutilizar las plantillas predeterminadas de Microsoft CA Web Server y User, o puede clonar y crear una nueva plantilla con el proceso que se describe en este documento. En función de estos requisitos de certificado, la configuración de CA y los certificados ISE y de punto final resultantes deben planificarse cuidadosamente para minimizar los cambios de configuración no deseados cuando se instalan en un entorno de producción.



Configuración de la plantilla de certificado

Como se indica en la introducción, SCEP se utiliza ampliamente en entornos VPN IPSec. Como resultado, la instalación de la función NDES configura automáticamente el servidor para utilizar la plantilla **IPSec (solicitud sin conexión)** para SCEP. Debido a esto, uno de los primeros pasos en la preparación de una CA de Microsoft para BYOD es crear una nueva plantilla con la política de aplicaciones correcta. En una implementación independiente, los servicios Certification Authority y NDES se colocan en el mismo servidor y las plantillas y las modificaciones del registro necesarias se incluyen en el mismo servidor. En una implementación de NDES distribuida, las modificaciones del registro se realizan en el servidor NDES; sin embargo, las plantillas reales se definen en el servidor de CA raíz o subraíz especificado en la instalación del servicio NDES.

Complete estos pasos para configurar la plantilla de certificado:

1. Inicie sesión en el servidor de CA como **admin**.

2. Haga clic en **Inicio > Herramientas administrativas > Autoridad de certificación**.

3. Expanda los detalles del servidor de la CA y seleccione la carpeta **Plantillas de certificado**. Esta carpeta contiene una lista de las plantillas que están habilitadas actualmente.

4. Para administrar las plantillas de certificado, haga clic con el botón derecho en la carpeta **Plantillas de certificado** y elija **Administrar**.

5. En la **Consola de plantillas de certificados**, se muestran varias plantillas inactivas.

6. Para configurar una nueva plantilla para su uso con SCEP, haga clic con el botón derecho en una plantilla que ya existe, como **Usuario**, y elija **Plantilla duplicada**.

7. Elija **Windows 2003** o **Windows 2008**, según el sistema operativo CA mínimo en el entorno.

8. En la ficha **General**, agregue un nombre para mostrar, como ISE-BYOD, y un período de validez; deje el resto de opciones sin marcar.
   Nota: El período de validez de la plantilla debe ser menor o igual al período de validez de los certificados raíz e intermedio de la CA.
9. Haga clic en la ficha **Nombre del asunto** y confirme que **Se ha seleccionado Suministrar en la solicitud**.

10. Haga clic en la pestaña **Requisitos de emisión**. Cisco recomienda que deje las **políticas de emisión** en blanco en un entorno de CA jerárquico típico.

11. Haga clic en la ficha **Extensiones**, **Políticas de aplicación** y, a continuación, **Editar**.

12. Haga clic en **Agregar** y asegúrese de que **Autenticación de Cliente** se agregue como política de aplicación. Click OK.

13. Haga clic en la ficha **Seguridad** y, a continuación, **Agregar...**. Asegúrese de que la cuenta de servicio SCEP definida en la instalación del servicio NDES tenga control total de la plantilla y, a continuación, haga clic en **Aceptar**.

14. Vuelva a la interfaz **GUI de la Autoridad de Certificación**.

15. Haga clic con el botón derecho del ratón en el directorio **Plantillas de certificados**. Vaya a **New > Certificate Template** para **Problema**.

16. Seleccione la plantilla **ISE-BYOD** configurada anteriormente y haga clic en **Aceptar**.

    Nota: Alternativamente, puede habilitar la plantilla a través de la CLI con el comando **certutil -SetCAtemplates +ISE-BYOD**.
    La plantilla ISE-BYOD debe aparecer en la lista de plantillas de certificados habilitadas.

Configuración del Registro de Plantilla de Certificado

Complete estos pasos para configurar las claves del Registro de Plantillas de Certificado:

