Configurazione del supporto ISE SCEP per BYOD

Sommario

Introduzione

In questo documento viene descritto come configurare correttamente il servizio Registrazione dispositivi di rete Microsoft (NDES) e il protocollo SCEP (Simple Certificate Enrollment Protocol) per portare il proprio dispositivo (BYOD) su Cisco Identify Services Engine (ISE).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- ISE release 1.1.1 o successive
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012 Standard
- Infrastruttura a chiave pubblica (PKI) e certificati

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- ISE release 1.1.1 o successive
- Windows Server 2008 R2 SP1 con gli aggiornamenti rapidi KB2483564 e KB2633200 installati
- Windows Server 2012 Standard

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Le informazioni relative ai servizi certificati Microsoft sono fornite come guida specifica per Cisco BYOD. Fare riferimento a Microsoft TechNet come fonte definitiva di informazioni per le configurazioni server relative a Microsoft Certification Authority, Network Device Enrollment Service (NDES) e SCEP.

Premesse

Uno dei vantaggi dell'implementazione di BYOD abilitata per Cisco ISE è la capacità degli utenti finali di eseguire la registrazione self-service dei dispositivi. In questo modo viene eliminato il carico amministrativo che grava sul reparto IT per distribuire le credenziali di autenticazione e abilitare i dispositivi sulla rete. Il cuore della soluzione BYOD è il processo di provisioning dei supplicant di rete, che tenta di distribuire i certificati richiesti ai dispositivi di proprietà dei dipendenti. Per soddisfare questo requisito, è possibile configurare un'Autorità di certificazione (CA) Microsoft per automatizzare il processo di registrazione dei certificati con SCEP.

SCEP viene utilizzato da anni in ambienti VPN (Virtual Private Network) per facilitare la registrazione e la distribuzione dei certificati ai client e ai router di accesso remoto. L'attivazione della funzionalità SCEP su un server Windows 2008 R2 richiede l'installazione di NDES. Durante l'installazione del ruolo NDES viene installato anche il server Web Microsoft Internet Information Services (IIS). IIS viene utilizzato per terminare le richieste di registrazione SCEP HTTP o HTTPS e le risposte tra il nodo dei criteri CA e ISE.

Il ruolo NDES può essere installato in una CA corrente oppure in un server membro. In una distribuzione autonoma, il servizio NDES viene installato in una CA esistente che include il servizio Autorità di certificazione e, facoltativamente, il servizio Registrazione Web Autorità di certificazione. In una distribuzione distribuita, il servizio NDES viene installato in un server membro. Il server NDES distribuito viene quindi configurato per comunicare con una CA radice o una CA radice secondaria upstream. In questo scenario, le modifiche del Registro di sistema descritte in questo documento vengono apportate sul server NDES con il modello personalizzato, in cui i certificati risiedono nella CA a monte.

Scenari di distribuzione CA/NDES testati

In questa sezione viene fornita una breve panoramica degli scenari di installazione di CA/NDES che sono stati testati nel laboratorio Cisco. Fare riferimento a Microsoft TechNet come fonte definitiva di informazioni per le configurazioni server relative a Microsoft CA, NDES e SCEP.

Distribuzioni autonome

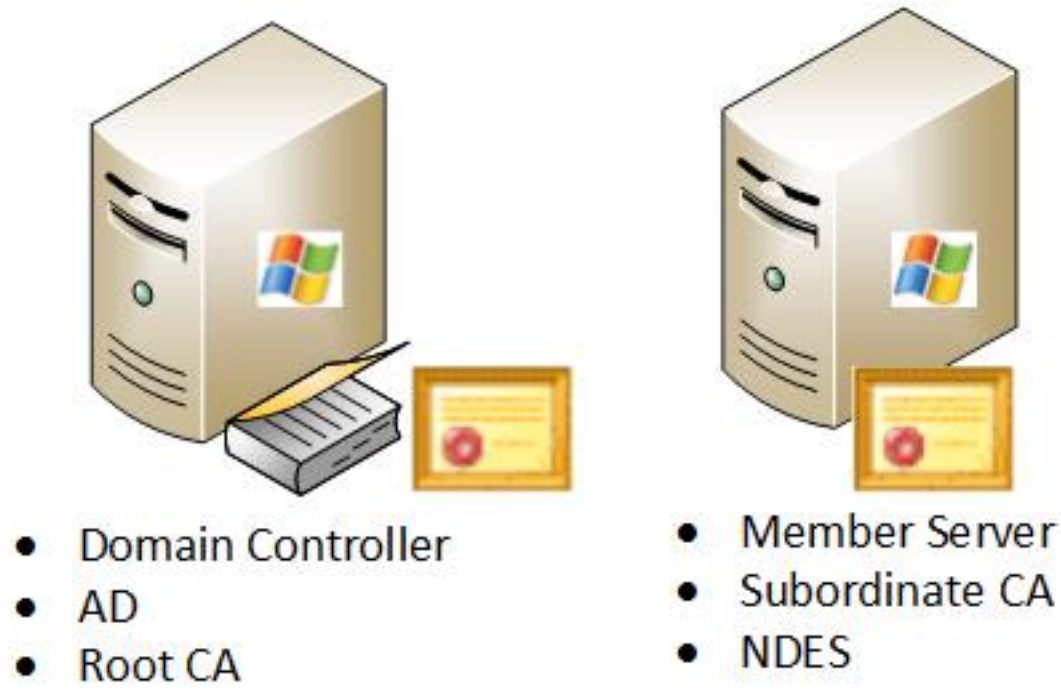
Quando ISE viene utilizzato in uno scenario Proof of Concept (PoC), è comune distribuire un computer Windows 2008 o 2012 autonomo che funge da controller di dominio Active Directory (AD), CA radice e server NDES:

