



Certificate Enrollment Guide for the Cisco 1000 Series Connected Grid Routers

Last Revised: March 20, 2012

This document covers the process of obtaining and enrolling digital certificates for the Cisco 1000 Series Connected Grid Routers (*hereafter* referred to as the Cisco CG-OS router) by employing the Simple Certificate Enrollment Protocol (SCEP) for secure communication in the network. Additionally, this document describes the systems involved in the certificate process and the required configuration of those systems.

This certificate guide includes the following sections:

- [Overview, page 1](#)
- [Prerequisites, page 3](#)
- [Configuring Systems, page 3](#)
- [Related Documentation, page 37](#)
- [Obtaining Documentation and Submitting a Service Request, page 37](#)

Overview

[Figure 1](#) displays the Cisco recommended network topology for generation and management of certificate enrollment for the Cisco CG-OS router.

Cisco Certificate Enrollment employs the following systems, processes or identities:

- IDevID–IEEE 802.11AR security device identity assigned by Cisco to the Cisco CG-OS router.
- LDevID–IEEE 802.11AR security device identity that serves as a local identity for the Cisco CG-OS router that is used for network traffic authentication such as IPSec or HTTPS.
- RSA key-pair–Allows digital signatures, based on public key cryptography, to digitally authenticate devices and individual users. Each key-pair contains both a private key and a public key. The private key is kept secret and is known only to the owning device or user only. However, the public key is known to everybody.



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

- Simple Certificate Enrollment Protocol (SCEP)—Allows automatic enrollment of the certificates on the Cisco CG-OS router without user intervention. During a SCEP request, if an authenticated IDevID belongs to one of the devices pre-configured on the RADIUS server, then the Registration Authority forwards the SCEP request to the CA behind the firewall.

Although SCEP is the recommended process for enrolling certificates, the Cisco CG-OS router also supports three other methods (see the “Configuring PKI” chapter in the [Cisco 1000 Series Connected Grid Routers Security Software Configuration Guide](#)).

- Registration Authority (RA)—Proxies as a Certificate Authority (CA) server on behalf of the Cisco CG-OS router to obtain certificates from the CA server.

**Caution**

You must configure the RA **before** configuring auto-enrollment on the Cisco CG-OS router.

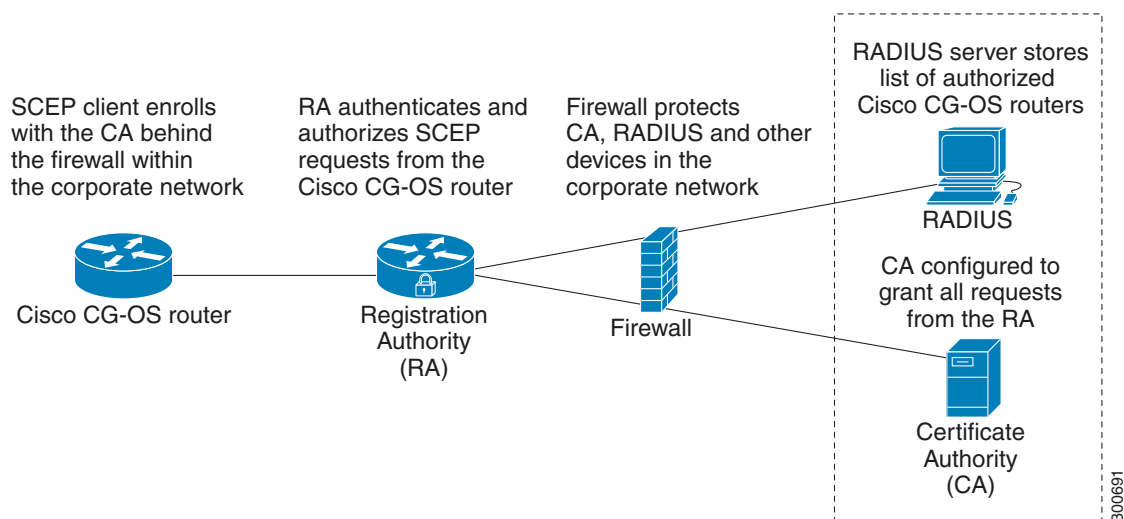
Cisco recommends that you employ the [Cisco 3945 Integrated Services Router](#) (Cisco ISR) as the RA in your network.

- RADIUS Server—Stores a list of authorized Cisco CG-OS routers and authorizes incoming SCEP requests by verifying that the IDevID of the requestor (Cisco CG-OS router) is present in its database. Each Cisco CG-OS router ships with a unique IDevID.
- Certificate Authority (CA)—Grants all SCEP requests received from the RA. In this example, the CA is a Microsoft server.
- Trustpoint—Manages certificates for a specified system. In the recommended configuration (see [Figure 1](#)), one trustpoint is defined for the Cisco CG-OS router and two trustpoints are defined for the RA.
- Firewall—Protects the private network resources within the Utility network such as RADIUS and Certificate Authority servers from intrusion by users on the Utility public network. Configure the firewall to permit communication between the RA and CA.

Listed below is a summary of the activities that occur in the Cisco certificate enrollment process.

- The Cisco CG-OS router enrolls with the Certificate Authority by employing the Registration Authority (RA) as its intermediary.
- The RA also authenticates and authorizes incoming Simple Certificate Enrollment Protocol (SCEP) requests from the Cisco CG-OS router.
 - Authentication occurs when the RA is able to verify that the requestor has a valid IDevID
 - Authorization occurs by using a RADIUS server to ensure that the requestor is a member of the authorized group of Cisco CG-OS routers.
- When the request is determined valid, then the RA forwards the request to the CA that is behind a firewall within the private network.

Figure 1 Recommended Network Topology



Prerequisites

Ensure that all those systems, employed by the certification enrollment process, are active in the network (see [Figure 1](#)).



Note

This document only provides those configuration steps required for certificate enrollment.

Configuring Systems

This section provides configuration details for the Cisco CG-OS router and the supporting systems involved in the certificate enrollment process, and includes the following topics:

- [Configuring the Cisco CG-OS Router, page 3](#)
- [Configuring the RA, page 7](#)
- [Configuring the RADIUS Server to Support SCEP, page 13](#)

Configuring the Cisco CG-OS Router

This section provides the configuration details for the Cisco CG-OS router, and includes the following topics:

- [Creating a Trustpoint on the Cisco CG-OS Router](#)
- [Authenticating and Enrolling the CA](#)

Creating a Trustpoint on the Cisco CG-OS Router

In Cisco CG-OS software, you can create trustpoints to manage certificates.

In the following steps, you create a new trustpoint (LDevID) and a new enrollment profile (LDevID_Prof) for SCEP enrollment.

The Cisco CG-OS router uses the new trustpoint to obtain its certificates from the RA. The new enrollment profile specifies the URL of the RA and the request credentials used by the SCEP request.

BEFORE YOU BEGIN

Configure the router acting as the RA.

DETAILED STEPS

	Command	Purpose
Step 1	configure terminal	Enters global configuration mode.
Step 2	crypto ca trustpoint <i>name</i>	Creates a new trustpoint that the Cisco CG-OS router can trust and enters trustpoint configuration mode. <i>name</i> —Alphanumeric, case sensitive, string with a maximum length of 64 characters. Note The maximum number of trustpoints that you can configure on the Cisco CG-OS router is 16.
Step 3	enrollment profile <i>name</i>	Specifies the use of an enrollment profile. Ensures that the RA requests the RA mode Certificate Service (CS) certificate from the CA server.
Step 4	rsa-keypair <i>rsa-keypair-label</i>	Enter the name of the RSA key-pair that the Cisco CG-OS router and RA will use.
Step 5	revocation-check none	Disables revocation of compromised certificates.
Step 6	serial-number	Enter this command to include the serial number of the Cisco CG-OS router in the certificate.
Step 7	fingerprint <i>hex-data</i>	Configures the expected SHA1 thumbprint of the CA server certificate. Note Thumbprint information is found in the Certificate > Details window of the Windows CA Server. Matching is performed during CA authentication and enrollment. Note The Cisco CG-OS router only supports SHA1 fingerprints.
Step 8	exit	Exits the trustpoint configuration mode and returns the Cisco CG-OS router to the global configuration mode.
Step 9	crypto ca profile enrollment <i>profile_name</i>	Creates a new enrollment profile.
Step 10	enrollment url <i>url</i>	Defines the URL of the RA that serves as CA proxy and enters the enrollment profile configuration submenu. The RA must be directly connected to the Cisco CG-OS router.

	Command	Purpose
Step 11	enrollment credential {IDevID trustpoint <i>name</i>}	Specifies either the IDevID or a trustpoint to authenticate the SCEP request. Note For this recommended configuration, Cisco employs the IDevID. IDevID—IEEE 802.11AR security device identity assigned by Cisco. Cisco CG-OS router locates the value when IDevID is entered for this command.
Step 12	exit	Exits the enrollment profile configuration mode and returns the Cisco CG-OS router to the global configuration mode.

EXAMPLE

This example shows how to define a new trustpoint named LDevID and enrollment profile, LDevID_Prof, which the trustpoint uses for SCEP enrollment.

LDevID serves as a local identity for the Cisco CG-OS router that can be used for network traffic authentication such as IPSec or HTTPS.



Note You must not use the IDevID credential that is initially assigned on the Cisco CG-OS router on the network.

```

router_cgr01# configure terminal
router_cgr01(config)# crypto ca trustpoint LDevID
router_cgr01(config-trustpoint)# enrollment profile LDevID_Prof
router_cgr01(config-trustpoint)# rsakeypair LDevID_Key 2048
router_cgr01(config-trustpoint)# revocation-check none
router_cgr01(config-trustpoint)# serial-number
router_cgr01(config-trustpoint)# fingerprint
AE:5C:DE:F2:A6:33:DE:F4:1D:5A:51:04:7D:6A:8B:D7:E0:8B:57:6C
router_cgr01(config-trustpoint)# exit
router_cgr01(config)# crypto ca profile enrollment LDevID_Prof
router_cgr01(config-enroll-profile)# enrollment url http://172.27.165.157
router_cgr01(config-enroll-profile)# enrollment credential IDevID
router_cgr01(config-enroll-profile)# exit
router_cgr01(config)#

```

Authenticating and Enrolling the CA

After configuring the trustpoint, RSA key-pair, and enrollment profile on the Cisco CG-OS router, you can initiate CA authentication and enrollment by using SCEP.

As part of the configuration, the system prompts you to enter a challenge password, which the CA might use to authenticate a certification revocation request.



Note The Cisco CG-OS router also supports using a terminal to cut-and-paste the certificate requests and resulting certificates between the Cisco CG-OS router and the CA (see [Configuring a Trustpoint to Authenticate the SCEP Request](#)).


BEFORE YOU BEGIN

Create a trustpoint (see [Creating a Trustpoint on the Cisco CG-OS Router, page 3](#)).

Create an enrollment profile.

Verify the system clock and timezone settings are correct.

