CHAPTER 3

Bring Your Own Device—Unified Device Authentication and Consistent Access Experience

This chapter focuses on identifying and authenticating users who connect to the network with different devices and at different places. The devices can be categorized as laptops, desktops, and smart phones and the different places could be on a campus or at a remote location. This chapter first outlines the core components that are needed to identify and authenticate users and then gives significant details on how to configure the core components that authenticate and identify users. This chapter is intended to build on existing best practices of authentication. Where needed this chapter provides references to additional information.

Executive Summary

Drivers for Bring Your Own Device—Unified Device Authentication and Consistent Access Experience

The rapid propagation of mobile devices and their introduction into the enterprise workplace has caused a paradigm shift in regards to the term “end points” and to the phrase “being at work”. The distinction between a device used exclusively for “work” and a device used exclusively for “personal use” is fading, a trend often referred to as Bring Your Own Device (BYOD). Additionally some enterprise environments are shifting away from providing their employees with a “standard imaged computing device” to an environment where the employee owns and controls the computing device that is used for work. The challenge for IT organizations is to provide the end user with the freedom to use any device while enforcing stringent security policies to protect corporate intellectual property when the user device joins the secure campus network. In addition to providing a proper security policy, it is also imperative to provide a consistent access experience.

There is also a need to provide the end user and end point devices with transparent access to corporate resources while enforcing the proper security policy for wired, wireless, and remote user authentication. The location of the end point and user (from a logical perspective as well as a physical perspective) should have no bearing on the experience that the user observes. The user should have the capacity to seamlessly move from wired, wireless, and remote locations, where each environment is employing different technologies. The user should not have to distinguish or understand the technology being

adopted that is providing authentication and access to the secure corporate network. Any user should be able to connect from any device at any time. The security controls in place, however, must be able to understand how the employee is connecting and apply the proper security policy for that connection.

The following are the challenges faced by an IT organization today:

- How to provide Secure Campus Wireless Access
- How to provide Secure Campus Wired Access
- How to provide Remote VPN Access

Secure Campus Wireless Access

Challenges to achieving secure access to the corporate campus network via a wireless (IEEE 802.11) connection using 802.1x authentication

Utilizing native operating system supplicants requires IT organizations to maintain and support a broad matrix of operating systems and 802.1x supplicants. Adding to the complexity, when an end point device physically or logically moves to other wireless networks such as airports, home networks, coffee shops, as well as other secure campus networks, additional network profiles are added to the end point device's configuration. This sprawl of network profiles on each device locally can directly affect the user experience by forcing users to know the network to which they want to connect. IT organizations are challenged with maintaining the integrity of the secure campus network profile for their organization's configuration which resides locally on the end point device for each user.

In addition to the many usability issues in utilizing native 802.1x supplicants in a secure campus environment, as previously stated, there are also severe security policy violations that can manifest.

With the proliferation of Personal Area Networks (PANs) and Wireless Personal Area Networks (WPANs), the need to have control of the end point's security policy becomes even more critical to the integrity of the IT organization's resources and intellectual property. An end point device may be authenticated and have access to the secure corporate network and at the same time have other devices tethered to it using different wired and wireless technologies. It is imperative to maintain the integrity of the data as it terminates on the end point device. In a second example, imagine a scenario where a user is physically connected via a wired connection in the secure campus network and simultaneously associated to a different wireless network. It could be argued that this end point device is now logically acting as a gateway or router as part of the secure campus network.

Over time, as these end point devices physically move and become part of a wide variety of disparate networks, all with unique security policies, a major problem manifests itself again from both a security and usability perspective. As the "scan list" within these 802.1x supplicants begins to grow, it is imperative for the IT organization to enforce and maintain a security policy for these end point devices. As mentioned earlier, the explosion and onset of PANs and WPANs increases the need to maintain control of the policies for these devices, which one could argue are becoming the edge of the network and, in some situations, these devices are becoming a forwarding engine on the network.

In many customer environments users are instructed to access a Web page/wiki or other resource in order to obtain the 802.1x settings to use (EAP-PEAP, EAP-TTLS, etc.). Granted, there is a solution for such settings for IT-owned assets as the IT organization has the ability to roll out pre-configured end point images, but as mentioned previously the pre-deployment of such images may not pertain to personal devices that users continue to bring into enterprise environments.

Secure Campus Wired Access

Challenges to achieving secure network access to the corporate campus network via a wired (IEEE 802.3) connection using 802.1x authentication

Gaining access to a secure campus network via an 802.1x wired connection has some challenges that are similar to those discussed in Secure Campus Wireless Access, but it also has its own set of unique challenges. Again, using the native supplicants provided by Microsoft® can be a great operational challenge. For example, the native 802.1x wired supplicant for Windows XP is not enabled by default, thus the end user must enable this service manually. As discussed earlier, this type of configuration change on the client can be solved by the IT organization rolling out pre-deployed images to IT end point assets; however, this may not solve the problem for non-IT owned assets. As suggested earlier, the paradigm shift that is taking shape in the industry is forcing IT organizations to support a wide variety of consumer-based products and provide enterprise-class security.

Some of the same usability and security issues discussed with accessing the secure corporate campus network via native 802.1x supplicants also exist for accessing the secure corporate campus network via 802.1x native wired supplicants.

A security policy within an organization encompasses a broad spectrum of entities, ranging from enforcing help desk social conduct, logical security, management policies on all enterprise devices, physical security, etc. The need to secure access ports is crucial. For some organizations, providing port-level security for each access port becomes a compliance issue.

Remote VPN Access

Challenges to achieving secure network access to the corporate campus network via a virtual private network (VPN) connection using both x.509 digital certificates and two-factor authentication

Just as the lines are being blurred between personal and work end point devices, so are the lines between how users access the secure corporate campus network via wireless, wired, and remote locations.

Traditionally, users that were on a public network would need to understand that they are not on the corporate network, manually launch a VPN software client, choose the correct location to terminate the VPN connection (head-end) based on proximity, and then finally authenticate.

This should no longer be the case. In order for users to access a resource on the secure corporate campus, the user should not have to take preemptive measures to do so. The user should not have to know the exact network where the resources they are attempting to access reside. Instead, the client end point should dynamically detect that the user is attempting to access a resource on a remote campus network and build the appropriate secure connection.

Challenges in Distributing Digital Certificates

Many IT organizations would like to provide identity and authentication services which include both digital certificates and a form of two-factor authentication for remote user access. However deploying client certificates to remote VPN end users can be extremely challenging. One of the challenges with deploying digital certificates to client end points accessing the campus network remotely is that the user and end point device may need to access the company's certification authority (CA) server directly (after being authenticated to the corporate campus network) in order to manually install the client certificate. This method requires the end user to manually install the client certificate while ensuring the certificate is installed in the proper certificate store on the local end point. As mentioned earlier, from a usability perspective, the user should not be required to know where on the end point device a digital certificate should be installed.

Deploying digital certificates on non-PC based devices can require a different process as many of these devices do not natively support all the features and functionality in order to create/download and install digital client certificates in the same manner as traditional PC-based devices.

Some end point devices do not support Simple Certificate Enrollment Protocol (SCEP) out of the box.

For example, in order for users to install digital client certificates using SCEP on Apple iOS devices, the IT administrator needs to manually create the configuration profile using the iPhone Configuration Utility and distribute the profile to user devices via E-mail, USB, or Web deployment. For additional information regarding the iPhone configuration utility, see the Apple Configuration Utility (http://developer.apple.com/library/ios/#featuredarticles/FA_iPhone_Configuration_Utility/Introduction/Introduction.html). The iPhone configuration utility can be downloaded from:

- iPhone Configuration Utility 3.3 for Mac OS X: http://support.apple.com/kb/DL851
- iPhone Configuration Utility 3.3 for Windows: http://support.apple.com/kb/DL926

Tradition full-featured PC-based devices are more apt to take advantage of the many services, such as Microsoft's NDES, to provide certificate enrollment. However, with the onset of so many non-PC-based mobile devices on the market today, it cannot be assumed that natively these devices can interoperate with many of the enterprise services currently deployed.

This solution provides guidance on enabling a unified access system in order to address the issue of achieving secure access to the corporate campus network via a wireless (IEEE 802.11) and wired (IEEE 802.3) connection using 802.1x authentication. This design also presents a migration from the existing Microsoft 802.1x native supplicants to a Cisco solution in order to solve many of the challenges facing a secure wireless and wired solution for campus and remote locations.

Consistent Access Experience provides design guidance on implementing a consistent network access experience on the campus or when remotely accessing the campus network.

This solution discusses the migration from the existing native 802.1x supplicants to the Cisco AnyConnect 3.0 Secure Mobility Client and describes the dynamic Web deployment of the Cisco AnyConnect 3.0 Secure Mobility including client profiles.

The solution discusses how the Cisco AnyConnect Secure Mobility Client, along with other integral products such as the Cisco Secure ACS, Cisco's next generation Layer 2 Access Switches, Cisco ASA 5500, and Cisco Access Points, enable end users and devices with secure and unified access to the corporate campus network using wired, wireless, and remote technologies.

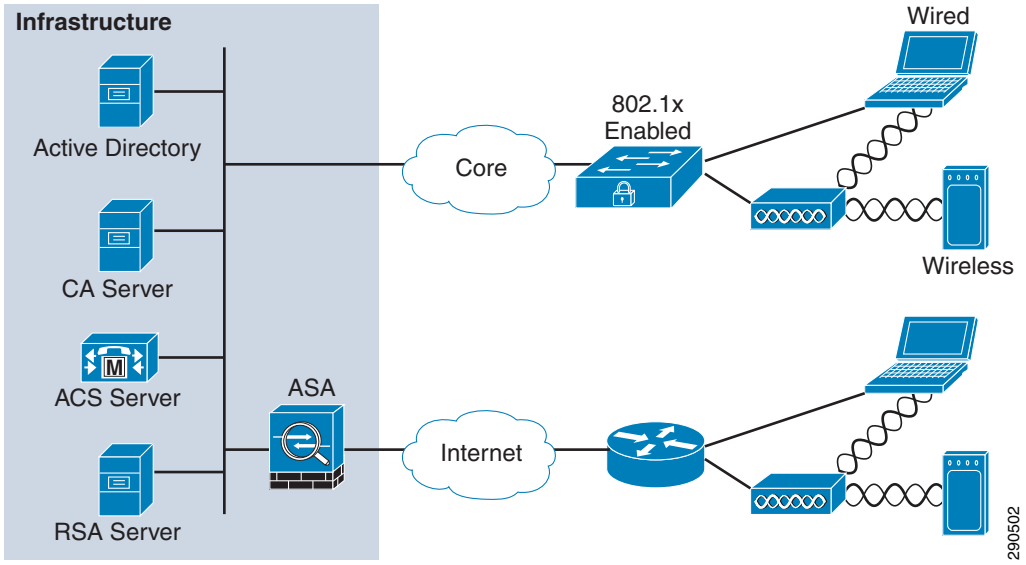
Unified Device Authentication

The main objectives of unified device authentication are:

- Enforce control on all the access layer switches that users use to connect to the network, including both wired and wireless users.
- Maintain centralized access control policy.

Traditionally wireless users are subjected to authentication when they access the network. Wired users connect and obtain their IP address without any kind of authentication. However, in certain organizations they are required by compliance to enforce access controls for wired users also. Unified Device Authentication helps organizations to authenticate both wired and wireless users using the same system and in the same way.

Figure 3-1 Core Components of Unified Device Authentication



This chapter focuses on properly designing and configuring the following items to enable an enterprise to utilize a Unified Device Authentication solution:

- Cisco AnyConnect Client
- Cisco Network Access Manager (NAM)
- Microsoft Active Directory (AD)
- RSA SecurID Authentication Server
- Microsoft Certificate Authority (CA)
- Cisco Adaptive Security Appliance (ASA)
- Cisco Secure Access Control System (ACS)

Active Directory Environment

In the Unified Access Solution, Microsoft Active Directory (AD) has been implemented to authenticate user credentials. To obtain more information on implementing Microsoft AD services, see: http://technet.microsoft.com/en-us/library/cc754438%28WS.10%29.aspx

The following services were configured in the Active Directory environment on the campus network:

- Enterprise CA Server with Network Device Enrollment Service—The internal Certificate Server running on the secure network segment of the campus network. The Network Device Enrollment (NDES) in enabled in order to provide clients with the ability to automatically enroll for client x.509 digital certificates.
- DHCP Server—The DHCP server on the secure campus network provides DHCP services for internal wired and wireless users.
- DNS Server—The DNS server provides internal name resolution for secure wired and wireless devices as well as providing name resolution for remote VPN users. As discussed later in this document, the AnyConnect client uses this internal name server in order to determine if a VPN connection should be established when using the Trusted Network Detection (TND), a feature within the AnyConnect client.

- IIS Server—The Web service is enabled so that users can use HTTP/HTTPS protocol to request certificates from a CA server via NDES as well as to provide internal users with a Web page link to download AnyConnect modules and profiles.

All the users in the campus network must be able to enroll their machines with the Active Directory Domain Controller. In our design, the only network device that is enrolled with the CA server is the Cisco Secure ACS Server.

RSA Server

VPN security is only as strong as the methods used to authenticate users (and device end points) at the remote end of the VPN connection. Simple authentication methods based on static passwords are subject to password "cracking" attacks, eavesdropping, or even social engineering attacks. Two-factor authentication, which consists of something you know and something you have, is a minimum requirement for providing secure remote access to the corporate network (http://www.cisco.com/web/about/security/intelligence/05_08_SSL-VPN-Security.html). This design includes the RSA SecurID Authentication Server 7.1 along with RSA SecurID hardware tokens in order to provide two-factor authentication. The passcode that the user presents is a combination of their secret PIN and the one time password (OTP) code that is displayed on their token at that moment in time. The OTP on the RSA SecurID token changes every 60 seconds. This design utilizes both RSA SecurID (two-factor authentication) in conjunction with the deployment and use of x.509 client digital certificates.

For information on how to configure the RSA Secure Authentication Manager, see: http://www.rsa.com/node.aspx?id=1166

When a remote user establishes a VPN connection to the ASA via the AnyConnect Secure Mobility Client and attempts to authenticate using two-factor authentication with a RSA SecurID token, the ASA communicates with the ACS Server using the RADIUS protocol. The ACS Server then communicates with the RSA Authentication Manager using the Security Dynamics Incorporated (SDI) protocol in order to provide authentication. Since the ASA is communicating through the ACS server to the RSA Server, it is critical that the RSA "text message prompts" be properly translated by the ACS Server to the ASA and finally back to the end user. Also, because the SDI messages are configurable on the SDI server, the message text on the ASA must match (in whole or in part) the message text on the SDI server. Otherwise, the prompts displayed to the remote client user may not be appropriate for the action required during authentication.

Certificate Authority Server

Identification is a critical part of an authentication strategy. Without a good authentication strategy, security does not provide any value to the network. Digital Certificates distributed by a CA provide the best form of identification for all devices on the network. Once users obtain their certificates, they can use them to identify themselves at different points in the network. Network devices such as the ASA, ACS, and wireless access points can also identify themselves using certificates. The best form of identification happens when both network users and network devices use certificates to identify themselves. Hence, we recommend that digital certificates be deployed at all places in the network. The Unified Access Solution is designed such that users and network devices authenticate each other using digital certificates.

Even though digital certificates provide many benefits to enterprise network deployments, the usual challenge has been in distributing these certificates to a large number of users. In the Unified Access Solution, this challenge has been addressed by providing two different methods of enrollment:

- Enrolling directly with the CA server using SCEP
- SCEP Proxy feature of ASA firewall

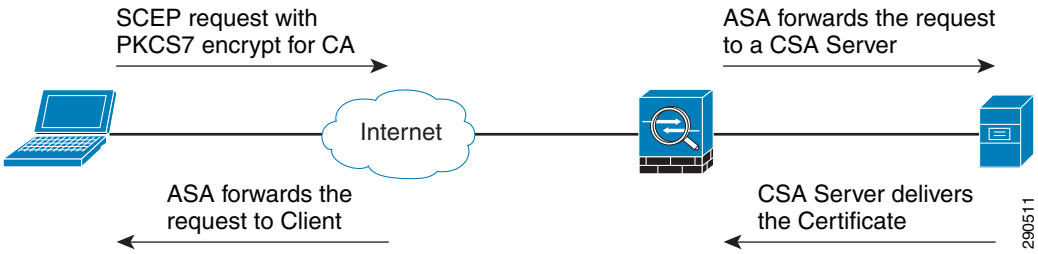
Enrolling Using SCEP

The user can use a Web browser to initiate certificate enrollment. The CA server can be set up either to issue certificates automatically or to be issued manually by an administrator. Granting certificates automatically is efficient for deployment, but the CA server must be set up with the right policies to verify user credentials before granting the certificate. If the granting mode is manual, then an administrator must issue certificates after verifying user credentials. CA server functionality is supported by several vendors. In the Unified Access Solution, the Microsoft CA server is deployed. To obtain more information about SCEP feature on the Microsoft CA server, see: http://www.microsoft.com/downloads/en/details.aspx?familyid=E11780DE-819F-40D7-8B8E-10845BC8D446&displaylang=en

Enrolling Using SCEP Proxy Feature of ASA Firewall

Even though SCEP is a great protocol for certificate enrollment, the major caveat is the requirement of a CA server be accessible to all clients. This requirement is fine with clients located at the campus site, but for clients that are outside the campus, such as remote clients, it is difficult to make the CA server accessible to them. In the Unified Access Solution, ASA's SCEP Proxy feature is implemented to address the connectivity problem for remote clients. This feature helps remote clients to make requests to the ASA, ASA forwards the requests to the CA server, and responds back to the clients with the certificates issued by the CA server. Figure 3-2 shows how the SCEP Proxy feature is deployed.