- Domain Controller
- AD
- Root CA
- NDES

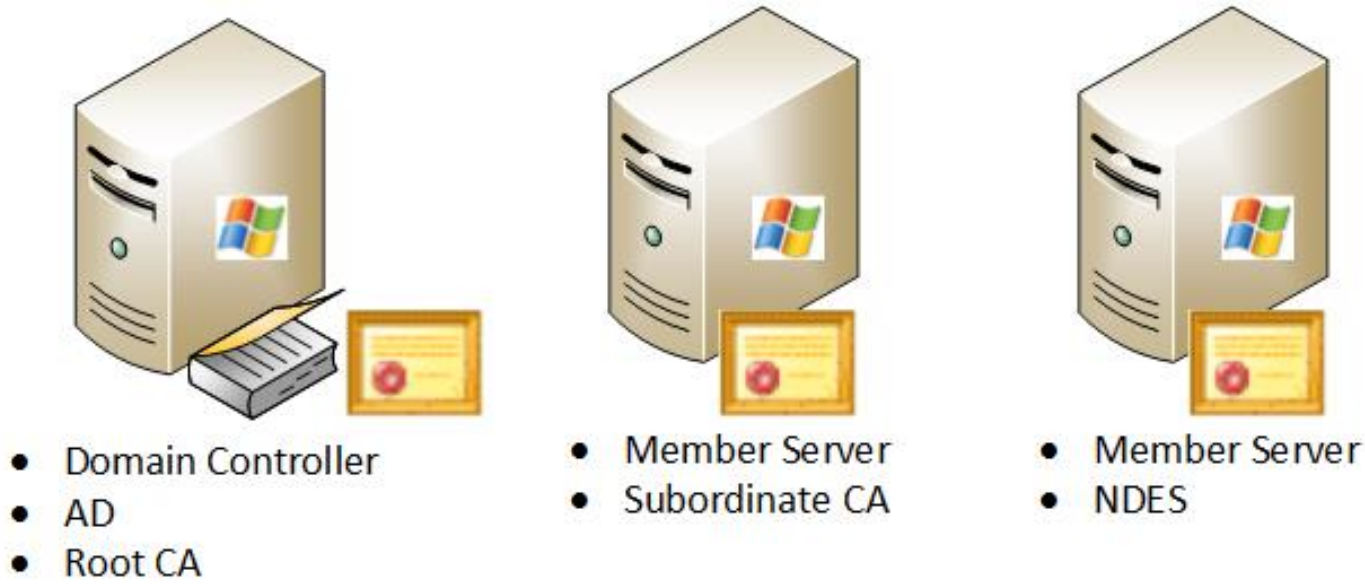
Distribuzioni distribuite

Quando l'ISE è integrato in un ambiente di produzione Microsoft AD/PKI corrente, è più comune vedere i servizi distribuiti su più server distinti Windows 2008 o 2012. Cisco ha testato due scenari per le distribuzioni.

In questa immagine viene illustrato il primo scenario testato per le distribuzioni distribuite:



In questa immagine viene illustrato il secondo scenario testato per le distribuzioni distribuite:



Aggiornamenti rapidi importanti Microsoft

Prima di configurare il supporto SCEP per BYOD, verificare che nel server Windows 2008 R2 NDES siano installati i seguenti aggiornamenti rapidi Microsoft:

- La richiesta di rinnovo di un certificato SCEP non riesce in Windows Server 2008 R2 se il certificato è gestito tramite NDES - Questo problema si verifica perché NDES non supporta l'operazione **GetCACaps**.

- NDES non invia richieste di certificati dopo il riavvio dell'autorità di certificazione dell'organizzazione (enterprise) in Windows Server 2008 R2 - Questo messaggio viene visualizzato nel **Visualizzatore eventi**: "*Servizio Registrazione dispositivi di rete: impossibile inviare la richiesta di certificato (0x800706ba). Il server RPC non è disponibile*."

Avviso: Quando si configura la CA Microsoft, è importante notare che l'ISE non supporta l'algoritmo di firma RSASSA-PSS. Cisco consiglia di configurare il criterio CA in modo che utilizzi sha1WithRSAEncryption o sha256WithRSAEncryption.

Porte e protocolli BYOD importanti

Di seguito è riportato un elenco di importanti porte e protocolli BYOD:

- TCP: Provisioning 8909: Installazione guidata da Cisco ISE (sistemi operativi Windows e Macintosh)
- TCP: 443 Provisioning: Installazione guidata da Google Play (Android)
- TCP: 8905 Provisioning: Processo di provisioning del richiedente
- TCP: 80 o TCP: 443 SCEP Proxy per CA (in base alla configurazione dell'URL SCEP RA)

Nota: Per l'elenco più recente delle porte e dei protocolli richiesti, fare riferimento alla Guida all'installazione dell'hardware ISE 1.2.

