Machine and User Authentication with Bluesocket Transparent 802.1x-PEAP-MSCHAPv2 and Windows clients

Authors: Vincent Larue, Mike Diss and Peter Reinders
Date: January 24, 2008
Revision: v2.0

Overview

The Bluesocket Transparent 802.1x authentication offers client PCs the possibility to have a seamless logon to their Windows domain and be automatically authenticated to the BlueSecure Wireless LAN over an encrypted wireless connection.

From a user's perspective, the implications of this approach are that they can move from a wired connection to a wireless connection completely transparently. Also the solution provides a single sign on experience, no additional credentials for the wireless connection are required.

The solution described in this tech note utilizes:

- BlueSecure Access Points (or 3rd party APs)
- BlueSecure Controller
- Microsoft Windows 2003 Enterprise Edition with built-in 802.1x compliant RADIUS server (IAS)
- Standard Windows "wireless zero configuration" supplicant on the client PC, i.e. no additional client software is required over and above the built-in Windows 802.1X supplicant.
- 802.1x authentication with EAP-PEAP-MSCHAPv2

The approach uses a two step 802.1x authentication:

Step 1: Machine Authentication to the domain

Step 2: User Authentication via the standard Windows login prompt

The use of transparent 802.1X authentication method is required in order to provide the initial machine authentication via 802.1X to the Windows domain and IAS. If only user authentication is required, you can also select the Bluesocket's Internal 802.1x authentication method. See our tech notes about *Internal 802.1x Authentication* and *Single Sign On with 802.1x Authentication*.

A separate LDAP query to the AD server can be used to dynamically place the users in a role based on their returned AD attributes.

Required configuration steps:

1. Configure transparent 802.1x on Bluesocket Controller
2. Configure the Microsoft 2003 certificate infrastructure
3. Configure Active Directory for accounts and groups
4. Configure IAS server for 802.1X authentication
5. Configure Windows Wireless clients

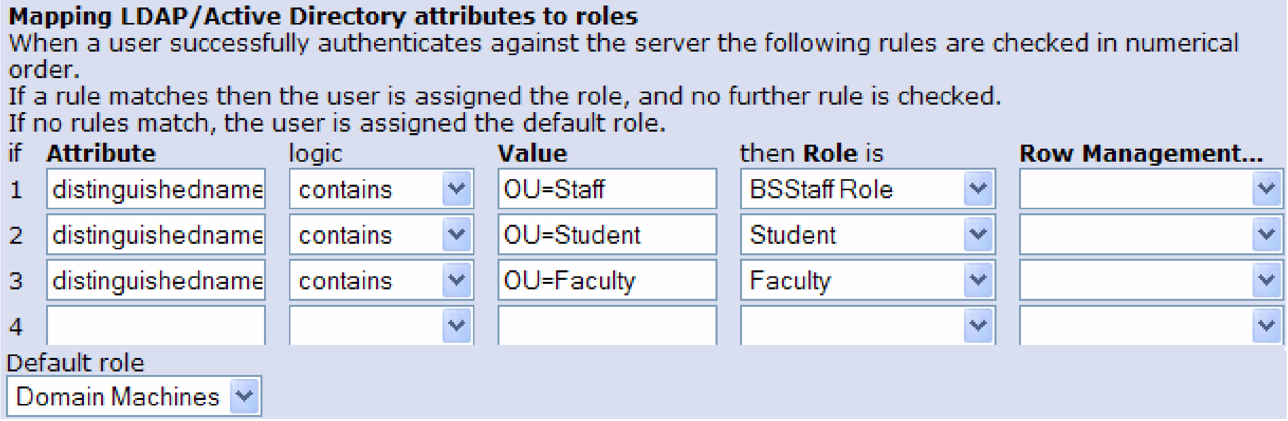
1. How to Configure Transparent 802.1X authentication on the BSC

The configuration on the BSC is simple and straight forward:

- an LDAP server for role placement
- Transparent 802.1X server for 802.1X authentication
- BlueSecure Access Points and SSID configuration

1a LDAP Server

On the LDAP configuration, we specify what role to put users into based on their Distinguished Name, but leave the default role as Domain Machines. This provides a simple mechanism for putting machines into a separate machine role when they initially authenticate as machine.



Mapping LDAP/Active Directory attributes to roles
When a user successfully authenticates against the server the following rules are checked in numerical order.
If a rule matches then the user is assigned the role, and no further rule is checked.
If no rules match, the user is assigned the default role.

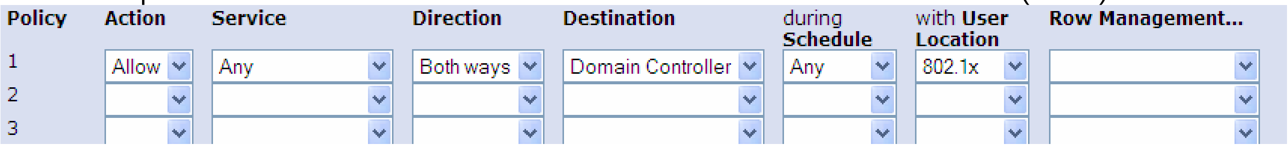
if	**Attribute**	logic	**Value**	then **Role** is	**Row Management...**
1	distinguishedname	contains	OU=Staff	BSStaff Role	
2	distinguishedname	contains	OU=Student	Student	
3	distinguishedname	contains	OU=Faculty	Faculty	
4					

Default role
Domain Machines

Role: Domain Machines

This role would allow access to just the Domain Controller and hence protect a stolen machine that's registered on the domain from being used to attack the network without the user logging on.

In the example below traffic is limited between the domain controller and 802.1x users (VLAN).



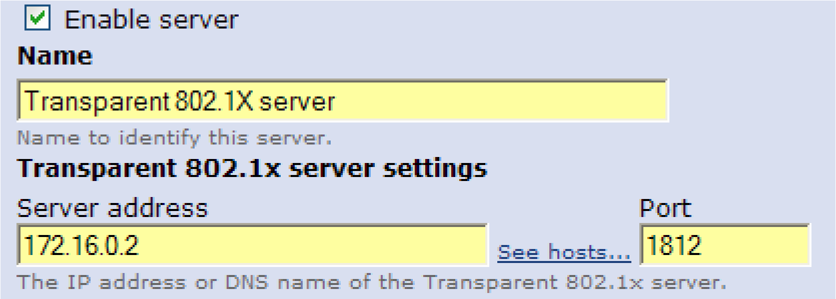
Policy	**Action**	**Service**	**Direction**	**Destination**	during **Schedule**	with **User Location**	**Row Management...**
1	Allow	Any	Both ways	Domain Controller	Any	802.1x	
2							
3							

It may also be useful to only opening ports in the "domain machine" role (or un-registered role) for windows authentication, so that the machine is allowed to talk to the domain controller on various NTLM ports (Kerberos, MS-DS, Loc-srv, netbios and LDAP). The required ports are:

135 TCP RPC Distributed File System DFS
138 UDP NetBIOS Datagram Service Distributed File System Dfs
139 TCP NetBIOS Session Service Distributed File System Dfs
389 TCP LDAP Server Distributed File System Dfs
389 UDP LDAP Server Distributed File System Dfs
445 TCP SMB Distributed File System Dfs
445 TCP SMB Net Logon Dfs

1b: Transparent 802.1x Server

The configuration of Transparent 802.1X server is very simple to configure; first we give it the address of the RADIUS server (in this case 172.16.0.2):



☑ Enable server

Name

Transparent 802.1X server

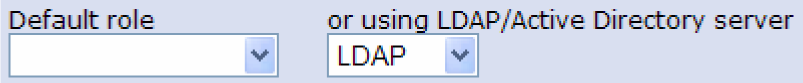
Name to identify this server.

Transparent 802.1x server settings

Server address		Port
172.16.0.2	See hosts...	1812

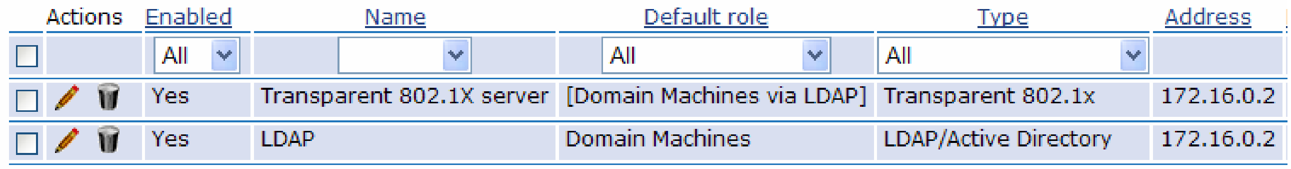
The IP address or DNS name of the Transparent 802.1x server.

