Contents

Introduction

This document describes the steps that are used in order to successfully configure the Microsoft Network Device Enrollment Service (NDES) and Simple Certificate Enrollment Protocol (SCEP) for Bring Your Own Device (BYOD) on the Cisco Identify Services Engine (ISE).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- ISE Release 1.1.1 or later
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012 Standard
- Public Key Infrastructure (PKI) and certificates

Components Used

The information in this document is based on these software and hardware versions:

- ISE Release 1.1.1 or later
- Windows Server 2008 R2 SP1 with KB2483564 and KB2633200 hotfixes installed
- 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.

The information related to Microsoft certificate services is provided as a guide specifically for Cisco BYOD. Refer to the Microsoft TechNet as the definitive source of truth for Microsoft certification authority, Network Device Enrollment Service (NDES), and SCEP-related server configurations.

Background Information

One of the benefits of the Cisco ISE-enabled BYOD implementation is the ability of the end users to perform self-service device registration. This eliminates the administrative burden on IT in order to distribute authentication credentials and enable devices on the network. At the heart of the BYOD solution is the network supplicant provisioning process, which seeks to distribute the requisite certificates to employee-owned devices. In order to satisfy this requirement, a Microsoft Certificate Authority (CA) can be configured in order to automate the certificate enrollment process with the SCEP.

SCEP has been used for years in Virtual Private Network (VPN) environments in order to facilitate certificate enrollment and distribution to remote access clients and routers. The enablement of SCEP functionality on a Windows 2008 R2 server requires the installation of the NDES. During the NDES role installation, the Microsoft Internet Information Services (IIS) web server is also installed. IIS is used in order to terminate HTTP or HTTPS SCEP registration requests and responses between the CA and ISE policy node.

The NDES role can be installed on a current CA, or it can be installed on a member server. In a standalone deployment, the NDES service is installed on an existing CA that includes the Certification Authority service and, optionally, the Certification Authority Web Enrollment service. In a distributed deployment, the NDES service is installed on a member server. The distributed NDES server is then configured in order to communicate with an upstream root or sub-root CA. In this scenario, the registry modifications outlined in this document are made on the NDES server with the custom template, where certificates reside on the upstream CA.

Tested CA/NDES Deployment Scenarios

This section provides a brief overview of the CA/NDES deployment scenarios that have been tested in the Cisco lab. Refer to the Microsoft TechNet as the definitive source of truth for Microsoft CA, NDES, and SCEP-related server configurations.

Standalone Deployments

When ISE is used in a Proof of Concept (PoC) scenario, it is common to deploy a self-contained Windows 2008 or 2012 machine that acts as an Active Directory (AD) domain controller, root CA,

and NDES server:

- Domain Controller
- AD
- Root CA
- NDES

Distributed Deployments

When the ISE is integrated into a current Microsoft AD/PKI production environment, it is more common to see services distributed accross multiple, distinct Windows 2008 or 2012 servers. Cisco has tested two scenarios for distributed deployments.

This image illustrates the first tested scenario for distributed deployments:

- Domain Controller
- AD
- Root CA

- Member Server
- Subordinate CA
- NDES

This image illustrates the second tested scenario for distributed deployments:

Important Microsoft Hotfixes

Before you configure SCEP support for BYOD, ensure that the Windows 2008 R2 NDES server has these Microsoft hotfixes installed:

- Renewal request for a SCEP certificate fails in Windows Server 2008 R2 if the certificate is managed by using NDES - This issue occurs because NDES does not support the **GetCACaps** operation.

- NDES does not submit certificate requests after the enterprise CA is restarted in Windows Server 2008 R2 - This message appears in the **Event Viewer**: "*The Network Device Enrollment Service cannot submit the certificate request (0x800706ba). The RPC server is unavailable*."

  Warning: When you configure the Microsoft CA, it is important to understand that the ISE does not support the RSASSA-PSS signature algorithm. Cisco recommends that you configure the CA policy so that it uses sha1WithRSAEncryption or sha256WithRSAEncryption instead.