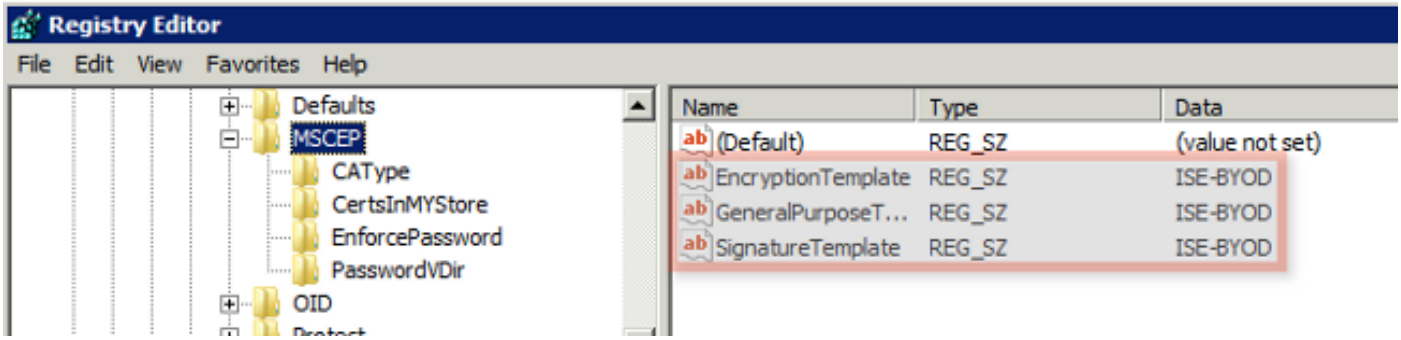
1. Conéctese al servidor NDES.

2. Haga clic en **Inicio** e introduzca **regedit** en la barra de búsqueda.

3. Vaya a Computer > HKEY_LOCAL_MACHINE > SOFTWARE > **Microsoft** > Cryptography > **MSCEP**.

4. Cambie las claves Template, **GeneralPurposeTemplate** y **SignatureTemplate** de **IPSec (solicitud fuera de línea)** a la plantilla ISE-BYOD creada anteriormente.

5. Reinicie el servidor NDES para aplicar la configuración del Registro.



Configuración de ISE como proxy SCEP

En una implementación de BYOD, el terminal no se comunica directamente con el servidor NDES backend. En su lugar, el nodo de política ISE se configura como proxy SCEP y se comunica con el servidor NDES en nombre de los terminales. Los terminales se comunican directamente con ISE. La instancia de IIS en el servidor NDES se puede configurar para soportar vinculaciones HTTP y/o HTTPS para los directorios virtuales SCEP.

Complete estos pasos para configurar ISE como proxy SCEP:

1. Inicie sesión en la **GUI de ISE** con las credenciales de administrador.

2. Haga clic en **Administration**, **Certificates** y, a continuación, en **SCEP CA Profiles**.

3. Haga clic en Add (Agregar).

4. Introduzca el nombre y la descripción del servidor.

5. Introduzca la dirección URL del servidor SCEP con la dirección IP o el nombre de dominio completo (FQDN) (http://10.10.10.10/certsrv/mscep/, por ejemplo).

6. Haga clic en **Probar conectividad**. Una conexión correcta genera un mensaje emergente de respuesta del servidor correcto.

7. Haga clic en **Guardar** para aplicar la configuración.

8. Para verificar, haga clic en **Administration**, **Certificates**, **Certificate Store,** y confirme que el certificado RA del servidor SCEP NDES se haya descargado automáticamente en el nodo ISE.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

Use esta sección para resolver problemas su configuración.

Notas generales de Troubleshooting

Esta es una lista de notas importantes que puede utilizar para resolver problemas de su configuración:

- Descomponga la topología de red BYOD en puntos lógicos para ayudar a identificar los puntos de depuración y captura a lo largo de la ruta entre los terminales ISE, NDES y CA.
- Asegúrese de que el nodo ISE y la CA compartan un origen de tiempo común de protocolo de tiempo de red (NTP).
- Los terminales deben poder establecer su hora automáticamente con las opciones de zona horaria y NTP aprendidas de DHCP.
- El servidor DNS del cliente debe poder resolver el FQDN del nodo ISE.
- Asegúrese de que TCP 80 y/o TCP 443 estén permitidos bidireccionalmente entre ISE y el servidor NDES.
- Pruebe con un equipo Windows debido al registro mejorado del lado del cliente. Opcionalmente, use un iDevice Apple junto con la utilidad de configuración de iPhone de

Apple para monitorear los registros de la consola del lado del cliente.

- Supervise los registros de la aplicación del servidor CA y NDES para detectar errores de registro, y utilice Google o TechNet para investigar esos errores.

- Durante la fase de prueba, utilice HTTP para SCEP para facilitar las capturas de paquetes entre ISE, NDES y CA.

- Utilice la utilidad TCP Dump en el nodo de servicio de políticas (PSN) de ISE y supervise el tráfico hacia y desde el servidor NDES. Esto se encuentra en **Operaciones > Herramientas de diagnóstico > Herramientas generales**.

- Instale Wireshark en el servidor CA y NDES, o utilice SPAN en los switches intermediarios, para capturar el tráfico SCEP hacia y desde ISE PSN.

- Asegúrese de que la cadena de certificados de CA adecuada esté instalada en el nodo de política de ISE para la autenticación de los certificados de cliente.

- Asegúrese de que la cadena de certificados de CA adecuada se instale automáticamente en los clientes durante la incorporación.