DETAILED STEPS

	Command	Purpose
Step 1	configure terminal	Enters global configuration mode.
Step 2	crypto ca authenticate <i>trustpoint-name</i>	Acquires the CA certificate from the URL specified in the enrollment url command (see Step 10).
Step 3	crypto ca enroll <i>trustpoint-name</i>	<p>Generates a certificate request for an authenticated CA and prompts you to create a challenge password.</p> <p>The CA might request this challenge password when you revoke a certificate.</p> <div style="text-align: center;">  </div> <p>Caution You must remember the challenge password. It is not saved with the configuration.</p> <p><i>trustpoint name</i>—Name of the trustpoint. The maximum size is 64 characters.</p>
Step 4	exit	Exits configuration mode.

EXAMPLE

This example shows how to initiate LDevID enrollment using SCEP.

```

router_cgr01# configure terminal
router_cgr01(config)# crypto ca authenticate LDevID

Trustpoint CA authentication in progress. Please wait for a response...
router_cgr01(config)# 2012 Feb 17 13:17:49 Router %$ VDC-1 %$ %CERT_ENROLL-2-
CERT_EN_SCEP_CA_AUTHENTICATE_OK: Trustpoint LDevID: CA certificates(s) authenticated.

router_cgr01(config)# crypto ca enroll LDevID

Create the certificate request ...
Create a challenge password. You will need to verbally provide this
password to the CA Administrator in order to revoke your certificate.
For security reasons your password will not be saved in the configuration.
Please make a note of it.
Challenge password:
Re-enter challenge password:
The serial number in the certificate will be: CGR1240/K9+JSJ1538000C
Certificate enrollment in progress. Please wait for a response...
router_cgr01(config)# 2012 Feb 17 13:18:17 Router %$ VDC-1 %$ %CERT_ENROLL-2-
CERT_EN_SCEP_ENROLL_OK: TrustpointLDevID: Device identity certificate successfully
enrolled to CA.
```

Configuring the RA

The RA provides SCEP request authentication and authorization. As part of that process, you must configure a trustpoint to authenticate the SCEP enrollment. Additionally, you must configure a PKI server on the RA to initiate the HTTP server, as well as configure a new trustpoint on that server to allow communication with the CA. Lastly, you must configure a RADIUS server on the RA to perform SCEP request authorization.

The RA is configured on the Cisco ISR (Cisco-recommended system for RA) and operates with Cisco IOS rather than the Cisco CG-OS software.



Note

For more information on the Cisco ISR, refer to the following URL:
<http://www.cisco.com/en/US/products/ps10536/index.html>



Caution

You must configure a RA **before** configuring the Cisco CG-OS router.

This section includes the following topics:

- [Configuring a Trustpoint to Authenticate the SCEP Request](#)
- [Configuring a PKI Server](#)
- [Configuring a RADIUS Server for SCEP Request Authorization](#)

Configuring a Trustpoint to Authenticate the SCEP Request

Authenticating the SCEP Request ensures that the Cisco CG-OS router is manufactured by Cisco.

BEFORE YOU BEGIN

You must configure the hostname and IP domain name of the RA if it is not yet configured.



Caution

Changing the hostname or IP domain name of the RA after generating the certificate can invalidate the certificate.

DETAILED STEPS

	Command	Purpose
Step 1	<code>configure terminal</code>	Enters global configuration mode.
Step 2	<code>crypto pki trustpoint <i>name</i></code>	Create a new trustpoint on the RA to authenticate the SCEP enrollment request and enters the trustpoint configuration mode. <i>name</i> —Alphanumeric, case sensitive, string with a maximum length of 64 characters. Note The maximum number of trustpoints that you can configure in Cisco IOS is 16.

	Command	Purpose
Step 3	enrollment mode terminal	Specifies that a terminal be employed to authenticate the CA. Operating in the terminal mode allows a certificate to be cut-and-paste at the terminal when prompted (see Step 7).
Step 4	revocation-check none	Disables revocation of compromised certificates.
Step 5	exit	Exits trustpoint configuration mode.
Step 6	crypto pki authenticate <i>name</i>	Authenticates the CA by importing the IDevID certificate using the console (terminal). Note Enter the name of the trustpoint created in Step 2 to authenticate the SCEP request. <i>name</i> —Name of the certificate.
Step 7	---	At the Cisco IOS prompt that appears on the console screen, paste the PEM formatted CA certificate. Note After pasting the CA certificate, the system prompts you to accept the fingerprint. Enter yes to accept.
Step 8	exit	Exits global configuration mode.

EXAMPLE

This example shows how to create a new trustpoint, ACT2_SUDI_CA, on the RA to authenticate the SCEP enrollment. Additionally, it shows the prompts that request pasting of the certificate and acceptance of the certificate fingerprint.

```
ISR_RA# configure terminal
ISR_RA(config)# crypto pki trustpoint ACT2_SUDI_CA
ISR_RA(ca-trustpoint)# enrollment terminal
ISR_RA(ca-trustpoint)# revocation-check none
ISR_RA(ca-trustpoint)# exit
ISR_RA(config)# crypto pki authenticate ACT2_SUDI_CA
```

Enter the base 64 encoded CA certificate. End with a blank line or the word "quit" on a line by itself

```
-----BEGIN CERTIFICATE-----
MIIEPDCCAYsGAWIBAgIKYQlufQAAAAAADANBgkqhkiG9w0BAQUFADA1MRyWFAYD
VQKKEw1DaXNjbYBTeXN0ZW1zMRSwGQYDVQQDEExJDaXNjbYBsB290IENBIDIwNDgw
HhcNMTEwNjMwMTc1NjU3WhcNMjkwNTE0MjAyNTQyWjAnMQ4wDAYDVQQKEwVDaXNj
bzEVMBMGA1UEAxMMQUNUMiBTVURJIEBMBIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEAA0m5l3THIxAtN/hS5qR/6UZRpdd+9aE2JbFkNjht6gfHKd477AkS
5XAtUs5oxDYvt/zEbslZq3+LR6qrqKQVU6JYvH05UYLBqCj38s76NLk53905Wzp
9pRcmRCPuX+a6tHF/qRuOiJ44mdeDYz03qPCpxzprWJDPc1M4iYKHumMQMqmgmg+
xghHIooWS80BOcdiynEbeP5rZ7qRuewKMpl1TiI3WdBNjZjnpfjg66F+P4SaDkGb
BXdGj13oVeF+EyFWLrFjj97fL2+8oauV43Qrvnf3d/GfqXj7ew+z/sX1XtEOjSXJ
URsyMEj53Rdd9tJwHky8neapszS+r+kdVQIDAQABo4IBWjCCAVYwCwYDVR0PBAQD
AgHGMB0GA1UdDgQWBBRI2PHxwnDVW7t8cwmTr7i4MAP4fzAfBgNVHSMEGDAWgBQn
88gVhm6aAgkWrSugiWBF2nsvqjBDBgNVHR8EPDA6MDigNqA0hjJodHRwOi8vd3d3
LmNpc2NvLmNvbS9zZW50cm10eS9wa2kvY3JsL2NyY2EyMDQ4LmNybDBQBggrBgEF
BQcBAQREMEIwQAYIKwYBBQUHMAKGNGh0dHA6Ly93d3cuY2l2Y28uY29tL3N1Y3Vy
aXR5L3BraS9wb2xpY2l2cy9pbmRleC50dG1sMBIGA1UdEwEB/wQIMAYBAf8CAQAwDQYJ
KoZIHvcNAQEFBQADggEBAGh1qc1r9tx4hzWgDERm371yeuEmqcIfi9b9+GbMSJbi
ZHc/CcC10lJu0a9zTXA9w47H9/t61eduGxb4WeLxcwCiUgvFtCa51Ik1t8nNbcKY
/4dw1ex+7amATUQ04QggIE67wVIPu6bgAE3Ja/nRS3xKYSnj8H5TehimBSv6TECI
```



```
i5jUhOWryAK4dVo8hCjkjEkzu3ufBTJapnv89g9OE+H3VKM4L+/KdkUO+52djFKn
hyl47d7cZR4DY4LIuFM2PlAs8YyjoNpK/urSRI14WdI1p1R1nH7KND15618yfVP
0IFJZBGrooCRBjOSwFv8cpWCbmWdPaCQT2nwIjTfY8c=
-----END CERTIFICATE-----
```

Trustpoint 'ACT2_SUDI_CA' is a subordinate CA and holds a non self signed cert
Certificate has the following attributes:

Fingerprint MD5: 542F6E73 28DA2611 8E50685D EB4B7194

Fingerprint SHA1: F6969BBB 48E5F612 5B934D01 E71FE9C2 7C6F547E

% Do you accept this certificate? [yes/no]: **yes**

Trustpoint CA certificate accepted.

% Certificate successfully imported

ISR_RA(config)# **exit**

Configuring a PKI Server

Configuring a PKI server on the RA allows the HTTP server to be enabled to support the transfer of SCEP messages over HTTP, and creation of a new trustpoint (MSCA) that is enrolled to the CA.

DETAILED STEPS

	Command	Purpose
Step 1	configure terminal	Enters global configuration mode.
Step 2	ip http server	Enables the HTTP server and allows the RA to start listening on port 80 (HTTP) and relay SCEP messages to the CA server.
Step 3	crypto pki trustpoint <i>name</i>	Creates a trustpoint that the RA registers with the CA and enters the trustpoint configuration mode.
Step 4	enrollment mode ra	Ensures that the RA router enrolls with the CA server in the RA mode.
Step 5	enrollment url <i>url</i>	Configures the URL address for the CA SCEP server. <i>url</i> —Specifies URL of the CA server. Note You can specify only one RSA key-pair per CA.
Step 6	serial-number	Enter this command to include the serial number of the Cisco CG-OS router in the RA certificate.
Step 7	fingerprint <i>hex-data</i>	Enters the expected SHA1 thumbprint of the CA server certificate. Note Thumbprint information is found in the Certificate > Details window of the Windows CA Server. Matching is performed during CA authentication and enrollment.
Step 8	revocation-check none	Disables the revocation of compromised certificates.
Step 9	rsakeypair <i>rsa-keypair-label</i>	Specifies the name of the private key for the trustpoint created in Step 3 .
Step 10	exit	Exits trustpoint configuration mode.

	Command	Purpose
Step 11	crypto pki server <i>name</i>	Creates a PKI server. Note The name of the PKI server must match the trustpoint name defined in Step 3 .
Step 12	grant auto trustpoint <i>name</i>	Specifies that the SCEP enrollment requests from the Cisco CG-OS router to the RA be granted if it can be verified using the trustpoint specified in this step. Note Enter the trustpoint name created in the following section: Configuring a Trustpoint to Authenticate the SCEP Request , page 7.
Step 13	hash sha1	Specifies SHA1 as the cryptographic hash function for SCEP.
Step 14	mode ra transparent	Enters the RA certificate server mode. The transparent keyword allows the proxy CA server in RA mode to operate with more than one type of CA server. Specifically, it allows a transparent path from the RA (CA proxy) to the actual CA server that stores the certificates.
Step 15	no shutdown	Enables the PKI server.
Step 16	exit	Exits PKI server configuration mode.
Step 17	exit	Exits global configuration mode.