Important BYOD Ports & Protocols

Here is a list of important BYOD ports and protocols:

- TCP: 8909 Provisioning: Wizard Install from Cisco ISE (Windows and Macintosh Operating Systems (OS))

- TCP: 443 Provisioning: Wizard Install from Google Play (Android)

- TCP: 8905 Provisioning: Supplicant Provisioning Process

- TCP: 80 or TCP: 443 SCEP Proxy to CA (based on the SCEP RA URL configuration)

  Note: For the lastest list of required ports and protocols, refer to the ISE 1.2 Hardware Installation Guide.

Configure

Use this section in order to configure NDES and SCEP support for BYOD on the ISE.

Disable SCEP Enrollment Challenge Password Requirement

By default, the Microsoft SCEP (MSCEP) implementation uses a dynamic challenge password in order to authenticate clients and endpoints throughout the certificate enrollment process. With this configuration requirement in place, you must browse to the MSCEP admin web GUI on the NDES server in order to generate a password on-demand. You must include this password as part of the registration request.

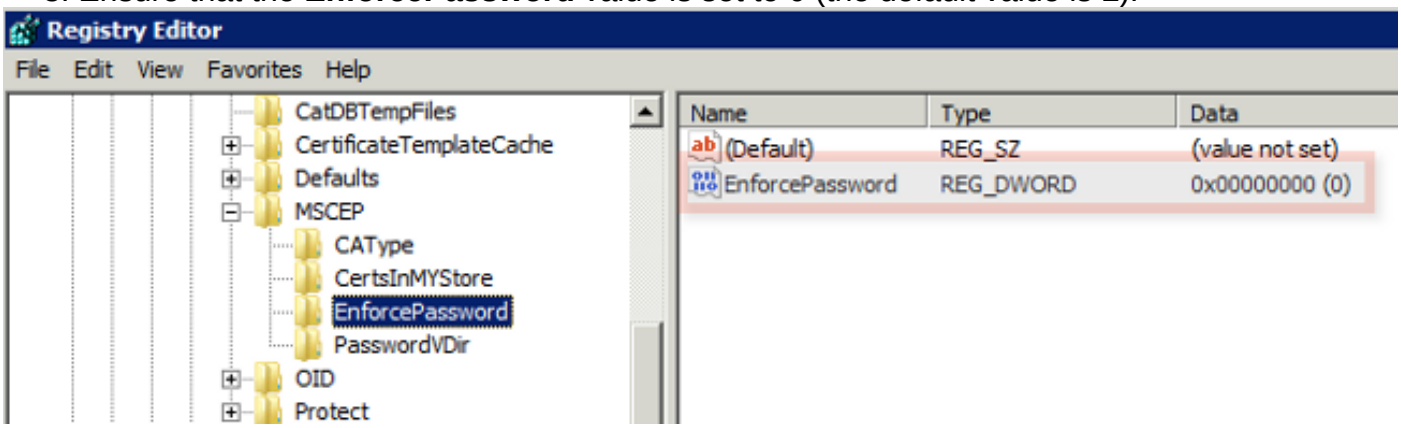
In a BYOD deployment, the requirement of a challenge password defeats the purpose of a user

self-service solution. In order to remove this requirement, you must modify this registry key on the NDES server:

1. Click **Start** and enter **regedit** in the search bar.

2. Navigate to **Computer** > **HKEY_LOCAL_MACHINE** > **SOFTWARE** > **Microsoft** > **Cryptography** > **MSCEP** > **EnforcePassword**.