- Prevea los certificados de identidad de terminales e ISE y confirme que los atributos EKU correctos están presentes.

- Supervise los registros de autenticación en tiempo real en la interfaz gráfica de usuario de ISE para detectar fallos de autenticación y autorización.
  Nota: Algunos suplicantes no inicializan un intercambio de certificados de cliente si la EKU incorrecta está presente, como un certificado de cliente con EKU de autenticación de servidor. Por lo tanto, es posible que los errores de autenticación no siempre estén presentes en los registros de ISE.
- Cuando se instala NDES en una implementación distribuida, una CA raíz o subraíz remota será designada por Nombre de la CA o Nombre del equipo en la instalación del servicio. El servidor NDES envía solicitudes de registro de certificados a este servidor de CA de destino. Si el proceso de registro del certificado del terminal falla, las capturas de paquetes (PCAP) podrían mostrar al servidor NDES un error **404 no encontrado** en el nodo ISE. Para resolver este problema, reinstale el servicio NDES y seleccione la opción Nombre del equipo en lugar del Nombre de la CA.

- Evite las alteraciones en la cadena de CA de SCEP después de que los dispositivos estén incorporados. Los sistemas operativos de terminales, como Apple iOS, no actualizan automáticamente un perfil BYOD previamente instalado. En este ejemplo de iOS, el perfil actual se debe eliminar del terminal y el terminal se debe eliminar de la base de datos de ISE, para que la incorporación se pueda realizar de nuevo.

- Puede configurar un servidor de certificados de Microsoft para conectarse a Internet y actualizar automáticamente los certificados del Programa de certificados raíz de Microsoft. Si configura esta opción de recuperación de red en entornos con políticas de Internet restringidas, los servidores CA/NDES que no puedan conectarse a Internet pueden tardar 15

segundos en agotar el tiempo de espera de forma predeterminada. Esto puede agregar un retraso de 15 segundos al procesamiento de solicitudes SCEP de proxies SCEP como ISE. ISE se programa para agotar las solicitudes SCEP después de 12 segundos si no se recibe una respuesta. Para resolver este problema, permita el acceso a Internet para los servidores CA/NDES o modifique la configuración de tiempo de espera de recuperación de red en la política de seguridad local de los servidores CA/NDES de Microsoft. Para localizar esta configuración en el servidor de Microsoft, navegue hasta **Inicio > Herramientas administrativas > Política de seguridad local > Políticas de clave pública > Configuración de validación de ruta de certificado > Recuperación de red**.

Registro del lado del cliente

Esta es una lista de técnicas útiles que se utilizan para resolver problemas de registro del lado del cliente:

- Introduzca el **registro %temp%\spwProfileLog.txt.** para ver los registros del lado del cliente para las aplicaciones de Microsoft Windows.
  Nota: WinHTTP se utiliza para la conexión entre el terminal de Microsoft Windows e ISE. Haga referencia al artículo Mensajes de Error de Microsoft Windows para obtener una lista de códigos de error.
- Ingrese el comando **/sdcards/downloads/spw.log** para ver los registros del lado del cliente para las aplicaciones Android.

- Para **MAC OSX**, use la aplicación Console y busque el **proceso SPW**.

- Para **Apple iOS**, use Apple Configurator 2.0 para ver los mensajes.

Registro de ISE

Complete estos pasos para ver el registro de ISE:

1. Navegue hasta **Administration > Logging > Debug Log Configuration** y seleccione el nodo de política ISE adecuado.

2. Configure los registros **cliente** y **aprovisionamiento** para depurarlos o rastrearlos, según sea necesario.

3. Reproduzca el problema y documente la información de inicialización relevante para facilitar la búsqueda, como MAC, IP y usuario.

4. Navegue hasta **Operaciones > Descargar registros** y seleccione el nodo ISE adecuado.

5. En la pestaña **Debug Logs**, descargue los logs denominados **ise-psc.log** en el escritorio.

6. Utilice un editor inteligente, como Bloc de notas ++ para analizar los archivos de registro.

7. Cuando se ha aislado el problema, devuelva los niveles de registro al nivel predeterminado.

Registro y resolución de problemas de NDES

Para obtener más información, consulte AD CS: Solución de problemas del artículo del Servicio de inscripción de dispositivos de red de Windows Server.

Información Relacionada

- Guía de soluciones BYOD - Configuración del servidor de la autoridad certificadora
- Descripción general de NDES en Windows 2008 R2
- Informe técnico de MSCEP
- Configuración del Servidor NDES para Soportar SSL
- Requisitos de certificado cuando utiliza EAP-TLS o PEAP con EAP-TLS
- Asistencia técnica y documentación