

# OEAP 602 Remote LAN 802.1x (Port 4) with Wired IP Phone and Laptop behind the IP Phone

---

- [Introduction](#) on page 1
- [Components Used](#) on page 1
- [Topology](#) on page 2
- [Configuration](#) on page 2

## Introduction

OEAP 602 Remote LAN 802.1x (Port 4) with Wired IP Phone and Laptop behind the IP Phone

## Components Used

1. WLC 5508 running 7.3.101.0
2. OEAP 602I
3. Windows 7 Client
4. Cisco IP Phone 7975
5. ACS 5.2

## Topology

## Configuration

STEP 1:

Creating a Remote LAN for OEAP Wired Clients (Port 4)

<input type="checkbox"/> WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
<input type="checkbox"/> <a href="#">1</a>	Remote LAN	oeap_remote	---	Enabled	802.1X

OEAP 602 Remote LAN 802.1x (Port 4) with Wired IP Phone and Laptop behind the IP Phone

**General** **Security** **Advanced**

Profile Name	oeap_remote
Type	Remote LAN
SSID	oeap_remote
Status	<input checked="" type="checkbox"/> Enabled
Egress Interface	management ▼

**General** **Security** **Advanced**

**Layer 2** **Layer 3** **AAA Servers**

Layer 2 Security	802.1X ▼
MAC Filtering	<input type="checkbox"/>

**General** **Security** **Advanced**

**Layer 2** **Layer 3** **AAA Servers**

Select AAA servers below to override use of default servers on this WLAN

**Radius Servers**

	<b>Authentication Servers</b>	<b>Accounting Servers</b>
	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled
Server 1	IP:192.168.154.171, Port:1812	None
Server 2	None	None
Server 3	None	None
Server 4	None	None
Server 5	None	None
Server 6	None	None

**General** **Security** **Advanced**

Allow AAA Override	<input type="checkbox"/> Enabled	<b>DHCP</b>
Enable Session Timeout	<input type="checkbox"/>	DHCP Server <input type="checkbox"/> Override
Override Interface ACL	IPv4 None	DHCP Addr. Assignment <input type="checkbox"/> Required
Client Exclusion <sup>3</sup>	<input type="checkbox"/> Enabled	
Maximum Allowed Clients <sup>8</sup>	0	

OEAP 602 Remote LAN 802.1x (Port 4) with Wired IP Phone and Laptop behind the IP Phone

STEP 2: Setting up wired ip phone for 802.1X authentication

On the phone go to Settings > Security Configuration > 802.1X Authentication > Device Authentication > Enabled

you do not need to enable password for EAP-MD5

the Phone does EAP-TLS authentication

### 802.1X Authentication and Status

The 802.1X Authentication and 802.1X Authentication Status menus allow you to enable 802.1X authentication and monitor its progress. These options are described in [Table 4-22](#).

You can access the 802.1X Authentication settings by pressing the **Settings** button and choosing **Security Configuration > 802.1X Authentication and Security Configuration > Authentication Status**.

**Table 4-21 802.1X Authentication Settings**

Option	Description	To Change
Device Authentication	Determines whether 802.1X authentication is enabled: <ul style="list-style-type: none"> <li>• <b>Enabled</b>—Phone uses 802.1X authentication to request network access.</li> <li>• <b>Disabled</b>—Default setting in which the phone uses CDP to acquire VLAN and network access.</li> </ul>	<ol style="list-style-type: none"> <li>1. Choose <b>Settings &gt; Security Configuration &gt; 802.1X Authentication &gt; Device Authentication</b>.</li> <li>2. Set the Device Authentication option to Enabled or Disabled.</li> <li>3. Press the <b>Save</b> softkey.</li> </ol>
EAP-MD5	Specifies a password for use with 802.1X authentication using the following menu options (described in the following rows): <ul style="list-style-type: none"> <li>• Device ID</li> <li>• Shared Secret</li> <li>• Realm</li> </ul>	Choose <b>Settings &gt; Security Configuration &gt; 802.1X Authentication &gt; EAP-MD5</b> .
	Device ID—Derivative of the phone's model number and unique MAC address displayed in this format: CP-<model>-SEP-<MAC>	Display only—Cannot configure.
	Shared Secret—Choose a password to use on the phone and on the authentication server. The password must be between 6 and 32 characters, consisting of any combination of numbers or letters. <b>Note</b> If you disable 802.1X authentication or perform a factory reset of the phone, the shared secret is deleted.	<ol style="list-style-type: none"> <li>1. Choose <b>EAP-MD5 &gt; Shared Secret</b>.</li> <li>2. Enter the shared secret.</li> <li>3. Press <b>Save</b>.</li> </ol> See the " <a href="#">Troubleshooting Cisco Unified IP Phone Security</a> " section on page 9-8 for assistance in recovering from a deleted shared secret.
	Realm—Indicates the user network domain, always set as <i>Network</i>	Display only—Cannot configure.