Secondly, we specify that the LDAP server should be used for role placement:



Default role	or using LDAP/Active Directory server
	LDAP

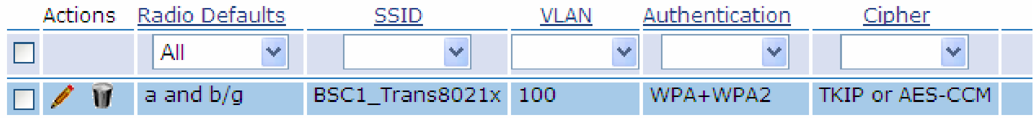
Summary external authentication servers:



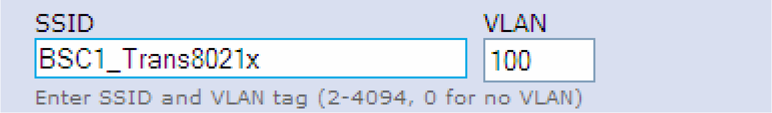
	Actions	Enabled	Name	Default role	Type	Address
☐		All		All	All	
☐	✎ 🗑	Yes	Transparent 802.1X server	[Domain Machines via LDAP]	Transparent 802.1x	172.16.0.2
☐	✎ 🗑	Yes	LDAP	Domain Machines	LDAP/Active Directory	172.16.0.2

1c: BlueSecure Access Points and SSID Configuration

We then configure the APs to act as the Authenticator for 802.1X. In this case, we are using BlueSecure Access Points (BSAPs) and hence via the BSC, we create a new SSID for 802.1X that will be loaded onto the BSAPs:



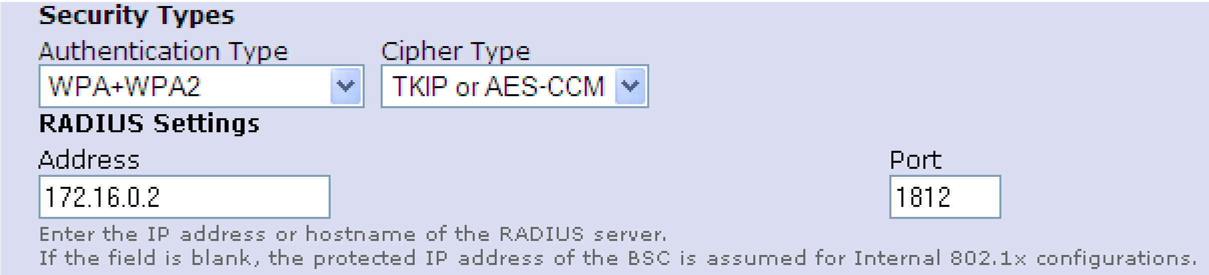
	Actions	Radio Defaults	SSID	VLAN	Authentication	Cipher
☐		All				
☐	✎ 🗑	a and b/g	BSC1_Trans8021x	100	WPA+WPA2	TKIP or AES-CCM



SSID	VLAN
BSC1_Trans8021x	100

Enter SSID and VLAN tag (2-4094, 0 for no VLAN)

The important setting here is the security settings for which we select WPA (or WPA2) and TKIP (or AES). Note the RADIUS server is configured to be the external Windows 2003 IAS RADIUS server.



Security Types

Authentication Type	Cipher Type
WPA+WPA2	TKIP or AES-CCM

RADIUS Settings

Address	Port
172.16.0.2	1812

Enter the IP address or hostname of the RADIUS server.
If the field is blank, the protected IP address of the BSC is assumed for Internal 802.1x configurations.

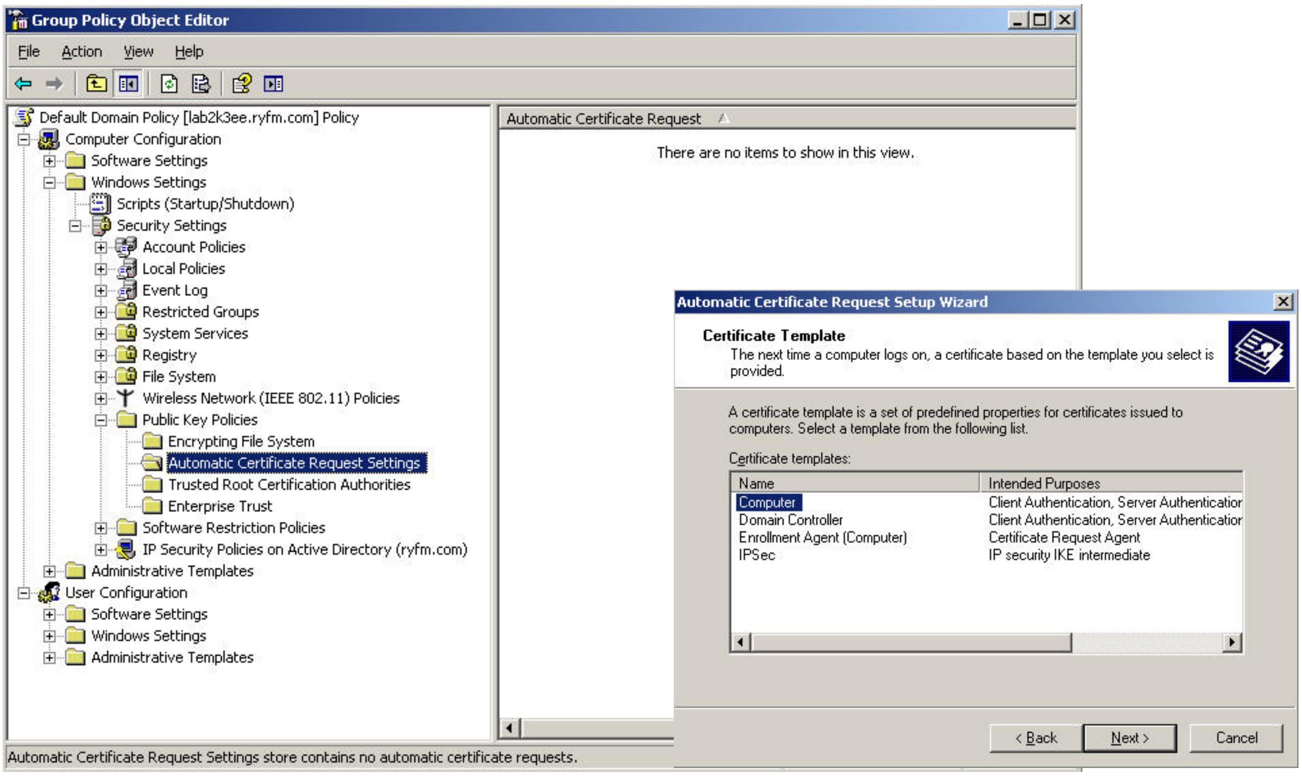
2. Configure the Microsoft 2003 certificate infrastructure

We assume a server certificate is already issued by a Certificate Authority and installed on the IAS server (see Appendix A for an example of doing this using the Windows CA).

If you would like to validate the server certificate on the client PCs (see also paragraph 5 ‘Configure Wireless clients’), you can configure a group policy for automatic distribution of the computer certificate to any computers in an Active Directory container (a domain, site, or organizational unit). Or you choose to copy manually the certificate.

To configure computer certificate auto enrollment for an enterprise CA:

1. Open the Active Directory Users and Computers snap-in.
2. In the console tree, double-click Active Directory Users and Computers, right-click the domain name to which your CA belongs, and then click Properties.
3. On the Group Policy tab, click the appropriate Group Policy object (the default object is Default Domain Policy), and then click Edit.
4. In the console tree, open Computer Configuration, then Windows Settings, then Security Settings, then Public Key Policies, then Automatic Certificate Request Settings.



There are no items to show in this view.

Automatic Certificate Request Settings store contains no automatic certificate requests.

Automatic Certificate Request Setup Wizard

Certificate Template

The next time a computer logs on, a certificate based on the template you select is provided.

A certificate template is a set of predefined properties for certificates issued to computers. Select a template from the following list.