Configurazione

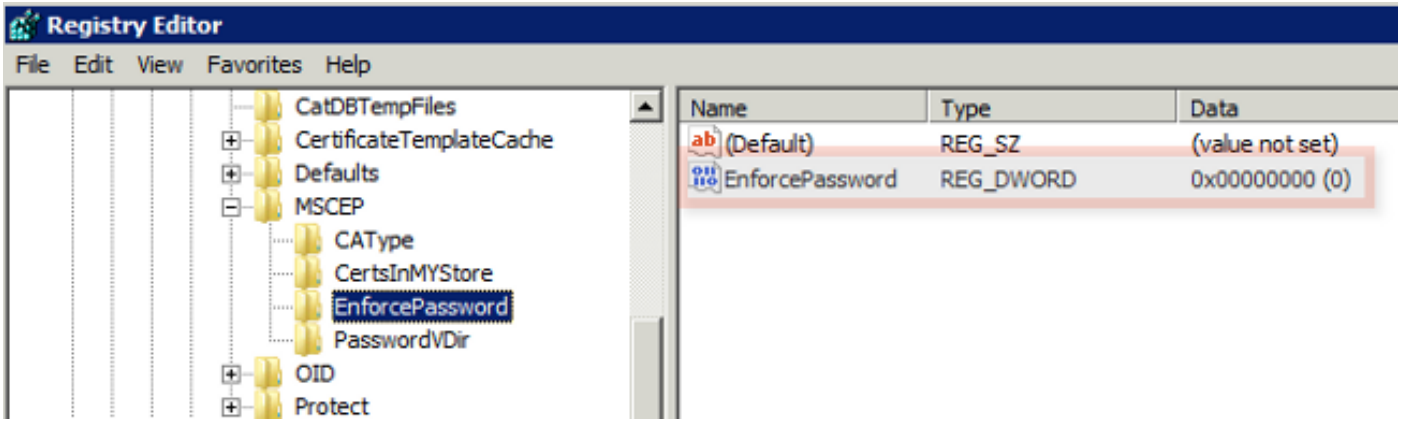
Utilizzare questa sezione per configurare il supporto NDES e SCEP per BYOD sull'ISE.

Disabilita requisito password di verifica registrazione SCEP

Per impostazione predefinita, nell'implementazione di Microsoft SCEP (MSCEP) viene utilizzata una password di verifica dinamica per autenticare i client e gli endpoint durante l'intero processo di registrazione dei certificati. Con questo requisito di configurazione, è necessario passare alla GUI Web di amministrazione di MSCEP sul server NDES per generare una password su richiesta. È necessario includere questa password nella richiesta di registrazione.

In un'implementazione BYOD, il requisito di una password di verifica vanifica lo scopo di una soluzione self-service per gli utenti. Per rimuovere questo requisito, è necessario modificare la chiave del Registro di sistema nel server NDES:

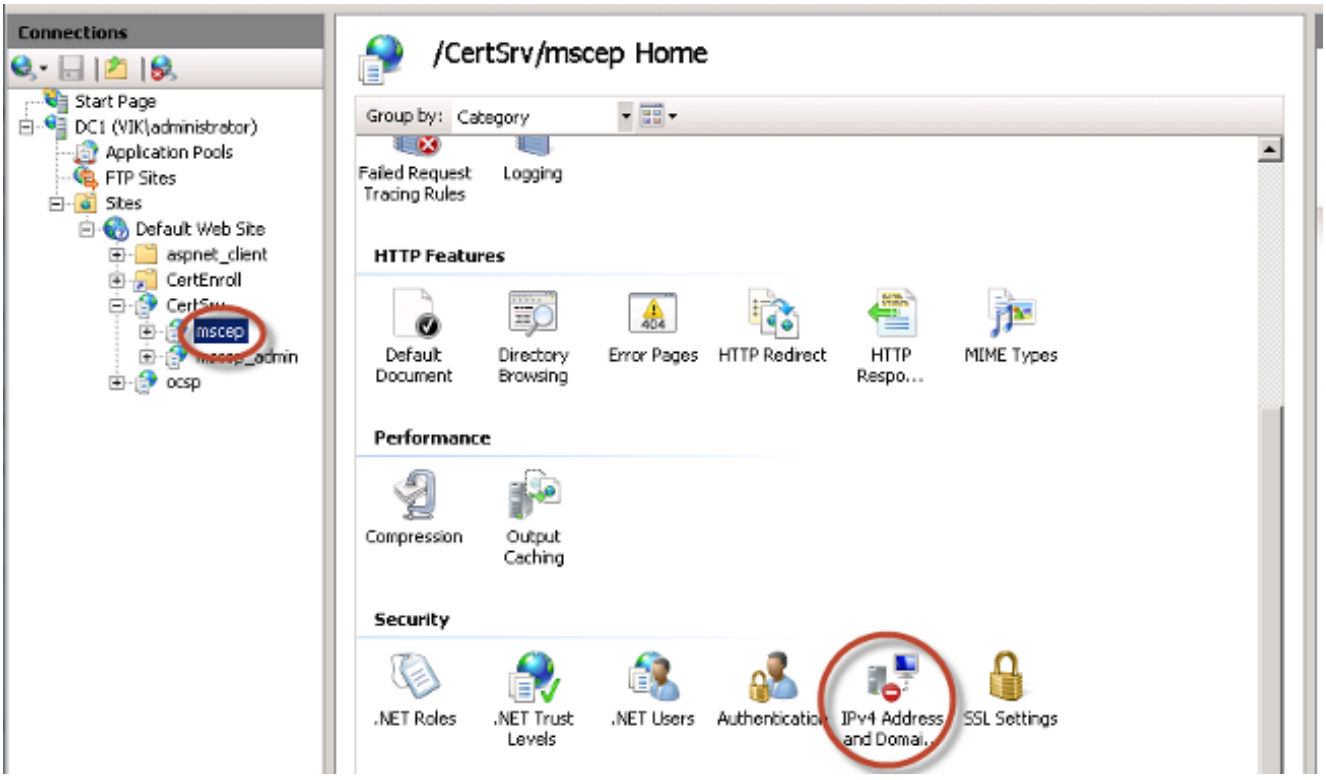
1. Fare clic su **Start** e immettere **regedit** nella barra di ricerca.
2. Selezionare Computer > HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > Crittografia > **MSCEP** > **EnforcePassword**.
3. Verificare che il valore **EnforcePassword** sia impostato su **0** (il valore predefinito è **1**).