Figure 3-2 SCEP Proxy Feature Deployment



NDES Server Configuration for SCEP

The Network Device Enrollment Service (NDES) is the Microsoft implementation of the SCEP, a communication protocol that makes it possible for network devices to enroll for X.509 certificates from a CA. In order to distribute and deploy digital x.509 client certificates to remote users, the Microsoft Network Device Enrollment Service (NDES) was utilized in conjunction with a Microsoft CA Server. To implement NDES service, see: http://technet.microsoft.com/en-us/library/cc753784%28WS.10%29.aspx

By default, the NDES service is configured to present one-time enrollment passwords for certificate enrollment. The use of one-time passwords by the NDES service is typically used to allow network and IT administrators to enroll certificates for network devices within the IT organization. However, in the Unified Access Solution this feature is disabled because remote endpoints are authenticated by using their RSA SecureID tokens.

Disabling the “one-time password” on the NDES server is configured in the following registry key: Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP\EnforcePassword

EnforcePassword value data is set to “0”. “0” ensures no password is requested by NDES.

Note In Windows Server 2003, Microsoft SCEP (MSCEP) was a Windows Server 2003 Resource Kit add-on that had to be installed on the same computer as the CA. In Windows Server 2008, MSCEP support has been renamed NDES and is part of the operating system; NDES can be installed on a different computer than the CA (http://technet.microsoft.com/en-us/library/cc753784%28WS.10%29.aspx).

The NDES extension to IIS uses the registry to store configuration settings. All settings are stored under one registry key:

HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\MSCEP

Certificate Template

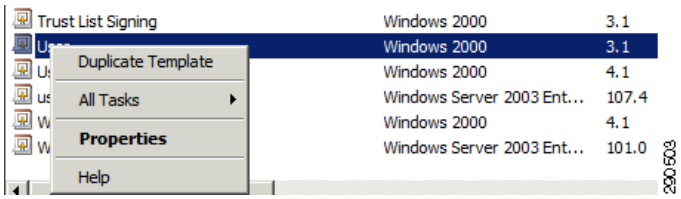
Digital certificates can be used for different purposes like server authentication, secure E-mail, encrypting the file system, and client authentication. Hence, it is important that a client is issued a certificate which serves its purpose. For example, a Web server may need a certificate that it uses primarily for server authentication. Similarly, a normal client needs a certificate mainly for client authentication. Therefore, certificate templates are needed to properly distribute certificates to users based on their specific needs. In the Unified Access Solution, a security template has been created on the Microsoft Windows 2008 CA server so that users can obtain the proper certificate. This section describes important steps to set up the certificate template on the Windows CA server and specific actions needed on the user.

For more information on certificate templates, see:
http://technet.microsoft.com/en-us/library/cc730826%28WS.10%29.aspx

Since we are using SCEP for auto enrollment of client end points using the AnyConnect VPN Client, we are utilizing the properties of the “User” template that is a default template in the Microsoft Server 2008 R2 CA Server deployment. Default templates in Microsoft Server 2008 R2 cannot be edited. Therefore, a customized template can be built that gives an administrator more flexibility in defining the certificate options. This section describes how to create a customized template, which is named user2 in this example.

The first step is to create a duplicate template from the pre-defined list of templates. Figure 3-3 shows how to create a duplicate template.

Figure 3-3 Creating a Duplicate Template

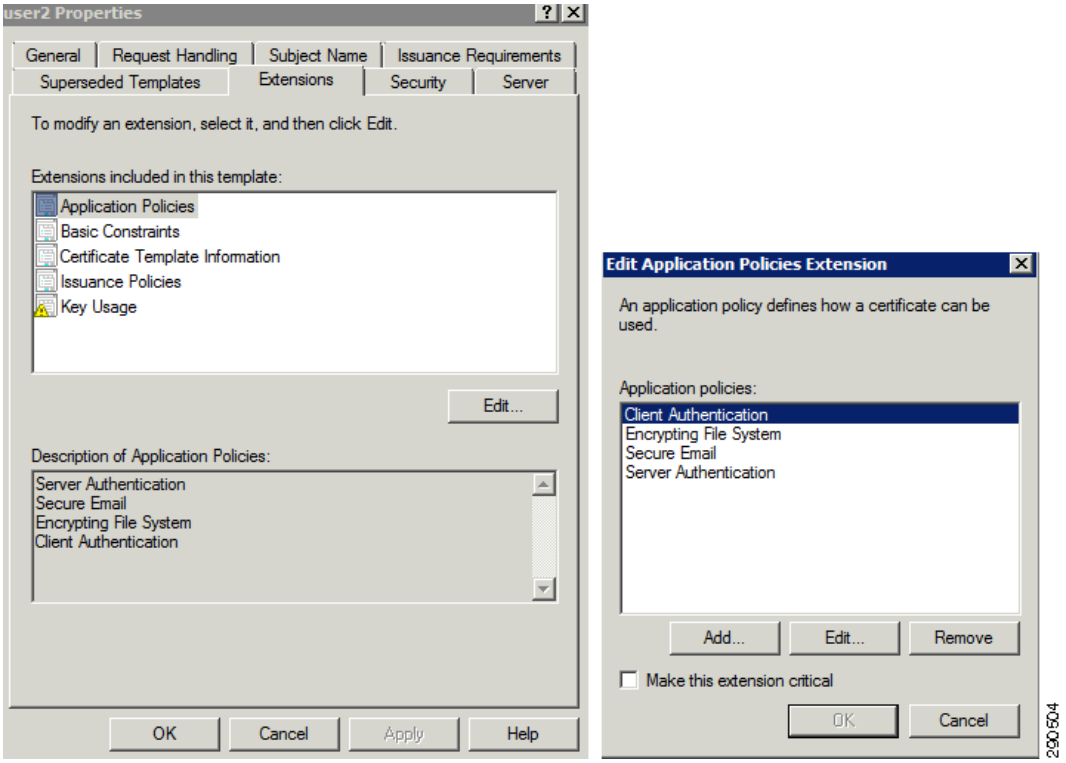


The default “User” template was copied and renamed as “user2”. Then the “user2” template was used to auto-enroll AnyConnect VPN clients with client certificates using this newly created template.

The next step is to configure the extensions of the certificates that are derived from the "user2" template. The EKU extension and extended property specify and limit the valid uses of a certificate. The extensions are part of the certificate itself. They are set by the issuer of the certificate and are read-only. Certificate-extended properties are values associated with a certificate that can be set in an application. To obtain more information about extended properties, see:
http://msdn.microsoft.com/en-us/library/aa380252%28v=vs.85%29.aspx

Figure 3-4 describes how to configure the extended properties for the certificates.

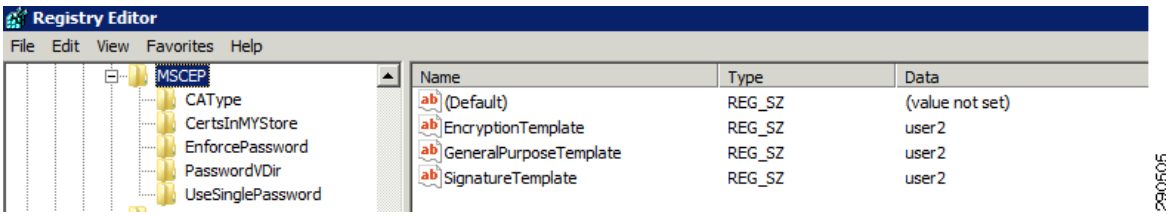
Figure 3-4 Configuring Extended Properties for Certificates



Notice the template named "user2". This value must be set in the registry as it correlates to the "user2" template, which was copied from the "Certificate Templates Console" on the CA Server.

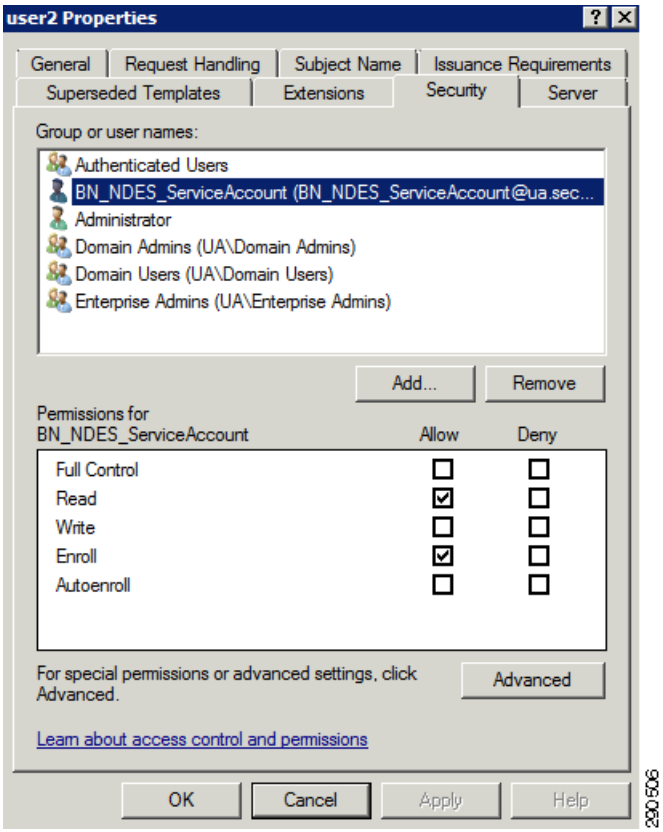
Figure 3-5 describes how the registry setting must be modified to reflect the newly-created template "user2".

Figure 3-5 Modifying the Registry



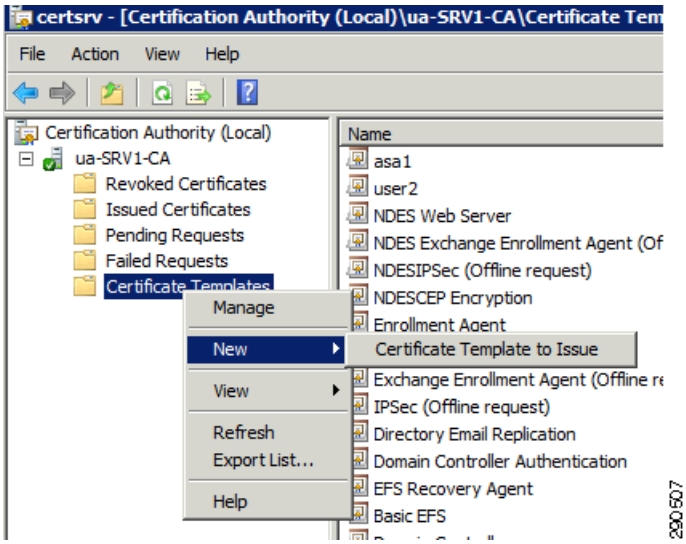
Once the template has been duplicated, the permissions are set for the NDES_ServiceAccount on the "user2" template to Read and Enroll. Figure 3-6 displays the Read and Enroll permissions that have been set for the NDES_ServiceAccount on the "user2" template.

Figure 3-6 Read and Enroll Permissions



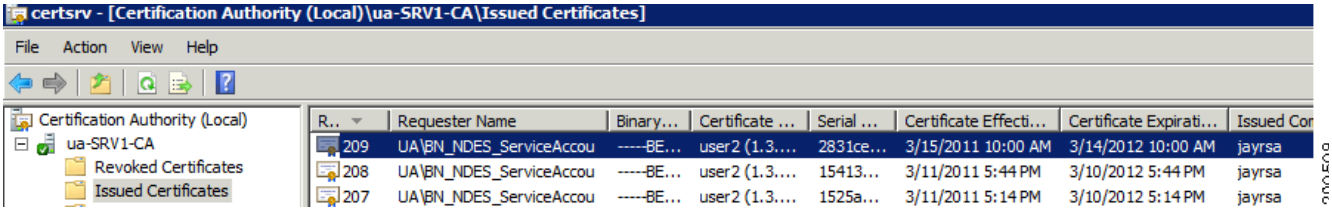
Ensure that the newly created "user2" template is available to be issued via the CA. Right click <Certificate Templates> | <Certificate Template to Issue> and choose newly-created "User2 Certificate".

Figure 3-7 Ensuring Template is Available From CA



Now the certificate template is fully configured and can be used by users to submit enrollment requests. Figure 3-8 shows a successful enrollment request to the "user2" template that was submitted by a user, "jayrsa".

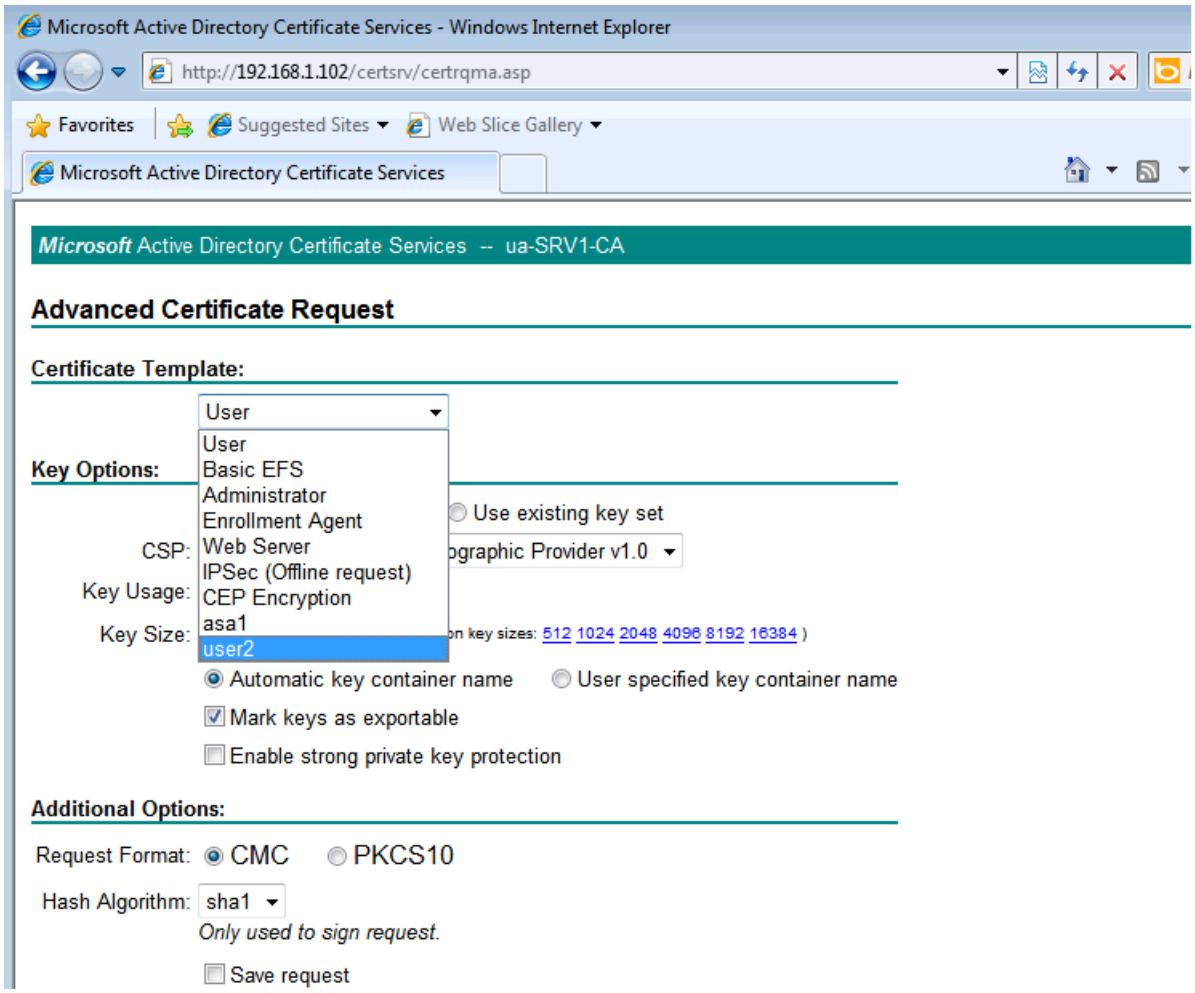
Figure 3-8 Successful Enrollment Request



A successful auto-enrollment request has occurred on the CA Server. Notice that the requester name is the NDES Service Account that is configured for Read and Enroll permissions and also notice that the "user2" certificate template was chosen.

Figure 3-9 shows how a user can submit a certificate enrollment request using a Web browser.

Figure 3-9 Submitting a Certificate Enrollment Request with a Web Browser

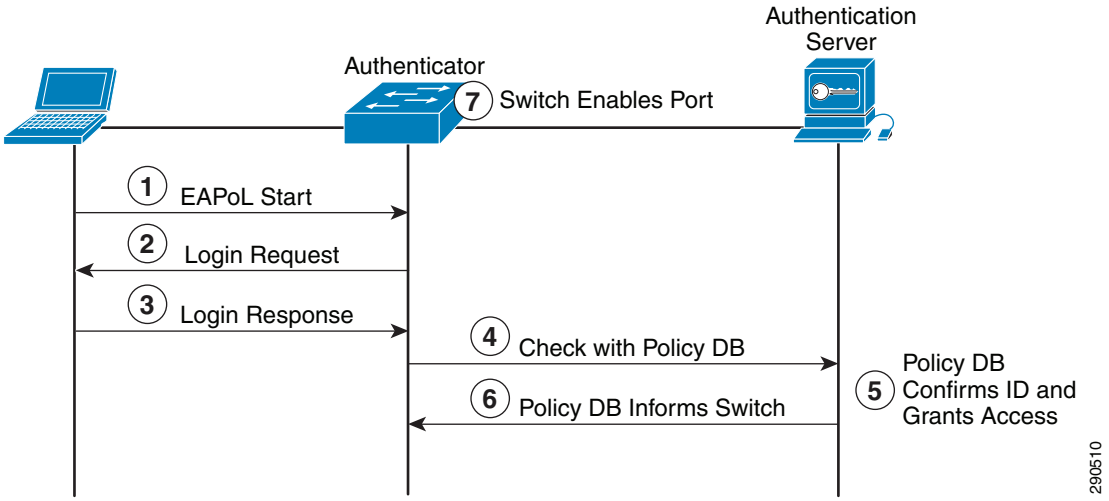


Authentication Protocols

The IEEE 802.1X protocol allows Cisco Catalyst switches to offer network access control at the port level. Every port on the switch is individually enabled or disabled based on the identity of the user or device connecting to it. When 802.1X is first enabled on a port, the switch automatically drops all traffic received on the port except the request to start 802.1X authentication. After the 802.1X authentication successfully completes, the switch starts accepting other kinds of traffic on the port.