EXAMPLE

This example shows how to create a PKI server and trustpoint on the RA named MSCA.

```
ISR_RA# configure terminal
ISR_RA(config)# ip http server
ISR_RA(config)# crypto pki trustpoint MSCA
ISR_RA(ca-trustpoint)# enrollment mode ra
ISR_RA(ca-trustpoint)# enrollment url http://172.27.168.17:80/certsrv/mscep/mscep.dll
ISR_RA(ca-trustpoint)# serial-number
ISR_RA(ca-trustpoint)# fingerprint AE5CDEF2A633DEF41D5A51047D6A8BD7E08B576C
ISR_RA(ca-trustpoint)# revocation-check none
ISR_RA(ca-trustpoint)# rsakeypair MSCA_Key 2048
ISR_RA(ca-trustpoint)# exit
ISR_RA(config)# crypto pki server MSCA
ISR_RA(cs-server)# grant auto trustpoint ACT2_SUDI_CA
ISR_RA(cs-server)# hash sha1
ISR_RA(cs-server)# mode ra transparent
ISR_RA(cs-server)# no shutdown
%Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key
% or type Return to exit
Password:

Re-enter password:
% Generating 2048 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 22 seconds)

Certificate has the following attributes:
  Fingerprint MD5: 2D830B47 83130C2B 7B64B338 835D7516
  Fingerprint SHA1: AE5CDEF2 A633DEF4 1D5A5104 7D6A8BD7 E08B576C
Trustpoint Fingerprint: AE5CDEF2 A633DEF4 1D5A5104 7D6A8BD7 E08B576C
Certificate validated - fingerprints matched.
Trustpoint CA certificate accepted.%
```

```

% Start certificate enrollment ...
% Create a challenge password. You will need to verbally provide this
password to the CA Administrator in order to revoke your certificate.

For security reasons your password will not be saved in the configuration.
Please make a note of it.

Password:

Re-enter password:
% The subject name in the certificate will include: ISR_RA
% The serial number in the certificate will be: FTX1228A466
% Include an IP address in the subject name? [no]: no
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate verbose MSCA' command will show the fingerprint.

% Enrollment in progress...
ISR_RA(cs-server)#% Exporting Certificate Server signing certificate and keys...

Feb 17 15:21:42: CRYPTO_PKI: Certificate Request Fingerprint MD5: F62785A5 E0637067
BD4CCD5E DA953881
Feb 17 15:21:42: CRYPTO_PKI: Certificate Request Fingerprint SHA1: D01BF695 23173490
45F97EFA 9FE54C8E 91CC216B

Feb 17 15:21:43: %PKI-6-CERTRET: Certificate received from Certificate Authority
Feb 17 15:21:48: %PKI-6-CS_ENABLED: Certificate server now enabled.

ISR_RA(cs-server)# exit
ISR_RA(config)# exit
ISR_RA#

```

Configuring a RADIUS Server for SCEP Request Authorization

SCEP request authorization ensures that any Cisco CG-OS router making a SCEP request is authorized to enroll with the Utility CA by having the RA (Cisco ISR) make an additional check. This check involves the RA making an AAA call to the RADIUS server to verify that the Cisco CG-OS router entry resides in its database.

To locate the serial number, enter the **show inventory | head lines 2** command to display the following information.

```

NAME: "Chassis", DESCR: "CGR1000 Chassis "
PID: CGR1240/K9 , VID: V00 , SN: JSJ1538000C Router#

```



Note

The serial number for each Cisco CG-OS router must be entered into the RADIUS server prior to SCEP enrollment.



Tip

After completing configuration of a RADIUS server on the RA for SCEP request authorization in the this section, you must then configure items within the AAA server to support that authorization. For details, see [Configuring the RADIUS Server to Support SCEP, page 13](#).

DETAILED STEPS

	Command	Purpose
Step 1	configure terminal	Enters global configuration mode.
Step 2	radius server <i>name</i>	Defines a RADIUS server.
Step 3	address ipv4 <i>address</i>	Enters the IPv4 address of the RADIUS server.
Step 4	key <i>password</i>	Specifies the RADIUS shared secret between the RA and RADIUS server.
Step 5	exit	Exits the RADIUS server configuration mode.
Step 6	aaa authorization network <i>list-name</i> group radius	Define an authorization list for Cisco CG-OS routers and associates it to the default RADIUS group.
Step 7	crypto pki trustpoint <i>name</i>	Declares a trustpoint that the RA should trust and enters trustpoint configuration mode. Note Specify the trustpoint created in Configuring a Trustpoint to Authenticate the SCEP Request, page 7 .
Step 8	authorization list <i>list-name</i>	Specifies the server group (authorization list) that the RADIUS server uses for PKI authorization. Note Enter the authorization list created in Step 6 .
Step 9	authorization username subjectname <i>subjectname</i>	Specifies the item to use as the authorization subject name (such as serial number).
Step 10	exit	Exits trustpoint configuration guide.
Step 11	exit	Exits configuration mode.

EXAMPLE

This example shows how to define an authorization list (CGRAuthList), configure a RADIUS server on the Cisco ISR, and modify the IDevID CA trustpoint (ACT2_SUDI_CA) to include PKI authorization using the defined authorization list.

```
ISR_RA# configure terminal
ISR_RA(config)# radius server MyRadius
ISR_RA(config-radius-server)# address ipv4 172.27.166.37
ISR_RA(config-radius-server)# key RadiusPassword
ISR_RA(config-radius-server)# exit
ISR_RA(config)# aaa authorization network CGRAuthList group radius
ISR_RA(config)# crypto pki trustpoint ACT2_SUDI_CA
ISR_RA(ca-trustpoint)# authorization list CGRAuthList
ISR_RA(ca-trustpoint)# authorization username subjectname serialnumber
ISR_RA(ca-trustpoint)# exit
ISR_RA(config)# exit
```

Configuring the RADIUS Server to Support SCEP

This section provides an overview of how to configure the Microsoft Windows 2008 Server Network Policy Server (NPS) and Cisco Access Control Server (Cisco ACS) to serve as the AAA (RADIUS) authorization server (referenced in [Configuring a RADIUS Server for SCEP Request Authorization](#)) to properly identify and authorize Cisco CG-OS routers in their database.

**Note**

Only one RADIUS server, Microsoft NPS or Cisco ACS, is required to support certificate enrollment.

This section includes the following sections:

- [Configuring a Microsoft Windows 2008 Server Network Policy Server \(NPS\), page 14](#)
- [Configuring Cisco ACS, page 34](#)

BEFORE YOU BEGIN

The following items must be configured on the RADIUS server for each Cisco CG-OS router to properly enroll its certificate:

- An entry in the RADIUS server database that can uniquely identify the Cisco CG-OS router.
- The Cisco CG-OS router entry must include its serial number (entered as a username) and employ the text string *cisco* as the password.
- The RADIUS server must be configured to return the following RADIUS attribute upon successful authorization of the user (Cisco CG-OS router): “cisco-av-pair=pki:cert-application=all”

The RADIUS attribute allows the PKI server on the RA to grant the SCEP request for any application (such as the CA enrollment operation).

Configuring a Microsoft Windows 2008 Server Network Policy Server (NPS)

The Network Policy Server serves as a RADIUS server.

This section defines the configuration necessary to enter information for an Cisco CG-OS router and includes the following topics:

- [Creating a New User Entry in the Active Directory, page 14](#)
- [Defining a Connection Policy, page 17](#)
- [Defining a Network Policy, page 22](#)
- [Viewing the Log for Cisco CG-OS Router Authentication Details, page 32](#)

BEFORE YOU BEGIN

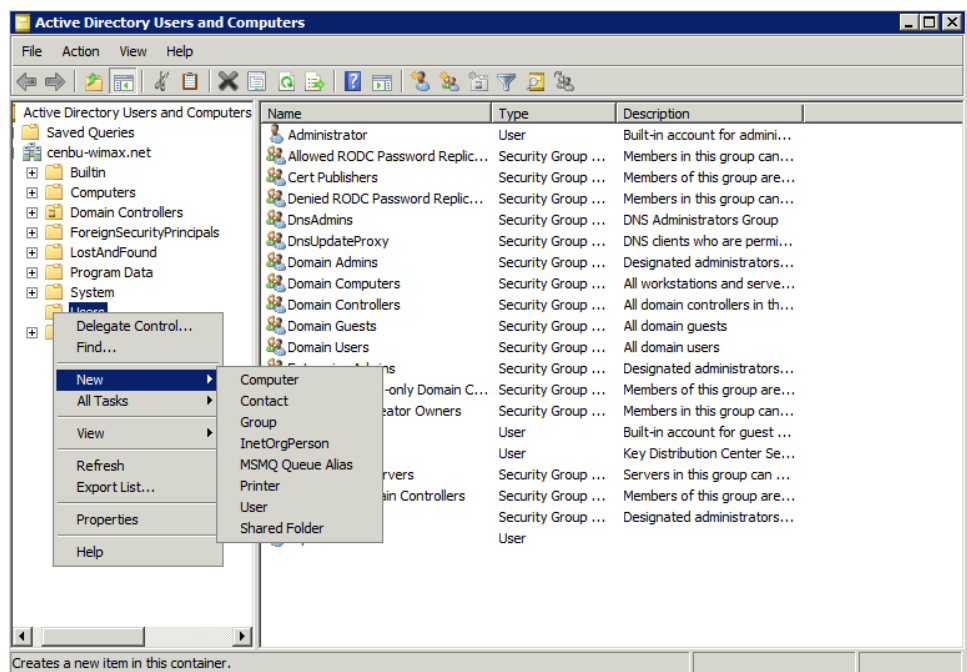
Ensure that a Microsoft Windows 2008 Server Network Policy Server (NPS) is active in the network.

Identify the Product ID (PID) and serial number of the Cisco CG-OS router.

Creating a New User Entry in the Active Directory

To create a new user entry for the Cisco CG-OS router in the Windows Active Directory, follow these steps.

-
- Step 1** Open the Active Directory window on the Windows server.
- Step 2** At the Active Directory Users and Computers window, right-click the Users folder and choose **New > User**.



Step 3 At the New Object-User panel that appears, enter the serial number of the Cisco CG-OS router in the following fields: First name, User logon name fields, and the Full name field (preceded by the PID).



Tip

Do not enter colons (:) in the User logon fields. Enter the serial number only. Additional information can be entered in the Full name field.