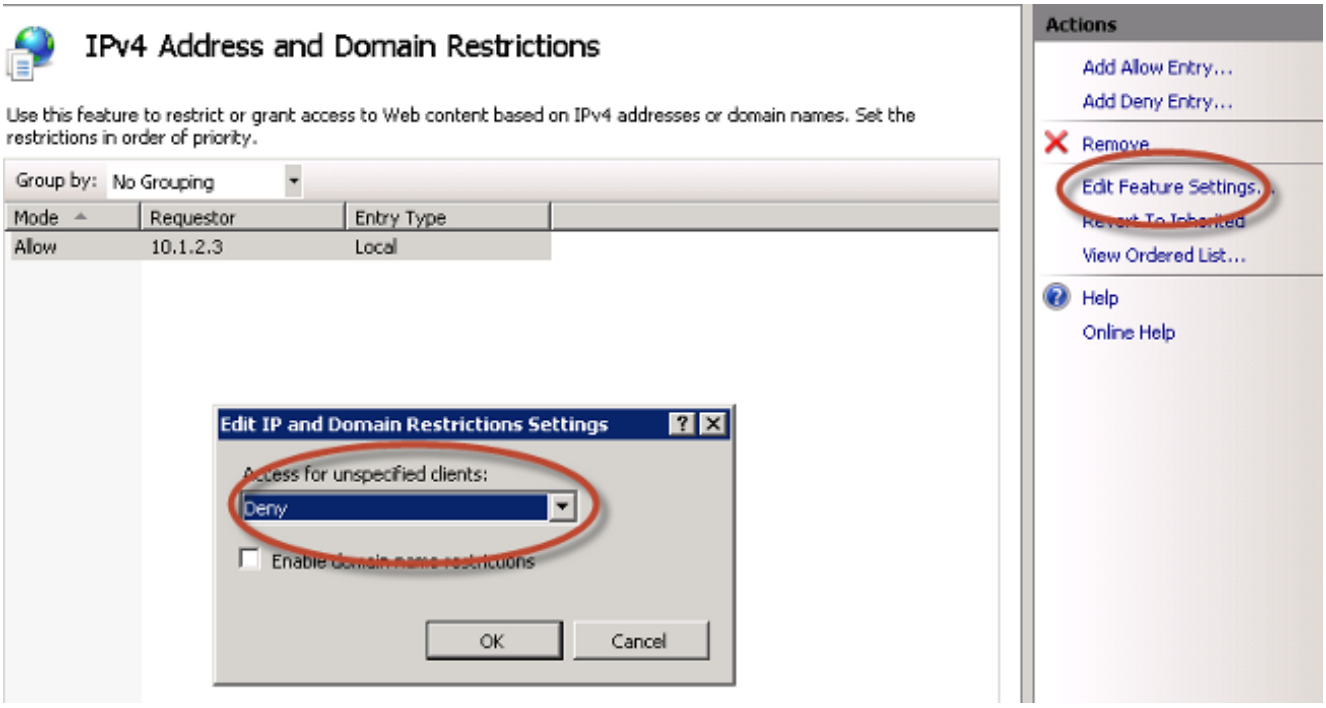
Limitazione della registrazione SCEP ai nodi ISE noti

In alcuni scenari di distribuzione, potrebbe essere preferibile limitare le comunicazioni SCEP a un elenco selezionato di nodi ISE noti. A tale scopo, è possibile utilizzare la funzionalità Restrizioni indirizzo IPv4 e dominio in IIS:

1. Aprire IIS e accedere al sito Web **/CertSrv/mscep**.



2. Fare doppio clic su **Protezione > Restrizioni indirizzo IPv4 e dominio.** Utilizzare le azioni **Aggiungi voce consentita** e **Aggiungi voce negata** per autorizzare o limitare l'accesso al contenuto Web basato su indirizzi IPv4 o nomi di dominio del nodo ISE. Utilizzare l'azione **Modifica impostazioni funzionalità** per definire una regola di accesso predefinita per i client non specificati.