The high-level message exchange shown in Figure 3-10 illustrates how port-based access control works within an identity-based system.

Figure 3-10 High-Level Message Exchange



The following steps describe the port-based access control flow:

1. A client, such as a laptop with an 802.1X supplicant, connects to an IEEE 802.1X-enabled network and sends a start message to the LAN switch (the authenticator).
2. When the start message is received, the LAN switch sends a login request to the client.
3. The client replies with a login response.
4. The switch forwards the response to the policy database (authentication server).
5. The authentication server authenticates the user.
6. After the user's identity is confirmed, the policy database authorizes network access for the user and informs the LAN switch.
7. The LAN switch then enables the port connected to the client.

The user or device credentials are processed by a AAA server. The AAA server is able to reference user or device profile information either internally, using the integrated user database, or externally using database sources like Microsoft Active Directory, Lightweight Directory Access Protocol (LDAP), Novell Directory Services, or Oracle databases. This enables the IBNS solution to be integrated into existing user management structures and schemes, which simplifies overall deployment.

802.1X and EAP

When authenticating users for network access, the client must provide user and/or device identification using strong authentication technologies. IEEE 802.1X does not dictate how this is achieved. Instead, the 802.1X protocol defines an encapsulation for the transport of the Extensible Authentication Protocol (EAP) from the client to the switch. The 802.1X encapsulation is sometimes referred to as EAP over LAN (EAPoL). The switch in turn relays the EAP information to the authentication server using the RADIUS protocol (EAP over RADIUS).

RFC 3748 defines EAP, which is a framework and not a specific authentication method. It provides a way for the client and the authentication server to negotiate an authentication method that they both support. There are many EAP methods, but the ones used more frequently for 802.1X wired authentication include EAP-TLS, EAP-PEAP, and EAP-FAST.

For the Unified Access Solution, we have chosen EAP-TLS and PEAP as the authentication protocols. We highly recommend using the EAP-TLS protocol for customers for the following reasons:

- Authentication using certificate provides the highest level of trust among all the methods available today.
- All the other protocols except EAP-TLS do not provide mutual authentication—only the access layer switch presents its identity, but not the client. EAP-TLS allows for mutual authentication—both the access layer switch and the user authenticate each other.
- When EAP-TLS is deployed and the user obtains the certificate, then the same certificate can be presented as a source of identity for remote connections also, which is an added benefit of deploying EAP-TLS.

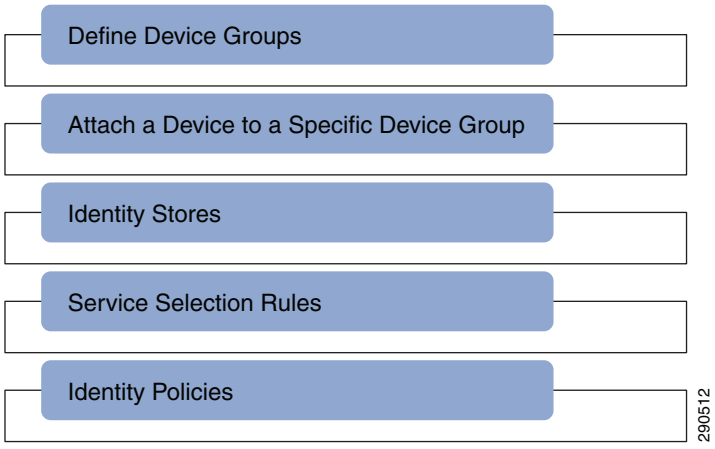
ACS Policy Definitions

Configuring ACS is an important step in developing a centralized access control system. Cisco Secure ACS is used in the solution such that all the authentication requests come to the ACS server; the ACS server re-directs the requests to various additional authentication servers such as Active Directory and the RSA server. All the authentication requests coming from various sources, such as access layer switches, access points, and remote users, come to the ACS server first; based on the policy defined on the ACS server, they are further directed to either Active Directory or the RSA secure server. The following section describes how to deploy this centralized access control system.

ACS Authentication Overview

In Cisco Secure ACS, when an authentication request comes from the client into the ACS server, the ACS server first tries to identify to which Network Device group the client belongs and, based on the Network Device Group, the request is directed to an appropriate Access service. In each Access service there are rules defined to further authenticate the request. Figure 3-11 shows an overview of ACS authentication.

Figure 3-11 ACS Authentication Overview



Device Groups

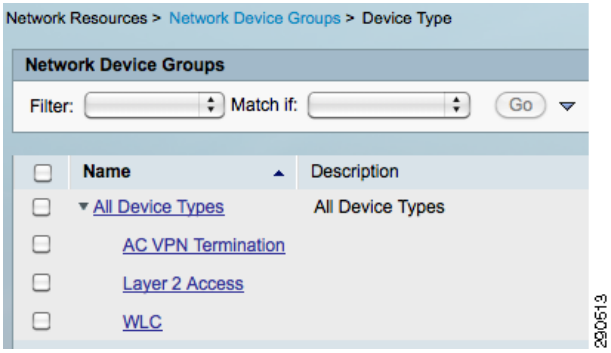
As shown in Figure 3-11, the first step is to define the network device groups. In the Unified Access Solution, three different types of device groups are defined:

- WLC—All wireless LAN controllers

- Layer 2 access—All access layer switches
- AC VPN termination—VPN gateways

Figure 3-12 shows how these device groups are defined on ACS.

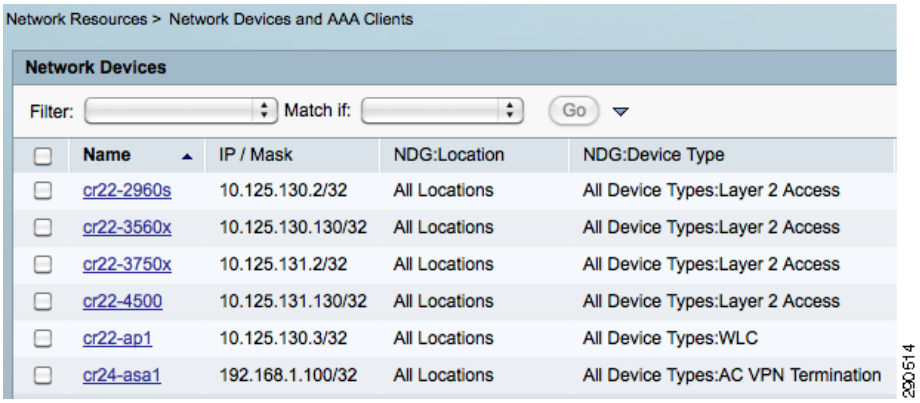
Figure 3-12 Device Groups on ACS



Mapping Devices to Device Groups

The second step in ACS configuration is to map the individual devices to a specific group. For example, a WLAN Controller must belong to the device group WLC, which is shown in Figure 3-12. Figure 3-13 shows how different devices are mapped to different device groups.

Figure 3-13 Mapping of Devices to Device Groups



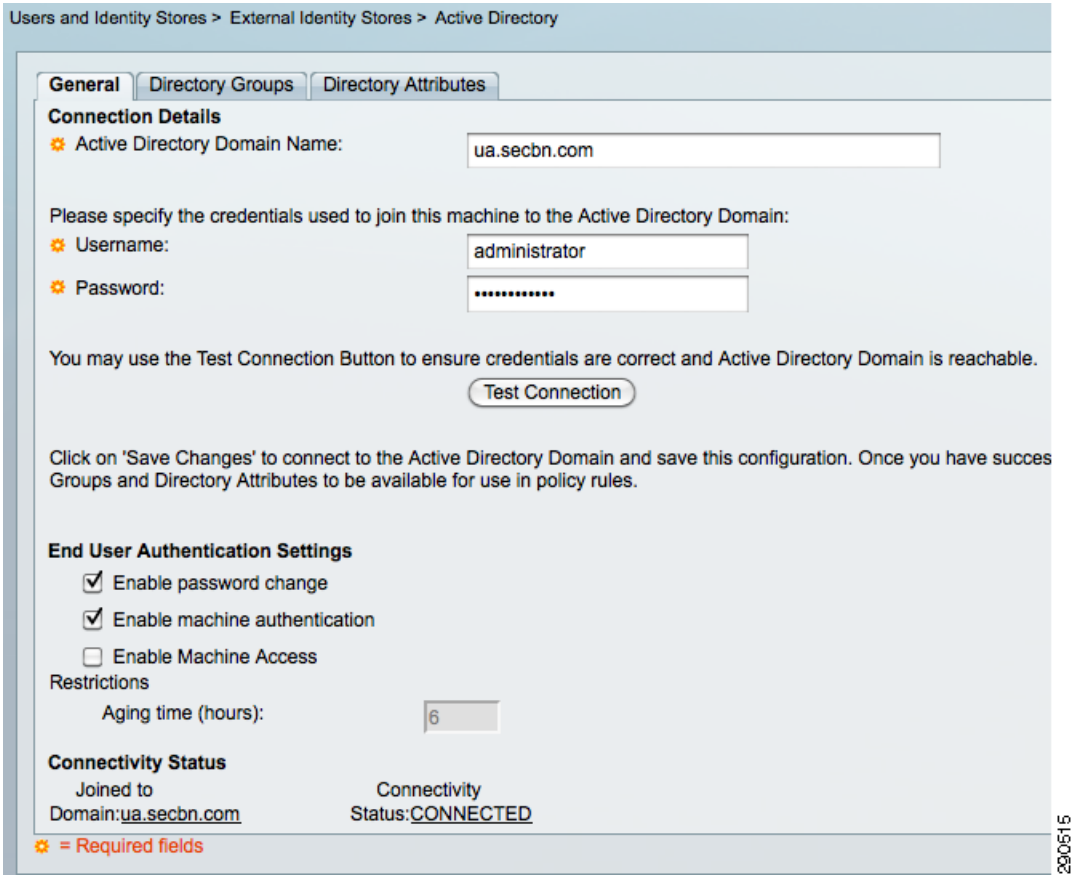
Identity Stores

The ACS server passes the identification requests to different identity stores to identify the users. The identity stores are external authentication devices that can perform the authentication of users. In the Unified Access Solution, there are three main identity stores:

- Active Directory
- RSA secure server
- Certificate Profile

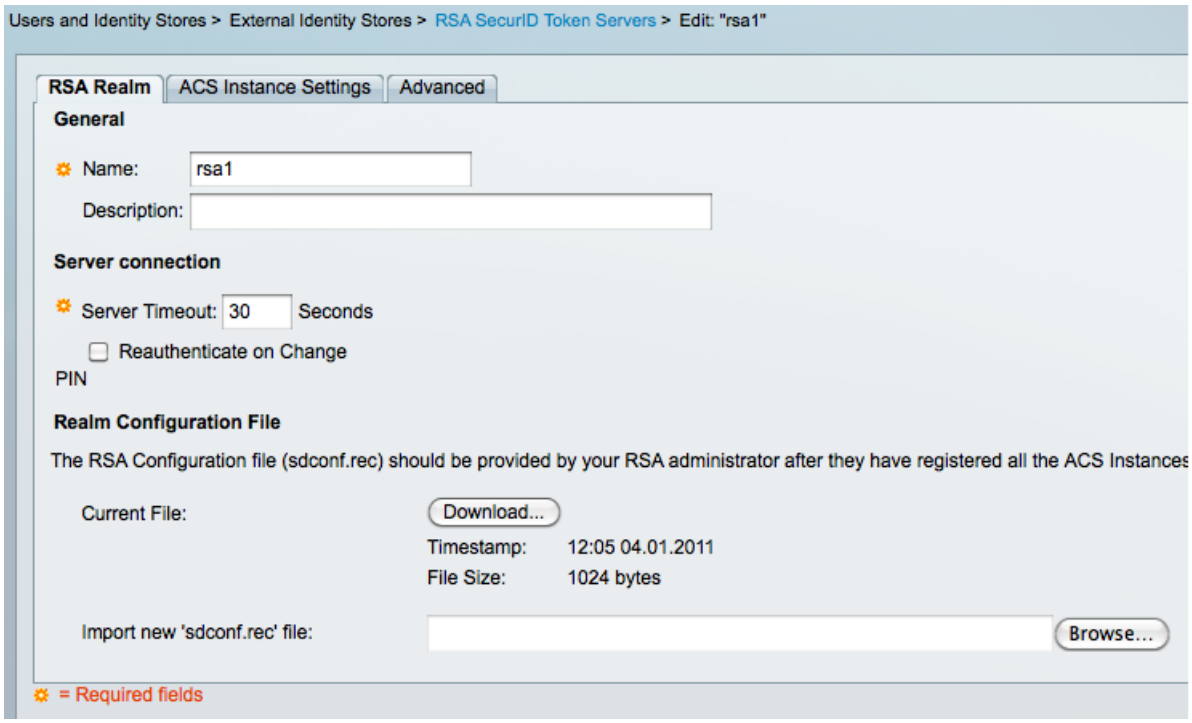
To use Active Directory as an identity store, the ACS must first join the active directory domain. Figure 3-14 shows how ACS should be configured to join the domain.

Figure 3-14 ACS Configuration for Active Directory



The RSA secure server is used to authenticate remote users. When remote users connect to the ASA to establish an AnyConnect VPN session, they are required to enter a one-time password using RSA tokens. ACS must be configured to join the RSA server, as shown in Figure 3-15.

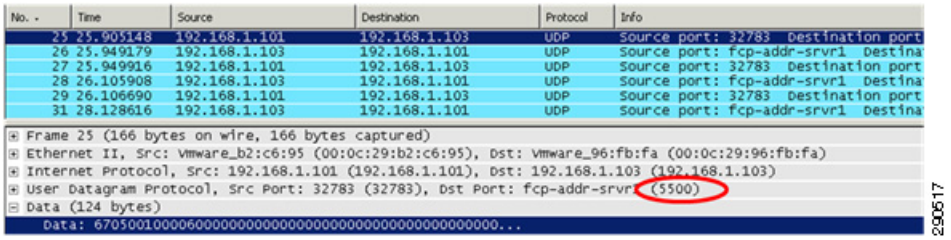
Figure 3-15 ACS Configuration for RSA



When the RSA Manager communicates with Cisco Secure ACS, it uses UDP port 5500. Figure 3-16 shows the communication between the RSA Manager and ACS during authentication.

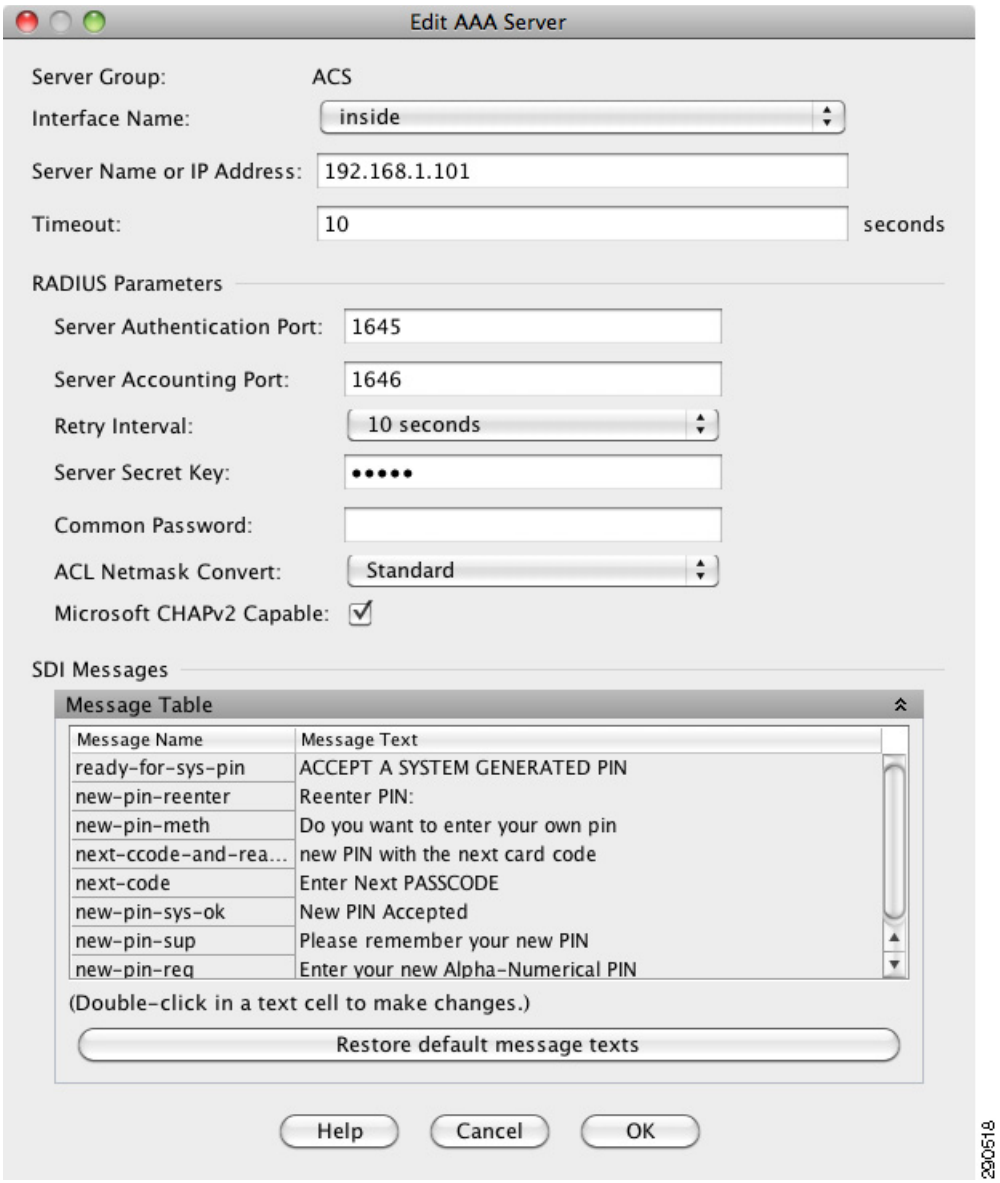
The trace in Figure 3-16 is taken on the RSA Authentication Manager (the IP address 192.168.1.101 is the ACS Server and 192.168.1.103 is the RSA server). Note that the ACS Server and the RSA Server are communicating on UDP:5500.

