Soporte de la configuración ISE SCEP para BYOD

Contenido

Introducción

Este documento describe los pasos que se utilizan para configurar con éxito el servicio de la inscripción del dispositivo de la red de Microsoft (NDE) y el protocolo simple certificate enrollment (SCEP) para Bring Your Own Device (BYOD) en Cisco identifica el motor de los servicios (ISE).

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Versión 1.1.1 ISE o más adelante
- R2 2008 del Microsoft Windows server
- Estándar del Microsoft Windows server 2012
- Public Key Infrastructure (PKI) y Certificados

Componentes Utilizados

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

- Versión 1.1.1 ISE o más adelante
- R2 2008 del Servidor Windows SP1 con el hotfixes KB2483564 y KB2633200 instalado
- Estándar del Servidor Windows 2012

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 la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

El relacionado con la información a los servicios de certificados de Microsoft se proporciona como guía específicamente para Cisco BYOD. Refiera al TechNet de Microsoft como la fuente definitiva de verdad para las autoridades de certificación de Microsoft, el servicio de la inscripción del dispositivo de red (NDE), y las Configuraciones del servidor SCEP-relacionadas.

Antecedentes

Una de las ventajas de la implementación ISE-habilitada Cisco BYOD es la capacidad de los usuarios finales de realizar el registro del dispositivo del autoservicio. Esto elimina la carga administrativa en el TIC para distribuir los credenciales de autenticación y habilitar los dispositivos en la red. En el corazón de BYOD la solución es el proceso de abastecimiento del supplicant de la red, que intenta distribuir los Certificados indispensables a los dispositivos propiedades de los empleados. Para satisfacer este requisito, un Microsoft Certificate Authority (CA) se puede configurar para automatizar el proceso de la inscripción del certificado con el SCEP.

El SCEP se ha utilizado por los años en los entornos del Red privada virtual (VPN) para facilitar la inscripción del certificado y la distribución a los clientes de acceso remoto y al Routers. La habilitación de las funciones SCEP en un servidor del r2 de Windows 2008 requiere la instalación de los NDE. Durante la instalación del papel NDE, el servidor Web de los Servicios de Internet Information Server de Microsoft (IIS) también está instalado. El IIS se utiliza para terminar el HTTP o los pedidos de inscripción y las respuestas HTTPS SCEP entre nodo de la directiva de CA y ISE.

El papel NDE se puede instalar en CA actual, o puede ser instalado en un servidor miembro. En un despliegue independiente, el servicio NDE está instalado en CA existente que incluye el servicio de las autoridades de certificación y, opcionalmente, el servicio de la inscripción de la red de las autoridades de certificación. En un despliegue distribuido, el servicio NDE está instalado en un servidor miembro. El servidor distribuido NDE entonces se configura para comunicar con una raíz o una sub-raíz por aguas arriba CA. En este escenario, las modificaciones del registro delineadas en este documento se hacen en el servidor NDE con la plantilla personalizada, donde los Certificados residen en la conexión en sentido ascendente CA.

Escenarios de instrumentación probados CA/NDES

Esta sección proporciona una breve descripción de los escenarios de instrumentación CA/NDES que se han probado en el laboratorio de Cisco. Refiera al TechNet de Microsoft como la fuente definitiva de verdad para Microsoft CA, NDE, y Configuraciones del servidor SCEP-relacionadas.

Implementaciones independientes

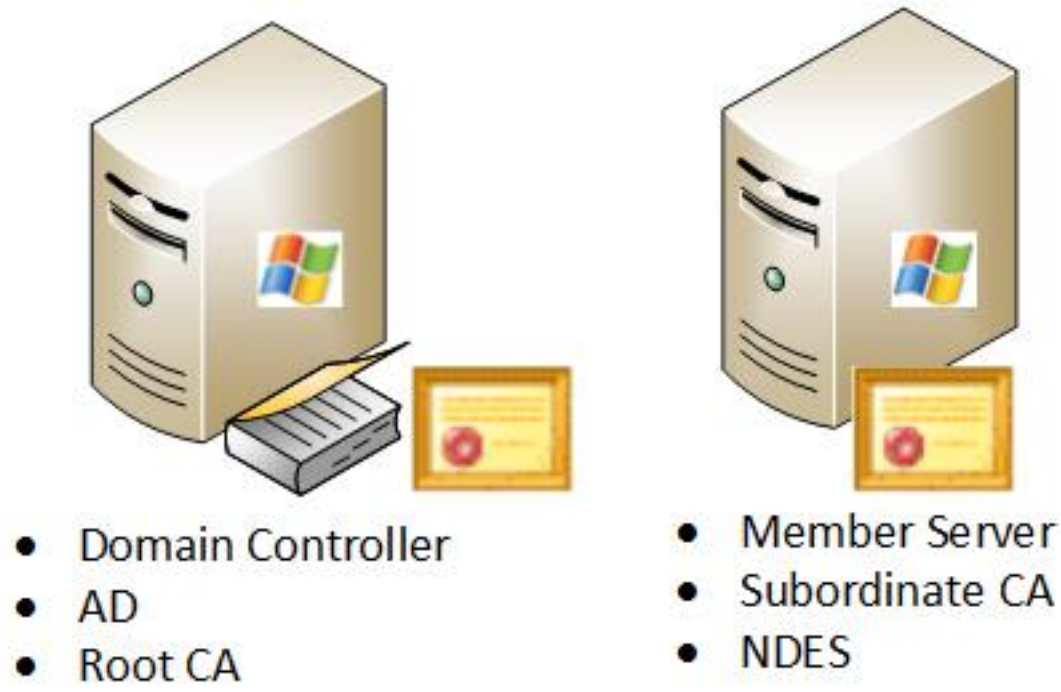
Cuando el ISE se utiliza en un escenario de la prueba de concepto (PC), es común desplegar Windows autónomo 2008 o 2012 trabaja a máquina que actúa como controlador de dominio del Active Directory (AD), raíz CA, y el servidor NDE:

- Domain Controller
- AD
- Root CA
- NDES

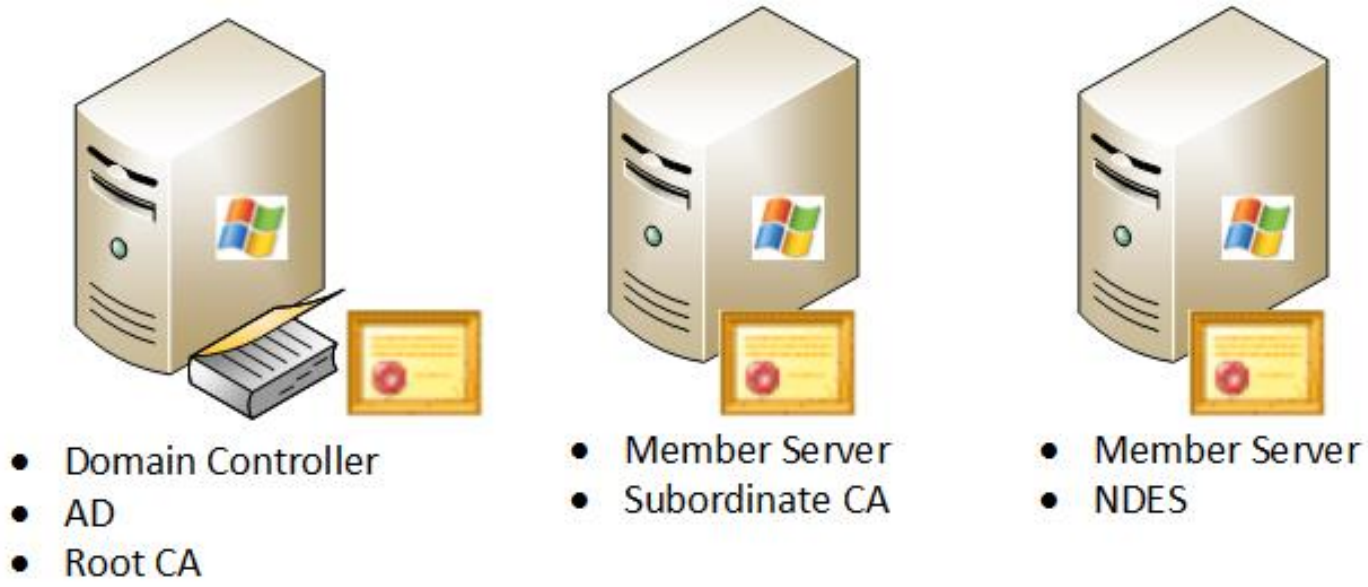
Implementaciones distribuidas

Cuando el ISE es integrado en un entorno de producción actual de Microsoft AD/PKI, es más común ver los servicios distribuidos a través del múltiplo, de los servidores distintos de Windows 2008 o 2012. Cisco ha probado dos escenarios para las implementaciones distribuidas.

Esta imagen ilustra el primer escenario probado para las implementaciones distribuidas:



Esta imagen ilustra el segundo escenario probado para las implementaciones distribuidas:



Hotfixes importante de Microsoft

Antes de que usted configure el soporte SCEP para BYOD, asegúrese de que el servidor del r2 NDE de Windows 2008 tenga este hotfixes de Microsoft instalado:

- El pedido de renovación para un certificado SCEP falla en el r2 2008 del Servidor Windows si el certificado se maneja usando los NDE - este problema ocurre porque los NDE no soportan la operación de **GetCACaps**.

- Los NDE no presentan los pedidos de certificado después de que la empresa CA se recomience en el Servidor Windows 2008 este mensaje R2- aparezca en el **visor de eventos**: "El *servicio de la inscripción del dispositivo de red no puede presentar el pedido de certificado (0x800706ba). El servidor RPC es inasequible*."

Advertencia: Cuando usted configura Microsoft CA, es importante entender que el ISE no soporta el algoritmo de la firma RSASSA-PSS. Cisco recomienda que usted configura la directiva de CA de modo que utilice sha1WithRSAEncryption o sha256WithRSAEncryption en lugar de otro.

Puertos importantes y protocolos BYOD

Aquí está una lista de puertos y protocolos importantes BYOD:

- TCP: 8909 Provisioning: El Asisitente instala de Cisco ISE (Windows y los sistemas operativos de Macintosh (el OS))
- TCP: 443 Provisioning: El Asisitente instala de Google Play (Android)
- TCP: 8905 Provisioning: Proceso de abastecimiento del supplicant
- TCP: 80 o TCP: 443 proxy SCEP a CA (basado en la configuración SCEP RA URL)

Nota: Para la última lista de puertos y protocolos requeridos, refiera al guía de instalación del hardware ISE 1.2.