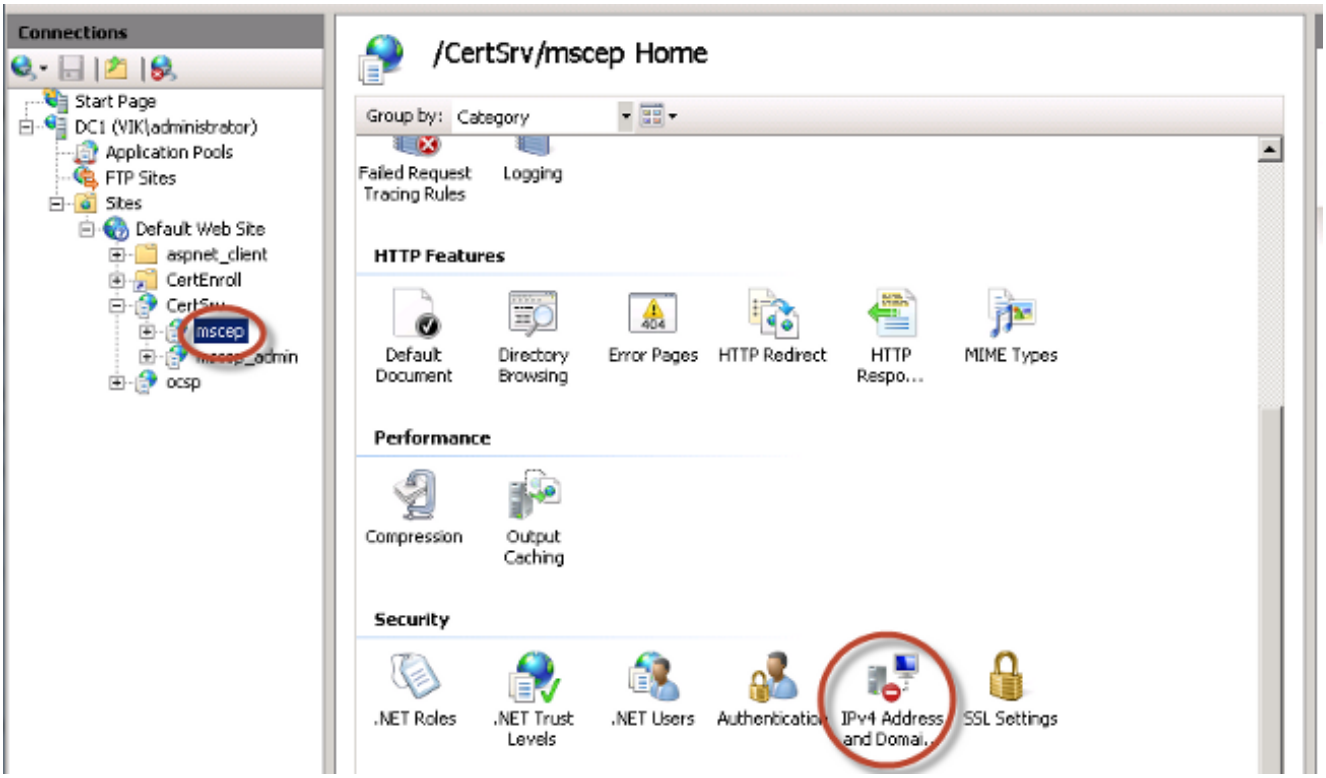
3. Ensure that the **EnforcePassword** value is set to **0** (the default value is **1**).