Figure 3-16 ACS/RSA Manager Communication During Authentication



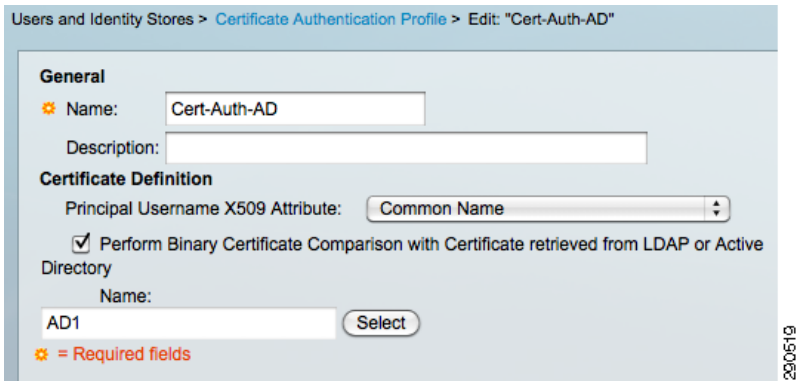
Configure the appropriate SDI messages in the AAA Server Group for the AnyConnect Clients on the ASA, as shown in Figure 3-17.

Figure 3-17 Configure SDI Messages



The Cert Authentication Profile feature allows ACS to match the certificates presented by the user to the Active Directory. Figure 3-18 shows how to configure it on this ACS server.

Figure 3-18 Configuring Cert Authentication Profile



Service Selection Policy

The Service Selection Policy acts like a gateway that forwards authentication requests to the various identification policies. In the Unified Access Solution, there are three different service selection policy elements—wired access policy, wireless access policy, and remote access policy. Figure 3-19 shows how the service selection policy works in the Unified Access Solution.

Figure 3-19 Service Selection Policy in UA Solution

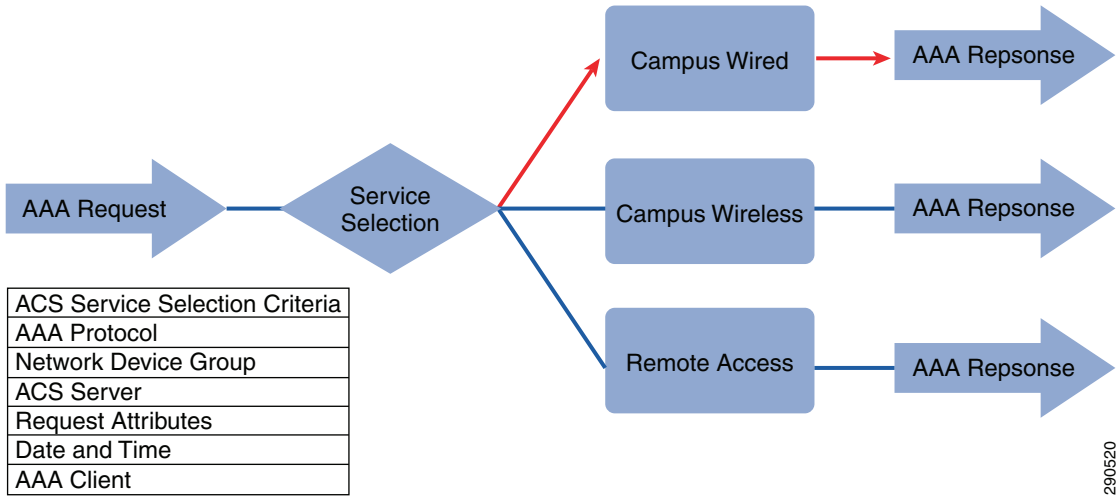
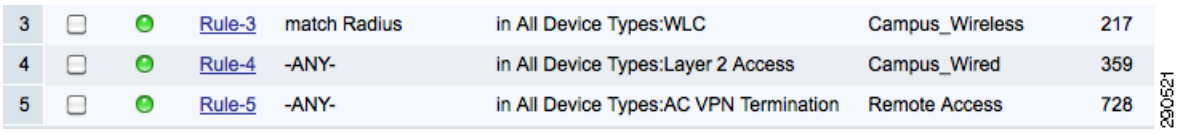


Figure 3-20 shows how the Service Selection Policy looks in Cisco ACS server.

Figure 3-20 Service Selection Policy Cisco ACS Server

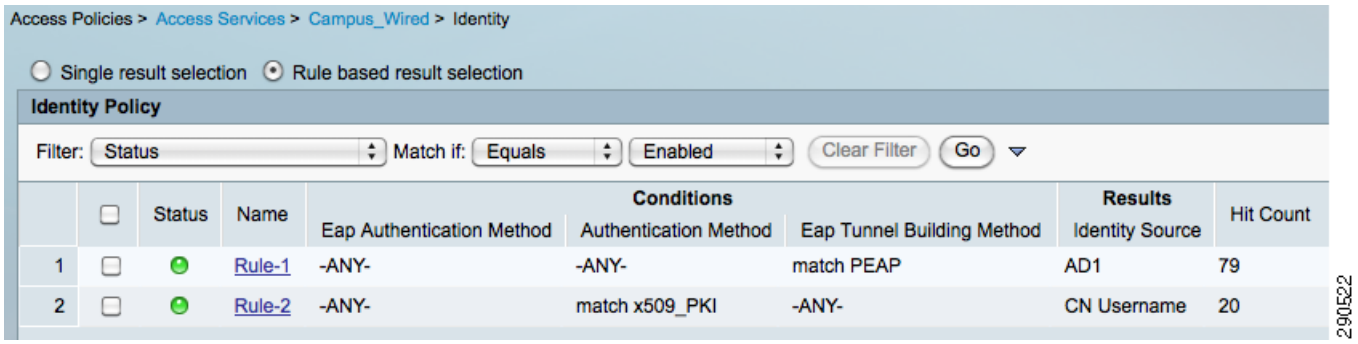


As shown in Figure 3-20, all the devices that belong to device type group WLC match the individual policy element Campus_Wireless. Similarly, all the devices that belong to Layer 2 access match Campus_Wired and all the devices that belong to the group VPN Termination match the group Remote_Access.

Individual Policy Elements

The service selection policy directs the authentication request to each individual policy. In the Unified Access Solution, the individual policies are Campus Wired, Campus Wireless, and Remote Access. These individual policies must be constructed carefully because the default behavior of an access policy is to reject an authentication if there is no match in the policy. In the Unified Access Solution, there are three fields that are matched for an authentication request—EAP Authentication Method, Authentication Method, and EAP Tunneling Protocol. Figure 3-21 shows how the Campus Wired Policy is constructed.

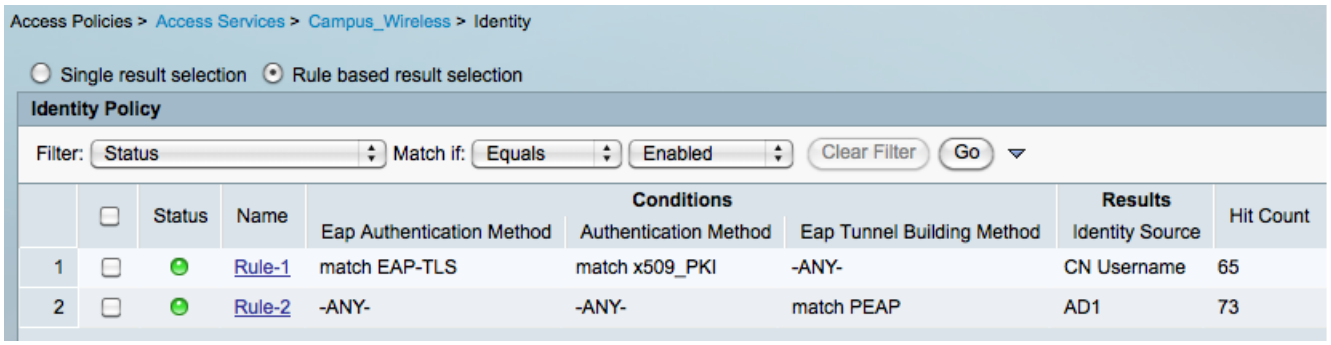
Figure 3-21 Campus Wired Policy



As shown in Figure 3-21, the selection policy has two different rules. The first rule is used to match PEAP with Active Directory as an identity store and the second rule matches EAP_TLS with digital certificates as an authentication method. The main point to note above is that PEAP is matched on the Tunneling method rather than on the EAP Authentication method because the PEAP protocol works differently then the EAP_TLS protocol. When PEAP is used, the first step is to establish a TLS tunnel and actual credentials are sent in the second stage, which is protected by the TLS tunnel that has been established. Therefore PEAP has an outer method and an inner method. The outer method is PEAP and the inner-method authentication type that is negotiated during phase two can be either EAP-MSCHAPv2 or EAP-GTC. The combination of the outer PEAP method with a specific inner EAP method is denoted using a slash character; for example, PEAP/EAP-MSCHAPv2 or PEAP/EAP-GT. The following link gives more information on deploying PEAP in ACS 5.2:
http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.2/user/guide/eap_pap_phase.html#wp1031414

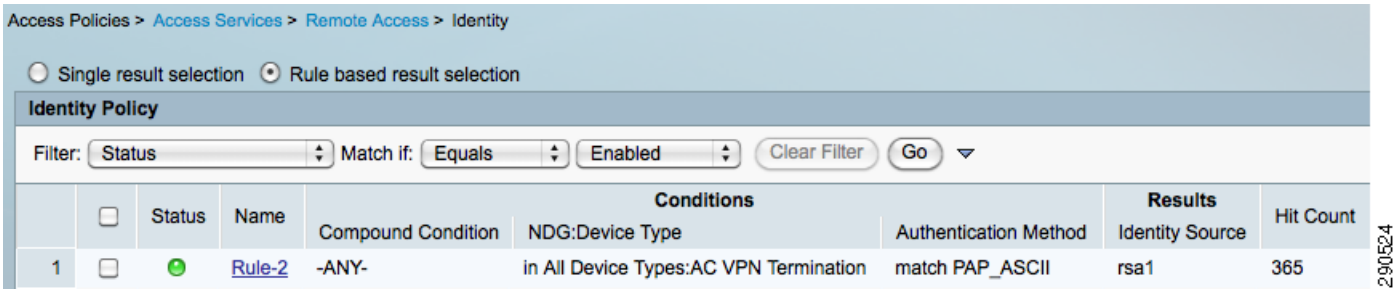
The second policy is Campus Wireless. The Unified Access Solution assumes that wireless users can use either EAP-TLS or PEAP protocol. The EAP_TLS protocol uses digital certificates as identity store and the PEAP protocol uses Active Directory as its identity store. Figure 3-22 shows how this policy is configured in ACS.

Figure 3-22 Campus Wireless Policy



The last policy is Remote Access. In the Unified Access Solution, remote users use two-factor authentication along with client digital certificates. The initial authentication happens between the ASA and the remote user. After the initial authentication is successful, the ASA prompts the user for an RSA code. Once the user inputs the code, the ASA passes the code to the ACS server. The ACS server in-turn passes the user response to the RSA server. Once the RSA server successfully authenticates the code, the user is allowed to access the network. Figure 3-23 depicts the remote access policy configuration in ACS.

Figure 3-23 Remote Access Policy



ASA Configuration

Some challenges faced by network architects when deploying a remote VPN solution for their network include:

- How do remote users trust the VPN gateway?
- How does the VPN gateway identify remote users?
- How to organize different types of users in groups so that different kinds of services can be provided?
- What kind of mobility client solution is needed for a particular client?
- Once the right kind of VPN solution is identified, how will the mobility client be installed on the remote device?
- How to centralize the policy settings for VPN users? It is always very annoying for remote users to configure a mobile device for VPN functionality.

The Cisco ASA coupled with the Cisco AnyConnect client addresses the above challenges. The Cisco AnyConnect client 3.0 is used to meet the need of wired, wireless, and remote users. The Cisco AnyConnect Secure Mobility client is the next-generation VPN client, providing remote users with

secure IPsec (IKEv2) or SSL VPN connections to the Cisco 5500 Series Adaptive Security Appliance (ASA). AnyConnect provides end users with a connectivity experience that is intelligent, seamless, and always-on, with secure mobility across today's proliferating managed and unmanaged mobile devices.

The Cisco AnyConnect Secure Mobility client, Version 3.0, integrates new modules into the AnyConnect client package:

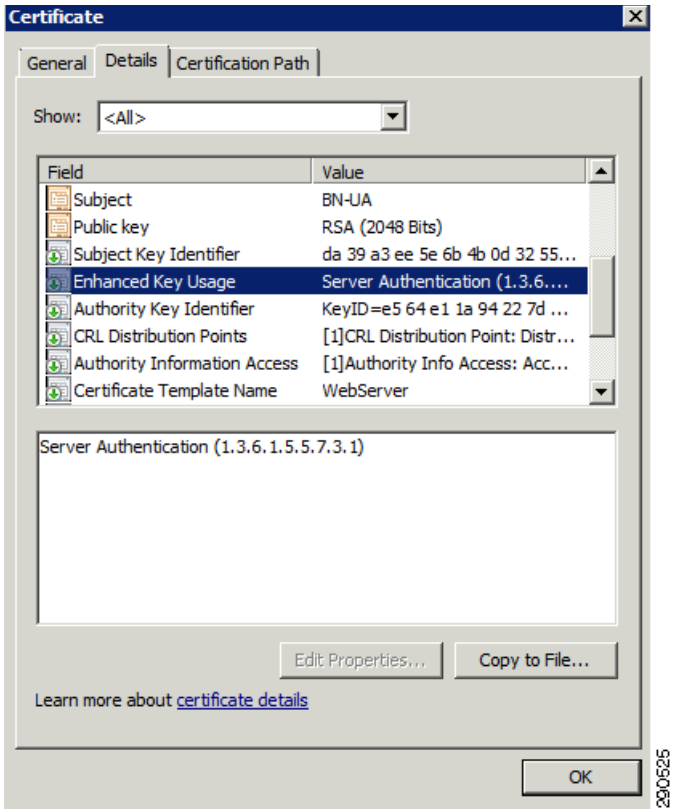
- Network Access Manager (NAM)—Formerly called the Cisco Secure Services Client, this module provides Layer 2 device management and authentication for access to both wired and wireless networks.
- Posture Assessment—The AnyConnect Posture Module provides the AnyConnect Secure Mobility Client with the ability to identify the operating system, antivirus, antispyware, and firewall software installed on the host prior to creating a remote access connection to the ASA. Based on this prelogin evaluation, you can control which hosts are allowed to create a remote access connection to the security appliance. The Host Scan application is delivered with the posture module and is the application that gathers this information.
- Telemetry—Sends information about the origin of malicious content detected by the antivirus software to the Web filtering infrastructure of the Cisco IronPort Web Security Appliance (WSA), which uses this data to provide better URL filtering rules.
- Web Security—Routes HTTP and HTTPS traffic to the ScanSafe Web Security scanning proxy server for content analysis, detection of malware, and administration of acceptable use policies.
- Diagnostic and Reporting Tool (DART)—Captures a snapshot of system logs and other diagnostic information and creates a .zip file on your desktop so you can conveniently send troubleshooting information to Cisco TAC.
- Start Before Logon (SBL)—Forces the user to connect to the enterprise infrastructure over a VPN connection before logging on to Windows by starting AnyConnect before the Windows login dialog box appears.

To obtain more information about Cisco AnyConnect 3.0, see:
http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect30/administration/guide/ac01intro.html

Remote Users Trusting VPN Gateway

The ASA can present a self-signed certificate, but presenting a certificate that is signed by a CA server increases the trust of the ASA. However, the certificate that the ASA presents must be a certificate that can be used for server authentication. In our testing scenario, we have used a Microsoft CA with the certificate template configured for Web Server. Figure 3-24 shows the certificate that can be used for server authentication.