### STEP3: Getting chained cert for the Cisco 7975 phone for EAP-TLS authentication

Note: Set the remote LAN to no security. Let the phone grab an ip address and register to the call manager. From the call manager enable the web mode. Navigate to the https page of the phone and grab the device cert of the phone using your web browser.



## This Connection is Untrusted

You have asked Firefox to connect securely to **192.168.75.111**, but we can't confirm that the connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove they are going to the right place. However, this site's identity can't be verified.

### What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is impersonating the site, and you shouldn't continue.

Get me out of here!

### ▼ Technical Details

192.168.75.111 uses an invalid security certificate.

The certificate is not trusted because no issuer chain was provided.  
The certificate is not valid for any server names.

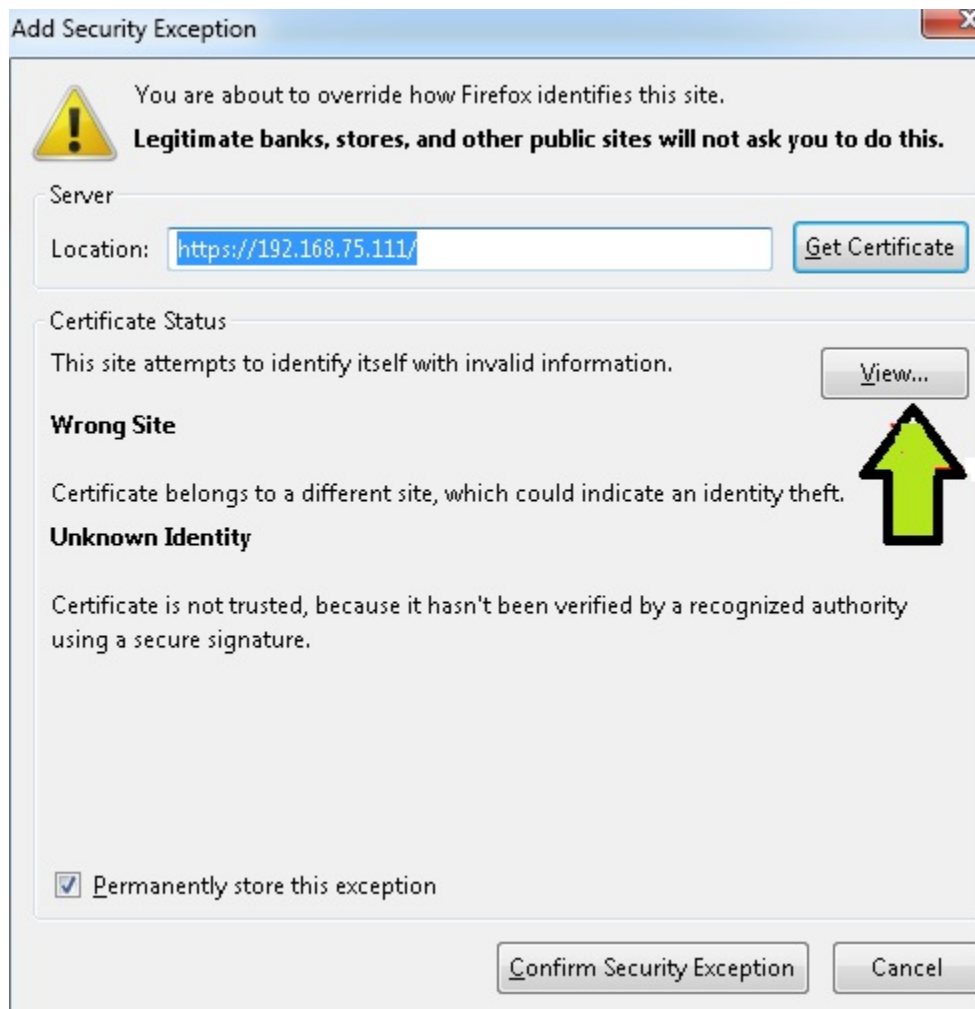
(Error code: sec\_error\_unknown\_issuer)

### ▼ I Understand the Risks

If you understand what's going on, you can tell Firefox to start trusting this site's identification. **You trust the site, this error could mean that someone is tampering with your connection.**

Don't add an exception unless you know there's a good reason why this site doesn't use secure identification.