Restrict SCEP Enrollment to Known ISE Nodes

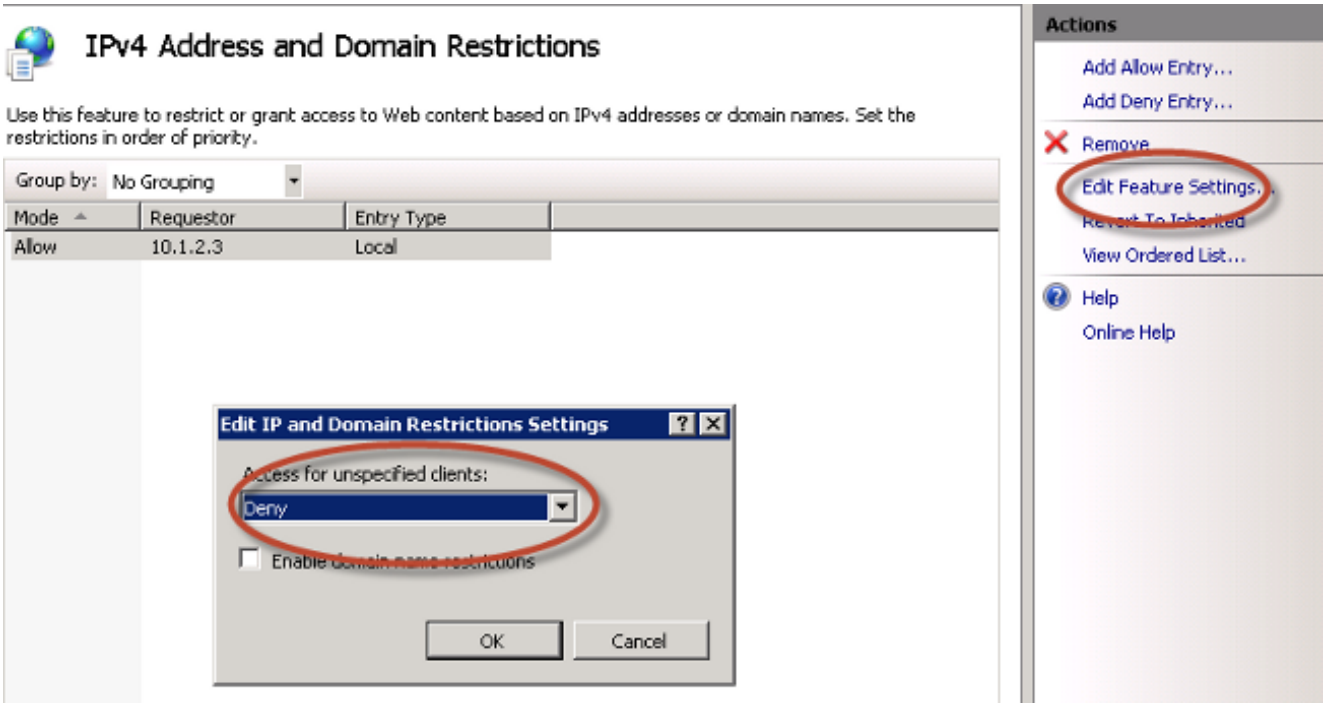
In some deployment scenarios, it might be preferred to restrict SCEP communications to a select list of known ISE nodes. This can be accomplished with the IPv4 Address and Domain Restrictions feature in IIS:

1. Open IIS and navigate to the **/CertSrv/mscep** web site.



2. Double click **Security > IPv4 Address and Domain Restrictions.** Use the **Add Allow Entry**

and **Add Deny Entry** actions in order to permit or restrict access to web content based on ISE node IPv4 addresses or domain names. Use the **Edit Feature Settings** action in order to define a default access rule for unspecified clients.

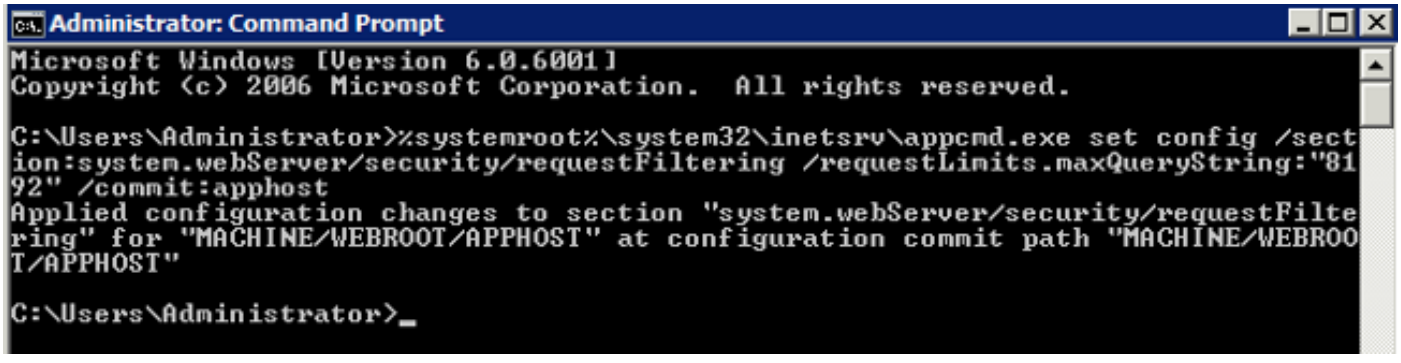


Extend the URL Length in IIS

It is possible for ISE to generate URLs that are too long for the IIS web server. In order to avoid this problem, the default IIS configuration can be modified to allow for longer URLs. Enter this command from the NDES server CLI:

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

Note: The query string size might vary dependent upon the ISE and endpoint configuration. Enter this command from the NDES server CLI with administrative privileges.