Figure 3-24 Certificate for Server Authentication



ASA can obtain the certificate from the CA server by using SCEP or by a manual cut-and-paste method. SCEP was used to obtain the certificate in this testing. To obtain more information on deploying certificates on the ASA, see:
http://www.cisco.com/en/US/docs/security/asa/asa80/configuration/guide/cert_cfg.html

Example 3-1 is the ASA configuration for certificate enrollment.

Example 3-1 ASA Configuration for Certificate Enrollment

```
crypto ca trustpoint f5
 enrollment url http://192.168.1.102:80/certsrv/mscep/mscep.dll
 subject-name CN=asa1
 no client-types
 crl configure
```

Identification of Remote Users

Identification is very important, particularly for remote users. Digital certificates play an important part in identifying remote users, however it is often difficult to deploy the certificates for remote users because they cannot access the CA server directly through the Internet. They can access the CA server through a VPN connection, but without having a digital certificate in first place, they cannot establish a VPN tunnel. To solve this problem the ASA supports the SCEP proxy feature.

SCEP enables network devices to enroll for x509 version 3 certificates from a CA. The ASA can proxy SCEP requests between AnyConnect and a third-party CA. The ASA supports SCEP-Proxy for AnyConnect clients.

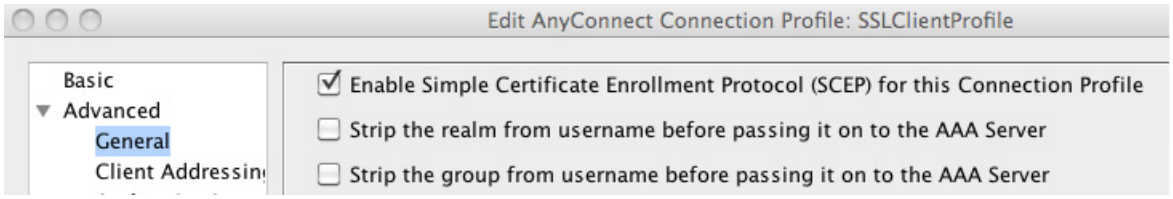
The CA only needs to be accessible to the ASA, as the ASA is acting as the proxy for the client. For the ASA to provide this service, the user must authenticate using any of the methods supported by AAA before the ASA sends an enrollment request. Enrollment occurs only after a VPN tunnel has been established between the AnyConnect client and the ASA. The AnyConnect client enrolls to the ASA Client Services interface using SSL. After the SSL VPN tunnel is established, the ASA proxies the SCEP enrollment to the CA on behalf of the client.

The VPN tunnel is disconnected after an enrollment success or failure. If the enrollment was a success, the AnyConnect client re-launches, allowing the user to authenticate with their credentials while using the newly-enrolled client certificate. ASA supports this feature only with an AnyConnect SSL or IKEv2 VPN session. The ASA supports all SCEP-compliant CAs, including IOS CS, Windows Server 2003 CA, and Windows Server 2008 CA.

Configuring SCEP for AnyConnect Clients on the ASA

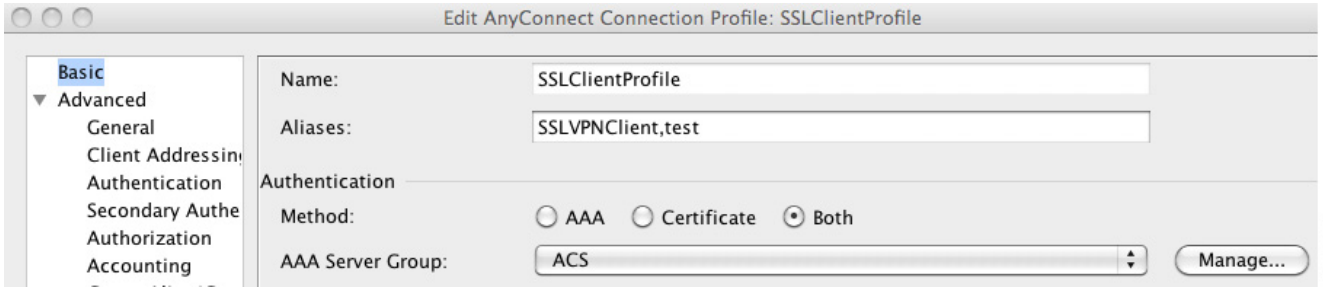
Enable SCEP for the Connection Profile:

Figure 3-25 Enable SCEP



Configure the Connection Profile for authentication (configure the Authentication Method for “Both” Active Directory username/password and PKI x.509 Certificates):

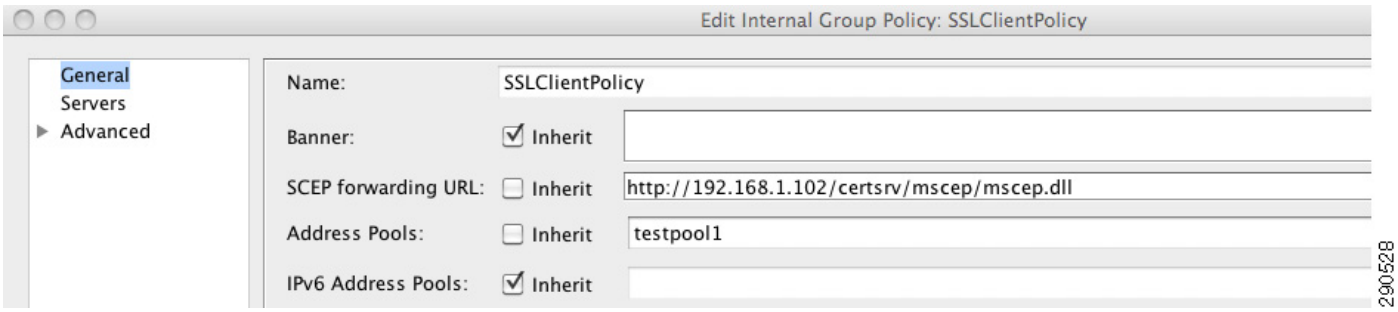
Figure 3-26 Configuring the Connection Profile



Configure the Group Policy for Network Client Access.

The SCEP forwarding URL points to the SCEP/NDES resource service.

Figure 3-27 Configuring the Group Policy

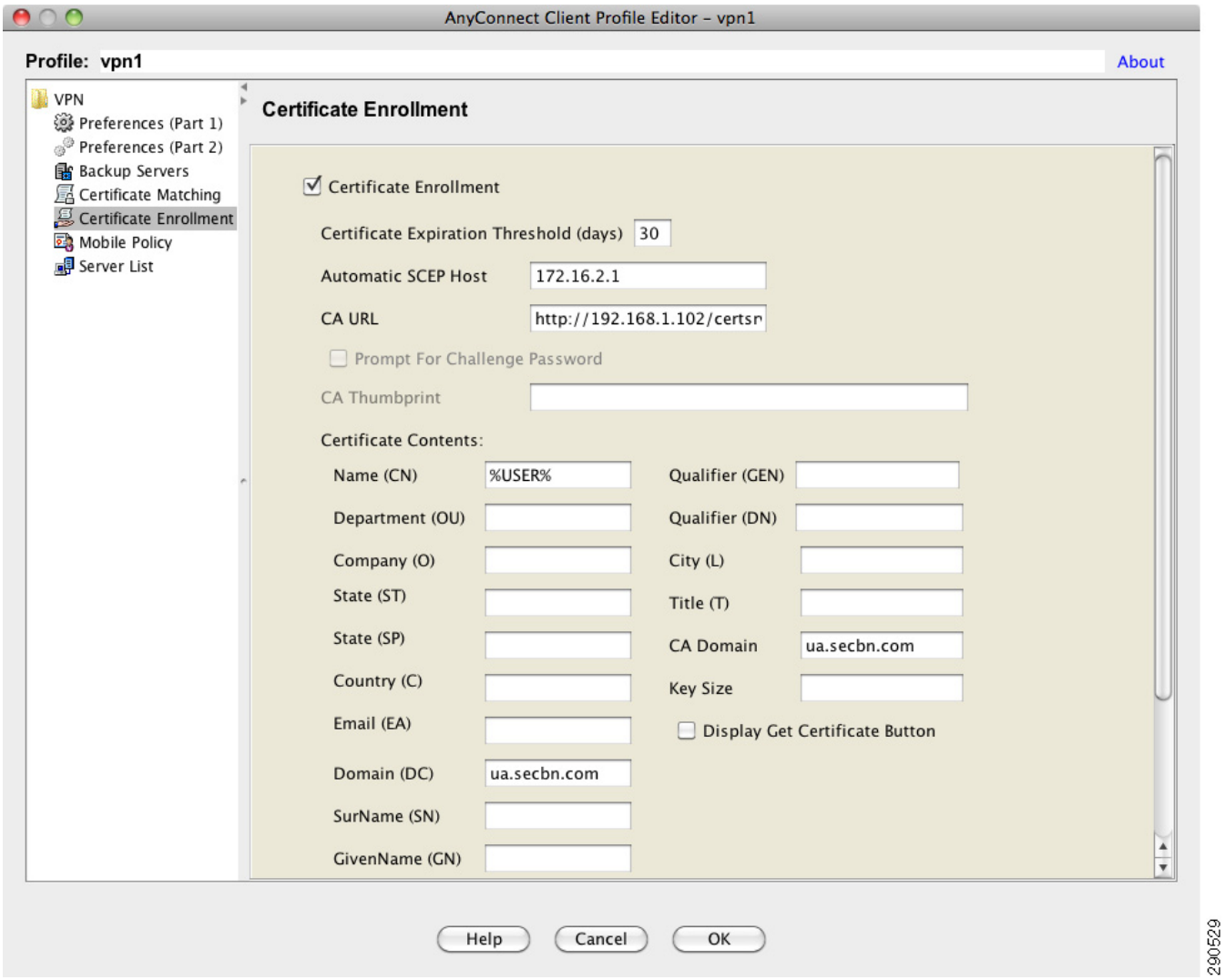


Configure the Client Profile with the Automatic SCEP Host which is the IP Address of Hostname of the ASA for which the ASA will proxy SCEP requests on behalf of the client. 172.16.2.1 is the outside IP address of the ASA.

The prompt for password is left blank as the purpose of our SCEP enrollment is for client end points performing auto-enrollment and not requiring the use of a password for each end point enrolling for a certificate.

Name(CN) is %USER%, which is used to create the enrollment with this CN.

Figure 3-28 Configuring the Client Profile



Creating Groups for Different Types of Users

Group Policy is an important building block for designing an effective access mechanism for users. The needs of specific users can differ. For example, one user might like to have a domain value of xyz.com and have 1.1.1.1 and 2.2.2.2 as their DNS servers. Another user might have similar requirements, but in addition might need a proxy server configured for his or her user name. If you have to attach all these attributes to each individual user, the configuration might become very large and complex. To solve this problem, multiple groups are created, each with its set of individual attributes. In this case you can simply associate a user with a group name, rather than the large number of attributes, thus minimizing the configuration complexity when you have multiple users.

By default, the Cisco ASA creates DftGrpPolicy and the other group polices that inherit most of the common attributes; only very specific attributes need to be configured explicitly for each group.

For more information about configuring tunnel groups, group policies, and users, see:
http://www.cisco.com/en/US/docs/security/asa/asa80/configuration/guide/vpngrp.html

In our Group policy definition the main attributes you need are vpn-tunnel protocol, split_tunnel_acl, and address pool location. Example 3-2 shows how this group policy was defined.

Example 3-2 Group Policy on the ASA

```
group-policy SSLClientPolicy internal
group-policy SSLClientPolicy attributes
 banner value Welcome to the SASU Group!
 vpn-tunnel-protocol ssl-client ssl-clientless
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value split_Acl
 default-domain none
 user-authentication disable
 address-pools value testpool1
 scep-forwarding-url value http://192.168.1.9/certsrv/mscep/mscep.dll
```

Connection Profile Configuration

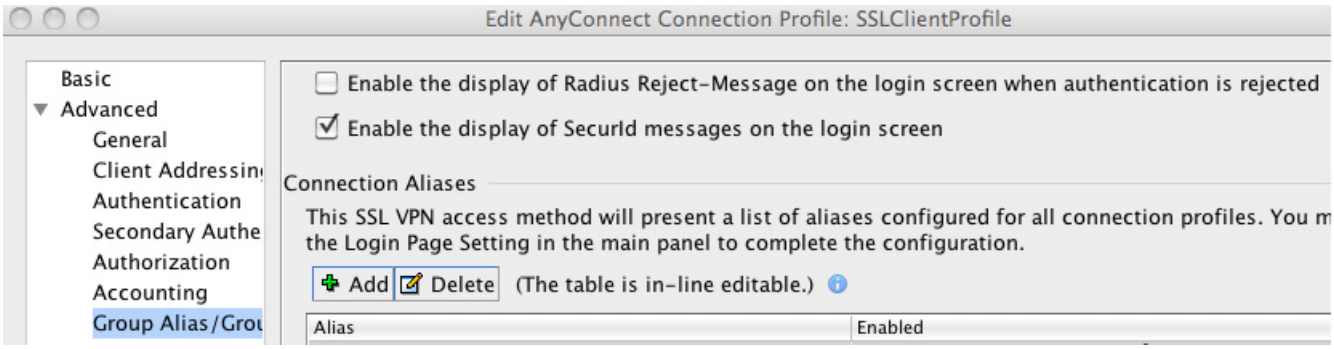
Group policies define the attributes for a group, but the connection profile specifies the attributes specific to a connection. For example, a connection profile for AnyConnect will specify if the users belonging to this connection are authenticated by a radius server or locally. The connection profile also points to the group profile to which it belongs. If no connection profile is defined on the system, the ASA points to a default connection profile, but to make administration simple it is better to define a specific group and connection profiles. Example 3-3 is the configuration on ASA for Any Connect connection profile.

Example 3-3 AnyConnect Connection Profile

```
tunnel-group SSLClientProfile type remote-access
tunnel-group SSLClientProfile general-attributes
 address-pool testpool
 authentication-server-group ACS
 default-group-policy SSLClientPolicy
 scep-enrollment enable
tunnel-group SSLClientProfile webvpn-attributes
 authentication aaa certificate
 proxy-auth sdi
 group-alias RSA enable
 group-alias SASU enable
 group-alias SSLVPNClient enable
 group-alias test enable
!
```

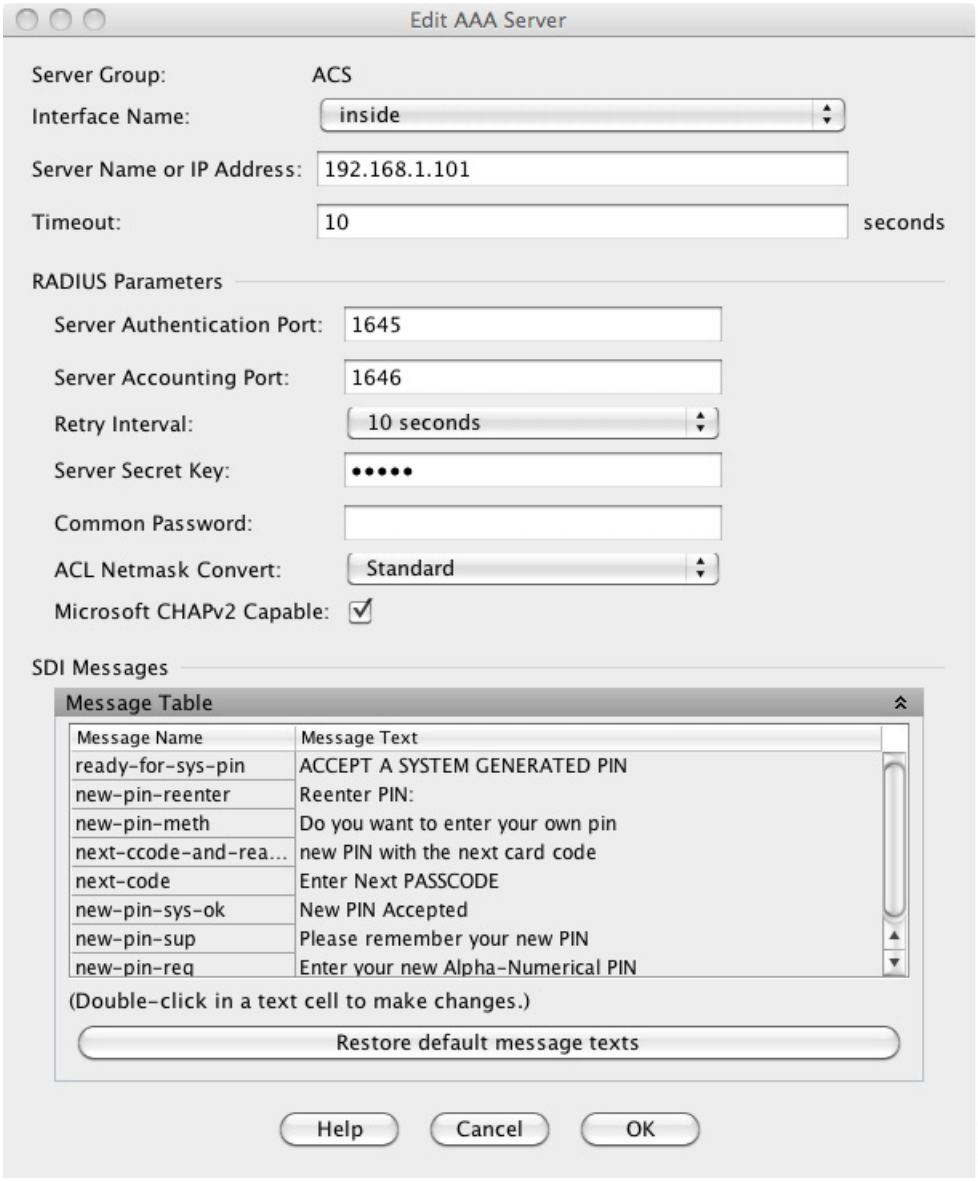
Configure the AnyConnect Connection Profile to Enable the display of SecureID Messages on the login screen of the AnyConnect Client.