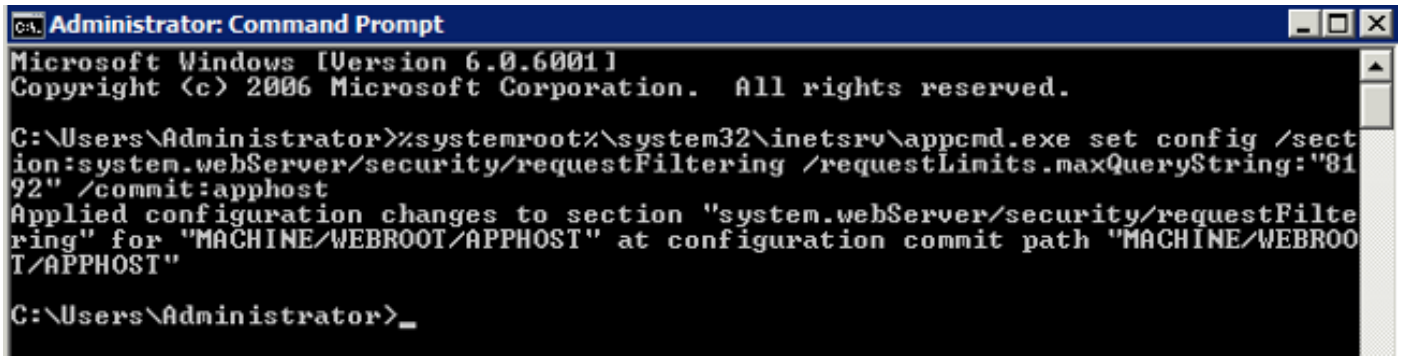


Estendi lunghezza URL in IIS

Èpossibile che ISE generi URL troppo lunghi per il server Web IIS. Per evitare questo problema, è possibile modificare la configurazione IIS predefinita in modo da consentire URL più lunghi. Immettere questo comando dalla CLI del server NDES:

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

> **Nota:** Le dimensioni della stringa di query potrebbero variare a seconda della configurazione di ISE e dell'endpoint. Immettere questo comando dalla CLI del server NDES con privilegi amministrativi.



Panoramica sui modelli di certificato

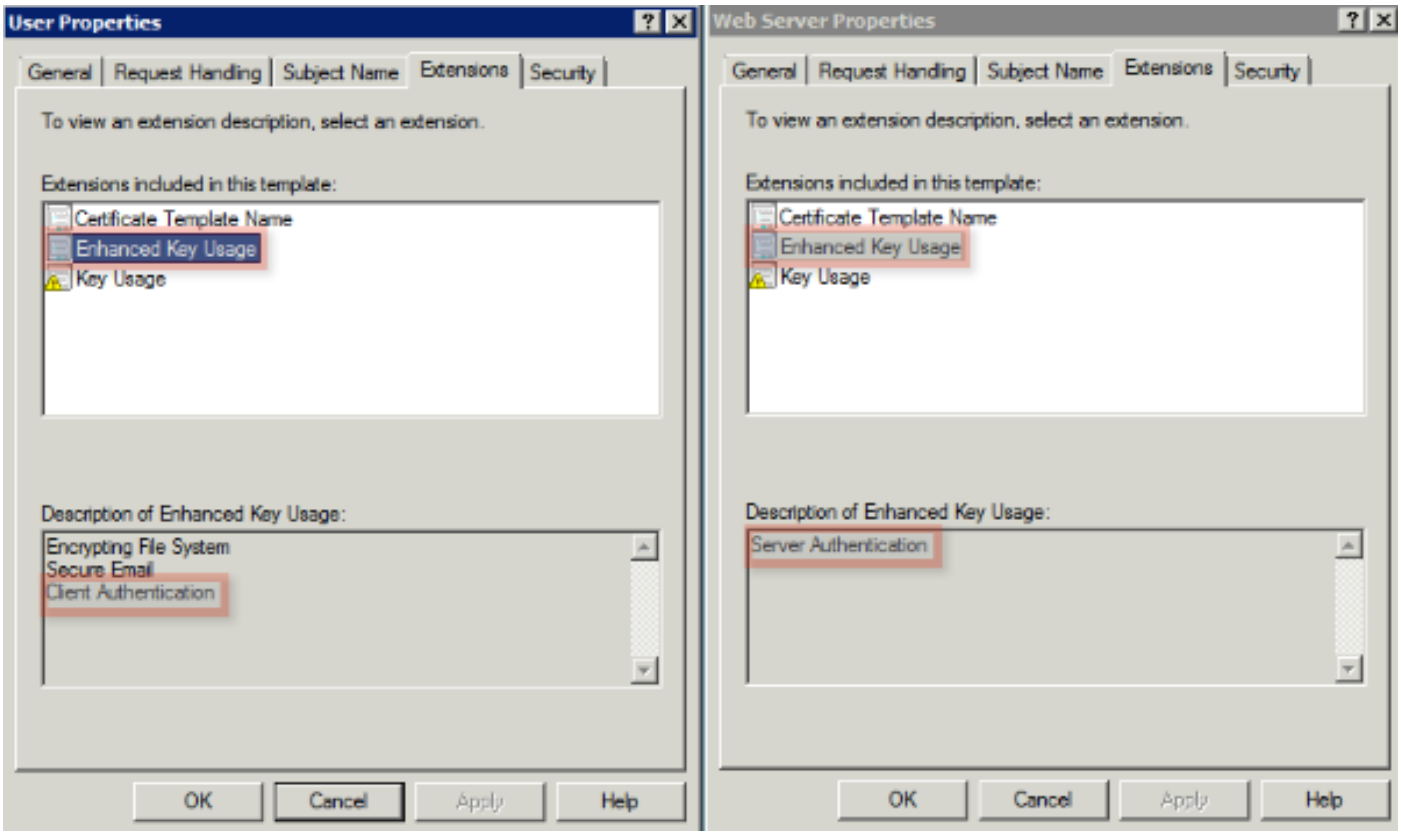
Gli amministratori di una CA Microsoft possono configurare uno o più modelli utilizzati per applicare i criteri dell'applicazione a un insieme comune di certificati. Questi criteri consentono di identificare la funzione per cui vengono utilizzati il certificato e le chiavi associate. I valori dei criteri di applicazione sono contenuti nel campo Utilizzo chiave esteso (EKU) del certificato. L'autenticatore analizza i valori nel campo EKU per garantire che il certificato presentato dal client possa essere utilizzato per la funzione desiderata. Alcuni degli utilizzi più comuni includono l'autenticazione server, l'autenticazione client, la VPN IPSec e la posta elettronica. In termini di

ISE, i valori dell'EKU più comunemente usati includono l'autenticazione del server e/o del client.