Certificate Template Overview

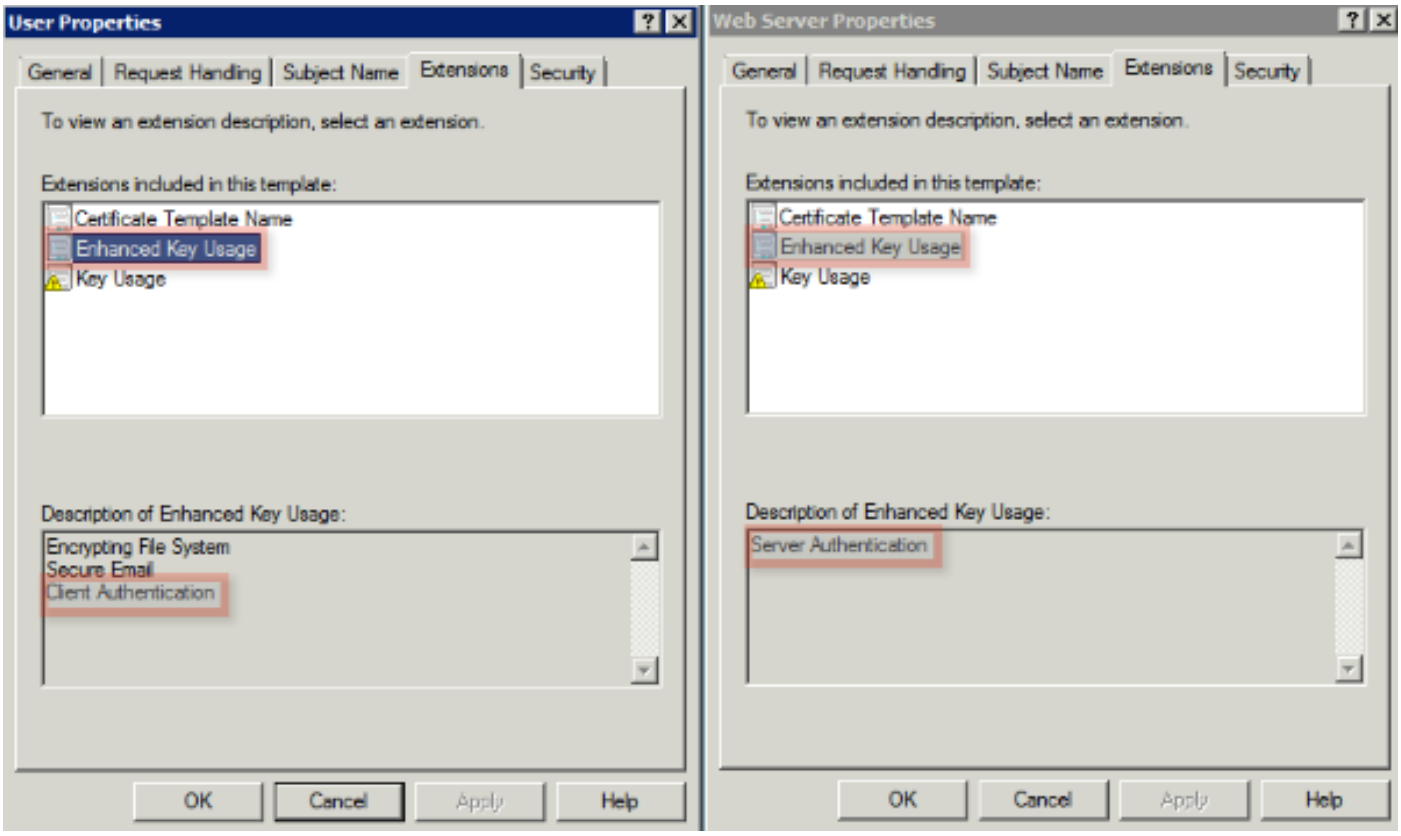
Administrators of a Microsoft CA can configure one or more templates that are used in order to apply application policies to a common set of certificates. These policies help to identify for which function the certificate and associated keys are used. The application policy values are contained in the Extended Key Usage (EKU) field of the certificate. The authenticator parses the values in the EKU field in order to ensure that the certificate presented by the client can be used for the

intended function. Some of the more common uses include server authentication, client authentication, IPSec VPN, and email. In terms of ISE, the more commonly used EKU values include server and/or client authentication.