Add Exception...

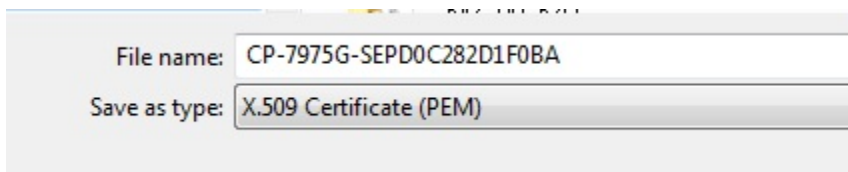


Click on the Details tab and hit Export

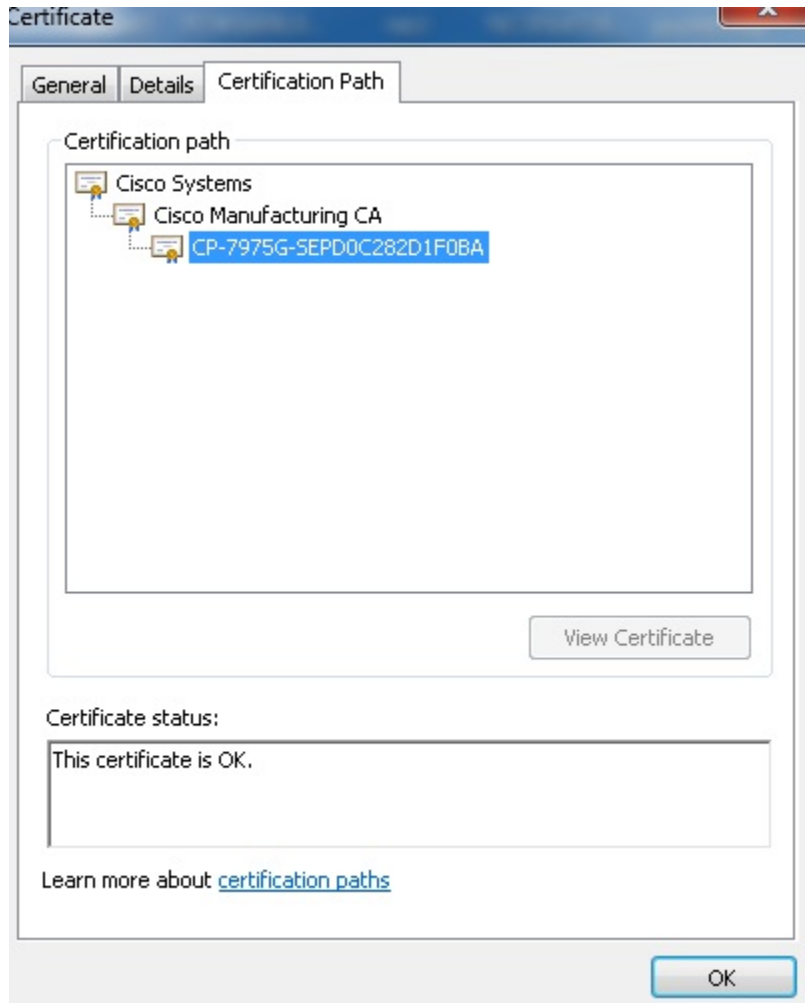




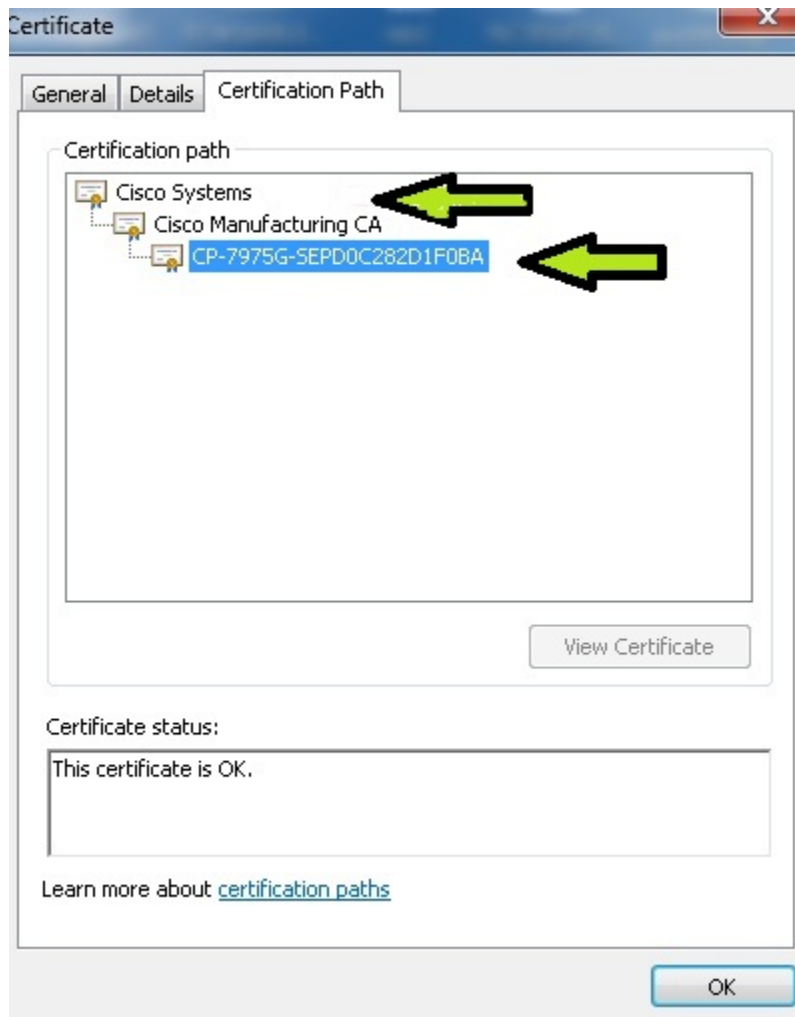
Save the cert on the local machine



Open the cert by double clicking on it and Click on the 'Certification Path'

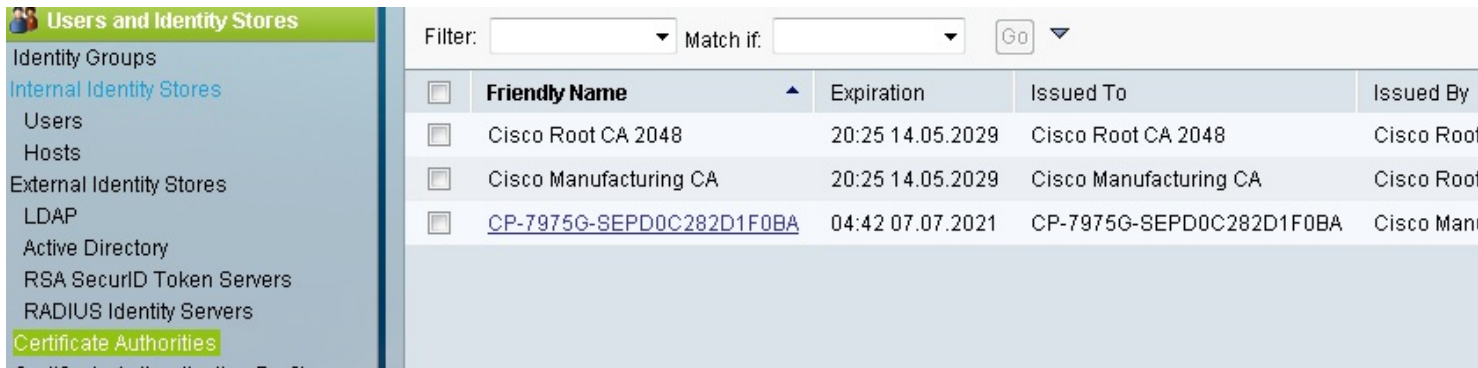


you can see the chained cert of the device. you already have the device cert. From this view save the Intermediate root and the Root CA cert.



Now you have a 3 certs, CP-7975G-SEPD0C282D1F0BA, Cisco Manufacturing CA and Cisco Systems.

STEP 4: Import these certs on the ACS Certificate Authorities for EAP-TLS authentication of 7975 IP Phone.



The screenshot shows the 'Users and Identity Stores' configuration page in Cisco ACS. The left sidebar lists various identity stores, with 'Certificate Authorities' highlighted. The main area displays a table of Certificate Authorities with columns for 'Friendly Name', 'Expiration', 'Issued To', and 'Issued By'. There are three entries in the table, with the third one being a link to a specific certificate.