Certificate templates:

Name	Intended Purposes
Computer	Client Authentication, Server Authenticatior
Domain Controller	Client Authentication, Server Authenticatior
Enrollment Agent (Computer)	Certificate Request Agent
IPSec	IP security IKE intermediate

5. Right-click Automatic Certificate Request Settings, point to New, and then click Automatic Certificate Request.
6. The Automatic Certificate Request wizard appears. Click next.
7. In Certificate templates, click Computer, and then click next.
8. Your enterprise CA appears on the list.
9. Click the enterprise CA, click next, and then click Finish.
10. Force a refresh of Computer Configuration Group Policy by typing **gpupdate /target:computer** from a command prompt.

3. Configure Active Directory for Accounts and Groups

We assume that Active Directory is already configured in order that user and computer accounts and groups have wireless access through 802.1x.

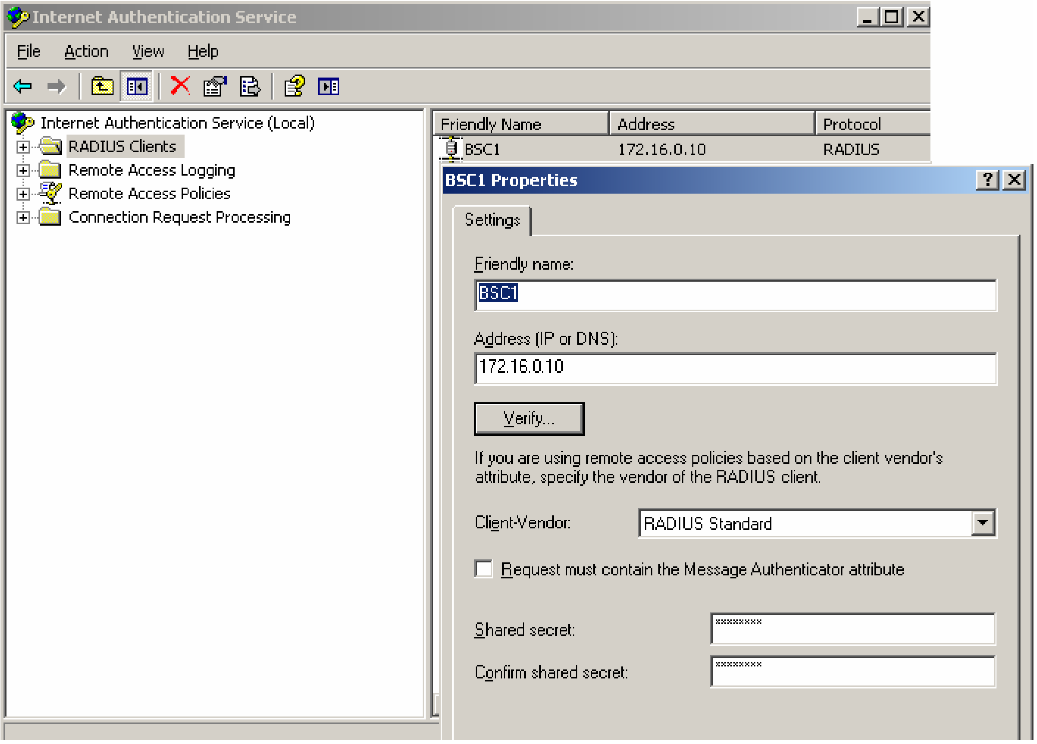
Some steps to ensure:

1. All users that are making wireless connections have a corresponding user account.
2. All computers that are making wireless connections have a corresponding computer account.
3. The remote access permission on user and computer accounts to the appropriate setting (either Allow access or Control access through Remote Access Policy).

To simplify the configuration of a wireless remote access policy on the IAS servers, organize your wireless access user and computer accounts into the appropriate groups. For a nativemode domain, you can use universal and nested global groups. For example, create a universal group named *'WirelessUsers'* that contains global groups of wireless user and computer accounts for intranet access.

4. Configuring IAS for 802.1X authentication

4a: Creating radius client representing the BSC



Friendly Name	Address	Protocol
BSC1	172.16.0.10	RADIUS

Friendly name: BSC1

Address (IP or DNS): 172.16.0.10

If you are using remote access policies based on the client vendor's attribute, specify the vendor of the RADIUS client.

Client-Vendor: RADIUS Standard

☐ Request must contain the Message Authenticator attribute

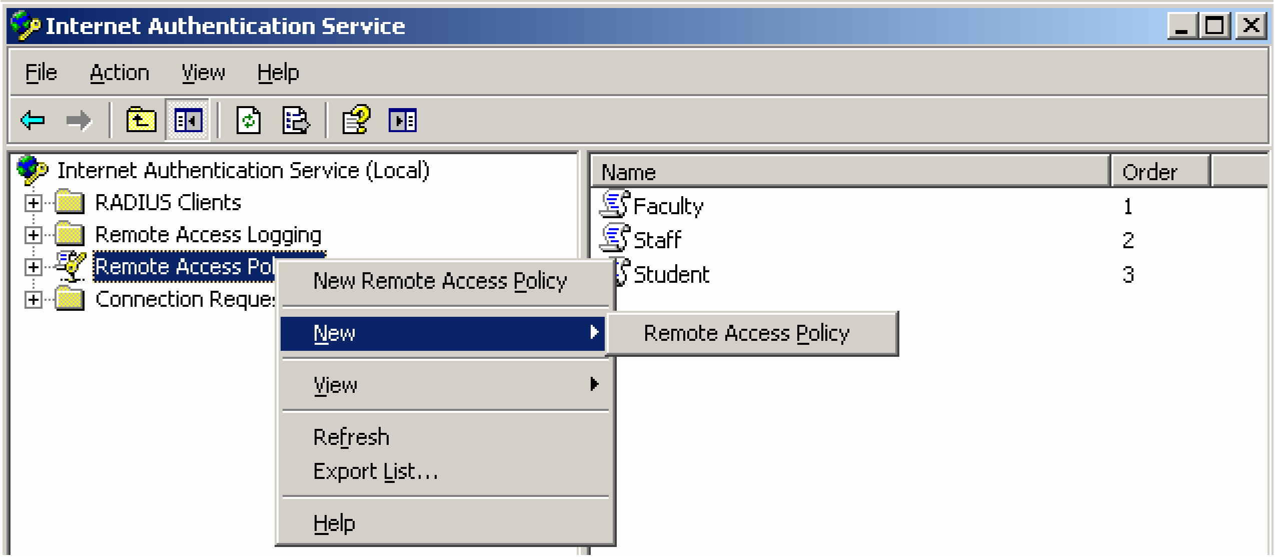
Shared secret: ********

Confirm shared secret: ********

First, we create a Radius client representing the BSC. Please note you don't need to create clients representing the individual BSAPs because the 802.1X authentication traffic that reaches the IAS server is actually sourced from the BSC rather than the BSAPs. This is due to the fact that traffic is tunneled from the BSAPs to the BSC and from there, to the IAS server. This is in contrast to using 3rd party APs where each AP would have to be added as a Radius client to the IAS server. This means we don't need to worry about amending the IAS server each time we wish to add a new BSAP.

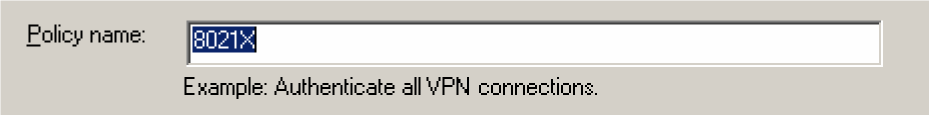
4b: Creating a new 802.1x Remote Access Policy

The shared secret you specify here will match the secret you configured on the BSAP when creating the 802.1X SSID. We now create a new Remote Access Policy associated with all users attempting to connect to the domain via 802.1X.



Name	Order
Faculty	1
Staff	2
Student	3

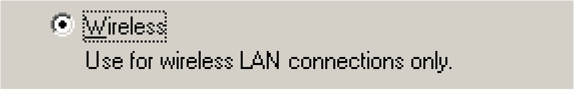
We'll create a new policy called "8021X":



Policy name: 8021X

Example: Authenticate all VPN connections.