When you browse to a secure bank website, for example, the web server that processes the request is configured with a certificate that has an application policy of server authentication. When the server receives an HTTPS request, it sends a server authentication certificate to the connecting web browser for authentication. The important point here is that this is a unidirectional exchange from the server to the client. As it relates to ISE, a common use for a server authentication certificate is admin GUI access. ISE sends the configured certificate to the connected browser and does not expect to receive a certificate back from the client.

When it comes to services such as BYOD that use EAP-TLS, mutual authentication is preferred. In order to enable this bidirectional certificate exchange, the template used in order to generate the ISE identity certificate must possess a minimum application policy of server authentication. The Web Server certificate template satisfies this requirement. The certificate template that generates the endpoint certificates must contain a minimum application policy of client authentication. The User certificate template satisfies this requirement. If you configure ISE for services such as Inline Policy Enforcement Point (iPEP), the template used in order to generate the ISE server identity certificate should contain both client and server authentication attributes if you use ISE Version 1.1.x or earlier. This allows the admin and inline nodes to mutually authenticate each other. The EKU validation for iPEP was removed in ISE Version 1.2, which makes this requirement less relevant.

You can reuse the default Microsoft CA Web Server and User templates, or you can clone and create a new template with the process that is outlined in this document. Based upon these certificate requirements, the CA configuration and resultant ISE and endpoint certificates should be carefully planned in order to minimize any unwanted configuration changes when installed in a production environment.



Certificate Template Configuration

As noted in the introduction, SCEP is widely used in IPSec VPN environments. As a result, installation of the NDES role automatically configures the server to utilize the **IPSec (Offline Request)** template for SCEP. Because of this, one of the first steps in the preparation of a Microsoft CA for BYOD is to build a new template with the correct application policy. In a standalone deployment, the Certification Authority and NDES services are collocated on the same server, and the templates and the required registry modifications are contained to the same server. In a distributed NDES deployment, the registry modifications are made on the NDES server; however, the actual templates are defined on the root or sub-root CA server specified in the NDES service installation.

Complete these steps in order to configure the Certificate Template:

1. Log on to the CA server as **admin**.

2. Click **Start** > **Administrative Tools** > **Certification Authority**.

3. Expand the CA server details and select the **Certificate Templates** folder. This folder contains a list of the templates that are currently enabled.

4. In order to manage the certificate templates, right-click on the **Certificate Templates** folder and choose **Manage**.

5. In the **Certificate Templates Console**, a number of inactive templates are displayed.

6. In order to configure a new template for use with SCEP, right-click on a template that already exists, such as **User**, and choose **Duplicate Template**.

7. Choose **Windows 2003** or **Windows 2008**, dependent upon the minimum CA OS in the environment.

8. On the **General** tab, add a display name, such as ISE-BYOD, and validity period; leave all other options unchecked.
   Note: The template validity period must be less than or equal to the validity period of the CA root and intermediate certificates.
9. Click on the **Subject Name** tab, and confirm that **Supply in the request** is selected.

10. Click on the **Issuance Requirements** tab. Cisco recommends that you leave the **Issuance policies** blank in a typical hierarchical CA environment.

11. Click on the **Extensions** tab, **Application Policies**, and then **Edit**.

12. Click **Add**, and ensure that **Client Authentication** is added as an application policy. Click **OK**.

13. Click on the **Security** tab, and then **Add...**. Ensure that the SCEP service account defined in the NDES service installation has full control of the template, and then click **OK**.

14. Return to the **Certification Authority GUI** interface.

15. Right-click on the **Certificate Templates** directory. Navigate to **New** > **Certificate Template to Issue**.

16. Select the **ISE-BYOD** template configured previously, and click **OK**.

    Note: Alternatively, you can enable the template via the CLI with the **certutil -SetCAtemplates +ISE-BYOD** command.
    The ISE-BYOD template should now be listed in the enabled certificate template list.