Configurar

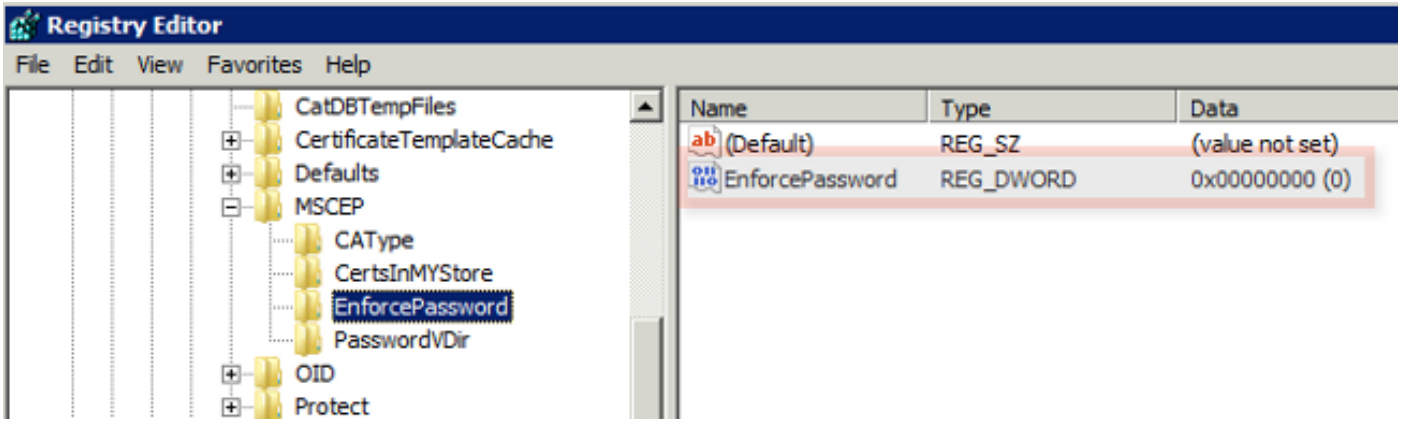
Utilice esta sección para configurar el soporte NDE y SCEP para BYOD en el ISE.

Inhabilite el requisito de la contraseña de impugnación de la inscripción SCEP

Por abandono, la implementación de Microsoft SCEP (MSCEP) utiliza una contraseña de impugnación dinámica para autenticar los clientes y los puntos finales en el proceso de la inscripción del certificado. Con estos requisitos para la configuración en el lugar, usted debe hojear a la red GUI MSCEP admin en el servidor NDE para generar una contraseña a pedido. Usted debe incluir esta contraseña como parte del pedido de inscripción.

En un despliegue BYOD, el requisito de una contraseña de impugnación derrota el propósito de una solución del autoservicio del usuario. Para quitar este requisito, usted debe modificar esta clave de registro en el servidor NDE:

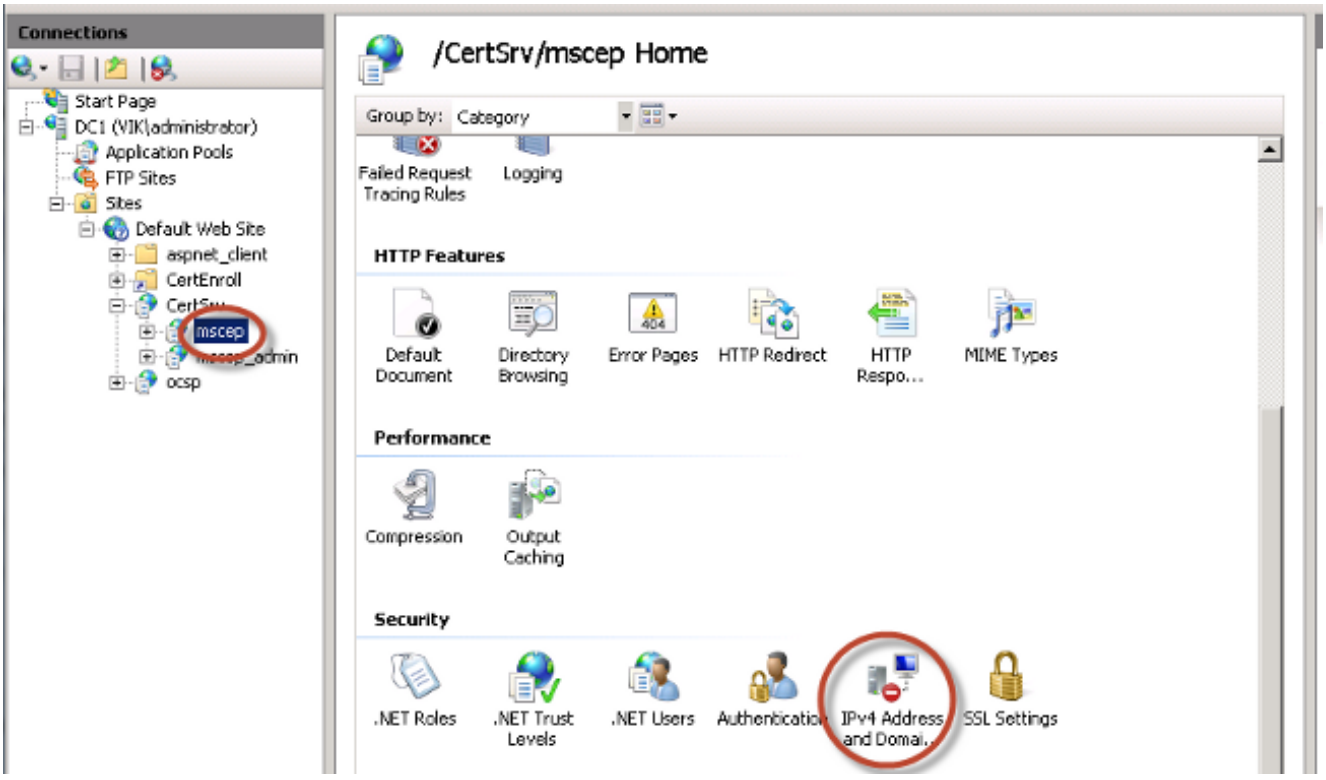
1. Haga clic el **comienzo** y ingrese el **regedit** en la barra de la búsqueda.
2. Navegue a la **Computadora** > al **HKEY_LOCAL_MACHINE** > al **SOFTWARE** > a **Microsoft** > a la **criptografía** > a **MSCEP** > a **EnforcePassword**.
3. Asegúrese de que el valor de **EnforcePassword** esté fijado a **0** (el valor predeterminado es **1)**.