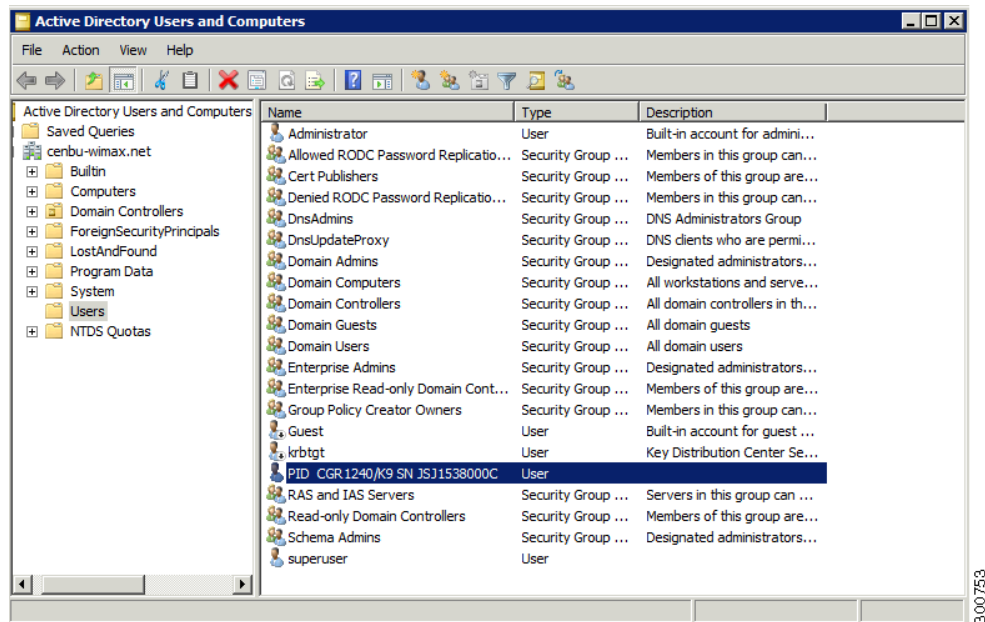
Step 4 Click **Next**.

Step 5 At the password panel that appears, enter *cisco* as the password in both fields and check the **Password never expires** check box. Click **Next**.

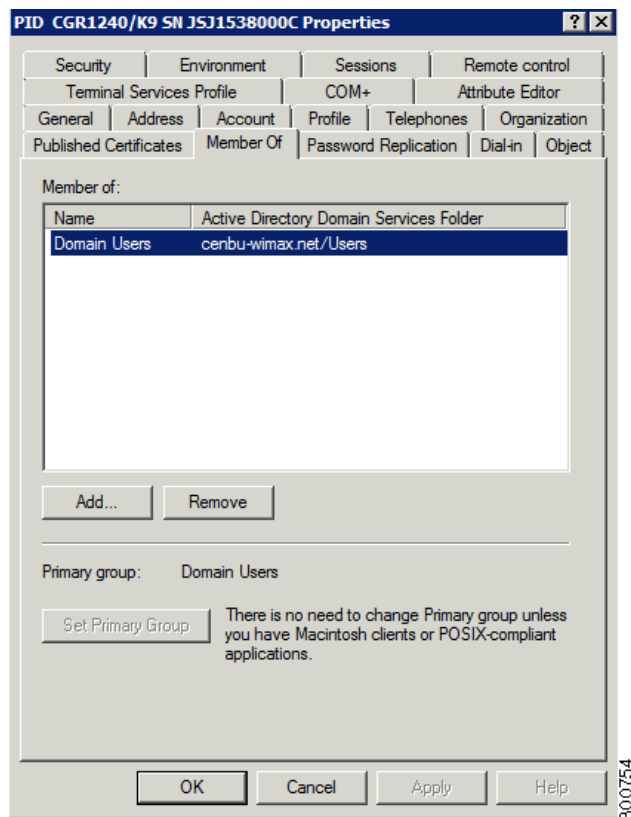
Step 6 At the confirmation panel that appears, do one of the following:

- Click **Finish** to accept the creation of the new user as defined, which appears in the right panel of the Users window.
- Click **Back** to reenter the information if errors exist.

Step 7 At the Users window, right click on the new Name entry and select **Properties**.



- Step 8** At the Properties panel that appears, select the **Member Of** tab. Confirm that the listed Domain matches that value displayed in [Step 3](#), then click **OK**.

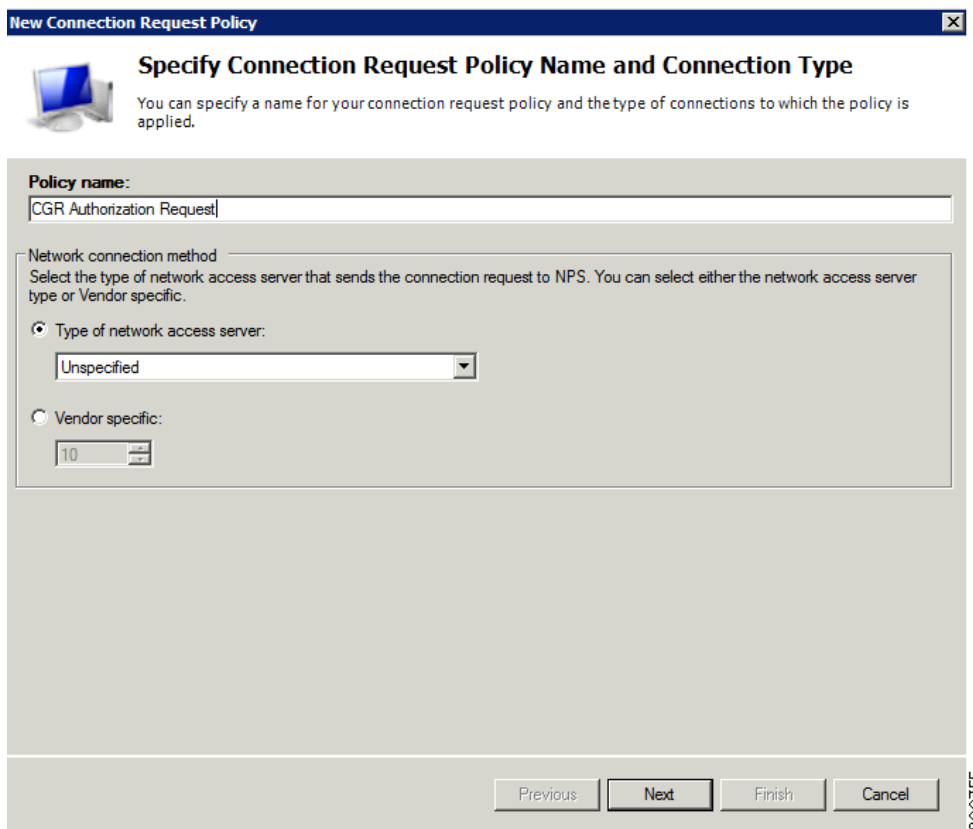


Defining a Connection Policy

Connection request policies allow you to define whether a local or remote RADIUS handles the connection request. Connection policies can also be used to modify the realm name of a system. To define a connection policy for the Cisco CG-OS router, follow these steps.

- Step 1** Log in to the Network Policy Server.
- Step 2** Under the NPS (local) menu, expand the Policies listing and right-click on the **Connection Request Policies** folder and select **New**.

- Step 3** In the New Connection Request Policy window that appears, enter CGR Authorization Request as the policy name. Click **Next**.



The image shows a screenshot of the 'New Connection Request Policy' window. The window has a title bar with the text 'New Connection Request Policy' and a close button. Below the title bar is a section with a computer icon and the heading 'Specify Connection Request Policy Name and Connection Type'. The text below the heading says: 'You can specify a name for your connection request policy and the type of connections to which the policy is applied.' The main area of the window contains a 'Policy name:' label followed by a text box containing 'CGR Authorization Request'. Below this is a section titled 'Network connection method' with the instruction: 'Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific.' There are two radio buttons: 'Type of network access server:' which is selected, and 'Vendor specific:'. The 'Type of network access server:' radio button is followed by a dropdown menu showing 'Unspecified'. The 'Vendor specific:' radio button is followed by a text box containing '10'. At the bottom of the window are four buttons: 'Previous', 'Next', 'Finish', and 'Cancel'. The 'Next' button is highlighted. On the right side of the window, there is a vertical text label '300755'.

New Connection Request Policy

Specify Connection Request Policy Name and Connection Type

You can specify a name for your connection request policy and the type of connections to which the policy is applied.

Policy name:

CGR Authorization Request

Network connection method

Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific.

☒ Type of network access server:

Unspecified

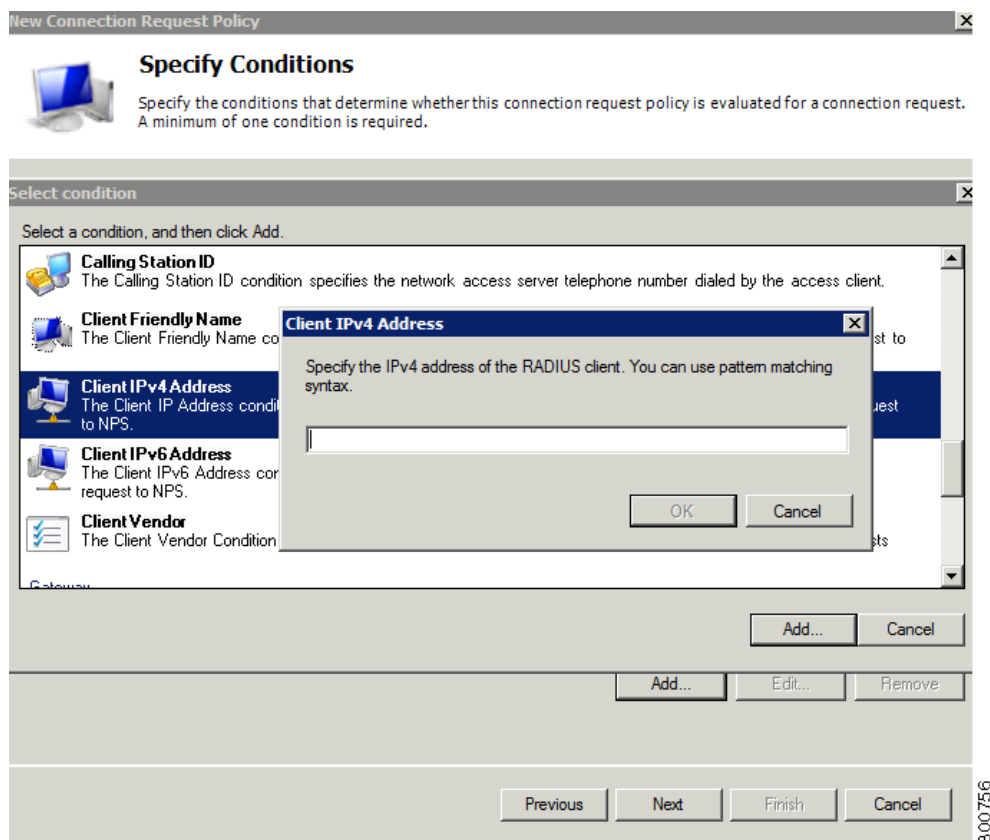
☐ Vendor specific:

10

Previous Next Finish Cancel

300755

- Step 4** At the Specify Conditions window that appears, click **Add**.
- Step 5** In the Select condition window that appears, scroll down to select the **Client IPv4 Address** option from the listing that displays. Click **Add**.
- Step 6** In the Client IPv4 Address panel that appears, enter the IPv4 address of the RADIUS client (RA). Click **OK**.