Figure 3-29 Configuring the AnyConnect Connection Profile



Configure the appropriate SDI messages in the AAA Server Group for the AnyConnect Clients.

Figure 3-30 Configuring SDI Messages

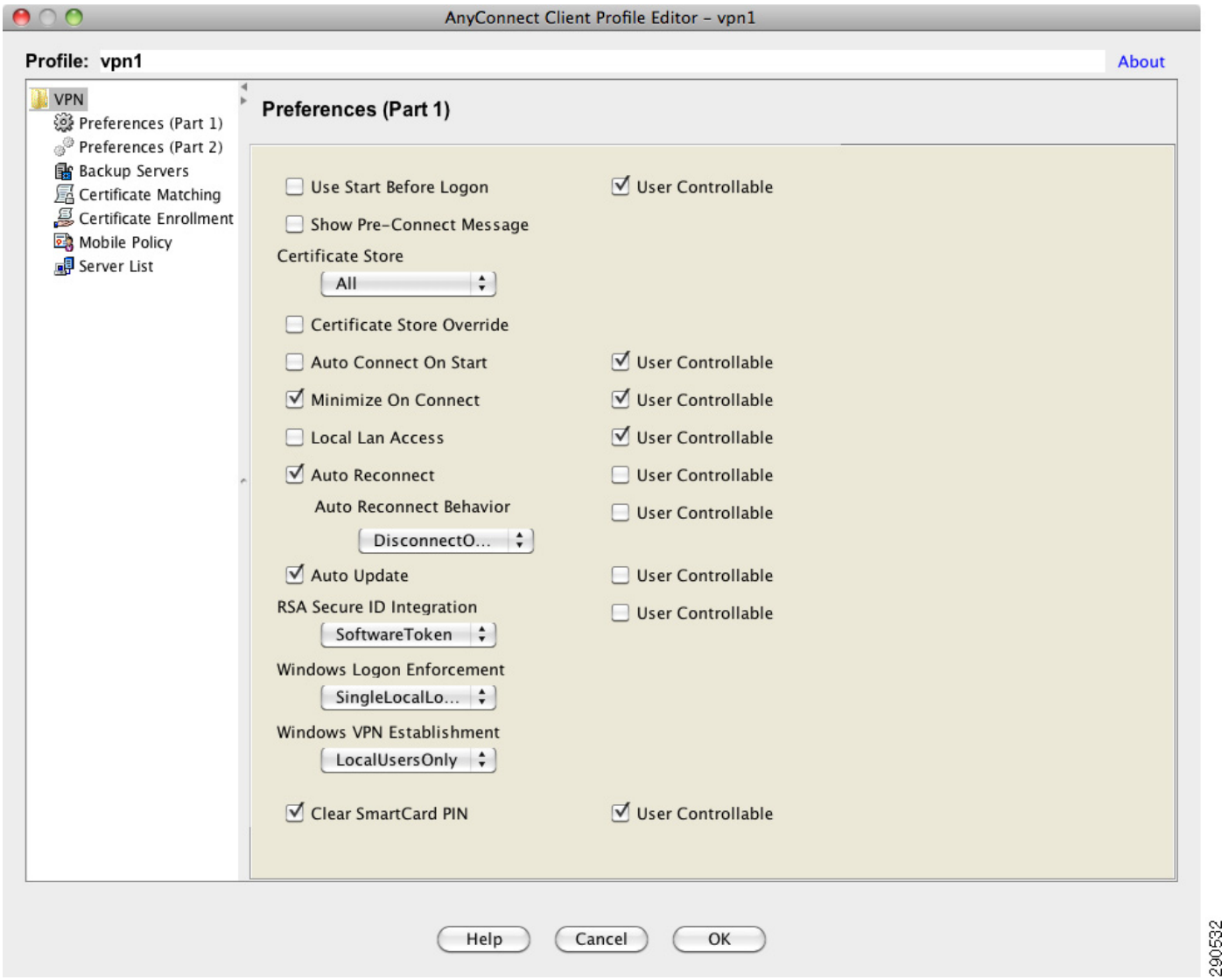


Centralizing Policy Setting for VPN Users

Remote users need more in-depth security settings then corporate users because they normally connect from un-trusted network, such as through the Internet. In the Unified Access Solution, we have enhanced the security for VPN users by mandating that remote users enter a RSA hardware token one-time password as a means to authenticate with the ASA. This section describes how to centralize policy settings by using Cisco's Adaptive Security Device Manager (ASDM). To obtain more information about ASDM, see:
http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/user/guide/usrguide.html

Figure 3-31 illustrates how to configure the VPN profile on the ASA.

Figure 3-31 Configuring the VPN Profile on the ASA



NAM Profile

The NAM profile editor is designed to allow you to create NAM configuration profiles and create pre-configured client profiles. This configuration is deployed on the endpoints so that NAM can enforce administratively-defined end user and authentication policies and make the pre-configured network profiles available to end users. To use the profile editor, create settings for a profile, save it, and then place the configurations on the client. AnyConnect includes the profile editor inside ASDM, but a standalone version is also available. Refer to the *Cisco AnyConnect Secure Mobility Client Administrator Guide*, Chapter 2, "Deploying the AnyConnect Secure Mobility Client" (http://www.cisco.com/en/US/partner/docs/security/vpn_client/anyconnect/anyconnect30/administration/guide/ac02asaconfig.html#wpxref89319) for profile editor requirements and deployment instructions.

Figure 3-32 AnyConnect Client Profiles—VPN and NAM

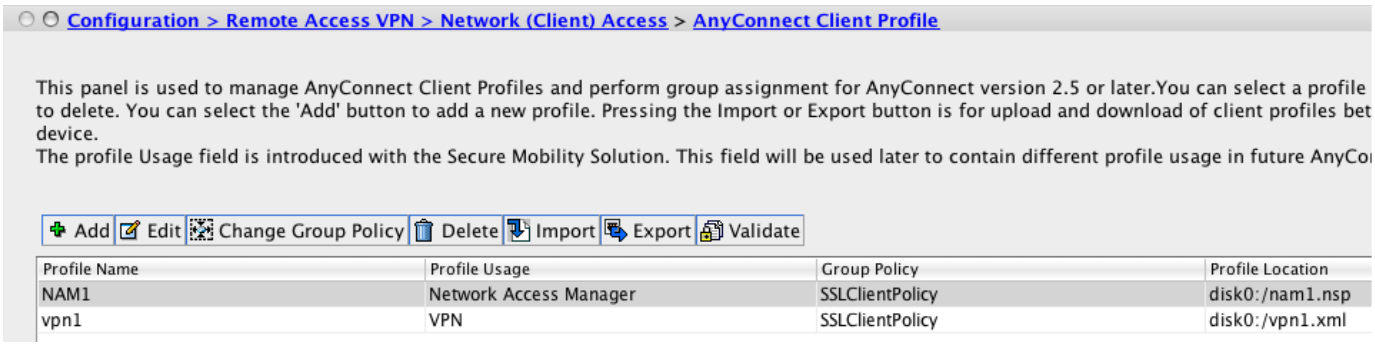
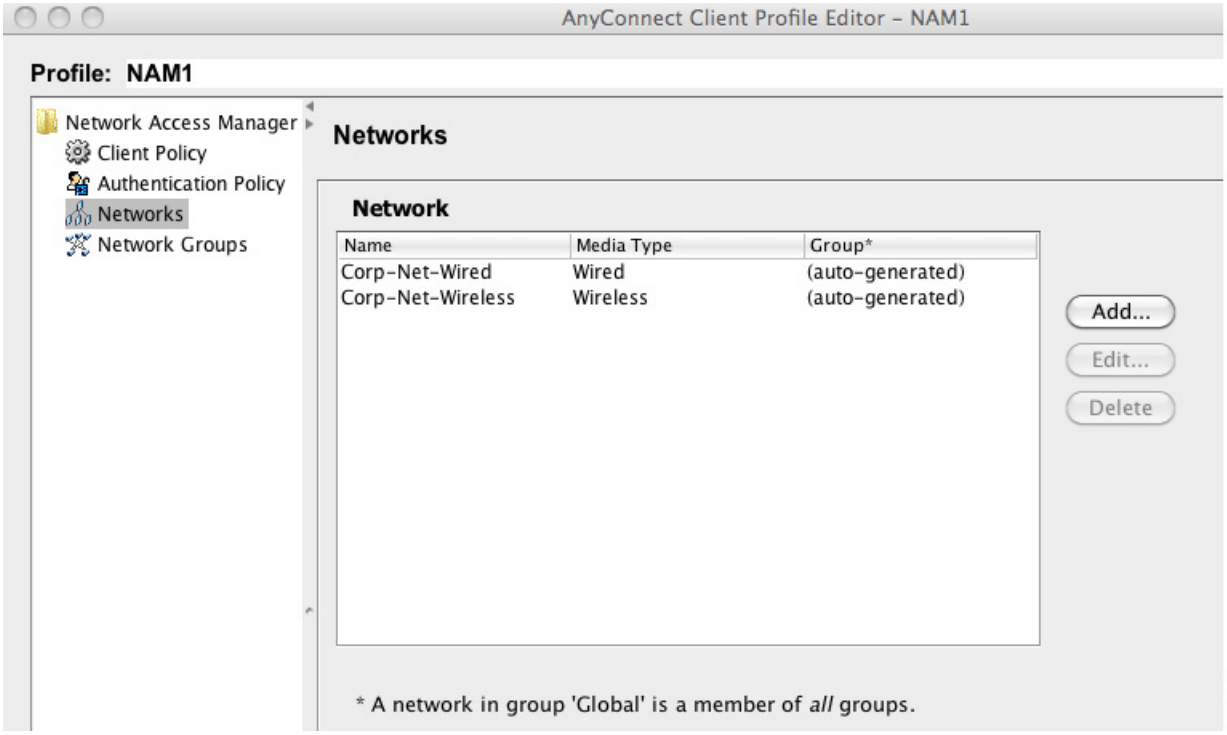


Figure 3-33 AnyConnect Client Profile Editor for NAM



The NAM profiles are loaded onto the AnyConnect client machine as XML files in the following directories:

- Windows XP:
  C:\Documents and Settings\All Users\Application Data\Cisco\Cisco AnyConnect Secure Mobility Client\Network Access Manager\newConfigFiles
- Vista/Windows 7:
  C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\ Network Access Manager\newConfigFiles

Figure 3-34 Example of the NAM XML File

Enabling AnyConnect VPN on the ASA

After defining the group-policy and connection profile on the ASA, the last piece is to enable the AnyConnect VPN feature on the ASA. After enabling AnyConnect, the administrator can also configure additional features, such as pointing to the AnyConnect image software, NAM profile, and VPN Profile. Example 3-4 is the configuration for enabling AnyConnect modules.

Example 3-4 AnyConnect Modules Definition

```
webvpn
  anyconnect keep-installer installed
  anyconnect modules value nam,telemetry,posture
  anyconnect profiles value NAM1 type nam
  anyconnect profiles value vpn1 type user
  anyconnect ask none default webvpn
  always-on-vpn profile-setting
```

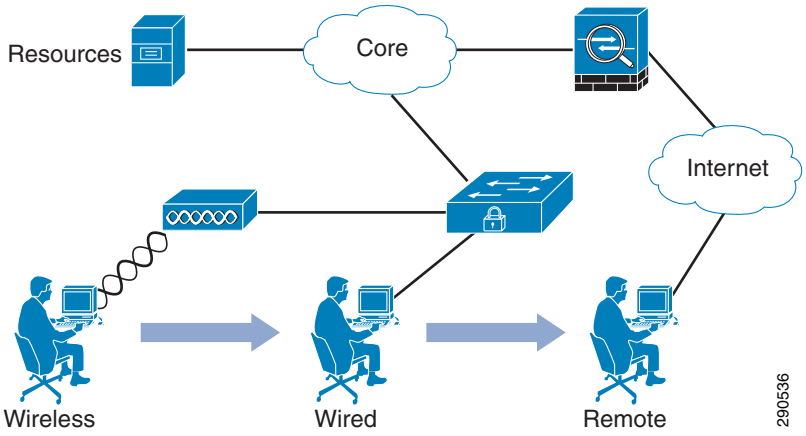
Consistent Access Experience

As mentioned in the executive summary, the Unified Access Solution addresses the user experience pain points by providing:

- Migration from an existing 802.1x wireless network that uses native supplicants to Cisco's AnyConnect mobility client.
- Deploying 802.1x solution for wired users using Cisco's AnyConnect mobility client.
- Deploying a remote access solution using Cisco's AnyConnect mobility client.
- Distributing certificates for remote users using Cisco's AnyConnect mobility client.

Figure 3-35 shows how a user can move around in an enterprise network.

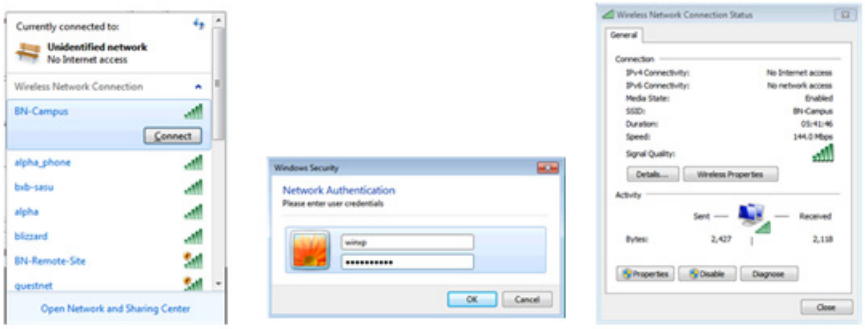
Figure 3-35 User Movement in an Enterprise Network



Users on the secure campus network currently use the existing native Microsoft 802.x wireless supplicant in order to authenticate and gain access to the network. The user is on the trusted campus network. The user has authenticated via 802.1x wireless connection from a Windows 7 client. The client is using the native Microsoft 802.1x supplicant in order to authenticate and gain access to the trusted campus wireless network. The Windows 7 Client is authenticating using PEAP (MSCHAPv2) to a Cisco 1142 AP authenticator. The authentication policy is located on the Authentication Server (Cisco ACS 5.2).

Figure 3-36 shows a successful authentication by a Microsoft 802.1x supplicant.

Figure 3-36 Successful Authentication



Campus Wireless

		Status	Name	Conditions			Results	Hit Count
				Eap Authentication Method	Authentication Method	Eap Tunnel Building Method	Identity Source	
1			Rule-1	match EAP-TLS	match x509_PKI	-ANY-	CN Username	15
2			Rule-2	-ANY-	-ANY-	match PEAP	AD1	21

Most Recent Authentication

Time:	February 16,2011 8:43:59.970 PM
RADIUS Status:	Authentication succeeded
NAS Failure:	
Username:	winxp
Network Device:	cr22-ap1 : 10.125.130.3 : 1043
Access Service:	Campus_Wireless
Authorization Profiles:	Permit Access
CTS Security Group:	
Authentication Method:	PEAP(EAP-MSCHAPv2)

290537

Migration from an Existing Native MS 802.1x Supplicant to a Cisco AnyConnect Solution

Once users have authenticated via the native 802.1x wireless supplicant, they are instructed to start the deployment of Cisco AnyConnect NAM/VPN Supplicant by clicking on a link via an internal campus Web page which redirects to the Cisco ASA trusted interface.