Quando si accede a un sito Web di una banca protetta, ad esempio, il server Web che elabora la richiesta viene configurato con un certificato con un criterio di applicazione di autenticazione server. Quando il server riceve una richiesta HTTPS, invia un certificato di autenticazione server al browser Web che si connette per l'autenticazione. Il punto importante è che si tratta di uno scambio unidirezionale dal server al client. In relazione all'ISE, un utilizzo comune per un certificato di autenticazione server è l'accesso tramite interfaccia grafica di amministrazione. ISE invia il certificato configurato al browser connesso e non si aspetta di ricevere un certificato dal client.

Quando si tratta di servizi come BYOD che utilizzano EAP-TLS, è preferibile l'autenticazione reciproca. Per abilitare lo scambio bidirezionale dei certificati, il modello utilizzato per generare il certificato di identità ISE deve disporre di una policy minima per l'applicazione dell'autenticazione server. Il modello di certificato del server Web soddisfa questo requisito. Il modello di certificato che genera i certificati degli endpoint deve contenere un criterio minimo di applicazione per l'autenticazione client. Il modello di certificato utente soddisfa questo requisito. Se si configura ISE per servizi come Inline Policy Enforcement Point (iPEP), il modello utilizzato per generare il certificato di identità del server ISE deve contenere entrambi gli attributi di autenticazione client e server se si utilizza ISE versione 1.1.x o precedenti. In questo modo, i nodi admin e inline possono autenticarsi reciprocamente. La convalida EKU per iPEP è stata rimossa in ISE versione 1.2, il che rende questo requisito meno rilevante.

Èpossibile riutilizzare i modelli predefiniti del server Web e dell'utente di Microsoft CA oppure duplicare e creare un nuovo modello con il processo descritto in questo documento. In base a questi requisiti, la configurazione della CA e i certificati ISE ed endpoint risultanti devono essere pianificati con attenzione per ridurre al minimo le modifiche indesiderate alla configurazione quando vengono installati in un ambiente di produzione.



Configurazione modello di certificato

Come indicato nell'introduzione, SCEP è ampiamente utilizzato in ambienti VPN IPSec. Di conseguenza, l'installazione del ruolo NDES configura automaticamente il server in modo che utilizzi il modello **IPSec (Offline Request)** per SCEP. Per questo motivo, uno dei primi passaggi nella preparazione di una CA Microsoft per BYOD consiste nella creazione di un nuovo modello con i criteri di applicazione corretti. In una distribuzione autonoma, i servizi Autorità di certificazione e NDES sono collocati nello stesso server e i modelli e le modifiche del Registro di sistema necessarie sono contenuti nello stesso server. In una distribuzione NDES distribuita, le modifiche del Registro di sistema vengono apportate sul server NDES; tuttavia, i modelli effettivi vengono definiti nel server CA radice o subradice specificato nell'installazione del servizio NDES.

Per configurare il modello di certificato, completare la procedura seguente:

1. Accedere al server CA come **amministratore**.

2. Fare clic su **Start** > **Strumenti di amministrazione** > **Autorità di certificazione**.

3. Espandere i dettagli del server CA e selezionare la cartella **Modelli di certificato**. Questa cartella contiene un elenco dei modelli attualmente abilitati.

4. Per gestire i modelli di certificato, fare clic con il pulsante destro del mouse sulla cartella **Modelli di certificato** e scegliere **Gestisci**.

5. Nella **console Modelli di certificato** vengono visualizzati diversi modelli inattivi.

6. Per configurare un nuovo modello da utilizzare con SCEP, fare clic con il pulsante destro del mouse su un modello esistente, ad esempio **Utente**, quindi scegliere **Duplica modello**.

7. Scegliere **Windows 2003** o **Windows 2008**, a seconda del sistema operativo CA minimo dell'ambiente.

8. Nella scheda **General** (Generale), aggiungere un nome visualizzato, ad esempio ISE-BYOD, e il periodo di validità. lasciare deselezionate tutte le altre opzioni.
   Nota: Il periodo di validità del modello deve essere minore o uguale al periodo di validità dei certificati radice e intermedi della CA.
9. Fare clic sulla scheda **Nome soggetto** e confermare che **Fornitura nella richiesta** è selezionata.

10. Fare clic sulla scheda **Requisiti di rilascio**. Cisco consiglia di lasciare vuoti i **criteri di rilascio** in un ambiente CA gerarchico tipico.

11. Fare clic sulla scheda **Estensioni**, **Criteri di applicazione**, quindi su **Modifica**.

12. Fare clic su **Aggiungi** e verificare che **Autenticazione client** sia stato aggiunto come criterio di applicazione. Fare clic su **OK**.

13. Fare clic sulla scheda **Protezione**, quindi su **Aggiungi...**. Verificare che l'account del servizio SCEP definito nell'installazione del servizio NDES disponga del controllo completo del modello e quindi fare clic su **OK**.

14. Tornare all'interfaccia **GUI Certification Authority**.

15. Fare clic con il pulsante destro del mouse sulla directory **Certificate Templates (Modelli di certificato)**. Passare a **Nuovo > Modello di certificato per emettere**.