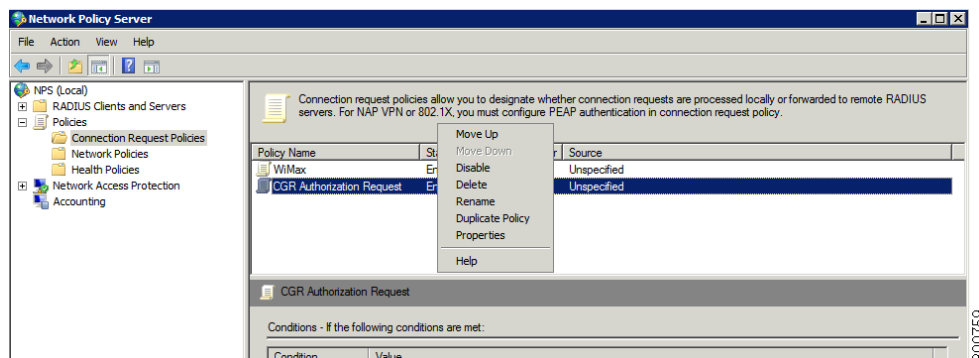
- Step 7** At the Specify Conditions window that appears, select the newly created Client IPv4 Address entry. Click **Next**.

- Step 8** At the Specify Connection Request Forwarding window that appears, keep the default settings. Click **Next** and then click **Finish**.

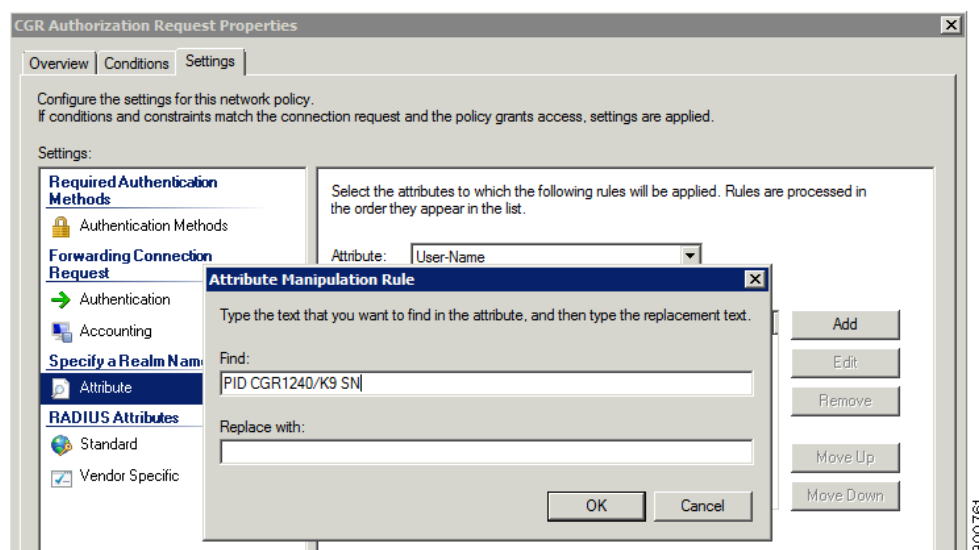
The system returns to the main window.

The screenshot shows a window titled "New Connection Request Policy" with a close button. Inside, the main heading is "Specify Connection Request Forwarding". Below this, a note states: "The connection request can be authenticated by the local server or it can be forwarded to RADIUS servers in a remote RADIUS server group." A sub-note reads: "If the policy conditions match the connection request, these settings are applied." Under the "Settings:" section, there is a tree view on the left with "Forwarding Connection Request" selected, containing "Authentication" (highlighted with a green arrow) and "Accounting". The main area on the right explains: "Specify whether connection requests are processed locally, are forwarded to remote RADIUS servers for authentication, or are accepted without authentication." It features three radio button options: "Authenticate requests on this server" (selected), "Forward requests to the following remote RADIUS server group for authentication:" (with a dropdown menu showing "<not configured>" and a "New..." button), and "Accept users without validating credentials". At the bottom, there are four buttons: "Previous", "Next", "Finish", and "Cancel". A vertical text "300757" is visible on the right edge of the window.

- Step 9** At the Network Policy Server main window, click on the Connection Request Policies folder and then right-click on the **CGR Authorization Request** listing and select **Properties**.

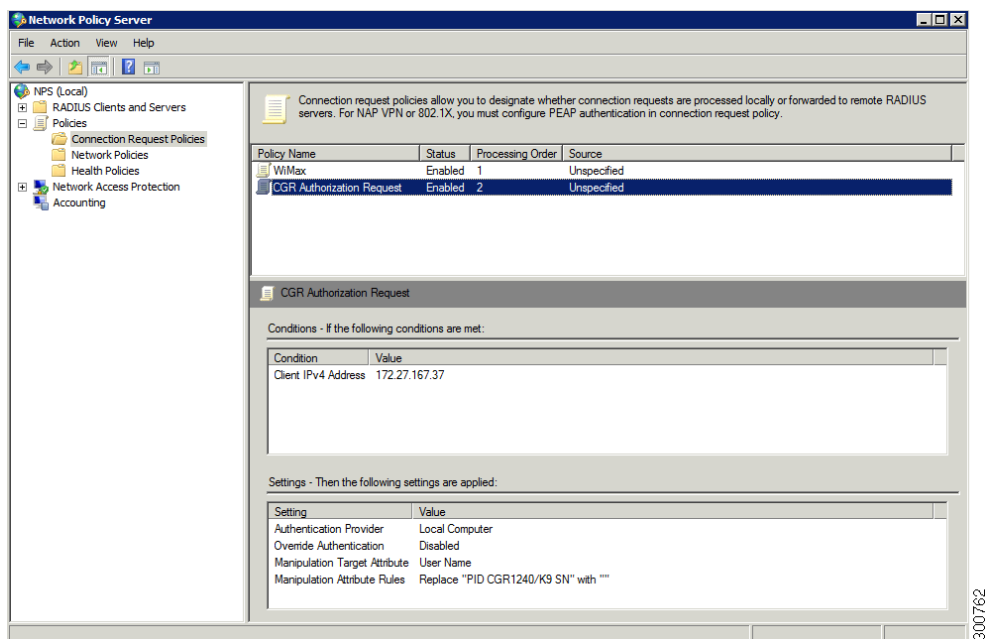


- Step 10** At the CGR Authorization Request Properties window that appears, select the **Settings** tab.



- Step 11** Under Specify a Realm Name (left-pane), click **Attribute**.
- Step 12** In the right-pane of the Settings window, select **User-Name** from the Attribute drop-down menu. Click **Add**.
- Step 13** In the Attribute Manipulation Rule panel that appears, enter the PID string and SN (such as PID CGR1240/K9 SN) in the Find field. Click **OK**.

- Step 14** Click **Apply** and then **OK** to return to a summary of the CGR Authorization Request that shows the Manipulation Attribute Rules in the right panel.



Defining a Network Policy

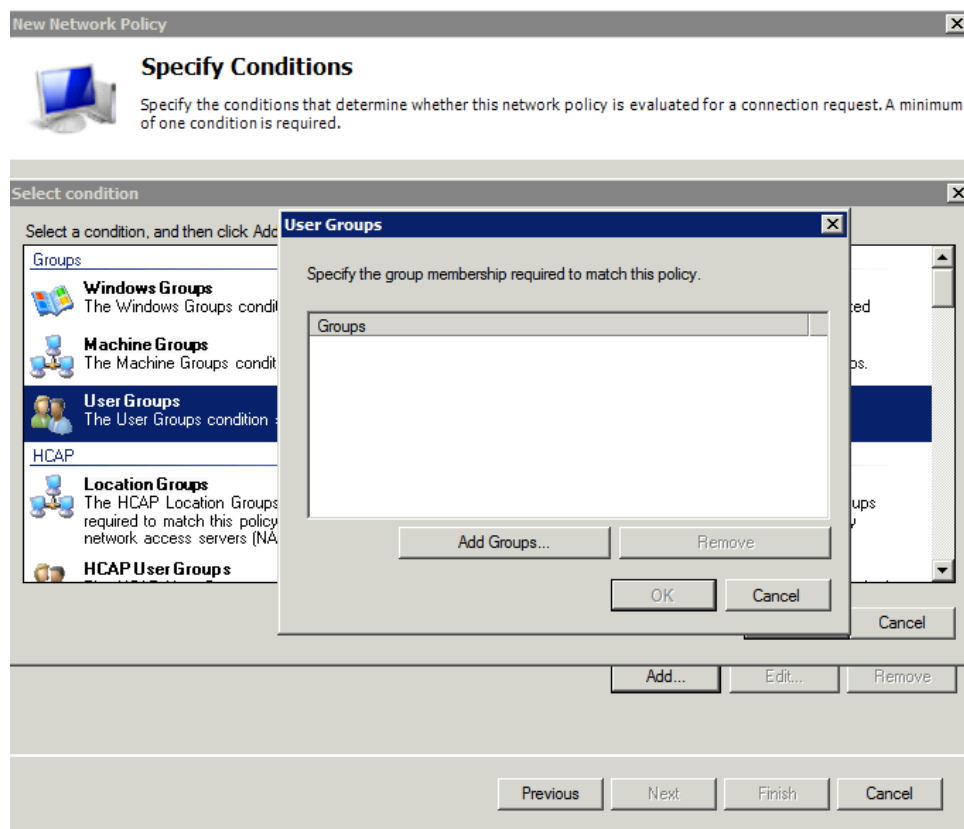
A Network Policy defines which users are authorized to connect to the network and in what circumstances the users can connect to the network.

Additionally, Network Policies allow you to configure the return RADIUS attribute that NPS sends after a successful Cisco CG-OS router authorization.

To define a Network Policy for the Cisco CG-OS router on the NPS, follow these steps.

- Step 1** Under the NPS (local) menu, expand the Policies listing and right-click on the **Network Policies** folder and select **New**.
- Step 2** At the New Network Policy window that appears, enter Authorized CGRs in the Policy name field. Click **Next**.