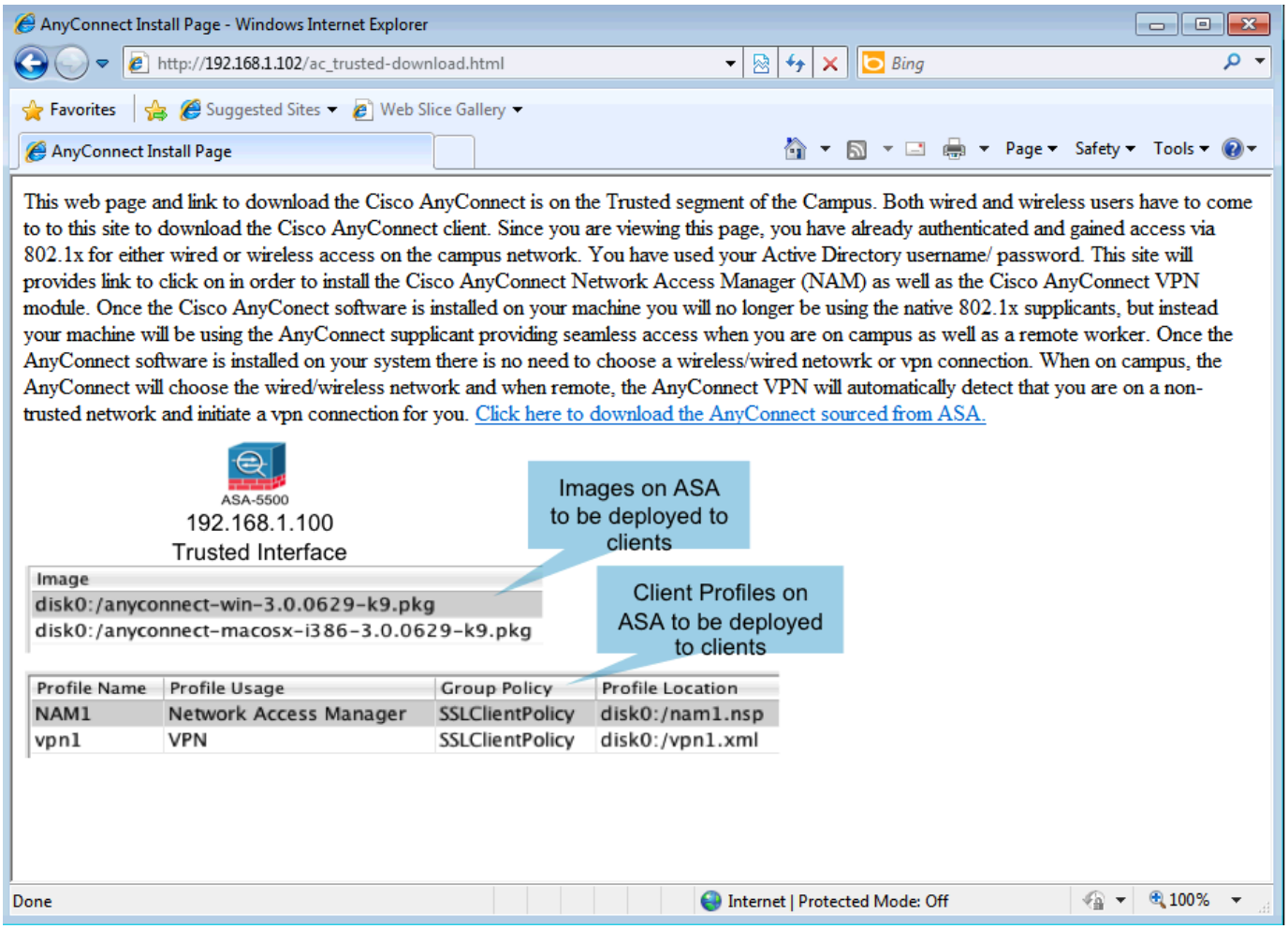
The users login to the ASA with either their RSA SecureID or Active Directory username/password. Once the user has authenticated to the ASA, the ASA determines which AnyConnect components are required to be downloaded to the client based on the client profile created by the administrator.

The NAM Supplicant must be deployed as part of the AnyConnect Secure Mobility Client VPN. The VPN is the core module for which all the other modules are installed. In order to install the AnyConnect NAM (802.1x Supplicant), the user may visit an internal Web page on the trusted campus network. This Web page points to the trusted (inside) interface of the ASA for which the ASA images are stored/maintained.

Note A Cisco ASA is not required in order to use the AnyConnect Network Access Manager. The AnyConnect Network Access Manager can be deployed without the use of an ASA. This solution uses the ASA in order to deploy both the NAM as well as the NAM profiles to the client end point. When the Cisco AnyConnect NAM module is installed, it takes over and assumes control of all 802.1x supplicant activity. The native 802.1x supplicant is no longer able to provide 802.1x services.

This allows administrators to maintain a repository of the latest AnyConnect modules, which are staged and ready to be dynamically deployed to users. Administrators could also choose to deploy the AnyConnect NAM via a software distribution system. However, having all the AnyConnect modules installed on the ASA allows for automatic unattended installs for all the AnyConnect modules to each user. Figure 3-37 shows an internal Web page presented to a user on the trusted campus network.

Figure 3-37 Web Page on Trusted Campus Network

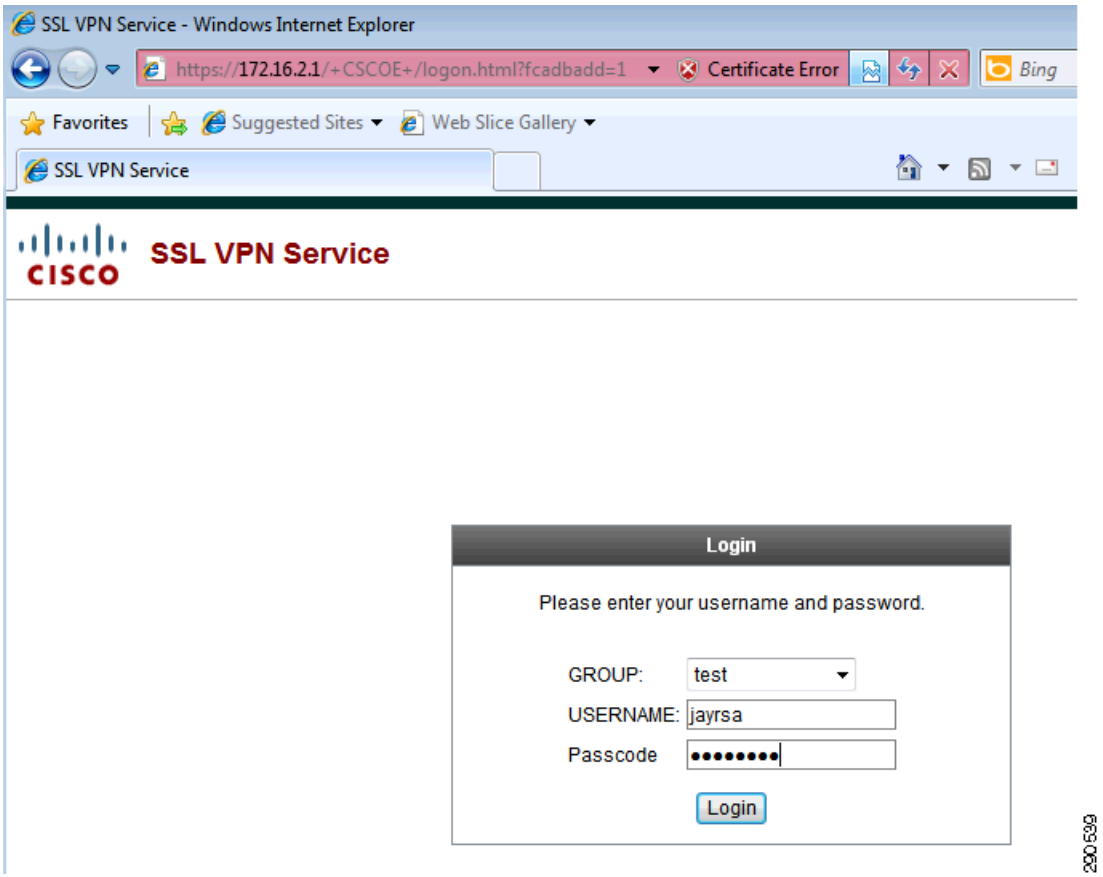


The Web page redirects clients to download the AnyConnect VPN and AnyConnect NAM module.

On the screen shown in Figure 3-37, the user clicks the link **Click here to download the AnyConnect sourced from ASA**, which redirects the user to the inside interface of the ASA for which all the AnyConnect modules are installed. Clients can also install the AnyConnect VPN and NAM modules from a VPN connection. If a client would like to install the AnyConnect modules via a VPN connection, the client simply accesses the outside interface (untrusted interface) of the ASA via HTTPS in order to begin the install process.

Once the user is redirected to the ASA via the trusted interface (users that are inside the ASA) or if users access the ASA on the untrusted interface (users residing on the public facing side of the ASA), they are both presented with the SSL VPN login screen shown in Figure 3-38.

Figure 3-38 SSL VPN Login Screen



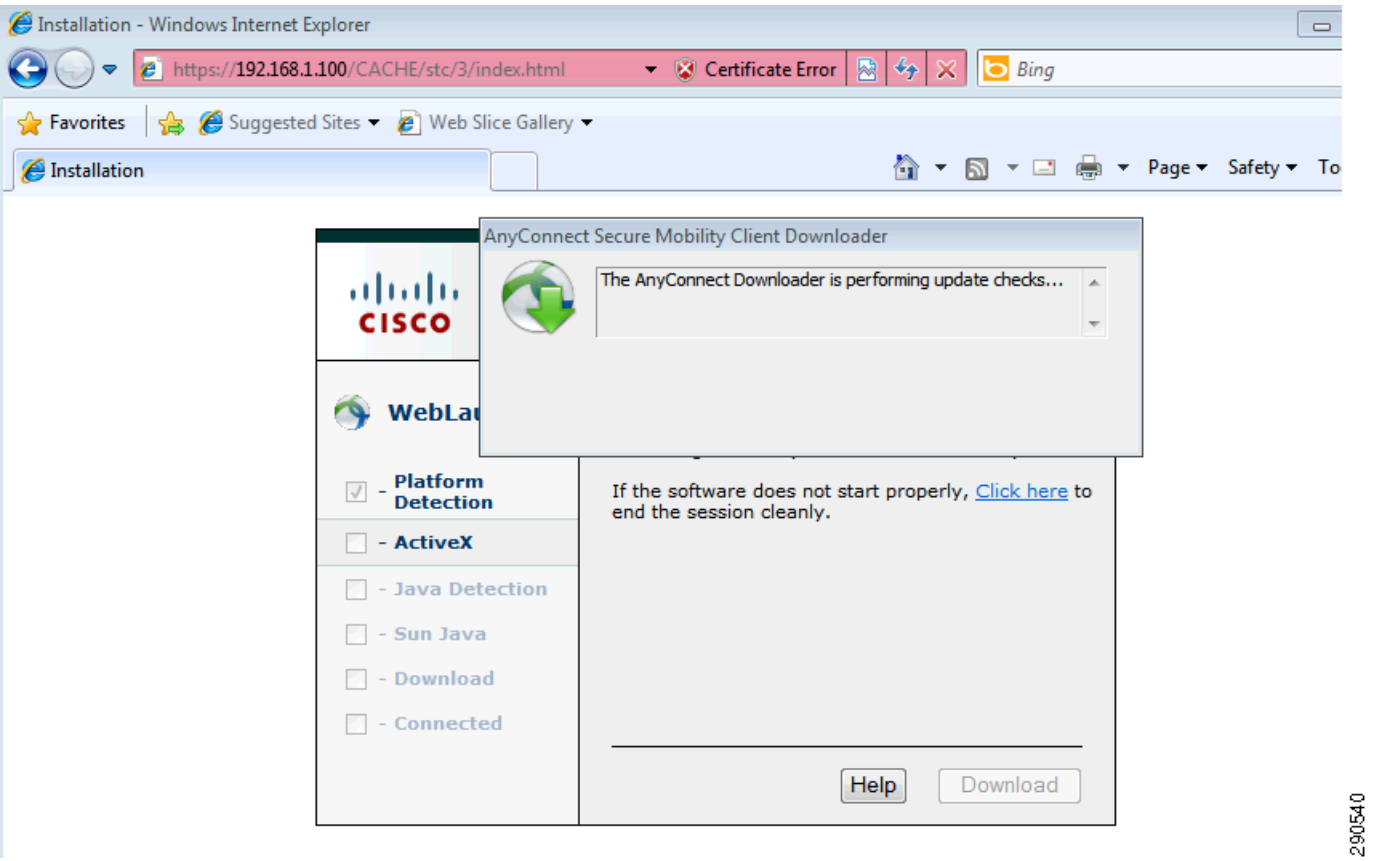
In Figure 3-38, notice the Group "test" is the user's assigned group, which will determine which type of authentication method and which AnyConnect software modules will be loaded onto the client machine.

Based on the Web page, the user is instructed to login using either their SecureID token or their Active Directory username/password. In this scenario, the user is logging in with their RSA SecureID token.

Once the user has authenticated, there are a number of checks that are performed on the client and the ASA in order to determine which AnyConnect software must be installed or updated and if any profile updates are needed for the client.

Figure 3-39 shows the ASA performing such checks.

Figure 3-39 Update Determination



The AnyConnect VPN module is the core AnyConnect module; thus, it must be installed prior to any other modules being installed. The AnyConnect VPN module is a requirement for all other AnyConnect modules. Based on the user's Connection Profile, the ASA determined that the user required the AnyConnect NAM supplicant to be installed and that two profiles needed to be sent to the client in the form of an XML file loaded onto the client's machine.

The location of the XML file, which is loaded onto the client machines, specifies the features and attribute values for each user type.

The location of the XML files are:

- Windows XP
  - Core client with VPN
    %ALLUSERSPROFILE%\Application Data\Cisco\ Cisco AnyConnect Secure Mobility Client\Profile
  - NAM (Network Access Manager)
    %ALLUSERSPROFILE%\Application Data\Cisco\ Cisco AnyConnect Secure Mobility Client\NetworkAccessManager\newConfigFiles
- Windows Vista
  - Core client with VPN
    %ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Profile

  - NAM NAM (Network Access Manager)
    %ProgramData%\Cisco\ Cisco AnyConnect Secure Mobility Client\NetworkAccessManager\newConfigFiles

- Windows 7
  - Core client with VPN
    %ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Profile
  - NAM NAM (Network Access Manager)
    %ProgramData%\Cisco\ Cisco AnyConnect Secure Mobility Client\NetworkAccessManager\newConfigFiles
- Mac OS X

  All modules
  /opt/cisco/vpn/profile
- Linux

  All modules
  /opt/cisco/vpn/profile
- iOS Devices—Apple iPhone/iPodTouch/iPad

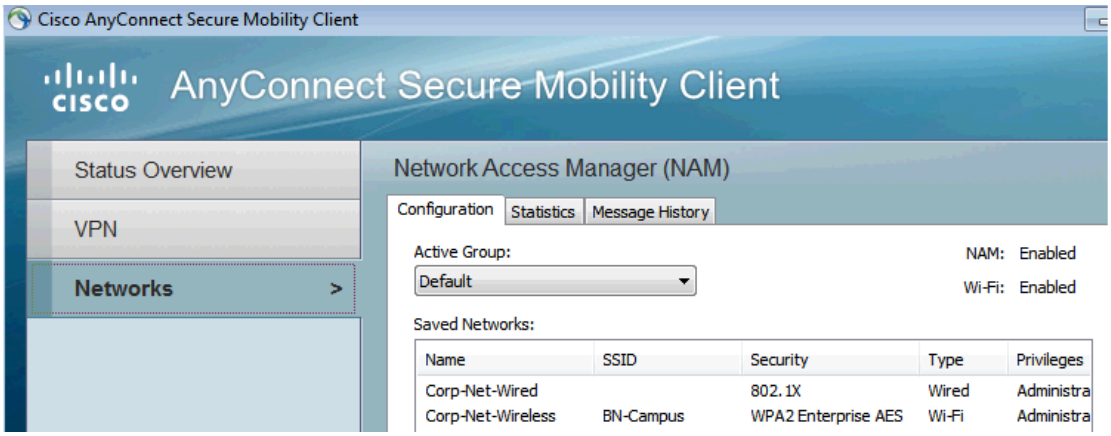
  The Apple iOS device supports only one AnyConnect XML profile. The contents of the generated configuration always match the most recent profile.

This AnyConnect NAM replaces the need for the user to use the native 802.1x supplicant and instead use the AnyConnect NAM, which has greater security and administrative control and allows the user to seamlessly connect to the campus network from both trusted and untrusted network segments using both wired and wireless networks. The client is connected to the trusted campus network dynamically when on the public Internet. The AnyConnect client understands the user is on an untrusted network and automatically establishes a VPN connection to the campus trusted network without any user intervention.

There are two profiles that are loaded onto the client machine during this process, one for secure wired access on the trusted campus and one for secure wireless access on the trusted campus network. Note that the privileges for both of these profiles (as seen below) are set to “Administrator”. This means that the security administrator on the ASA created these profiles and that the end user does not have access to alter or remove these campus trusted wired and wireless connection profiles.

Figure 3-40 shows the two client connection profiles that were loaded into the NAM on the client machine.

Figure 3-40 Two Client Connection Profiles



Once the AnyConnect NAM and AnyConnect VPN modules are installed, there is no need for the user to manually reconnect to the wireless campus. The NAM dynamically launches and connects to the Corp-Net-Wireless network (the same network for which the client was authenticated when using the Microsoft Native 802.1x Supplicant). The user is prompted to enter their username/password credentials into the AnyConnect supplicant software in a similar manner as the user was presented a username/password for the Native Microsoft Supplicant.

Figure 3-41 Username/Password Screen

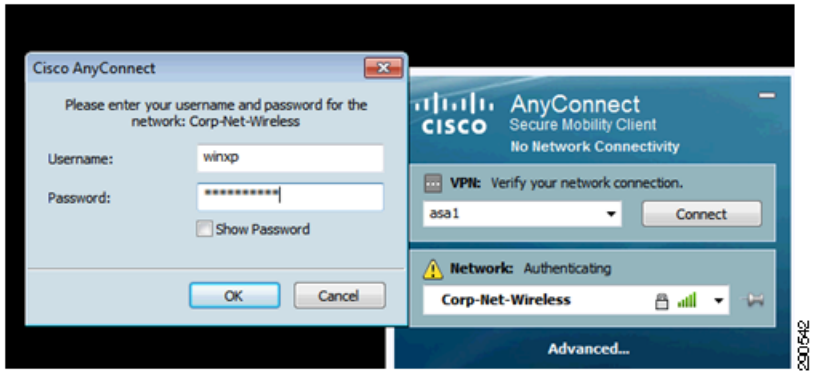


Figure 3-42 Connection Established Screen

Figure 3-42 shows that the user has authenticated to the campus wireless network and that the AnyConnect VPN Module has determined that a VPN connection is not necessary. The AnyConnect profile, which was created by the administrator on the ASA and pushed out to the client, is utilizing the feature Trusted Network Detection (TND). When TND is enabled for a connection profile, the AnyConnect supplicant determines if it is on a trusted network by sending TCP/UDP DNS queries in order to reach pre-configured secure campus name servers. If the AnyConnect supplicant is unable to reach the name server, the supplicant assumes is it on an un-trusted network and automatically launches a VPN connection.