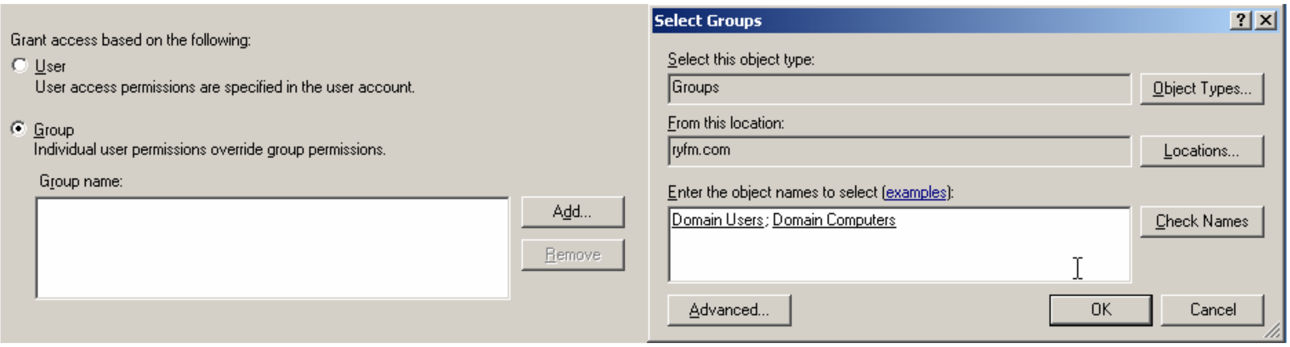
The access method for this policy will be "Wireless":



● Wireless

Use for wireless LAN connections only.

We want the policy to grant access to Domain Users and Domain Computers:



Grant access based on the following:

○ User

User access permissions are specified in the user account.

● Group

Individual user permissions override group permissions.

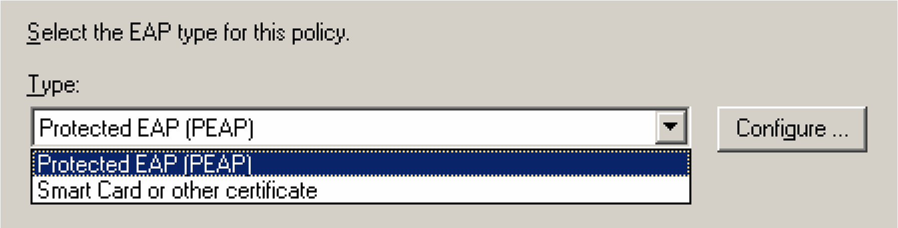
Group name:

Select this object type: Groups

From this location: ryfm.com

Enter the object names to select (examples): Domain Users; Domain Computers

Now we can select the EAP type for the policy which in this case will be PEAP:

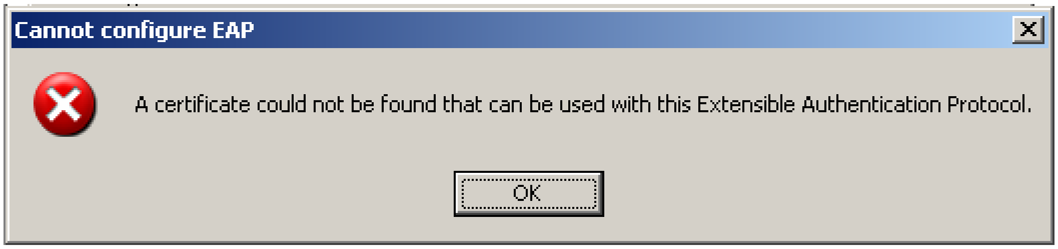


Select the EAP type for this policy.

Type: Protected EAP (PEAP)

Protected EAP (PEAP)
Smart Card or other certificate

If the IAS server has not been issued with a certificate, the following error message will be given:

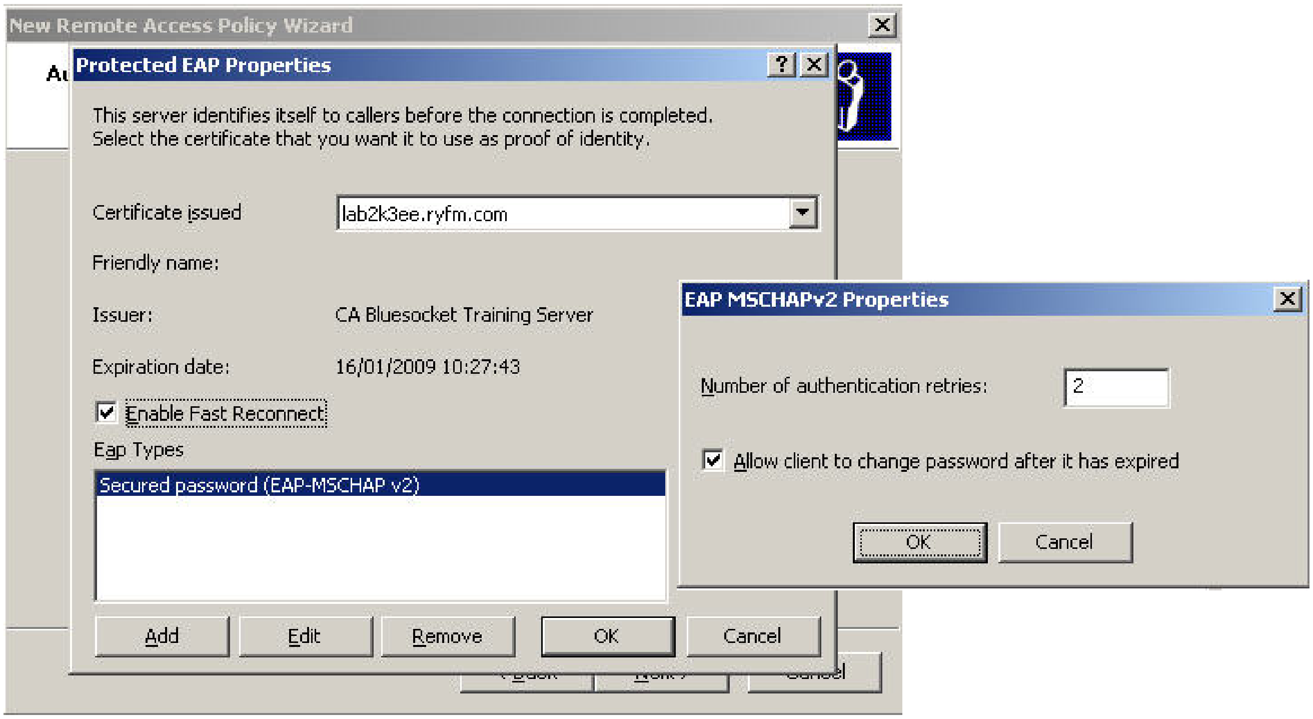


Cannot configure EAP

A certificate could not be found that can be used with this Extensible Authentication Protocol.

A server certificate will have to be issued by a Certificate Authority and installed on the IAS server (see Appendix A for an example of doing this using the Windows CA).

If a server certificate is already installed on this machine, you'll get the EAP properties for the 8021X remote access policy. Select "Enable Fast Reconnect" because we'll be using that on the 802.1X supplicant.



New Remote Access Policy Wizard

Protected EAP Properties

This server identifies itself to callers before the connection is completed. Select the certificate that you want it to use as proof of identity.

Certificate issued: lab2k3ee.ryfm.com

Friendly name:

Issuer: CA Bluesocket Training Server

Expiration date: 16/01/2009 10:27:43

☑ Enable Fast Reconnect

Eap Types

Secured password (EAP-MSCHAP v2)