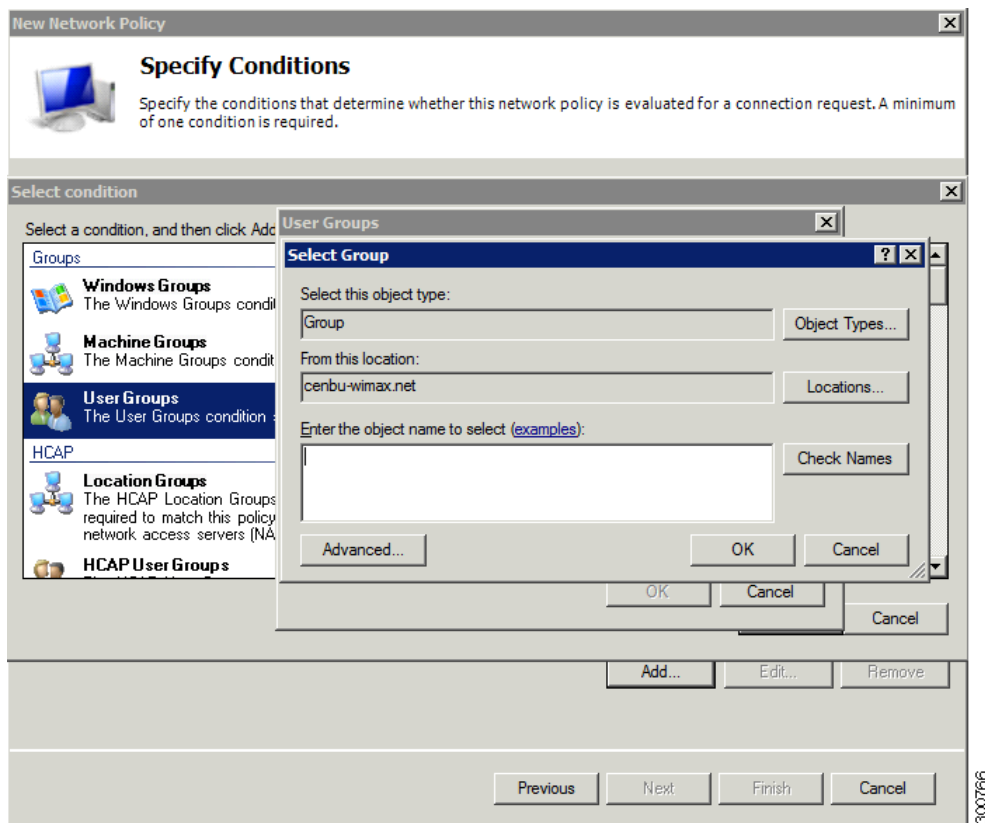
Step 3 At the Specify Conditions window, click **Add**.



Step 4 In the Select condition window that appears, scroll down to select **Users Group** from the listing that displays. Click **Add**.

Step 5 In the User Groups panel that appears, click **Add Groups**.

Step 6 In the Select Group panel that appears, click **Advanced**.



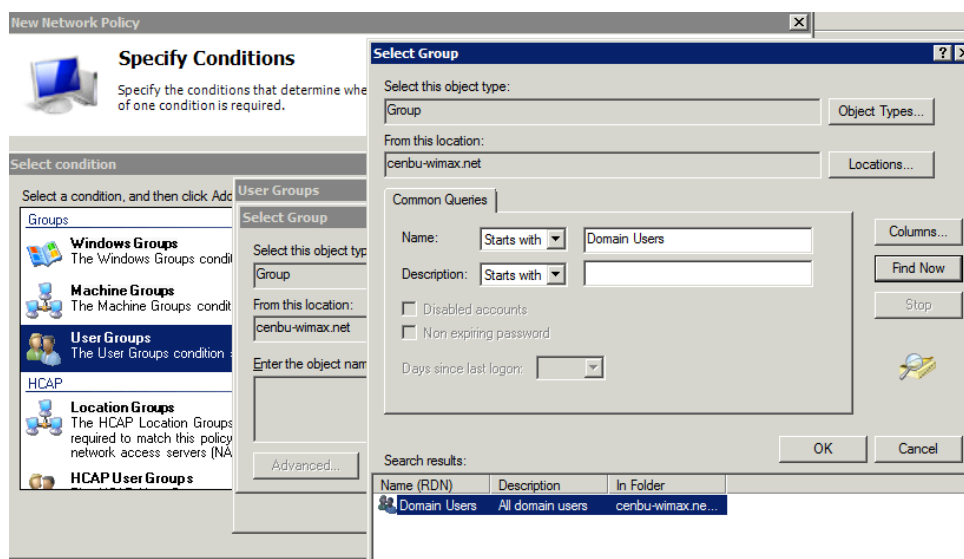
300768

Step 7 In the Select Group search panel that appears, enter Domain Users in the Name field of the Common Queries section of the panel. Click **Find Now**.

The Domain Users entry displays in the Search results panel at the bottom of the screen.

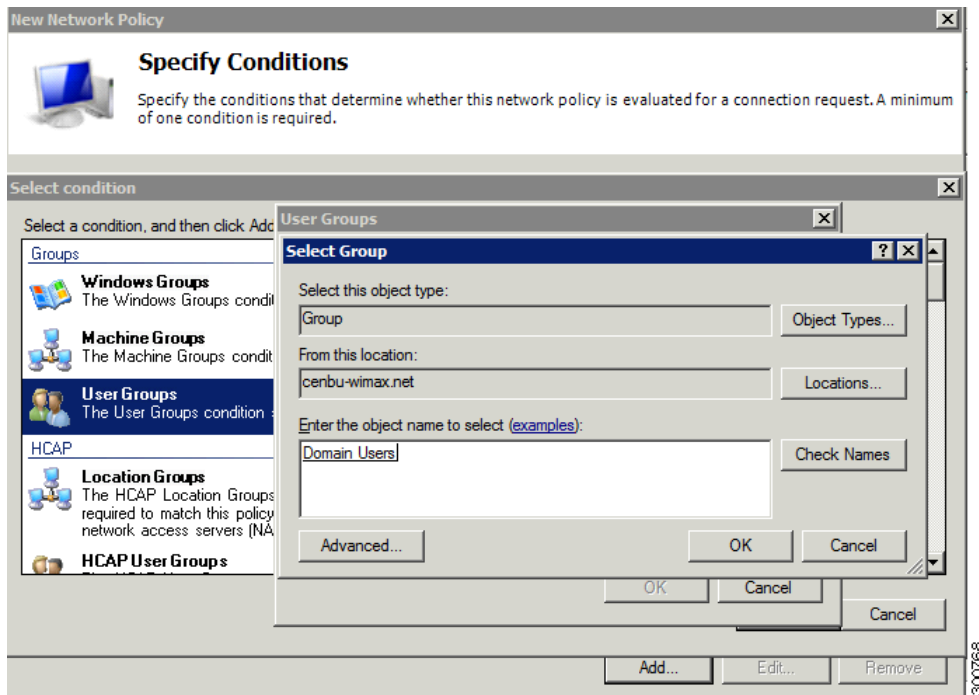


Note The User Group you select is the one created in the [Creating a New User Entry in the Active Directory](#) section above.

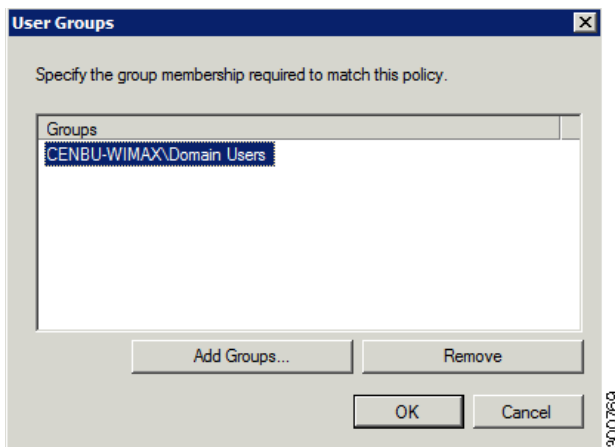


Step 8 Click **OK** to confirm the selection of the Domain Users entry.

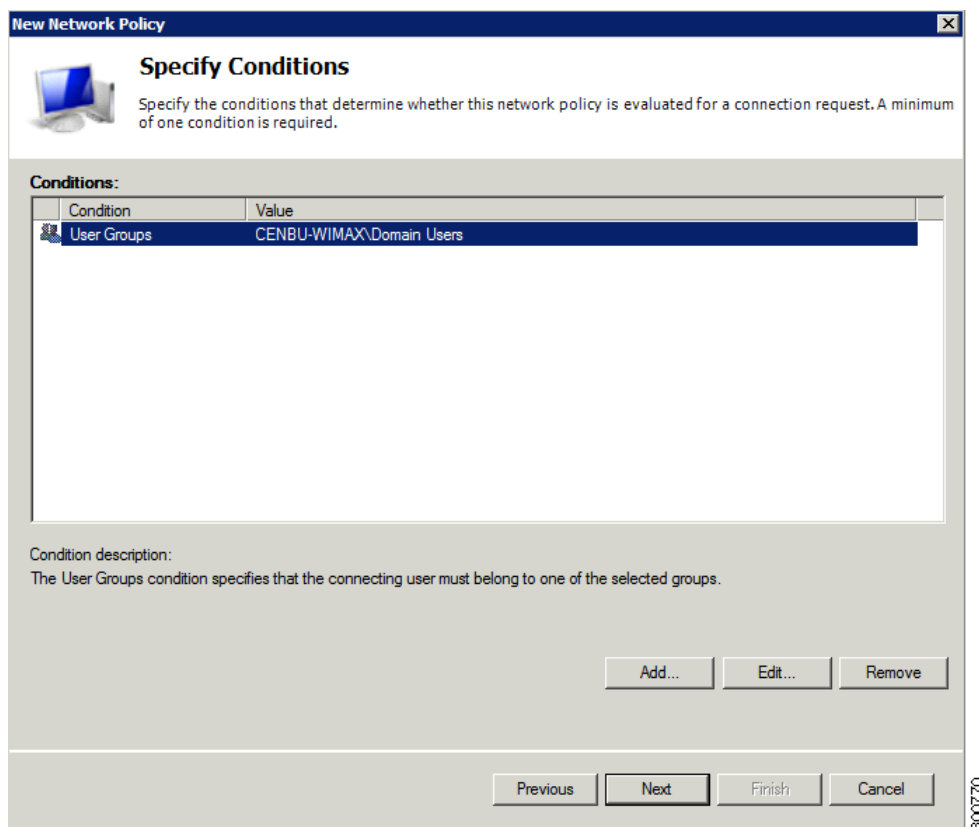
The system returns to the Select Group panel and the Domain Users option now populates the Enter the object name to select field within that window.