<input type="checkbox"/>	Friendly Name	Expiration	Issued To	Issued By
<input type="checkbox"/>	Cisco Root CA 2048	20:25 14.05.2029	Cisco Root CA 2048	Cisco Root
<input type="checkbox"/>	Cisco Manufacturing CA	20:25 14.05.2029	Cisco Manufacturing CA	Cisco Root
<input type="checkbox"/>	<a href="#">CP-7975G-SEPD0C282D1F0BA</a>	04:42 07.07.2021	CP-7975G-SEPD0C282D1F0BA	Cisco Man

When you add the cert check the 'trust for Client with EAP-TLS' option

**Issuer**

**Friendly Name:** CP-7975G-SEPD0C282D1F

**Description:**

**Issued To:** CP-7975G-SEPD0C282D1F0BA


**Issued By:** Cisco Manufacturing CA

**Valid From:** 04:32 07.07.2011

**Valid To (Expiration):** 04:42 07.07.2021

**Serial Number:** fc9b0000000a729b

**Usage**

Trust for client with EAP-TLS:  

**Certificate Revocation List Configuration**

Download CRL:

CRL Distribution URL:

Retrieve CRL:  Automatically 5 Minutes

Every 0 Weeks

If download failed, wait 10 Minutes before retry.

Bypass CRL Verification if CRL is not Received:

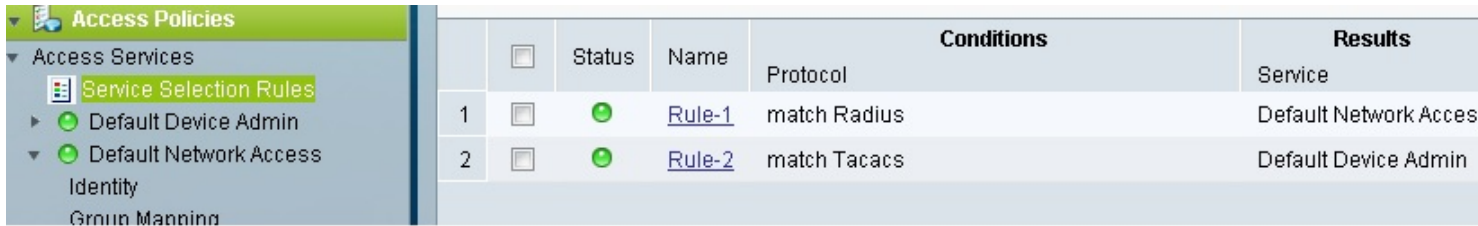
Ignore CRL Expiration:

**\* = Required fields**

## STEP 5: Configuring Access Policies on ACS

From Service Selection Rules check Rule based result selection.

I have configured Rule 1 for Radius with service set to Default Network Access and Rule 2 for TACACS with service set to Default Device Admin