EAP MSCHAPv2 Properties

Number of authentication retries: 2

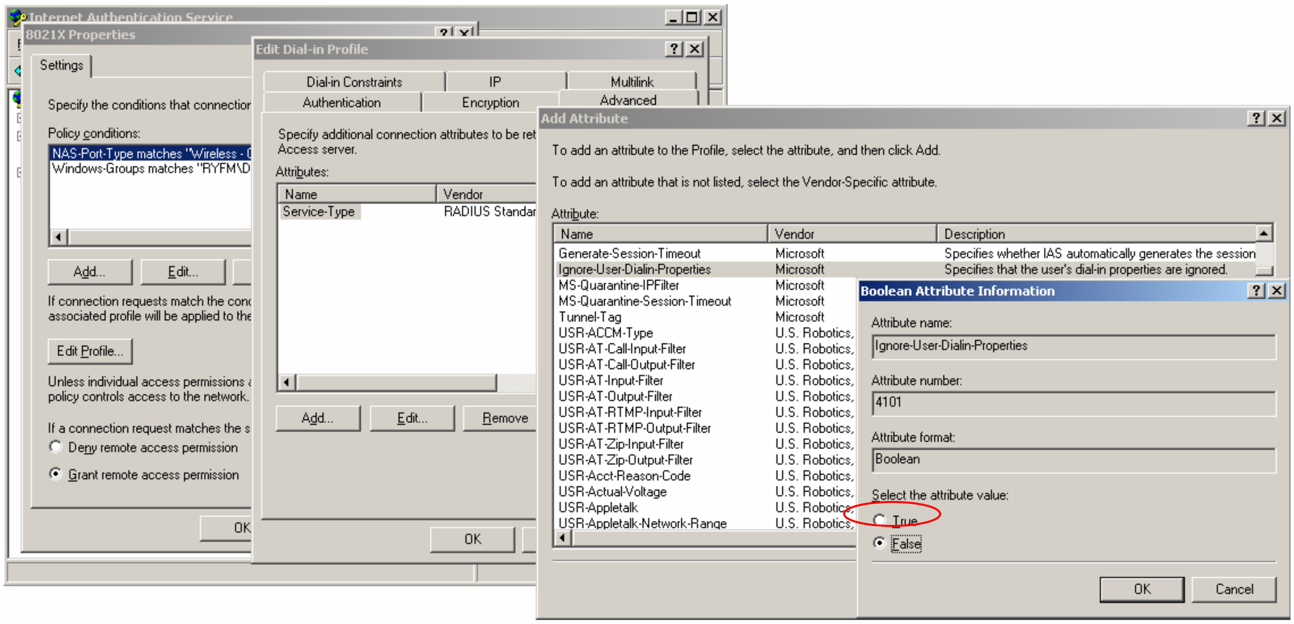
☑ Allow client to change password after it has expired

4c: Edit Remote Access Policy in order to ignore User Dail-in Properties

Edit the new 8021X remote access policy by right mouse click and click on properties.

- Click on edit profile to add an attribute to the dial-in profile of the policy
- Select advanced tab
- Add attribute
- Select *'Ignore User Dial-in Properties'*
- Set the attribute to True
- Click on ok

This attribute in the remote policy just avoids the need to change all the user's accounts to "Allow access" – however, this is done mainly to circumvent the default settings of new user accounts – in a real deployment, this may not be desirable or necessary.



Specify the conditions that connectior

Policy conditions:

NAS-Port-Type matches "Wireless - (
Windows-Groups matches "RYFM\D

If connection requests match the conc associated profile will be applied to the

Unless individual access permissions a policy controls access to the network.

If a connection request matches the s

○ Deny remote access permission

● Grant remote access permission

Specify additional connection attributes to be ret Access server.

Attributes:

Name	Vendor
Service-Type	RADIUS Standar

To add an attribute to the Profile, select the attribute, and then click Add.

To add an attribute that is not listed, select the Vendor-Specific attribute.

Attribute:

Name	Vendor	Description
Generate-Session-Timeout	Microsoft	Specifies whether IAS automatically generates the session
Ignore-User-Dialin-Properties	Microsoft	Specifies that the user's dial-in properties are ignored.
MS-Quarantine-IPFilter	Microsoft	
MS-Quarantine-Session-Timeout	Microsoft	
Tunnel-Tag	Microsoft	
USR-ACCM-Type	U.S. Robotics,	
USR-AT-Call-Input-Filter	U.S. Robotics,	
USR-AT-Call-Output-Filter	U.S. Robotics,	
USR-AT-Input-Filter	U.S. Robotics,	
USR-AT-Output-Filter	U.S. Robotics,	
USR-AT-RTMP-Input-Filter	U.S. Robotics,	
USR-AT-RTMP-Output-Filter	U.S. Robotics,	
USR-AT-Zip-Input-Filter	U.S. Robotics,	
USR-AT-Zip-Output-Filter	U.S. Robotics,	
USR-Acct-Reason-Code	U.S. Robotics,	
USR-Actual-Voltage	U.S. Robotics,	
USR-Appletalk	U.S. Robotics,	
USR-Appletalk-Network-Range	U.S. Robotics,	

Attribute name: Ignore-User-Dialin-Properties

Attribute number: 4101

Attribute format: Boolean

Select the attribute value:

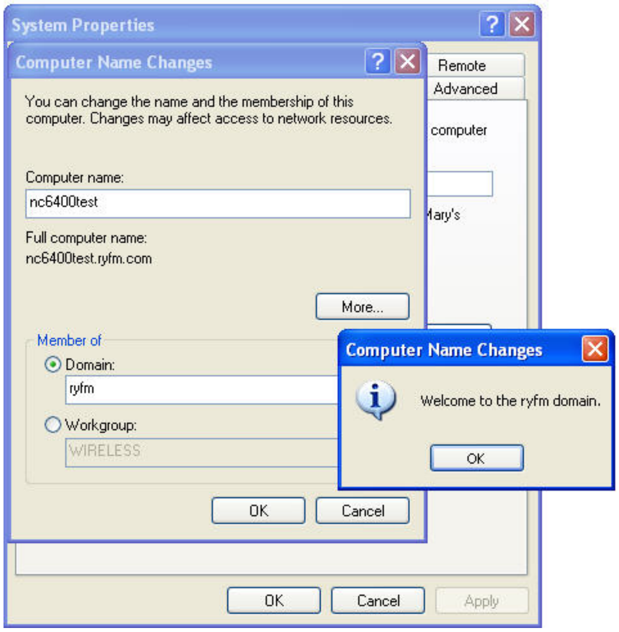
○ True

● False

5. Configuring the Windows Wireless Clients

5a: Adding new client to the domain

If the client PC is not added the domain, please add the client to domain with the right computer name, domain and user credentials. After restarting the client will receive the appropriate policies, including computer certificates and Trusted Root Certification Authority, if the domain is configured for autoenrollment of computer certificates.



Computer Name Changes

You can change the name and the membership of this computer. Changes may affect access to network resources.

Computer name: nc6400test

Full computer name: nc6400test.ryfm.com

Member of

● Domain: ryfm

○ Workgroup: WIRELESS

Computer Name Changes

Welcome to the ryfm domain.

5b: Installing Computer Certificates on Wireless Clients

This step is not necessary for EAP-PEAP-MSCHAPv2, because this EAP doesn’t require validation of the server certificate (Trusted Root Certification Authority). Of course you can select it optionally. For computer authentication with EAP-TLS or PEAP-TLS, you must install a computer certificate on the wireless client computer. See also tech note: Machine and User Authentication with PEAP-TLS/EAP-TLS.

To install a computer certificate on a wireless client computer running Windows Vista, Windows XP, or Windows Server 2003, connect to the organization intranet using an Ethernet port and do the following:

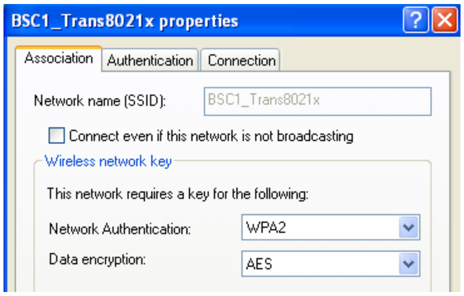
- If the domain is configured for autoenrollment of computer certificates, each computer that is a member of the domain requests a computer certificate when Computer Configuration Group Policy is refreshed. To force a refresh of Computer Configuration Group Policy for a computer running Windows Vista, Windows XP, or Windows Server 2003, restart the computer or type **gpupdate /target:computer** at a command prompt.
- If the domain is not configured for autoenrollment, you can request a “Computer” certificate using the Certificates snap-in or you can execute a CAPICOM script to install a computer certificate. For information about CAPICOM, search for "CAPICOM" at http://msdn.microsoft.com/.

Additionally, a large organization's information technology (IT) group can install a computer certificate before the computer, typically a laptop, is delivered to its user.