User Moves to a Wired Connection

When an end point that is using the AnyConnect NAM supplicant moves to a wired network connection, the AnyConnect NAM supplicant prefers all wired connections over wireless connections when AnyConnect is configured for "automatic mode"; this functionality can be overridden when the AnyConnect supplicant is in "manual mode". AnyConnect automatically chooses the "Corp-Net-Wired" network profile over the existing "Corp-Net-Wireless" network profile. Only one connection is allowed at a time; all other connections on the end point machine are blocked. The AnyConnect UI automatically prompts the user if the EAP method requires (MSCHAPv2) and if the credentials are not cached. If the connection profile is configured to use SSO credentials and the credentials are incorrect, the user is required to change their password. Since the administrator on the ASA configures the network profiles, the user does not have access to edit/remove the network profiles. This greatly enhances the overall security and robustness of having AnyConnect as an 802.1x supplicant.

Figure 3-43 shows AnyConnect supplicant automatically selecting a wired connection.

Figure 3-43 Automatic Selection of Wired Connection

Example 3-5 shows the required configuration of the wired ports on the 802.1x-enabled switch.

Example 3-5 Configuration of Wired Ports on 802.1x-Enabled Switch

```
interface GigabitEthernet1/0/2
 description 1X-ONLY
 switchport access vlan 140
 switchport mode access
 switchport block unicast
 switchport voice vlan 141
 ip arp inspection limit rate 100
 load-interval 30
 srr-queue bandwidth share 10 10 60 20
```

```
 queue-set 2
 priority-queue out
 authentication port-control auto
 authentication fallback WEB-AUTH
 mab
 mls qos trust cos
 dot1x pae authenticator
 auto qos voip trust
 storm-control broadcast level pps 1k
 storm-control multicast level pps 2k
 storm-control action trap
 spanning-tree portfast
 spanning-tree bpduguard enable
 ip verify source
 ip dhcp snooping limit rate 15
end
```

User Moves to a Remote Location

The user has now moved to an untrusted segment (the public Internet) and is no longer on the campus trusted wired or wireless network. Once the wireless AnyConnect client is associated and obtains a valid IP address for the new network they just joined, the AnyConnect client again tries to establish contact with the internal name servers configured in the AnyConnect client profile. This time, the AnyConnect client is not able to establish connectivity to the trusted name servers and thus the AnyConnect client assumes it is on an untrusted segment and launches the AnyConnect VPN module. Figure 3-44 shows how AnyConnect client initiates a VPN connection when the user is on a un-trusted network, provided Trusted Network Detection is enabled.

Figure 3-44 AnyConnect Initiates VPN Connection

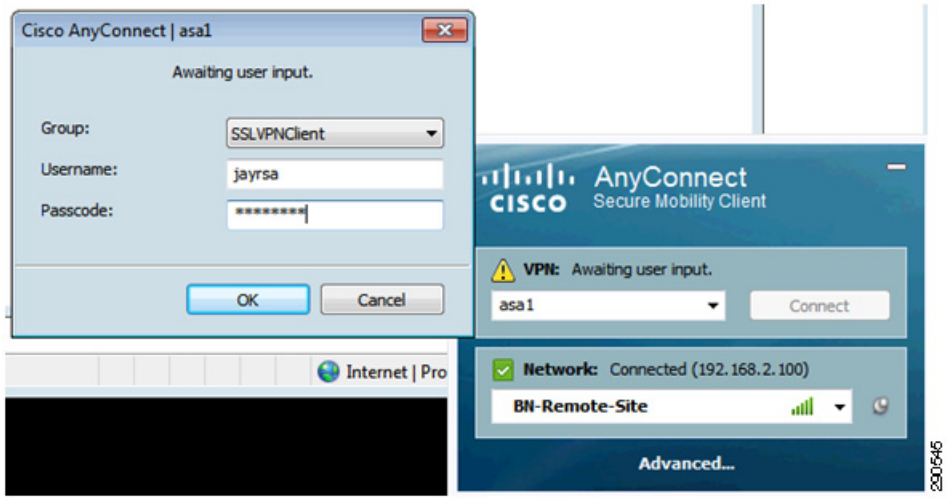
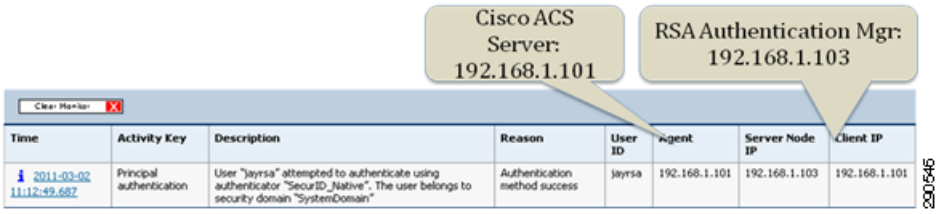


Figure 3-45 shows a successful RSA SecureID login via AnyConnect SSL VPN on the RSA Server.

Figure 3-45 Successful RSA SecureID Login



AnyConnect Secure Mobility Client 2.4 for iOS Devices

We discussed earlier that the AnyConnect Security mobility client 3.0 supports Web deployment. The Security Mobility client version 2.4 which runs on iOS mobile devices does not support Web deployment; instead, users download and install the AnyConnect Security mobility client via the Apple iTunes Store.

AnyConnect 2.4, which is the supported version on the iOS devices (iPad, iPhone, and iTouch), supports SCEP by having the client mobile device send a SCEP request directly to the CA server once the VPN has been established. Figure 3-46 shows the required configuration on AnyConnect Client Profile Editor on ASA for SCEP.

Figure 3-46 Configuration on AnyConnect Client Profile Editor on ASA for SCEP

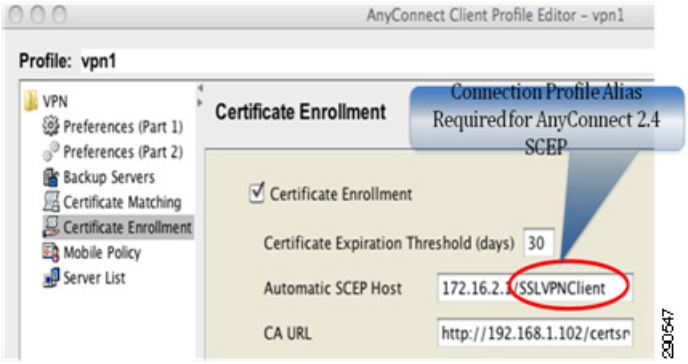


Figure 3-47 shows a trace on the CA server of the AnyConnect 2.4 client making a SCEP request directly to the CA server using the client source IP address. As mentioned the AnyConnect 2.4 client does not support the new 3.0 SCEP-Proxy feature; instead, the AnyConnect 2.4 clients sends a SCEP request directly to the CA server, rather than having the ASA proxy the SCEP, as shown in Figure 3-47. Figure 3-47 shows an AnyConnect 2.4 client running on an iPad. Notice the source IP address is that of the iPad and not the ASA. This trace was taken on the CA server itself.

Figure 3-47 Trace on CA Server

The user logs in using RSA Secured ID credentials in order to set up a SSL VPN so that the certificate enrollment process is conducted over a secure channel. Figure 3-48 shows how the user selects a connection profile after entering RSA credentials.

Figure 3-48 Connection Profile Selection

In Figure 3-48, notice that the Group "SSLVPNClient" must match the group configuration in the above VPN Profile configuration. This is a requirement in order to support SCEP on AnyConnect 2.4. AnyConnect 3.0 does not require the Group "SSLVPNClient" to be specified in the VPN Profile configuration, however it is recommended in order to support both AnyConnect 3.0 SCEP-Proxy as well as AnyConnect 2.4 SCEP forwarding.

In Figure 3-49, the AnyConnect is displaying a message which indicates the enrollment process using SCEP on the AnyConnect client has succeeded.

Figure 3-49 Enrollment Process Success

A valid client certificate is now available to be used for the next SSL VPN connection. Figure 3-50 shows the IP address obtained by the iPad.

Figure 3-50 iPad Client IP Address

In Figure 3-51, the user chooses the newly enrolled client certificate, which the AnyConnect client sends to the ASA during authentication of the SSL VPN connection.

Figure 3-51 Selecting the Newly Enrolled Client Certificate

In Figure 3-52, the AnyConnect client is displaying the client IP address that is the source IP address of the end point for the SSL VPN Connection. Notice that this IP address (192.168.1.11) is the source IP address which was used as the source of the SCEP request in order to obtain the client certificate during the certificate enrollment process.

Figure 3-52 Client IP Address

AnyConnect Secure Mobility Client 3.0

This section discusses a scenario where a remote user is in possession of an RSA SecureID token, but still does not have possession of a digital certificate. When the user initiates an SSL VPN session using the AnyConnect client, the ASA which is configured for two-factor authentication, as well as client certificate authentication, authenticates the user initially using the RSA two-factor authentication token. After validating the user/token, the ASA then sends the AnyConnect client a request for a certificate. However, since the client does not yet have a certificate, the ASA begins the SCEP process on behalf of the client. The SCEP process is completed over the SSL VPN connection. Once the certificate enrollment is successful (the client has received the certificate from the CA), the VPN connection is terminated. Immediately following the termination of the VPN connection, the AnyConnect client again initiates a connection to the ASA, but this time the user logs in with both two-factor authentication as well as presenting the newly-obtained client certificate to the ASA. Figure 3-53 shows the configuration of the ASA acting as a SCEP-Proxy. Also note that the IP address 172.16.2.1 shown in Figure 3-53 is the outside interface of the ASA.

Figure 3-53 AnyConnect Client Issuing a SCEP Request

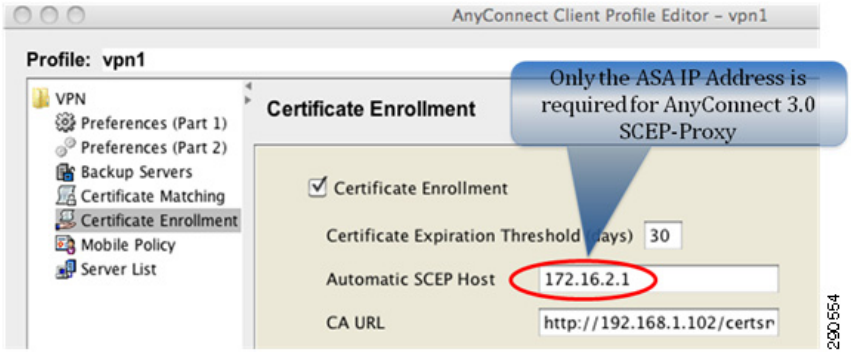


Figure 3-54 displays a packet capture, which was taken on the CA Server. This packet capture shows the client IP address which is the trusted interface of the ASA. The ASA is proxying the SCEP request on behalf of the client. The source IP address of the SCEP request is 192.168.1.100, which is the inside/trusted interface of the ASA. The destination IP address (192.168.1.102) is the CA server.

Figure 3-54 Packet Capture on CA Server

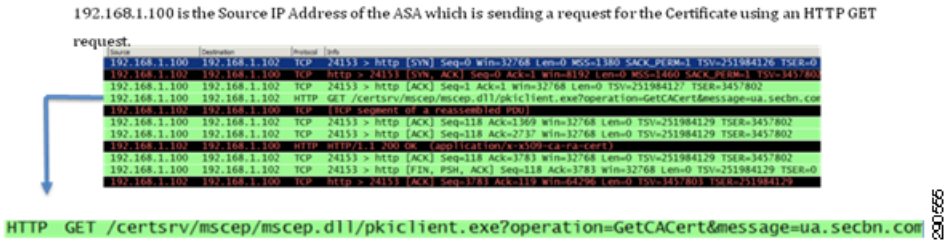


Figure 3-55 displays a Windows 7 client running AnyConnect Secure Mobility Client 3.0 using the same VPN Group (SSLVPNClient) as the AnyConnect Secure Mobility Client 2.4 used.

Figure 3-55 Windows 7 Client Running AnyConnect Secure Mobility Client 3.0 Using VPN Group

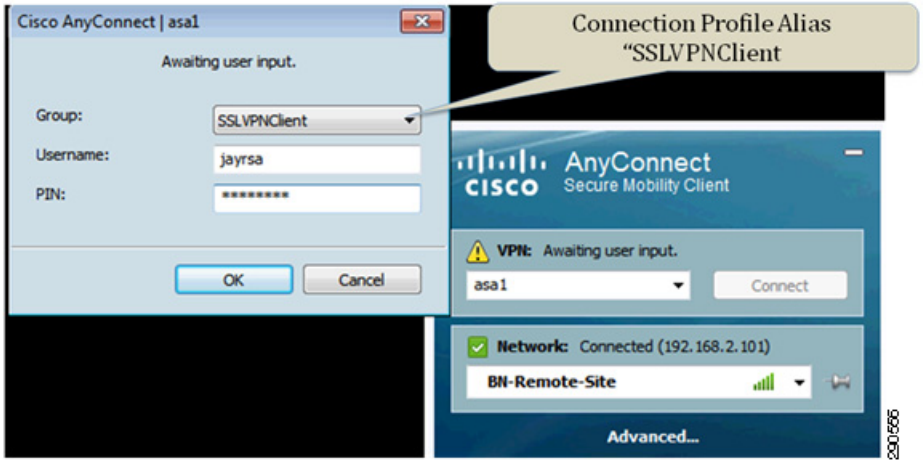


Figure 3-56 displays a Windows 7 client running AnyConnect Secure Mobility Client 3.0 has successfully received a client certificate via the SCEP-Proxy feature on the ASA.

Figure 3-56 Windows 7 Client Running AnyConnect Secure Mobility Client 3.0—Successful Clent Certificate

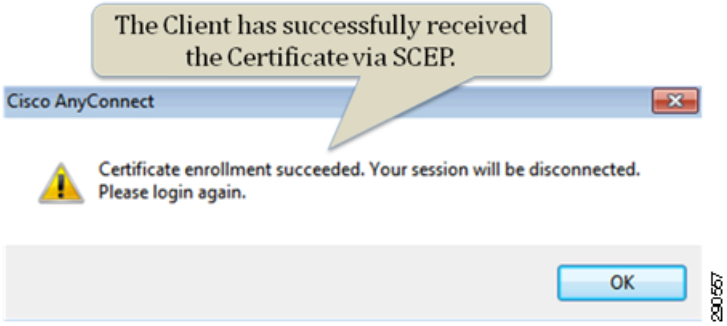


Figure 3-57 displays a Windows 7 client running AnyConnect Secure Mobility Client 3.0 where the user is prompted to choose the certificate to send to the ASA during authentication for the SSL VPN connection.

Figure 3-57 Windows 7 Client Running AnyConnect Secure Mobility Client 3.0—Certificate Selection

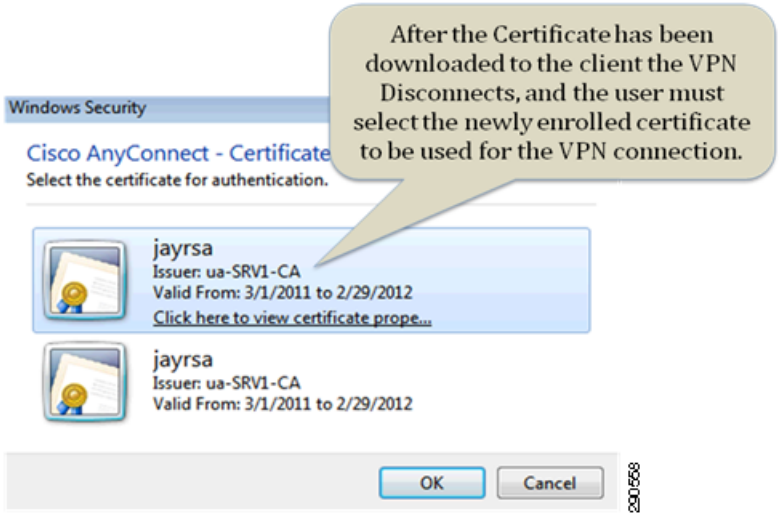


Figure 3-58 displays a Windows 7 client running AnyConnect Secure Mobility Client 3.0 and displaying that the source IP address of the AnyConnect client is 192.168.1.13. Note that during the SCEP process, this source IP address (192.168.1.13) was not used as the SCEP source; rather, the trusted/inside interface of the ASA was used.

Figure 3-58 Windows 7 Client Running AnyConnect Secure Mobility Client 3.0—Source IP Address

Summary

There has been major adoption of 802.1x technology for wireless devices because of the many benefits the technology provides in authentication and authorization. For wired users, the deployment of 802.1x technology is challenging because of the inconsistent behavior of supplicants on the native operating systems. Moreover, with the evolution of mobile devices in the market today, many employees require

access to business resources using both their traditional devices, such as laptops and desktops, and their personal devices, such as smart phones and tablets. While the productivity of employees is greatly improved with the ability to access the network with different end points, it also increases security risks. To balance the productivity gains versus the security risks, network architects must design the network such that users are securely authenticated and identified and their transactions are logged with a single solution for wired, wireless, and remote users.

The Unified Access Solution for security enables the network architect to:

- Maintain a centralized access control on all the access points of the network by authenticating both wired and wireless users.
- Identify users with digital certificates along with strong two-factor authentication.
- Provide digital certificates to users who can access the CA server directly with the help of the SCEP protocol and also to remote users by the SCEP-PROXY feature supported by ASA.
- Support different flavors of EAP authentication methods.
- Provide a method to easily migrate from an existing 802.1x environment with native supplicants to the Cisco AnyConnect client.
- Enforce two-factor authentication for remote users by using RSA SecureID tokens.
- Centralize the network profiles for 802.1x clients for both wired and wireless users.