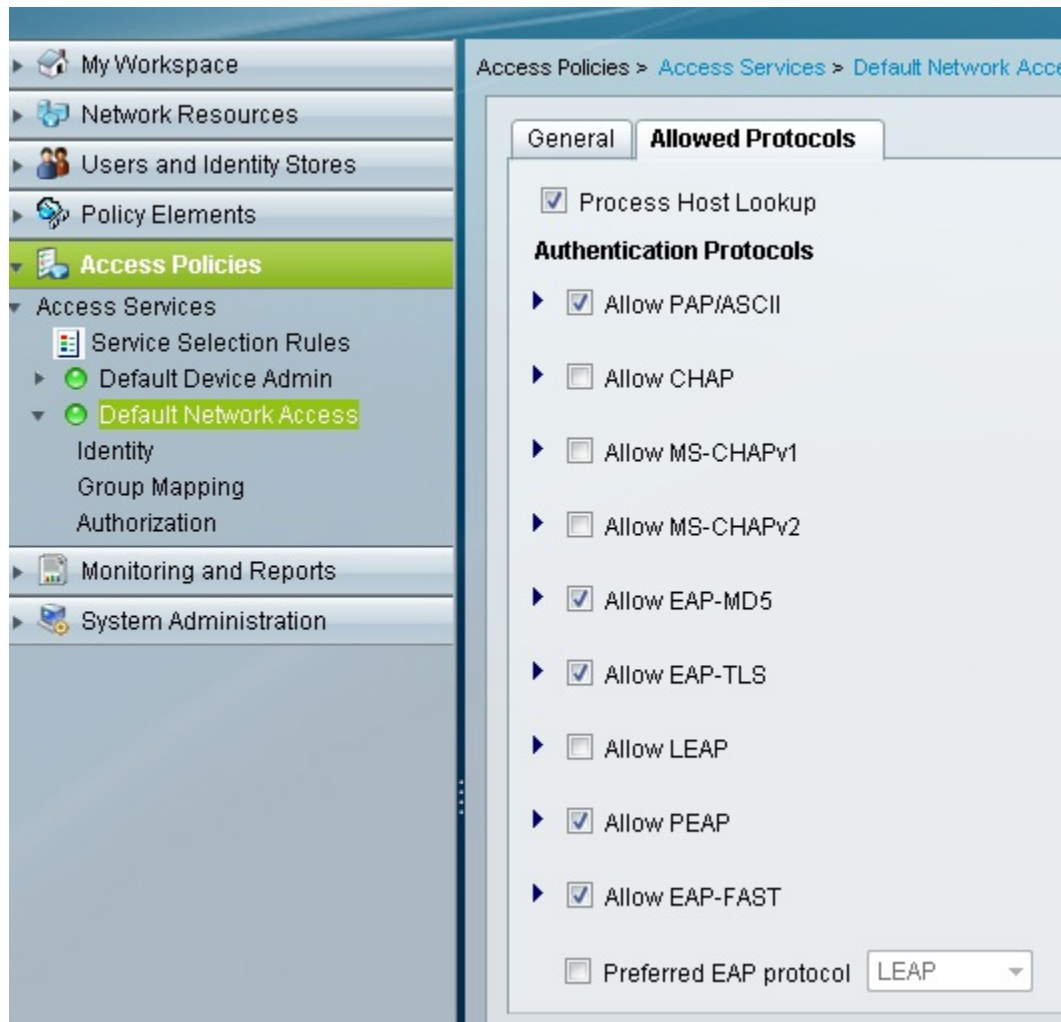


The screenshot shows the 'Access Policies' configuration page. On the left is a navigation tree with 'Access Policies' expanded to show 'Access Services', 'Service Selection Rules', 'Default Device Admin', and 'Default Network Access'. The main area displays a table of rules:

	<input type="checkbox"/>	Status	Name	Protocol	Conditions	Results
1	<input type="checkbox"/>	●	<a href="#">Rule-1</a>	match Radius		Default Network Acces
2	<input type="checkbox"/>	●	<a href="#">Rule-2</a>	match Tacacs		Default Device Admin