5b: Configuring Windows “wireless zero configuration” supplicant without certificate validation

On the Windows built-in supplicant, add a new wireless network with:

- The SSID name, for example ‘BSC1_Trans8021x’
- Specifying WPA/WPA2 as the network encryption (also know as 802.11i Enterprise mode)
- EAP authentication mechanism
  - PEAP as the Outer EAP type
  - MS-MSCHAPv2 as the Inner EAP type (Secured Password)
- Uncheck box ***“validate server certificate”***



BSC1_Trans8021x properties

Network name (SSID): BSC1_Trans8021x

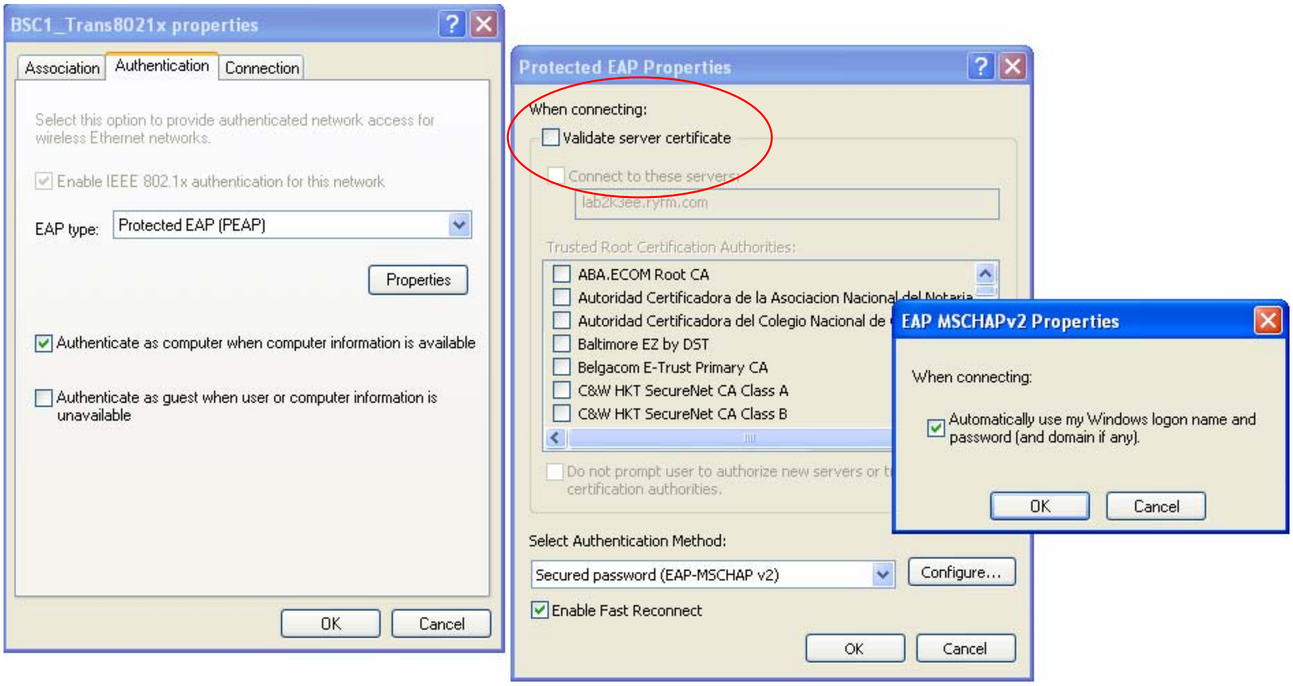
□ Connect even if this network is not broadcasting

Wireless network key

This network requires a key for the following:

Network Authentication: WPA2

Data encryption: AES



BSC1_Trans8021x properties

Select this option to provide authenticated network access for wireless Ethernet networks.

☑ Enable IEEE 802.1x authentication for this network

EAP type: Protected EAP (PEAP)

☑ Authenticate as computer when computer information is available

□ Authenticate as guest when user or computer information is unavailable

Protected EAP Properties

When connecting:

□ Validate server certificate

□ Connect to these servers:

lab2k3ee.ryfm.com

Trusted Root Certification Authorities:

□ ABA.ECOM Root CA
□ Autoridad Certificadora de la Asociacion Nacional del Notaria
□ Autoridad Certificadora del Colegio Nacional de
□ Baltimore EZ by DST
□ Belgacom E-Trust Primary CA
□ C&W HKT SecureNet CA Class A
□ C&W HKT SecureNet CA Class B

□ Do not prompt user to authorize new servers or t certification authorities.

Select Authentication Method:

Secured password (EAP-MSCHAP v2)

☑ Enable Fast Reconnect

EAP MSCHAPv2 Properties

When connecting:

☑ Automatically use my Windows logon name and password (and domain if any).

Note the following:

a) We enable machine authentication via 802.1X via the “Authenticate as computer when computer information is available”

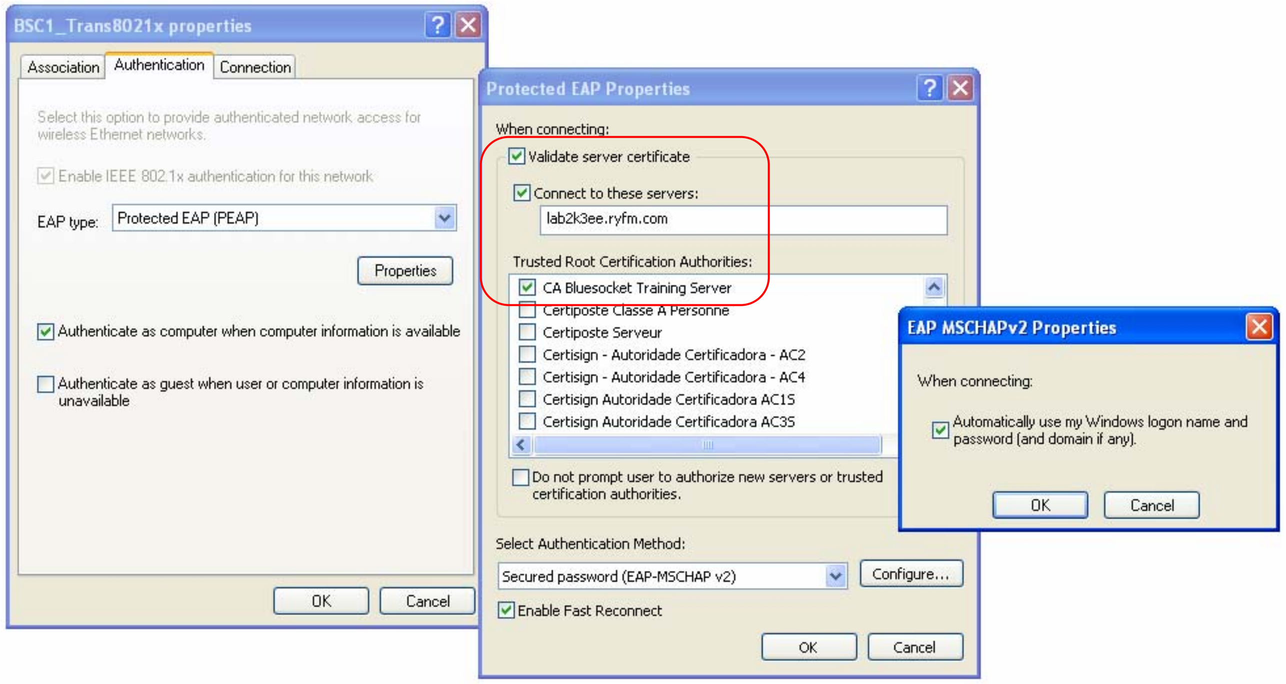
b) Select “Enable Fast Reconnect” to match the setting on the IAS RADIUS server

c) Within the MSCHAPv2 properties, we need to tell the client to pass the Windows logon name and password which makes the authentication process transparent to the user.

5c: Configuring Windows “wireless zero configuration” supplicant with certificate validation

The settings are the same as in paragraph 5b. In addition select checkbox “validate server certificate”.

- Select Trusted Root Certification Authority
- Select checkbox “connect to these servers” and enter name of trusted server



BSC1_Trans8021x properties

Association | Authentication | Connection

Select this option to provide authenticated network access for wireless Ethernet networks.

☑ Enable IEEE 802.1x authentication for this network

EAP type: Protected EAP (PEAP)

☑ Authenticate as computer when computer information is available

☐ Authenticate as guest when user or computer information is unavailable

Protected EAP Properties

When connecting:

☑ Validate server certificate

☑ Connect to these servers:

lab2k3ee.ryfm.com

Trusted Root Certification Authorities:

☑ CA Bluesocket Training Server
☐ Certiposte Classe A Personne
☐ Certiposte Serveur
☐ Certisign - Autoridade Certificadora - AC2
☐ Certisign - Autoridade Certificadora - AC4
☐ Certisign Autoridade Certificadora AC1S
☐ Certisign Autoridade Certificadora AC3S

☐ Do not prompt user to authorize new servers or trusted certification authorities.