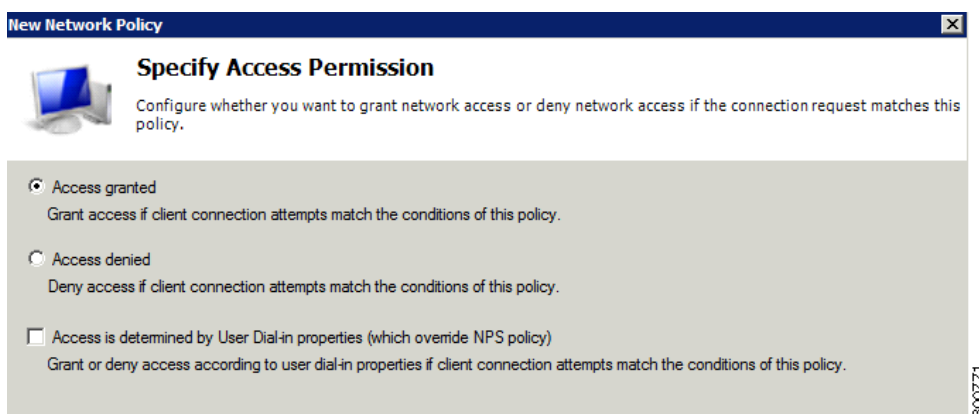
Step 9 When a User Groups panel appears listing the group membership required to match this policy, click **OK**.



- Step 10** At the Specify Conditions window that appears, the newly assigned Domain Users group displays in the Value column. Click **Next**.

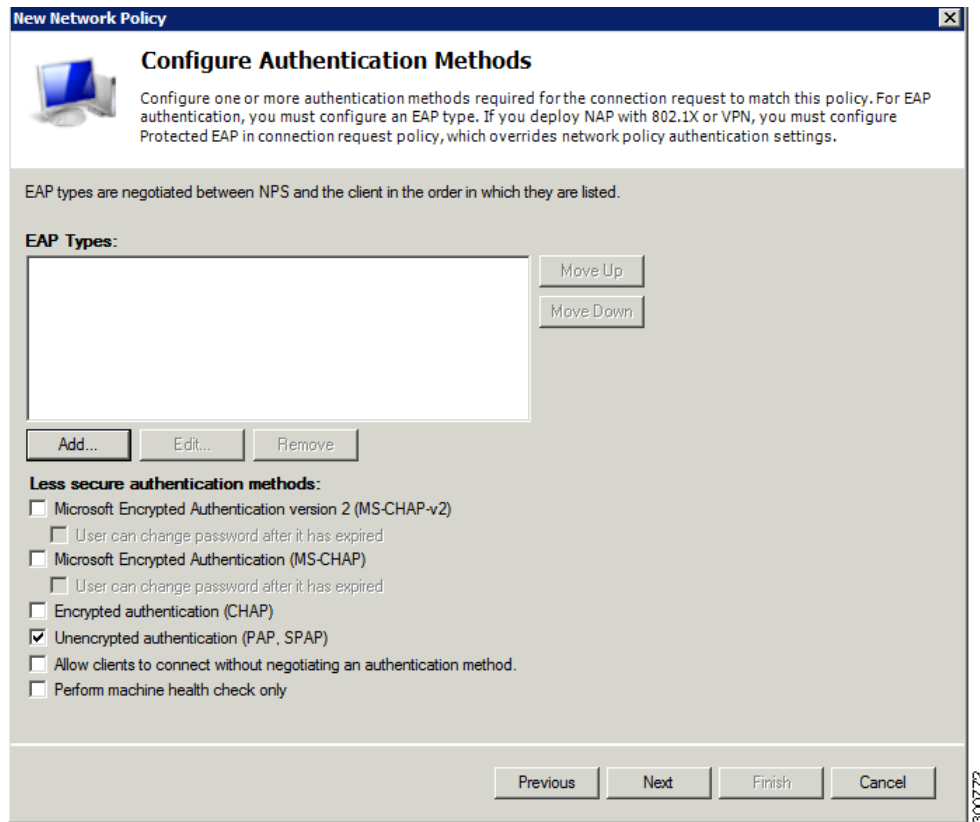


- Step 11** At the Specify Access Permission window, click the **Access Granted** radio button (if not already selected) to allow the Cisco CG-OS router access when its Network Policy matches. Click **Next**.



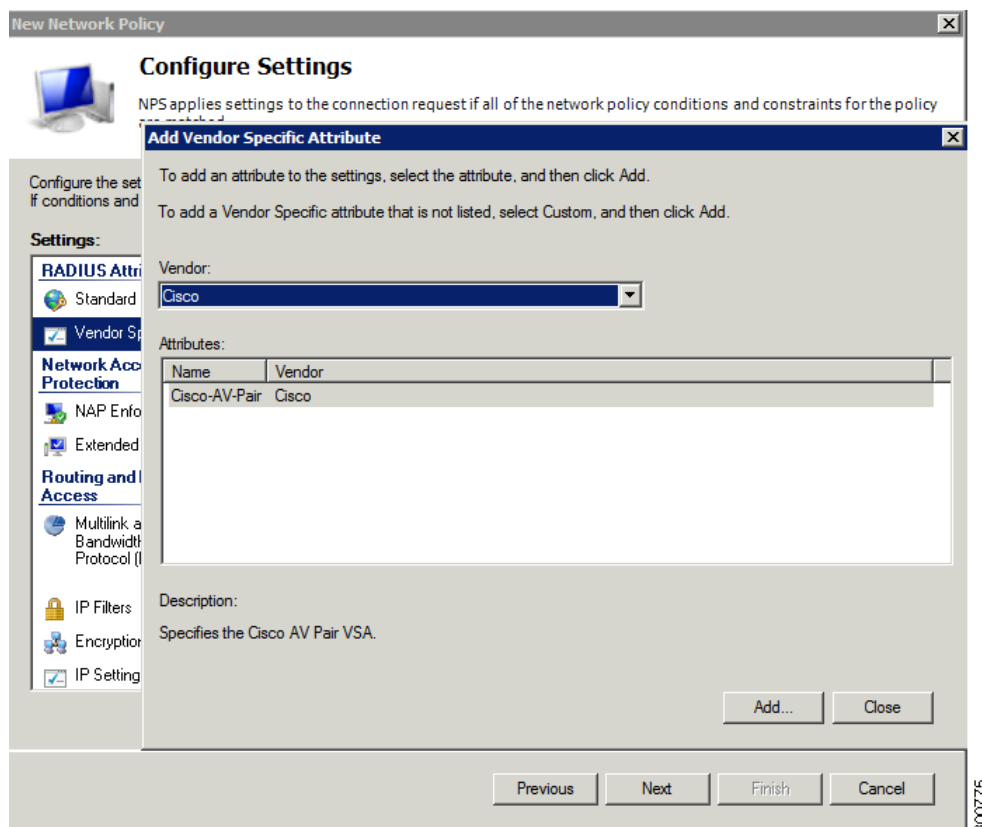
Step 12 At the Configure Authentication Methods window that appears, check the Unencrypted authentication (PAP, SPAP) check box. Uncheck all other check boxes. Click **Next**.

PKI authorization, which is supported on the Cisco CG-OS router, employs Password Authentication Protocol (PAP).



Step 13 At the Configure Constraints window that appears, no configuration is required. Click **Next**.

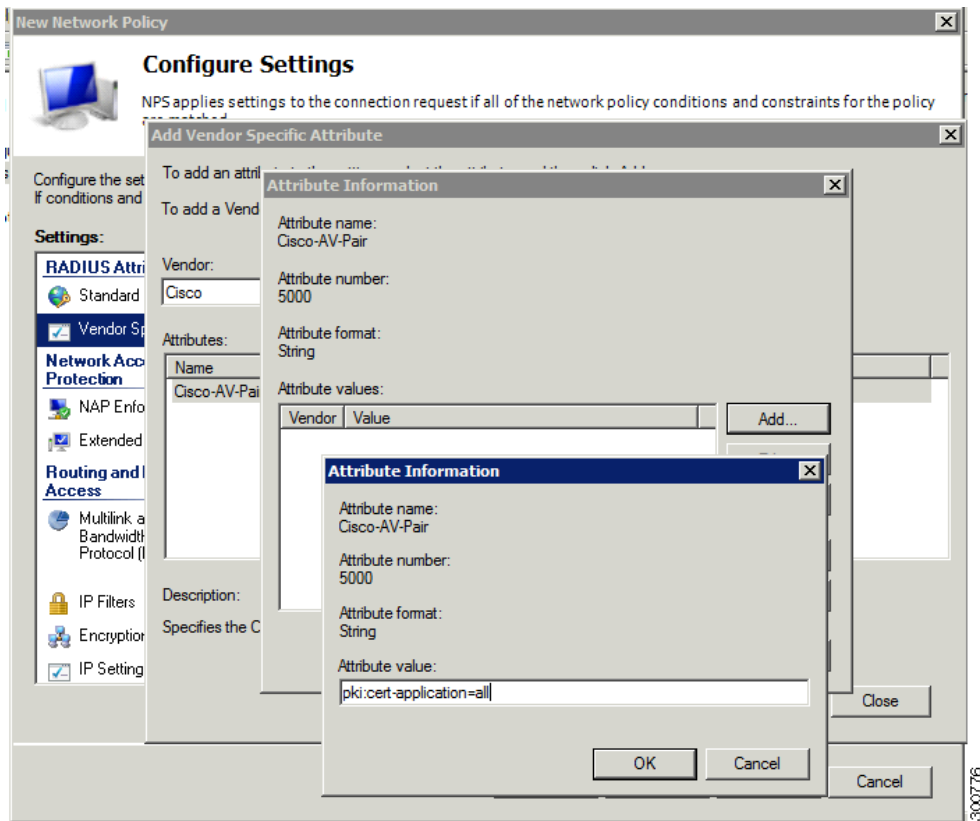
- Step 14** At the Configure Settings window that appears, do the following:
- Select **Vendor Specific** from the Settings listing and click **Add**.
 - At the Add Vendor Specific Attribute panel that appears, select **Cisco** from the Vendor drop-down menu.
The Cisco AV-Pair populates the Attributes section.
 - Click **Add**.



Step 15 At the Attribute Information panel that appears, click **Add** to open a panel to enter the PKI Cisco AV-Pair value, pki:cert-application=all, in the Attribute value field. Click **OK**.

The system returns to the Attribute Information window showing the newly added Cisco AV Pair, pki:cert-application=all, in the Value column of the new attribute.