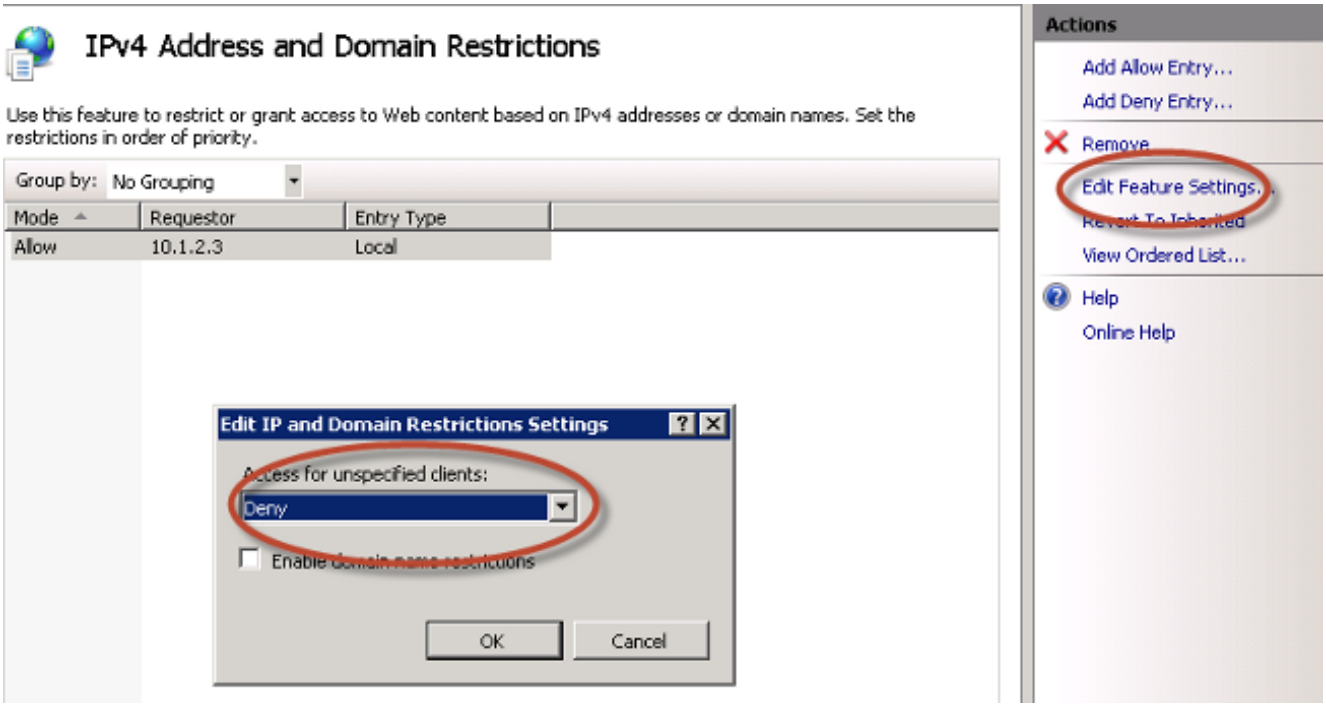
Restrinja la inscripción SCEP a los Nodos sabidos ISE

En algunos escenarios de instrumentación, puede ser que sea preferido para restringir las comunicaciones SCEP a una lista selecta de Nodos sabidos ISE. Esto se puede lograr con la característica de las restricciones del direccionamiento y del dominio del IPv4 en el IIS:

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



2. Doble las **restricciones de la Seguridad del** tecleo **> del direccionamiento y del dominio del IPv4.** Utilice el **agregar permiten la entrada** y **agregan niegan las** acciones de la **entrada** para permitir o restringir el acceso al contenido de la Web basado en los direccionamientos o los Domain Name del IPv4 del nodo ISE. Utilice la acción de las **configuraciones de la función del editar** para definir una regla de acceso predeterminada para los clientes sin especificar.