Select Authentication Method:

Secured password (EAP-MSCHAP v2)

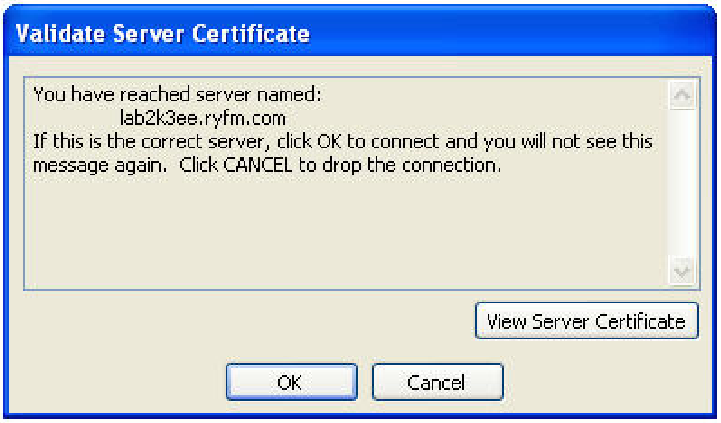
☑ Enable Fast Reconnect

EAP MSCHAPv2 Properties

When connecting:

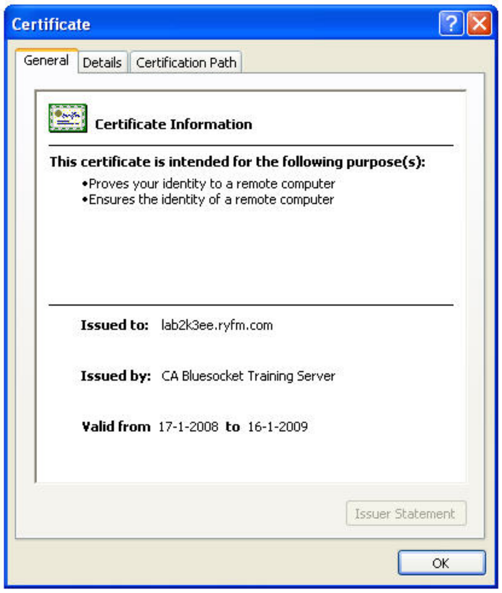
☑ Automatically use my Windows logon name and password (and domain if any).

If you didn’t enter the name of the trusted server and you selected “connect to these servers”, Windows will prompt you with the message below to enable you to confirm the right server.



Validate Server Certificate

You have reached server named:
lab2k3ee.ryfm.com
If this is the correct server, click OK to connect and you will not see this message again. Click CANCEL to drop the connection.



Certificate

General | Details | Certification Path

Certificate Information

This certificate is intended for the following purpose(s):
- Proves your identity to a remote computer
- Ensures the identity of a remote computer

Issued to: lab2k3ee.ryfm.com

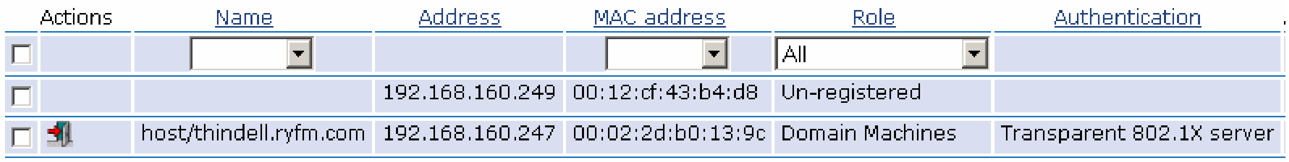
Issued by: CA Bluesocket Training Server

Valid from 17-1-2008 to 16-1-2009

6. User experience

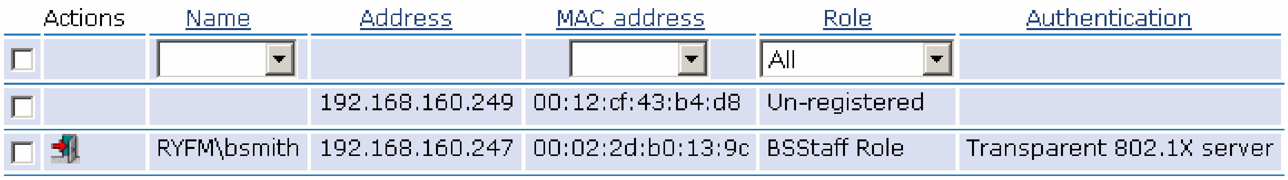
6a: User experience and connection table on the controller

When a user powers up their machine that has already registered on the domain, it will authenticate to the domain via 802.1X and the IAS server, and appear in the BSC connection table with the name “host/machine_name.domain_name” and in the default “Domain Machines” role.



	Actions	Name	Address	MAC address	Role	Authentication
□		▾		▾	All ▾	
□			192.168.160.249	00:12:cf:43:b4:d8	Un-registered	
□		host/thindell.ryfm.com	192.168.160.247	00:02:2d:b0:13:9c	Domain Machines	Transparent 802.1X server

The user logs on (Ctrl-Alt-Del) and authenticates via 802.1X and appears in the BSC connection table as the appropriate user.



	Actions	Name	Address	MAC address	Role	Authentication
□		▾		▾	All ▾	
□			192.168.160.249	00:12:cf:43:b4:d8	Un-registered	
□		RYFM\bsmith	192.168.160.247	00:02:2d:b0:13:9c	BSStaff Role	Transparent 802.1X server

If the user logs off, the connection reverts to the host in the “Domain Machines” role. When a new user logs on to the same machine, they will authenticate to the domain, and be transparently authenticated on the BSC into their appropriate role based on the AD attributes.

If a user has an authenticated (i.e. logged on to the domain) wired connection to their network and then disconnects from the wired connection and enables their wireless connection, they will be transparently authenticated via 802.1X into the appropriate role without having to log in again.

6b: Seamless Single Sign On

Machine & User authentication with transparent 802.1x offers seamless logon to the Windows domain, including login scripts and network drives.

Windows XP defaults to allowing the user to login before network services are established to help reduce login time (known as Fast Logon Optimization) whereas Windows 2000 defaults to forcing the user to wait to login until all the network services are up and running.

Windows XP can be configured to behave like Windows 2000, if needed.

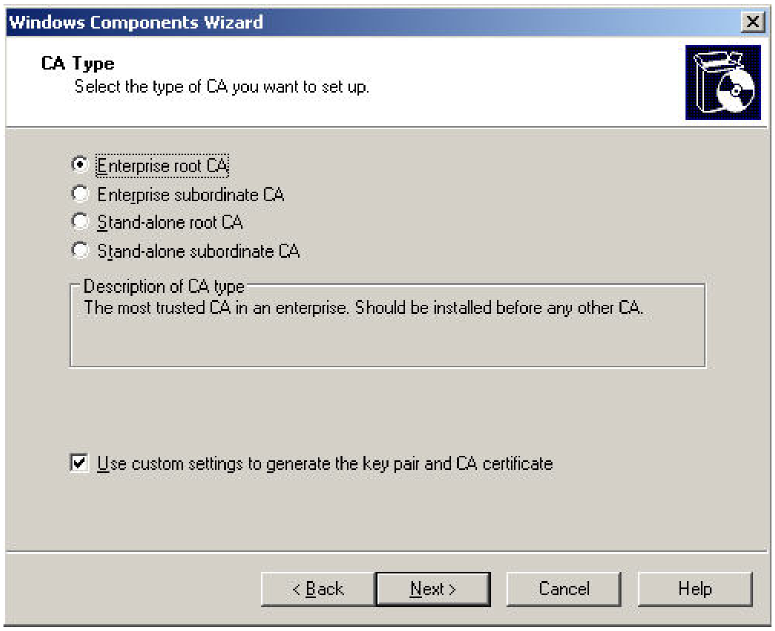
See also Tech Note: Ensuring network services are loaded prior to logging in

Appendix A : Configure Microsoft 2003 CA Certificate Infrastructure and creating a server certificate for IAS

Go to add or remove programs and add/removes Windows Components

Step 1: Install Internet Information Services,
Required for downloading (user) certificates from the server to the client.
Only needed for EAP-TLS or EAP-PEAP-TLS.