Certificate Template Registry Configuration

Complete these steps in order to configure the Certificate Template Registry keys:

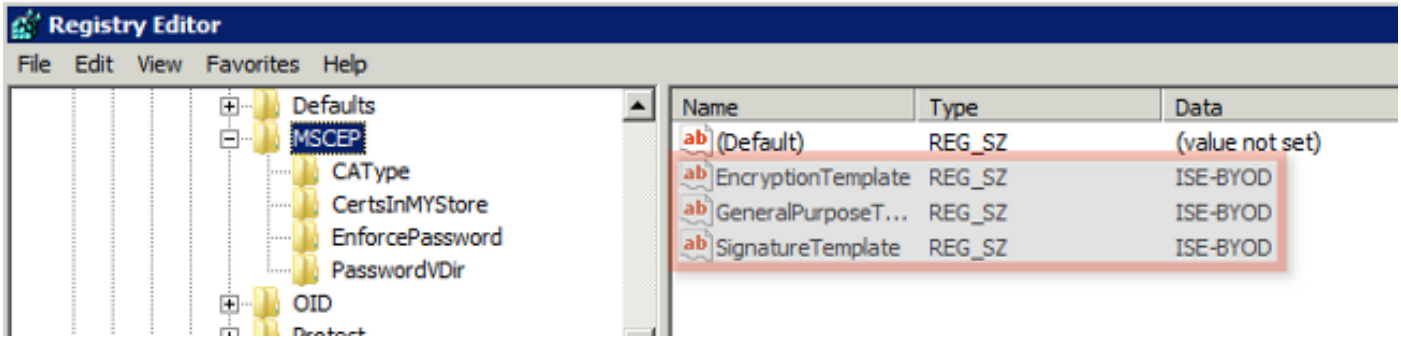
1. Connect to the NDES server.

2. Click **Start** and enter **regedit** in the search bar.

3. Navigate to **Computer** > **HKEY_LOCAL_MACHINE** > **SOFTWARE** > **Microsoft** > **Cryptography** > **MSCEP**.

4. Change the **EncryptionTemplate**, **GeneralPurposeTemplate**, and **SignatureTemplate** keys from **IPSec (Offline Request)** to the **ISE-BYOD** template previously created.

5. Reboot the NDES server in order to apply the registry setting.



Configure ISE as a SCEP Proxy

In a BYOD deployment, the endpoint does not communicate directly with the backend NDES server. Instead, the ISE policy node is configured as a SCEP proxy and communicates with the NDES server on behalf of the endpoints. The endpoints communicate directly with the ISE. The IIS instance on the NDES server can be configured in order to support HTTP and/or HTTPS bindings for the SCEP virtual directories.

Complete these steps in order to configure ISE as a SCEP Proxy:

1. Log into the **ISE GUI** with admin credentials.

2. Click **Administration**, **Certificates**, and then **SCEP CA Profiles**.

3. Click **Add**.

4. Enter the server name and description.

5. Enter the URL for the SCEP server with the IP or Fully Qualified Domain Name (FQDN) (**http://10.10.10.10/certsrv/mscep/**, for example).

6. Click **Test Connectivity**. A successful connection results in a successful server response pop-up message.

7. Click **Save** in order to apply the configuration.

8. In order to verify, click **Administration**, **Certificates**, **Certificate Store,** and confirm that the SCEP NDES server RA certificate has been automatically downloaded to the ISE node.

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

Use this section in order to troubleshoot your configuration.

General Troubleshoot Notes

Here is a list of important notes that you can use in order to troubleshoot your configuration:

- Break down the BYOD network topology into logical waypoints in order to help identify debug and capture points along the path between the ISE, NDES, and CA endpoints.
- Ensure that the ISE node and CA share a common Network Time Protocol (NTP) time source.
- Endpoints should be able to set their time automatically with the NTP and time zone options learned from DHCP.
- The DNS server of the client must be able to resolve the FQDN of the ISE node.
- Ensure that TCP 80 and/or TCP 443 are permitted bidirectionally between ISE and the NDES server.
- Test with a Windows machine because of the improved client-side logging. Optionally, use an Apple iDevice along with the Apple iPhone Configuration Utility in order to monitor client-side console logs.
- Monitor the CA and NDES server application logs for registration errors, and use Google or TechNet in order to research those errors.