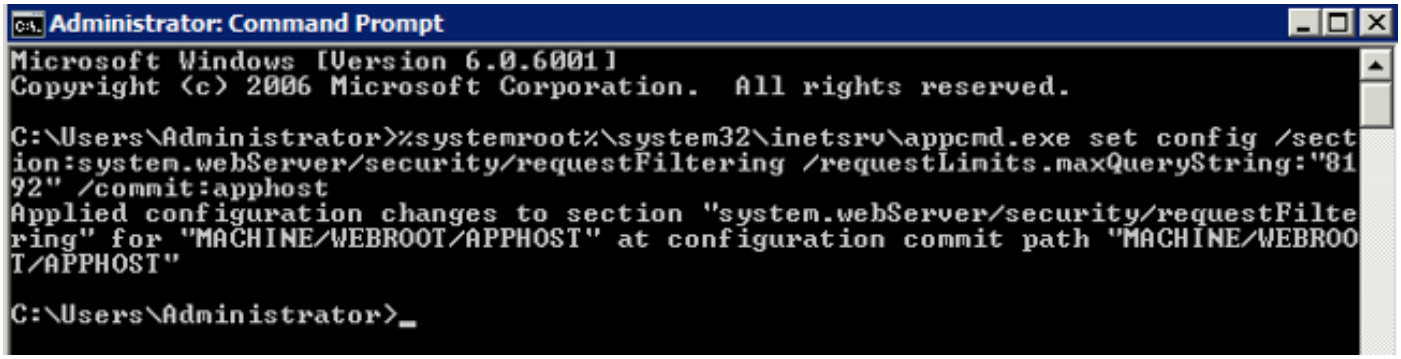


Amplíe la longitud URL en el IIS

Es posible que el ISE genere los URL que son demasiado largos para el servidor Web IIS. Para evitar este problema, la configuración IIS predeterminada se puede modificar para tener en cuenta URL más largos. Ingrese este comando del servidor CLI NDE:

```
%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 pudo variar al dependiente sobre la configuración ISE y del punto final. Ingrese este comando del servidor CLI NDE con los privilegios administrativos.



Descripción del Certificate Template plantilla de certificado

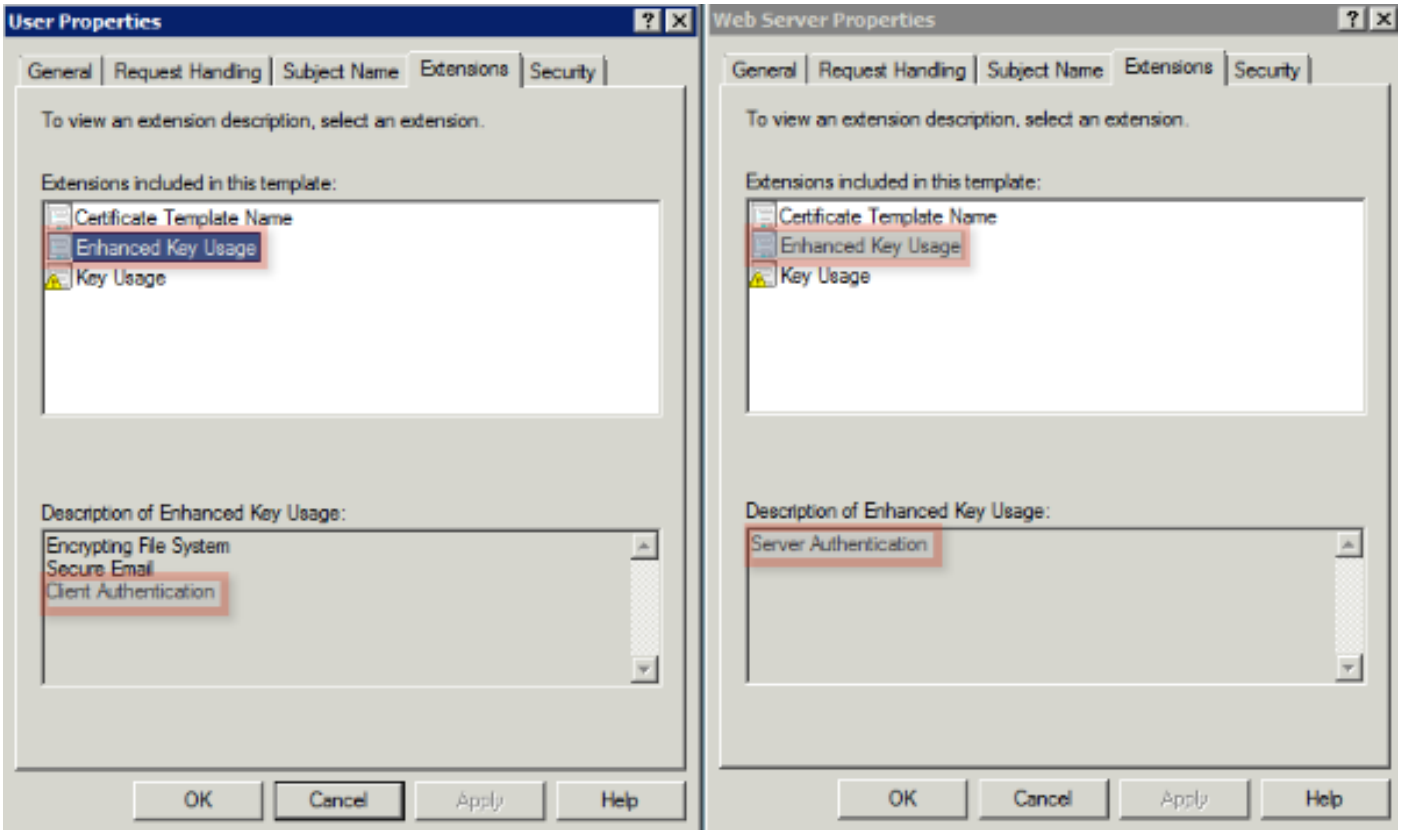
Los administradores de Microsoft CA pueden configurar una o más plantillas que se utilicen para aplicar las directivas de la aplicación a un conjunto común de Certificados. Estas directivas ayudan a identificar para qué función se utilizan el certificado y las claves asociadas. Los valores de directiva de la aplicación se contienen en el campo dominante extendido del uso (EKU) del certificado. El authenticator analiza los valores en el campo del EKU para asegurarse de que el certificado presentado por el cliente se puede utilizar para la función prevista. Algunas de las aplicaciones mas comunes incluyen la autenticación de servidor, la autenticación de cliente, el IPSec VPN, y el correo electrónico. En términos de ISE, los valores generalmente usados del

EKU incluyen el servidor y/o la autenticación de cliente.

Cuando usted hojea a un sitio web seguro del banco, por ejemplo, configuran al servidor Web que procesa la petición con un certificado que tenga una directiva de la aplicación de la autenticación de servidor. Cuando el servidor recibe una petición HTTPS, envía un Certificado de autenticación de servidor al buscador Web de conexión para la autenticación. El punto importante aquí es que esto es un intercambio unidireccional del servidor al cliente. Pues se relaciona con el ISE, un de uso común para un Certificado de autenticación de servidor es acceso a GUI admin. El ISE envía el certificado configurado al navegador conectado y no lo espera recibir un certificado detrás del cliente.

Cuando se trata de los servicios tales como BYOD que utilicen el EAP-TLS, se prefiere la autenticación recíproca. Para habilitar este intercambio bidireccional del certificado, la plantilla usada para generar el certificado de identidad ISE debe poseer una directiva mínima de la aplicación de la autenticación de servidor. El Certificate Template plantilla de certificado del servidor Web satisface este requisito. El Certificate Template plantilla de certificado que genera los Certificados del punto final debe contener una directiva mínima de la aplicación de la autenticación de cliente. La plantilla del Certificado de usuario satisface este requisito. Si usted configura el ISE para los servicios tales como punta en línea de la aplicación de políticas (iPEP), la plantilla usada para generar el certificado de identidad del servidor ISE debe contener ambos atributos de la autenticación de cliente y servidor si usted utiliza la versión 1.1.x o anterior ISE. Esto permite que el admin y los Nodos en línea se autentiquen mutuamente. La validación del EKU para el iPEP fue quitada en la versión 1.2 ISE, que hace este requisito menos relevante.

Usted puede reutilizar el servidor Web y las plantillas del usuario predeterminados de Microsoft CA, o usted puede reproducir y crear una nueva plantilla con el proceso que se delinea en este documento. Basado sobre estos requisitos del certificado, la configuración de CA y el ISE resultante y los Certificados del punto final se deben planear cuidadosamente para minimizar cualquier cambio de configuración no deseada cuando está instalada en un entorno de producción.



Configuración del Certificate Template plantilla de certificado