Step 2: Install Certificate Services



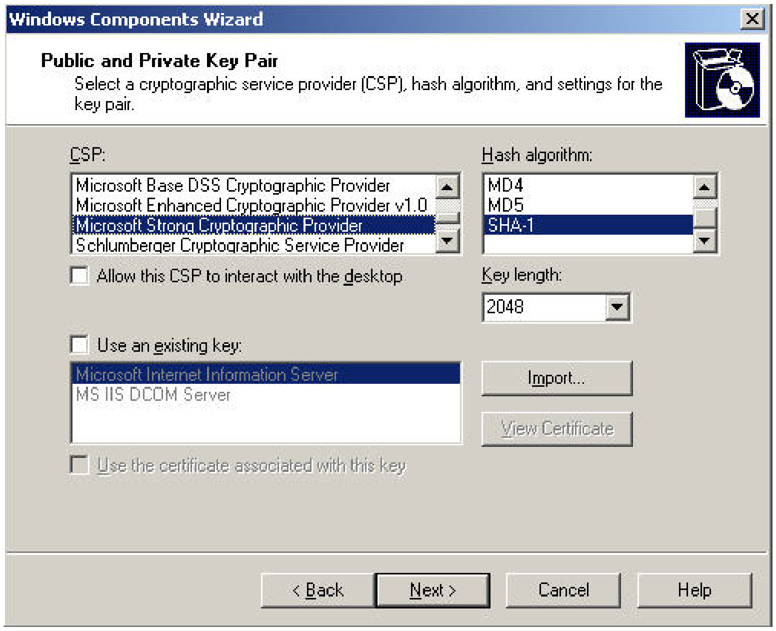
Windows Components Wizard

CA Type
Select the type of CA you want to set up.

● Enterprise root CA
○ Enterprise subordinate CA
○ Stand-alone root CA
○ Stand-alone subordinate CA

Description of CA type
The most trusted CA in an enterprise. Should be installed before any other CA.

☑ Use custom settings to generate the key pair and CA certificate



Windows Components Wizard

Public and Private Key Pair
Select a cryptographic service provider (CSP), hash algorithm, and settings for the key pair.

CSP:
Microsoft Base DSS Cryptographic Provider
Microsoft Enhanced Cryptographic Provider v1.0
Microsoft Strong Cryptographic Provider
Schlumberger Cryptographic Service Provider

Hash algorithm:
MD4
MD5
SHA-1

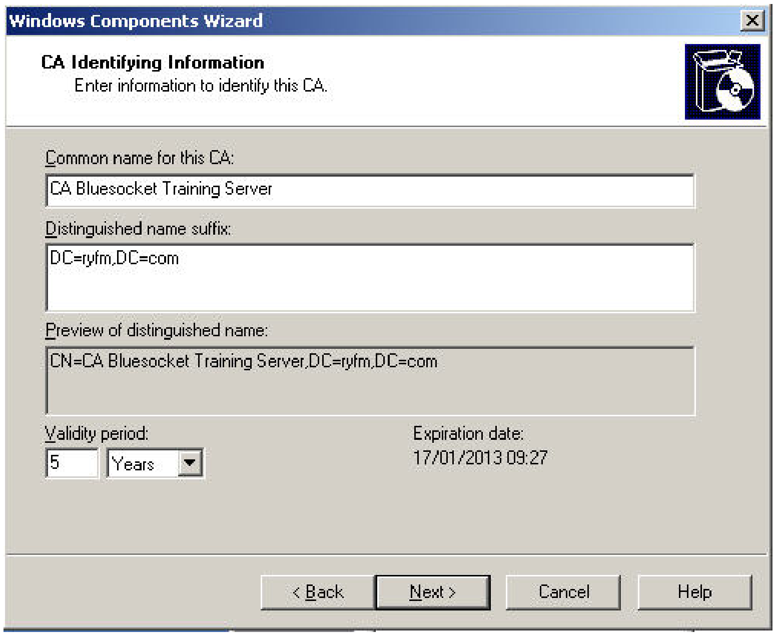
☐ Allow this CSP to interact with the desktop

Key length: 2048

☐ Use an existing key:
Microsoft Internet Information Server
MS IIS DCOM Server

☐ Use the certificate associated with this key

Enter the common name for the CA and the validity period.



CA Identifying Information
Enter information to identify this CA.

Common name for this CA:
CA Bluesocket Training Server

Distinguished name suffix:
DC=ryfm,DC=com

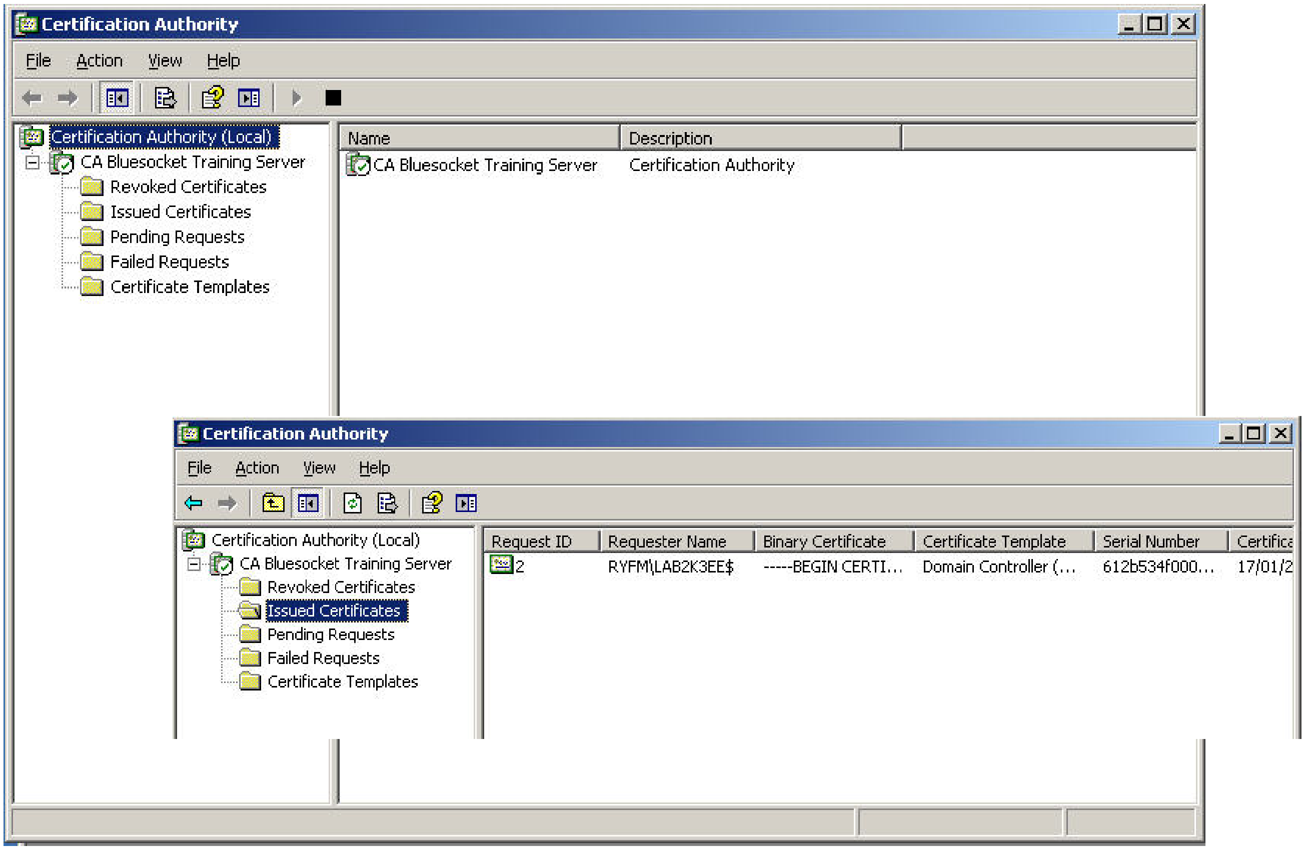
Preview of distinguished name:
CN=CA Bluesocket Training Server,DC=ryfm,DC=com

Validity period:
5 Years

Expiration date:
17/01/2013 09:27

Certification Authority

Shows the issued & revoked certificates and pending/failed requests



Name	Description
CA Bluesocket Training Server	Certification Authority

Request ID	Requester Name	Binary Certificate	Certificate Template	Serial Number	Certifica
2	RYFM\LAB2K3EE$	-----BEGIN CERTI...	Domain Controller (...	612b534f000...	17/01/2