Under Default Network Access

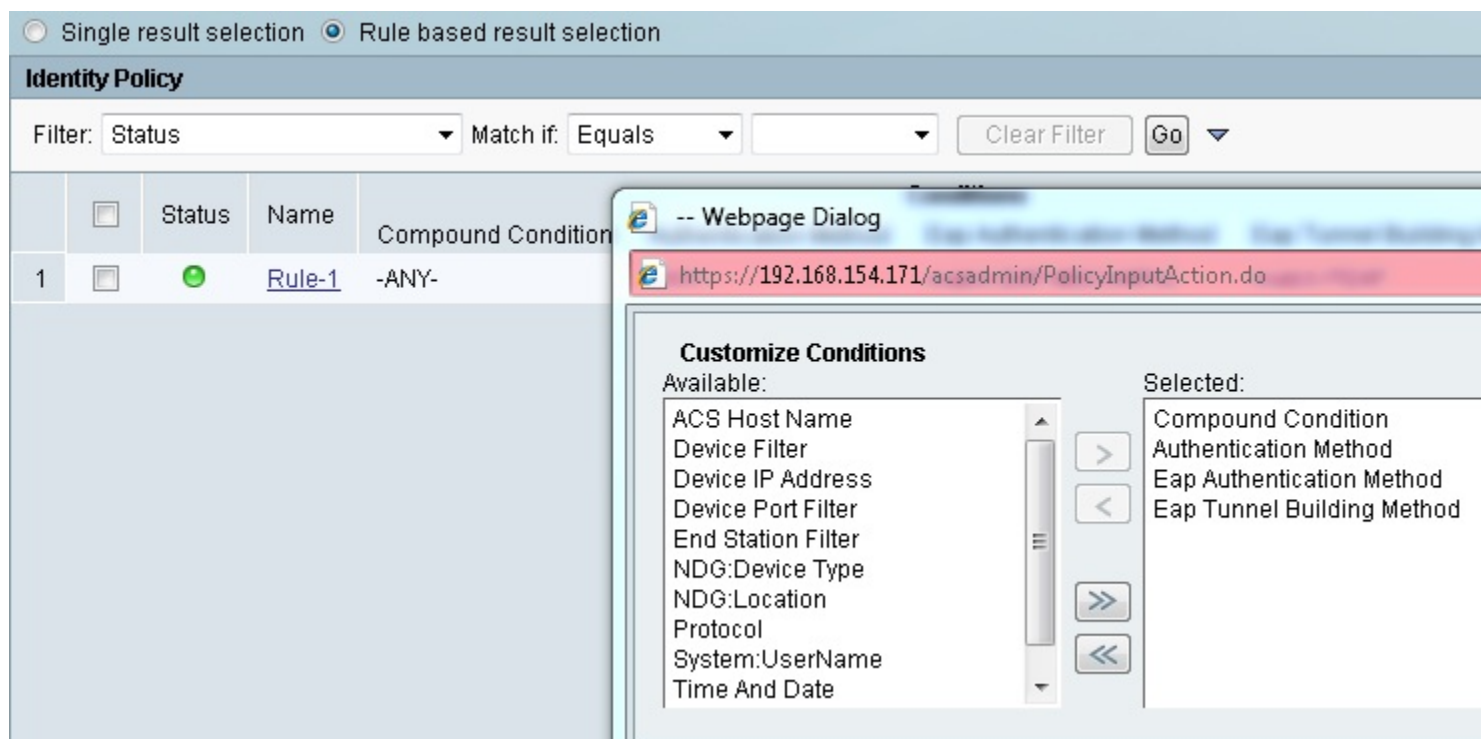
Allow the necessary protocols



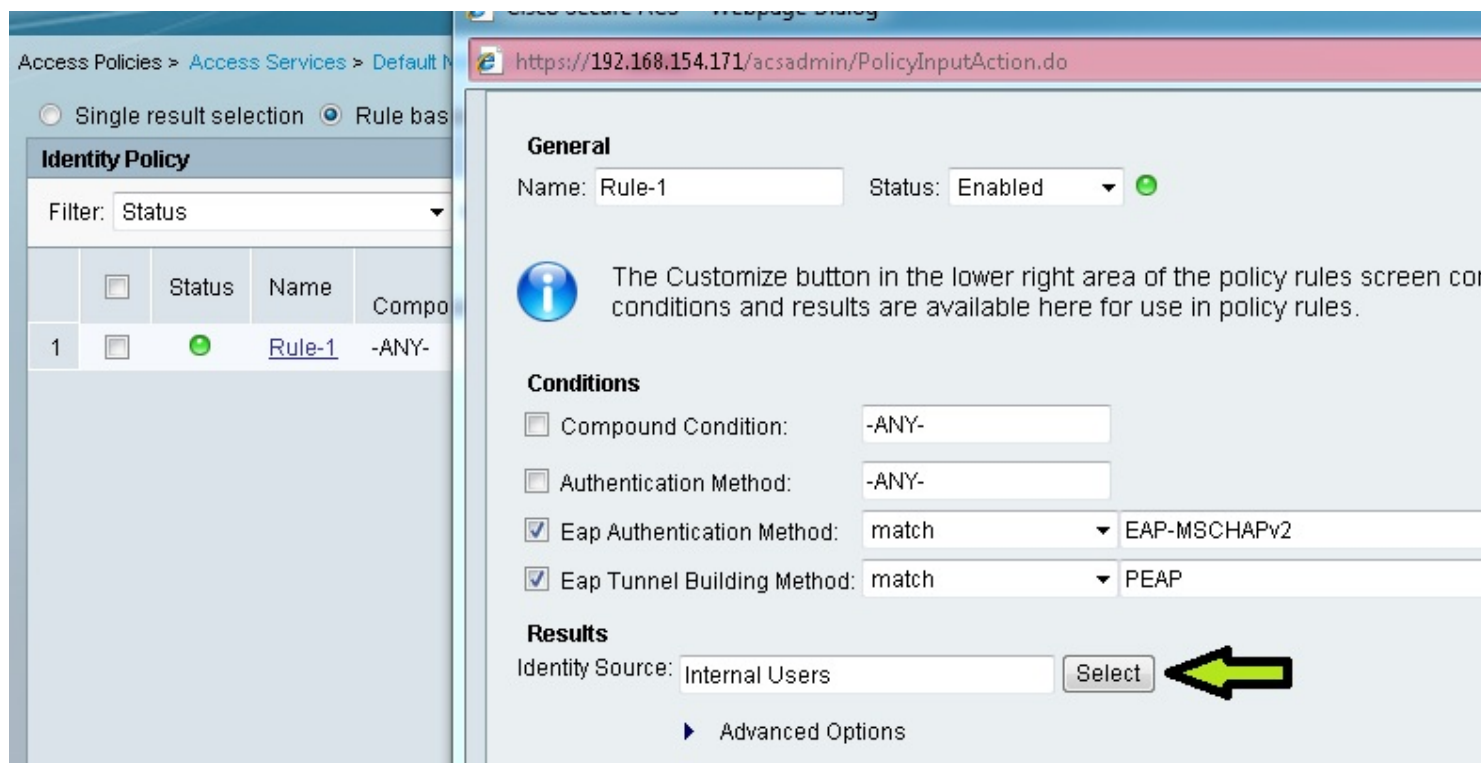
Select Default Network Access > Identity and click on Rule based result selection