Como se apunta en la introducción, el SCEP es ampliamente utilizado en los entornos del IPSec VPN. Como consecuencia, la instalación del papel NDE configura automáticamente el servidor para utilizar la plantilla del **IPSec (petición offline)** para el SCEP. Debido a esto, uno de los primeros pasos en la preparación de Microsoft CA para BYOD es construir una nueva plantilla con la directiva correcta de la aplicación. En un despliegue independiente, colocan a las autoridades de certificación y a los servicios NDE en el mismo servidor, y las plantillas y las modificaciones requeridas del registro se contienen al mismo servidor. En un despliegue distribuido NDE, las modificaciones del registro se hacen en el servidor NDE; sin embargo, las plantillas reales se definen en el servidor de CA de la raíz o de la sub-raíz especificadas en la instalación del servicio NDE.

Complete estos pasos para configurar el Certificate Template plantilla de certificado:

1. Abra una sesión al servidor de CA como **admin**.

2. Haga clic el **Start (Inicio) > Administrative Tools (Herramientas administrativas) >** las **autoridades de certificación**.

3. Amplíe los detalles del servidor de CA y seleccione la carpeta de los **Certificate Template plantilla de certificado**. Esta carpeta contiene una lista de las plantillas que se habilitan actualmente.

4. Para manejar los Certificate Template plantilla de certificado, el click derecho en la carpeta de los **Certificate Template plantilla de certificado** y elegir **maneja**.

5. En la **consola de los Certificate Template plantilla de certificado**, se visualizan varias plantillas inactivas.

6. Para configurar una nueva plantilla para el uso con el SCEP, click derecho en una plantilla que existe ya, por ejemplo el **usuario**, y elige la **plantilla duplicado**.

7. Elija **Windows 2003** o **Windows 2008**, dependiente sobre CA mínimo OS en el entorno.

8. En la **ficha general**, agregue un nombre de la visualización, tal como ISE-BYOD, y el período de validez; deje todas las otras opciones desmarcadas.
   Nota: El período de validez de la plantilla debe ser inferior o igual el período de validez de los Certificados de la raíz y del intermedio de CA.
9. Haga clic en la lengueta del **asunto**, y confirme que la **fuente en la petición** está seleccionada.

10. Haga clic en los **requisitos de la emisión que** cuadro Cisco recomienda que usted deja el espacio en blanco de las **directivas de la emisión** en un entorno jerárquico típico CA.

11. Haga clic en la lengueta de las **Extensiones**, las **directivas de la aplicación**, y después **editela**.

12. El tecleo **agrega**, y se asegura de que la **autenticación de cliente** está agregada como

directiva de la aplicación. Haga clic en OK.

13. Haga clic en la **ficha de seguridad**, y después **agregue….** Asegúrese de que la Cuenta de servicio SCEP definida en la instalación del servicio NDE tenga control total de la plantilla, y después haga clic la **AUTORIZACIÓN**.

14. Vuelva a la **interfaz GUI de las autoridades de certificación**.

15. Haga clic con el botón derecho del ratón en el directorio de los **Certificate Template plantilla de certificado**. Navegue a **nuevo > Certificate Template plantilla de certificado a publicar**.

16. Seleccione la plantilla **ISE-BYOD** configurada previamente, y haga clic la **AUTORIZACIÓN**.

    Nota: Alternativamente, usted puede habilitar la plantilla vía el CLI con el **certutil -** comando de **SetCAtemplates +ISE-BYOD**.
    La plantilla ISE-BYOD se debe ahora enumerar en la lista habilitada del Certificate Template plantilla de certificado.

Configuración del registro del Certificate Template plantilla de certificado

Complete estos pasos para configurar las claves de registro del Certificate Template plantilla de certificado:

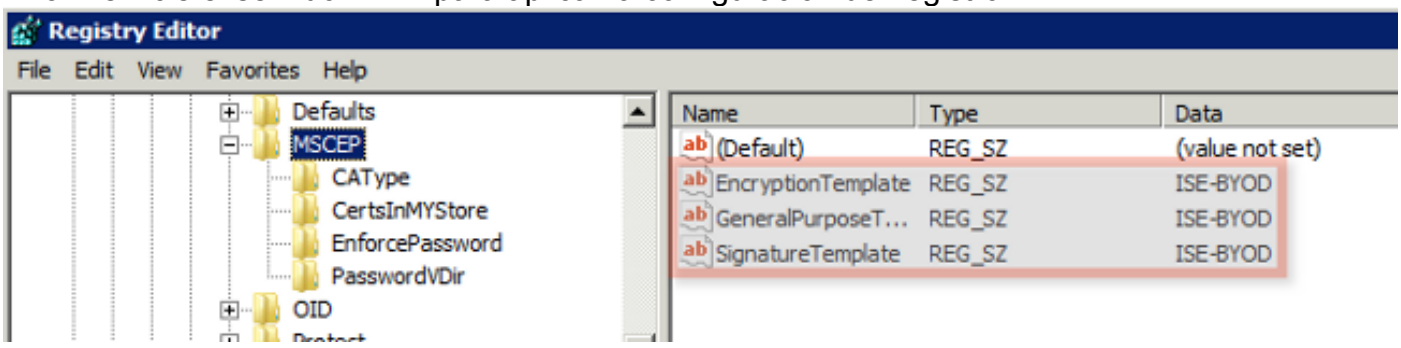
1. Conecte con los NDE el servidor.

2. Haga clic el **comienzo** y ingrese el **regedit** en la barra de la búsqueda.

3. Navegue a la **Computadora** > al **HKEY_LOCAL_MACHINE** > al **SOFTWARE** > a **Microsoft** > a la **criptografía** > a **MSCEP**.

4. Cambie las claves de **EncryptionTemplate**, de **GeneralPurposeTemplate**, y de **SignatureTemplate del IPSec (petición offline) a la** plantilla **ISE-BYOD** creada previamente.

5. Reinicie el servidor NDE para aplicar la configuración del registro.



Configure el ISE como proxy SCEP