16. Selezionare il modello **ISE-BYOD** configurato in precedenza e fare clic su **OK**.

    Nota: In alternativa, è possibile abilitare il modello dalla CLI con il comando **certutil -SetCAtemplates +ISE-BYOD**.
    Il modello ISE-BYOD dovrebbe ora essere incluso nell'elenco dei modelli di certificato abilitati.

Configurazione Registro di sistema modello di certificato

Completare questa procedura per configurare le chiavi del Registro di sistema per i modelli di certificato:

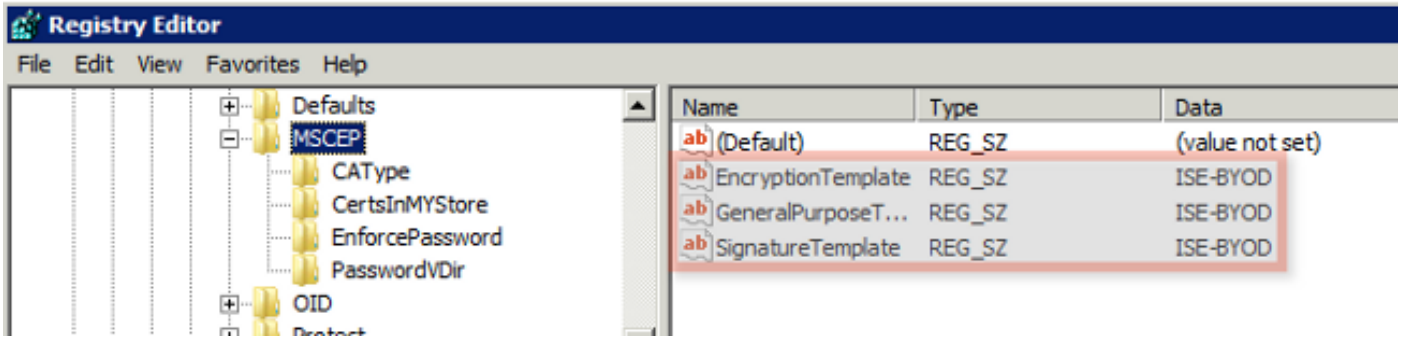
1. Connettersi al server NDES.

2. Fare clic su **Start** e immettere **regedit** nella barra di ricerca.

3. Selezionare Computer > HKEY_LOCAL_MACHINE > SOFTWARE > **Microsoft** > **Crittografia** > **MSCEP**.

4. Modificare le chiavi EncryptionTemplate, **GeneralPurposeTemplate** e **SignatureTemplate** da **IPSec (Offline Request)** al **modello ISE-BYOD** creato in precedenza.

5. Riavviare il server NDES per applicare l'impostazione del Registro di sistema.



Configurazione di ISE come proxy SCEP

In una distribuzione BYOD, l'endpoint non comunica direttamente con il server NDES back-end. Al contrario, il nodo dei criteri ISE è configurato come proxy SCEP e comunica con il server NDES per conto degli endpoint. Gli endpoint comunicano direttamente con l'ISE. È possibile configurare l'istanza di IIS nel server NDES in modo da supportare i binding HTTP e/o HTTPS per le directory virtuali SCEP.

Completare questa procedura per configurare ISE come proxy SCEP:

1. Accedere alla **GUI** di **ISE** con le credenziali di amministratore.

2. Fare clic su **Amministrazione**, **Certificati** e quindi su **Profili CA SCEP**.

3. Fare clic su **Add**.

4. Immettere il nome e la descrizione del server.

5. Immettere l'URL del server SCEP con il nome di dominio completo (FQDN) o IP (ad esempio http://10.10.10.10/certsrv/mscep/).

6. Fare clic su **Test connettività**. Se la connessione riesce, viene visualizzato un messaggio popup di risposta del server.

7. Per applicare la configurazione, fare clic su **Save** (Salva).

8. Per procedere alla verifica, fare clic su **Amministrazione**, **Certificati**, **Archivio certificati** e verificare che il certificato RA del server SCEP NDES sia stato scaricato automaticamente nel nodo ISE.

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Consultare questa sezione per risolvere i problemi di configurazione.

Note generali sulla risoluzione dei problemi

Di seguito è riportato un elenco di note importanti che è possibile utilizzare per risolvere i problemi relativi alla configurazione:

- Suddividere la topologia di rete BYOD in punti di riferimento logici per identificare i punti di debug e di acquisizione lungo il percorso tra gli endpoint ISE, NDES e CA.
- Verificare che il nodo ISE e l'autorità di certificazione condividano un'origine ora NTP (Network Time Protocol) comune.
- Gli endpoint dovrebbero essere in grado di impostare automaticamente la propria ora con le opzioni NTP e fuso orario apprese da DHCP.
- Il server DNS del client deve essere in grado di risolvere l'FQDN del nodo ISE.
- Verificare che TCP 80 e/o TCP 443 siano consentiti in modo bidirezionale tra ISE e il server NDES.
- Eseguire il test con un computer Windows grazie alla registrazione lato client migliorata. Facoltativamente, utilizzare un iDevice Apple insieme all'utility di configurazione iPhone Apple

per monitorare i log della console lato client.

- Monitorare i registri delle applicazioni server CA e NDES per individuare eventuali errori di registrazione e utilizzare Google o TechNet per ricercarli.

- Durante la fase di test, usare HTTP per SCEP per facilitare l'acquisizione dei pacchetti tra ISE, NDES e CA.