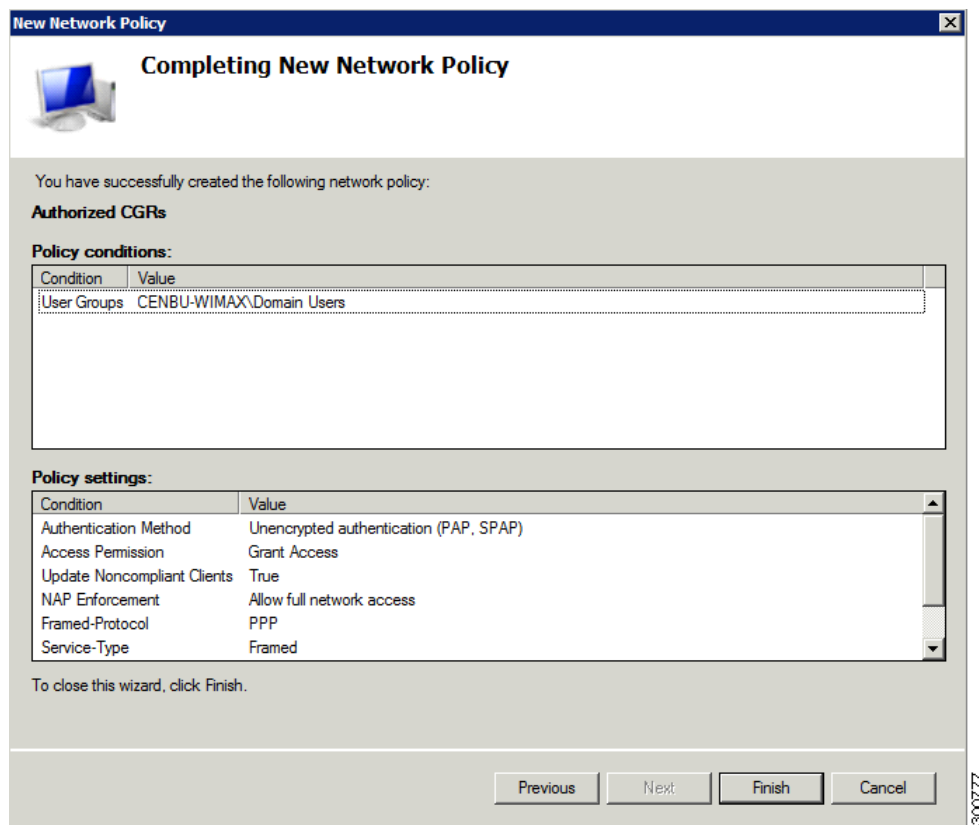
This step ensures that the RADIUS server returns the PKI Cisco AV Pair to the Cisco CG-OS router.

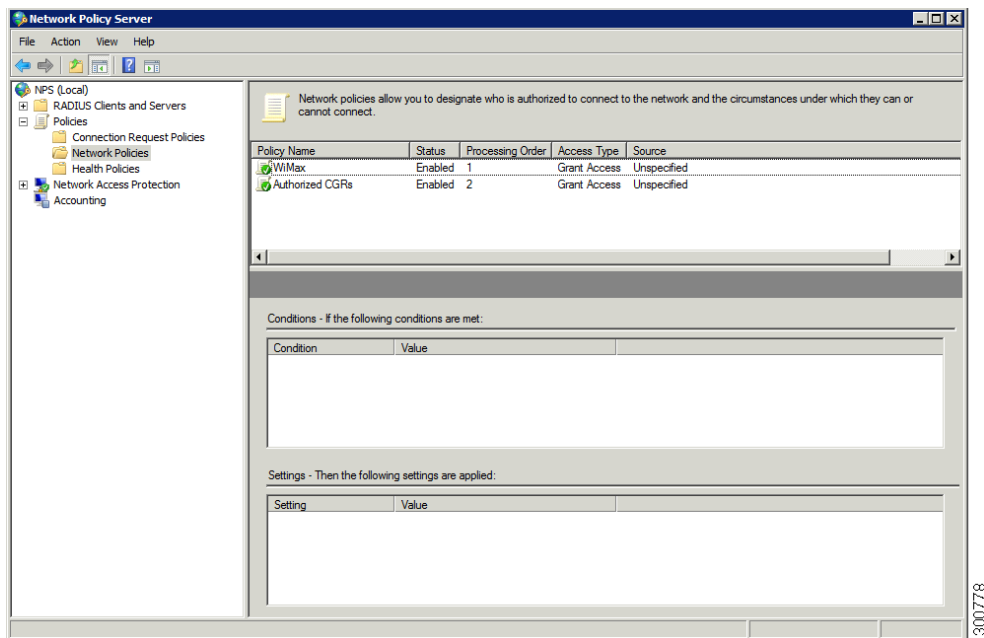


Step 16 Click **OK**. Click **Close**.

Step 17 At the **New Network Policy > Configure Settings** window that appears, click **Next**.

- Step 18** At the Completing New Network Policy window that appears, click **Finish**.
In the Network Policy window that appears, Authorized CGRs appears as a supported policy.





Viewing the Log for Cisco CG-OS Router Authentication Details

Listed below is an example of details that appear in the log after a successful authentication of the Cisco CG-OS router using PAP, which servers the role of PKI authorization for the RA.

```
Log Name:          Security
Source: Date:      Microsoft-Windows-Security-Auditing
Date:             02/18/2012 5:50:12 PM
Event ID:         6278
Task Category:    Network Policy Server
Level:            Information
Keywords:         Audit success
User:             N/A
Computer:         cenbu-wimax.net
Description:
Network Policy Server granted full access to a user because the host
met the defined health policy.

User:
    Security ID:          CENBU\JSJ1538000C
    Account Name:         JSJ1538000C
    Account Domain:       CENBU
    Fully Qualified Account Name: cenbu.wimax.net/Users/PID:CGR1240/K9
    SN:JSJ1538000C

Client Machine:
    Security ID:          NULL SID
    Account Name:         -
    Fully Qualified Account Name:-
    OS-Version:          -
    Called Station Identifier: -
    Calling Station Identifier: -
```



```

Account Name: -

NAS:
  NAS IPv4 Address: 172.27.165.157
  NAS IPv6 Address: -
  NAS Identifier: -
  NAS Port-Type: -
  NAS Port: -
-
RADIUS Client:
  Client Friendly Name: AL_3825
  Client IP Address: 172.27.165.157

Authentication Details:
Connection Request Policy Name: CGR Authorization Request
Network Policy Name: Authorized CGRs
Authentication Provider: Windows
Authentication Server: CENBU-RSA-CA.cenbu.wimax.net
Authentication Type: PAP
EAP Type:
Account Session Identifier:

Quarantine Information:
Result: Full Access
Extended-Result: -
Session Identifier:
Help URL
System Health Validator Results(s): -

```

Importing Cisco CG-OS Router Identifying Information into the NPS Active Directory (AD) Database

Listed below is a Visual BASIC script that can import the product ID (PID) and serial number (SN) of the Cisco CG-OS Router (CGR) into the NPS AD database.

To do so, the script reads a CSV file named SN.txt and then creates a user entry in the AD. Each line of the CSV file represents a distinct Cisco CG-OS router, which is identified by its PID and SN. The PID and SN are separated by a comma.

```

' Sample Visual Basic script to load CGR entries in a file called "SN.txt" into the
' Active 'Directory database
'
' Each line in "SN.txt" corresponds to 1 CGR and has the format of <pid>, <sn>
' where pid is the Product ID such as CGR1240/K9
'      sn is the unit's serial number such as JSJ15380000
'
'
Const ADS_UF_NORMAL_ACCOUNT      = &h0200
Const ADS_UF_DONT_EXPIRE_PASSWD = &h10000
Const SN_TXT_FILENAME = "SN.txt"
Dim oContainer 'Parent container of new user
Dim oUser 'Created user
Dim oFile
Dim oFileStream
Dim cgrEntry
'
'Subroutine to create a user entry in the AD
'

```

```

Sub createUser(oContainer, pid, sn)
    Dim oUser
    username = "PID:"&pid&" SN:"&sn

    'Create user
    set oUser = oContainer.Create("User", "CN="&username)

    'Assign properties values to user
    oUser.put "displayName", username
    oUser.Put "sAMAccountName", sn
    oUser.Put "givenName", pid
    oUser.Put "name", username
    oUser.Put "userPrincipalName", sn"@cenbu.wimax.net"
    oUser.SetInfo

    'Finally, set the password and enable user
    oUser.setpassword "cisco"
    oUser.Put "userAccountControl", _
        ADS_UF_NORMAL_ACCOUNT Or ADS_UF_DONT_EXPIRE_PASSWD
    oUser.SetInfo
    Set oUser = Nothing
End Sub

'Get parentcontainer
Set oContainer = GetObject("LDAP://CN=Users,DC=cenbu,DC=wimax,DC=net")

'Looping through the entries in the CSV file
Set oFile = CreateObject("Scripting.FileSystemObject")
Set oFileStream = oFile.OpenTextFile(SN_TXT_FILENAME, 1)
do while oFileStream.AtEndOfStream <> true

    'Split the CSV based on ,
    cgrEntry = Split(oFileStream.ReadLine, ",", 2)

    'Remove any spaces
    cgrEntry(1) = Replace(cgrEntry(1), " ", "")

    'WScript.Echo "Adding CGR entry for PID: " & cgrEntry(0) & " SN: " & cgrEntry(1)
    createUser oContainer, cgrEntry(0), cgrEntry(1)

    count = count + 1
loop

'Clean up
oFileStream.close
Set oContainer = Nothing

WScript.Echo count & " entries added to Active Directory"

```

Configuring Cisco ACS

BEFORE YOU BEGIN

Verify that you are operating with the following minimum Cisco ACS software requirements:
Cisco ACS software, version 4.2 or Cisco ACS appliance version 5.2

DETAILED STEPS

To create a group of authorized Cisco CG-OS routers (CGR) and users on the Cisco ACS, do the following:

- Step 1** Log on to Cisco ACS.
- Step 2** At the opening window, click **Group Setup** (navigation pane).
- Step 3** At the Group Setup window, do the following:
 - In the Select pane (left pane), select **2: Group 2** from the Group drop-down menu.
 - To create a new group, click **Rename Group**.
 - In the Renaming Group window that appears, enter **2: Authorized CGRs** in the Group field.
 - To save the entry, Click **Submit**.
- Step 4** At the Group Setup window, select the newly created group (2: Authorized CGRs) from the Group drop-down menu. Click **Edit Settings**.

- Step 5** At the Edit Settings window, select **RADIUS (Cisco IOS 6.0)** from the Jump To drop-down menu and then do the following:
- Scroll down to the Cisco IOS/PIX 6.x RADIUS Attributes section and do the following:
 - Check the [009\001] cisco-av-pair check box.
 - Enter the following into the box below: pki:cert-application=all
 - Click **Submit**.
- Step 6** To add a Cisco CG-OS router as a user to Cisco ACS, click **User Setup** (navigation pane).
- Step 7** To add the PID and SN for the Cisco CG-OS router in the User field, click **Add/Edit**.
- Step 8** To save the entry, click **Add/Edit**.
- Step 9** At the User Setup window that appears, do the following:
- In the Real Name field, enter the PID and SN number (such as PID:CGR1240/K9 SN:JSJ1538000B). This value is the same name used to create the entry.
 - In the Password and Confirm Password fields, enter **cisco**.
 - In the Group to which the user is assigned drop-down menu, select **2: Authorized CGRs**.
 - Click **Submit**.

- Step 10** Repeat [Step 9](#) for each User that you want to create.

Related Documentation

For information on supporting systems referenced in this certificate guide, see the following documentation on Cisco.com:

[Cisco 1000 Series Connected Grid Routers](#)

[Cisco 3945 Integrated Services Router](#)

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the What's New in Cisco Product Documentation as an RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.

This document is to be used in conjunction with the documents listed in the [Related Documentation](#) section.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

No combinations are authorized or intended under this document.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2012 Cisco Systems, Inc. All rights reserved