Hit Customize to add 'EAP Authentication Method' and 'EAP Tunnel Building Method'





Create a new Rule which matches PEAP and MSCHAP-v2 for Windows 7 authentication which points to the Internal Users Identity Source



I have the Default rule at the end pointing to CN username for EAP-TLS authentication of the 7975 IP Phone

## OEAP 602 Remote LAN 802.1x (Port 4) with Wired IP Phone and Laptop behind the IP Phone

The screenshot displays the Cisco Secure ACS configuration interface. At the top, there are two radio buttons: "Single result selection" (unselected) and "Rule based result selection" (selected). Below this is the "Identity Policy" section, which includes a "Filter" dropdown set to "Status" and a "Match if:" field. A table lists the identity policies:

	<input type="checkbox"/>	Status	Name	Compound Cond
1	<input type="checkbox"/>	●	<a href="#">Rule-1</a>	-ANY-

A "Webpage Dialog" window is overlaid on the configuration. The title bar reads "Cisco Secure ACS -- Webpage Dialog". The address bar shows "https://192.168.154.171/acsadmin/PolicyInputAction.do". The main content area is titled "Results" and contains the following elements:






- Identity Source:
- 
- ▶ [Advanced Options](#)

At the bottom of the dialog are "OK" and "Cancel" buttons. The status bar at the bottom of the dialog shows "https://192.168.154.171/acsadmin/Po" and "Internet | Protected Mode: Off".

### STEP 6: Setting up wired 802.1X authentication for Windows 7

STEP 7: Enable 802.1X authentication on the Remote LAN and sit tight

Below you can see successful authentication for 7975 phone using x509\_PKI and Windows 7 using PEAP (EAP-MSCHAPV2)

Logged At	RADIUS Status	NAS Failure	Details	Username	MAC/IP Address	Access Service	Authentication Method	Network Device
Nov 7, 12 8:18:48.436 PM	✓		 <a href="#">user1</a>	<a href="#">user1</a>	<a href="#">c0-c1-c0-88-3a-1e</a>	<a href="#">Default Network Access</a>	<a href="#">PEAP (EAP-MSCHAPv2)</a>	<a href="#">5508-7</a>
Nov 7, 12 8:03:33.236 PM	✗		 <a href="#">user1</a>	<a href="#">user1</a>	<a href="#">c0-c1-c0-88-3a-1e</a>	<a href="#">Default Network Access</a>	<a href="#">PEAP (EAP-MSCHAPv2)</a>	<a href="#">5508-7</a>
Nov 7, 12 8:02:10.786 PM	✗		 <a href="#">host/wirelesspc2-PC</a>	<a href="#">host/wirelesspc2-PC</a>	<a href="#">c0-c1-c0-88-3a-1e</a>	<a href="#">Default Network Access</a>	<a href="#">PEAP (EAP-MSCHAPv2)</a>	<a href="#">5508-7</a>
Nov 7, 12 8:00:45.706 PM	✗		 <a href="#">host/wirelesspc2-PC</a>	<a href="#">host/wirelesspc2-PC</a>	<a href="#">c0-c1-c0-88-3a-1e</a>	<a href="#">Default Network Access</a>	<a href="#">PEAP</a>	<a href="#">5508-7</a>
Nov 7, 12 6:47:07.370 PM	✓		 <a href="#">CP-7975G-SEPD0C282D1F0BA</a>	<a href="#">CP-7975G-SEPD0C282D1F0BA</a>	<a href="#">d0-c2-82-d1-f0-ba</a>	<a href="#">Default Network Access</a>	<a href="#">x509_PKI</a>	<a href="#">5508-7</a>