- Throughout the test phase, use HTTP for SCEP in order to facilitate packet captures between ISE, NDES, and CA.

- Use the TCP Dump utility on the ISE Policy Service Node (PSN), and monitor traffic to and from the NDES server. This is located under **Operations** > **Diagnostic Tools** > **General Tools**.

- Install Wireshark on the CA and NDES server, or use SPAN on intermediary switches, in order to capture SCEP traffic to and from the ISE PSN.

- Ensure that the appropriate CA certificate chain is installed on the ISE policy node for the authentication of the client certificates.

- Ensure that the appropriate CA certificate chain is automatically installed onto the clients during onboarding.

- Preview the ISE and endpoint identity certificates and confirm that the correct EKU attributes are present.

- Monitor the live authentication logs in the ISE GUI for authentication and authorization failures.
  Note: Some supplicants do not initialize a client certificate exchange if the wrong EKU is present, such as a client certificate with EKU of server authentication. Therefore, authentication failures might not always be present in the ISE logs.
- When NDES is installed in a distributed deployment, a remote root or sub-root CA will be designated by CA Name or Computer Name in the service installation. The NDES server sends certificate registration requests to this target CA server. If the endpoint certificate registration process fails, packet captures (PCAP) might show the NDES server return a **404 Not Found** error to the ISE node. In order to resolve this issue, reinstall the NDES service and select the Computer Name option instead of the CA Name.

- Avoid alterations to the SCEP CA chain after devices are onboarded. Endpoint OSs, such as Apple iOS, do not automatically update a previously installed BYOD profile. In this iOS example, the current profile must be deleted from the endpoint, and the endpoint removed from the ISE database, so that onboarding can be performed again.

- You can configure a Microsoft certificate server in order to connect to the Internet and automatically update certificates from the Microsoft Root Certificate Program. If you configure this network retrieval option in environments with restricted Internet policies, CA/NDES servers that cannot connect to the Internet can take 15 seconds to timeout by default. This can add a 15-second delay to the processing of SCEP requests from SCEP proxies such as ISE. ISE is programmed in order to timeout SCEP requests after 12 seconds if a response is not received. In order to resolve this issue, either permit Internet access for the CA/NDES servers, or modify the Network Retrieval timeout settings in the local security policy of the Microsoft CA/NDES servers. In order to locate this configuration on the Microsoft server, navigate to **Start > Administrative Tools > Local Security Policy > Public Key Policies > Certificate Path Validation Settings > Network Retrieval**.

Client-Side Logging

Here is a list of useful techniques that are used in order to troubleshoot client-side logging issues:

- Enter the **Log %temp%\spwProfileLog.txt.** command in order to view the client-side logs for Mircosoft Windows applications.
  Note: WinHTTP is used for the connection between the Microsoft Windows endpoint and ISE. Reference the Microsoft Windows Error Messages article for a list of error codes.
- Enter the **/sdcards/downloads/spw.log** command in order to view the client-side logs for Android applications.

- For **MAC OSX**, use the Console application, and look for the **SPW** process.

- For **Apple iOS**, use Apple Configurator 2.0 in order to view messages.

ISE Logging

Complete these steps in order to view the ISE log:

1. Navigate to **Administration** > **Logging** > **Debug Log Configuration**, and select the appropriate ISE policy node.

2. Set the **client** and **provisioning** logs to debug or trace, as required.

3. Reproduce the problem and document relevant seed info in order to facilitate searching, such as MAC, IP, and user.

4. Navigate to **Operations** > **Download Logs**, and select the appropriate ISE node.

5. On the **Debug Logs** tab, download the logs named **ise-psc.log** to the desktop.

6. Use an intelligent editor, such as Notepad ++ in order to parse the log files.

7. When the issue has been isolated, then return the log levels to the default level.

NDES Logging and Troubleshooting

For more information, refer to the AD CS: Troubleshooting Network Device Enrollment Service Windows Server article.

Related Information

- **BYOD Solutions Guide - Certificate Authority Server Configuration**
- **NDES Overview in Windows 2008 R2**
- **MSCEP White Paper**
- **Configuring NDES Server to Support SSL**
- **Certificate requirements when you use EAP-TLS or PEAP with EAP-TLS**

- **Technical Support & Documentation**