En un despliegue BYOD, el punto final no comunica directamente con el servidor backend NDE. En lugar, el nodo de la directiva ISE se configura como proxy SCEP y comunica con el servidor NDE en nombre de los puntos finales. Los puntos finales comunican directamente con el ISE. El

caso IIS en el servidor NDE se puede configurar para soportar los atascamientos HTTP y/o HTTPS para los directorios virtuales SCEP.

Complete estos pasos para configurar el ISE como proxy SCEP:

1. Registro en el **ISE GUI** con las credenciales admin.
2. **La administración del** tecleo, **Certificados**, y entonces **perfiles SCEP CA**.
3. Haga clic en Add (Agregar).
4. Ingrese Nombre del servidor y la descripción.
5. Ingrese el URL para el servidor SCEP con el IP o el Nombre de dominio totalmente calificado (FQDN) (FQDN) (http://10.10.10.10/certsrv/mscep/, por ejemplo).
6. Haga clic la **Conectividad de la prueba**. Una conexión satisfactoria da lugar a un mensaje móvil de la respuesta del servidor acertada.
7. **Salvaguardia del** tecleo para aplicar la configuración.
8. Para verificar, hacer clic la **administración**, **Certificados**, **almacén de certificados,** y confirmar que el certificado del servidor RA SCEP NDE se ha descargado automáticamente al nodo ISE.

Verificación

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

Troubleshooting

Use esta sección para resolver problemas su configuración.

Notas generales del Troubleshooting

Aquí está una lista de NOTAS IMPORTANTES que usted pueda utilizar para resolver problemas su configuración:

- Analice la topología de red BYOD en los puntos de referencia lógicos para ayudar a identificar el debug y a capturar las puntas a lo largo de la trayectoria entre los puntos finales ISE, NDE, y de CA.
- Asegúrese que eso el nodo y CA ISE compartan una fuente horaria común del Network Time Protocol (NTP).
- Los puntos finales deben poder fijar su hora automáticamente con las opciones NTP y del huso horario aprendidas del DHCP.

- El servidor DNS del cliente debe poder resolver el FQDN del nodo ISE.
- Asegúrese de que el TCP 80 y/o el TCP 443 estén permitidos bidireccional entre el ISE y el servidor NDE.
- Pruebe con una máquina de Windows debido al registro mejorado del client cara. Opcionalmente, utilice un iDevice de Apple junto con la utilidad de configuración del iPhone de Apple para monitorear los registros de la consola del client cara.
- Monitoree los registros de la aplicación del servidor de CA y NDE para los errores de inscripción, y utilice Google o TechNet para investigar esos errores.
- En la fase de prueba, utilice el HTTP para el SCEP para facilitar a las capturas de paquetes entre el ISE, los NDE, y CA.
- Utilice la utilidad del volcado TCP en el nodo del servicio de la directiva ISE (PSN), y monitoree el tráfico a y desde el servidor NDE. Esto está situada bajo las **operaciones** > las **herramientas de diagnóstico** > las **herramientas generales**.
- Instale Wireshark en el servidor de CA y NDE, o el SPAN del uso en el Switches del intermediario, para capturar el tráfico SCEP a y desde el ISE PSN.
- Asegúrese de que el encadenamiento apropiado del certificado de CA esté instalado en el nodo de la directiva ISE para la autenticación de los certificados del cliente.
- Asegúrese de que el encadenamiento apropiado del certificado de CA esté instalado automáticamente sobre los clientes durante onboarding.
- Vea los certificados de identidad ISE de antemano y del punto final y confirme que los atributos correctos del EKU están presentes.
- Monitoree la autenticación viva abre una sesión el ISE GUI para los errores de la autenticación y autorización.
  Nota: Algunos suplicantes no inicializan un intercambio del certificado del cliente si el EKU incorrecto está presente, por ejemplo un certificado del cliente con el EKU de la autenticación de servidor. Por lo tanto, las fallas de autenticación no pudieron siempre estar presentes en los registros ISE.