- Usare l'utility TCP Dump sul PSN (Policy Service Node) di ISE e monitorare il traffico da e verso il server NDES. È disponibile in **Operazioni > Strumenti diagnostici > Strumenti generali**.

- Installare Wireshark sul server CA e NDES o utilizzare SPAN sugli switch intermedi per acquisire il traffico SCEP da e verso il numero PSN ISE.

- Verificare che nel nodo dei criteri ISE sia installata la catena di certificati CA appropriata per l'autenticazione dei certificati client.

- Verificare che la catena di certificati CA appropriata sia installata automaticamente sui client durante l'onboarding.

- Visualizzare in anteprima i certificati di identità ISE ed endpoint e verificare che siano presenti gli attributi EKU corretti.

- Monitoraggio dei log di autenticazione attivi nell'interfaccia grafica di ISE per errori di autenticazione e autorizzazione.
  Nota: Alcuni supplicant non inizializzano uno scambio di certificati client se è presente l'EKU errato, ad esempio un certificato client con l'EKU dell'autenticazione server. Pertanto, gli errori di autenticazione potrebbero non essere sempre presenti nei log ISE.
- Quando NDES viene installato in una distribuzione distribuita, nell'installazione del servizio una CA radice remota o una CA radice secondaria viene designata da Nome CA o Nome computer. Il server NDES invia le richieste di registrazione dei certificati a questo server CA di destinazione. Se il processo di registrazione del certificato dell'endpoint ha esito negativo, le acquisizioni dei pacchetti (PCAP) potrebbero indicare che il server NDES ha restituito un errore **404 Not Found** al nodo ISE. Per risolvere il problema, reinstallare il servizio NDES e selezionare l'opzione Nome computer anziché il nome CA.

- Evitare modifiche alla catena di CA SCEP dopo l'onboarding dei dispositivi. I sistemi operativi degli endpoint, ad esempio Apple iOS, non aggiornano automaticamente un profilo BYOD installato in precedenza. Nell'esempio di iOS, il profilo corrente deve essere eliminato dall'endpoint, e l'endpoint rimosso dal database ISE, in modo che sia possibile eseguire di nuovo l'onboarding.

- Èpossibile configurare un server certificati Microsoft per la connessione a Internet e l'aggiornamento automatico dei certificati dal programma Microsoft Root Certificate. Se si configura questa opzione di recupero dalla rete in ambienti con criteri Internet limitati, per impostazione predefinita i server CA/NDES che non possono connettersi a Internet possono impiegare 15 secondi per il timeout. Questo può aggiungere un ritardo di 15 secondi all'elaborazione delle richieste SCEP dai proxy SCEP come ISE. ISE è programmato per

impostare il timeout delle richieste SCEP dopo 12 secondi, in caso non venga ricevuta una risposta. Per risolvere il problema, autorizzare l'accesso a Internet per i server CA/NDES o modificare le impostazioni di timeout per il recupero dalla rete nei criteri di protezione locali dei server CA/NDES Microsoft. Per individuare questa configurazione sul server Microsoft, selezionare **Start > Strumenti di amministrazione > Criteri di protezione locali > Criteri chiave pubblica > Impostazioni di convalida del percorso dei certificati > Recupero dalla rete**.

Registrazione lato client

Di seguito sono elencate alcune tecniche utili utilizzate per risolvere i problemi di registrazione sul lato client:

- Immettere il **registro %temp%\spwProfileLog.txt.** per visualizzare i log sul lato client per le applicazioni Microsoft Windows.
  Nota: WinHTTP viene utilizzato per la connessione tra l'endpoint Microsoft Windows e ISE. Fare riferimento all'articolo Messaggi di errore di Microsoft Windows per un elenco di codici di errore.
- Immettere il comando **/sdcards/downloads/spw.log** per visualizzare i log sul lato client per le applicazioni Android.
- Per **MAC OSX**, utilizzare l'applicazione Console e cercare il processo **SPW**.
- Per **Apple iOS**, usare Apple Configurator 2.0 per visualizzare i messaggi.

Registrazione ISE

Completare questa procedura per visualizzare il log ISE:

1. Passare a **Amministrazione** > **Registrazione** > **Configurazione log di debug** e selezionare il nodo della policy ISE appropriato.
2. Impostare i registri **client** e **provisioning** su debug o trace, come richiesto.
3. Riprodurre il problema e documentare le informazioni di seeding rilevanti per facilitare la ricerca, come MAC, IP e utente.
4. Passare a **Operations** > **Download Logs** (Operazioni > Registri download) e selezionare il nodo ISE appropriato.
5. Nella scheda **Debug log**, scaricare i log denominati **ise-psc.log** sul desktop.
6. Utilizzare un editor intelligente, ad esempio Blocco note ++ per analizzare i file di registro.
7. Dopo aver isolato il problema, ripristinare i livelli di registro predefiniti.

Registrazione NDES e risoluzione dei problemi

Per ulteriori informazioni, fare riferimento a Servizi certificati Active Directory: Risoluzione dei

problemi relativi al servizio Registrazione dispositivi di rete Articolo di Windows Server.

Informazioni correlate

- Guida alle soluzioni BYOD - Configurazione del server Certificate Authority
- Panoramica di NDES in Windows 2008 R2
- White paper MSCEP
- Configurazione di NDES Server per il supporto di SSL
- Requisiti del certificato quando si utilizza EAP-TLS o PEAP con EAP-TLS
- Documentazione e supporto tecnico