- Cuando los NDE están instalados en un despliegue distribuido, una raíz o una sub-raíz remota CA será señalada por el nombre o el nombre de computadora de CA en la instalación del servicio. El servidor NDE envía los pedidos de inscripción del certificado a este servidor de CA de la blanco. Si el proceso de inscripción del certificado del punto final falla, las capturas de paquetes (PCAP) pudieron mostrar a la vuelta del servidor NDE un error **no encontrado 404 al** nodo ISE. Para resolver este problema, reinstale el servicio NDE y seleccione la opción del nombre de computadora en vez del nombre de CA.
- Evite las alteraciones al encadenamiento SCEP CA después de que los dispositivos onboarded. El punto final OS, tales como IOS de Apple, no pone al día automáticamente un

perfil previamente instalado BYOD. En este ejemplo IOS, el perfil actual se debe borrar del punto final, y del punto final quitado de la base de datos ISE, para poder realizarse onboarding otra vez.

- Usted puede configurar un Microsoft certificate server para conectar con Internet y poner al día automáticamente los Certificados del programa del certificado raíz de Microsoft. Si usted configura esta opción de la extracción de la red en los entornos con las políticas de Internet restrictas, los servidores CA/NDES que no pueden conectar con Internet pueden llevar 15 segundos el descanso por abandono. Esto puede agregar un retardo 15-second al proceso de las peticiones SCEP de los proxys SCEP tales como ISE. El ISE es para peticiones programadas del descanso SCEP después de 12 segundos si una respuesta no se recibe. Para resolver este problema, permite el acceso a internet para los servidores CA/NDES, o modifica las configuraciones de tiempo de espera de la extracción de la red en Local Security (Seguridad local) la directiva de los servidores de Microsoft CA/NDES. Para localizar esta configuración en el servidor de Microsoft, navegue al **Start (Inicio) > Administrative Tools (Herramientas administrativas) > Local Security (Seguridad local) las directivas de la directiva > de la clave pública > las configuraciones de la validación de trayecto del certificado > extracción de la red**.

Registro del client cara

Aquí está una lista de técnicas útiles que se utilicen para resolver problemas los problemas del registro del client cara:

- Ingrese el **comando del registro el %temp% \ spwProfileLog.txt** para ver los registros del client cara para las aplicaciones de Windows de Mircosoft.
  Nota: WinHTTP se utiliza para la conexión entre el punto final de Microsoft Windows y el ISE. Refiérase al artículo de los mensajes de error de Microsoft Windows para una lista de códigos de error.
- Ingrese el comando de **/sdcards/downloads/spw.log** para ver los registros del client cara para las aplicaciones androides.

- Para el **MAC OSX**, utilice la aplicación de consola, y busque el proceso **SPW**.

- Para el **IOS de Apple**, utilice el configurador 2.0 de Apple para ver los mensajes.

Registro ISE

Complete estos pasos para ver el registro ISE:

1. Navegue a la **administración** > a la **configuración del registro del registro** > del **debug**, y seleccione el nodo apropiado de la directiva ISE.

2. Fije el **cliente** y los registros del **aprovisionamiento** para hacer el debug de o para localizar, como sea necesario.

3. Reproduzca el problema y documente la información relevante del germen para facilitar el buscar, por ejemplo el MAC, el IP, y el usuario.

4. Navegue a las **operaciones** > a los **registros de la descarga**, y seleccione el nodo apropiado ISE.

5. En los **registros del debug** tabule, descargue los registros nombrados **ise-psc.log al** escritorio.

6. Utilice un editor inteligente, tal como libreta ++ para analizar los archivos del registro.

7. Cuando se ha aislado el problema, después vuelva los niveles del registro al nivel predeterminado.

NDE que registran y que resuelven problemas

Para más información, refiera al AD CS: Resolver problemas el artículo del Servidor Windows del servicio de la inscripción del dispositivo de red.

Información Relacionada

- Guía de las soluciones BYOD - Configuración del servidor del Certificate Authority
- Descripción NDE en el r2 de Windows 2008
- White Paper MSCEP
- Configurar el servidor NDE para soportar el SSL
- Requisitos del certificado cuando usted utiliza el EAP-TLS o el PEAP con el EAP-TLS
- Soporte técnico y documentación