

How to Logon with Domain Credentials to a Server in a Workgroup

Johan Loos

johan@accessdenied.be

Version 1.0

Authentication Overview

Basically when you logon to a Windows Server you can logon locally using a local username and password or you can use a username and password from Active Directory when your server is joined into a domain. What if your server belongs to a workgroup and you need to logon with your domain credentials? That's what this paper is all about.

Our goal is to logon with our domain credentials even when the server is not a member of the domain. The tool used to accomplish this task is pGina. pGina is an Open Source Windows Authentication and Access Management tool to logon with a username using a backend of your choice. For example the backend can be a LDAP Server or a RADIUS Server.

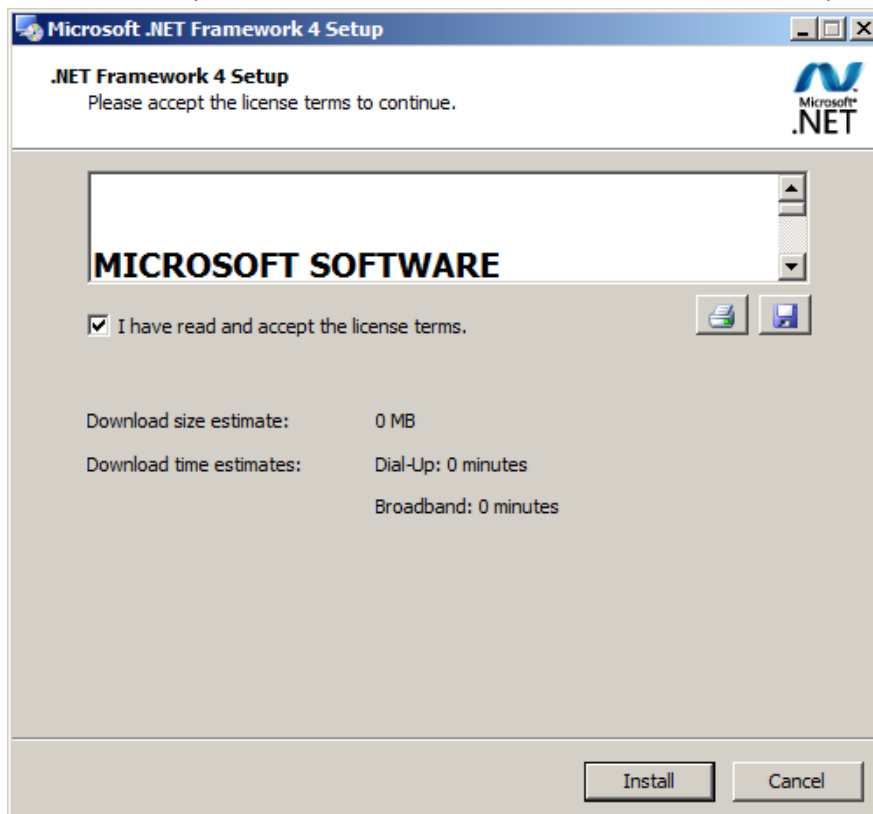
In the next two sections you can find the procedure how to logon to a server in a workgroup with your domain credentials if the backed authentication server is a LDAP server. In the second part you can find the procedure how to logon to a server in a workgroup with your domain credentials if the backed authentication server is a RADIUS server.

pGina Installation Task List

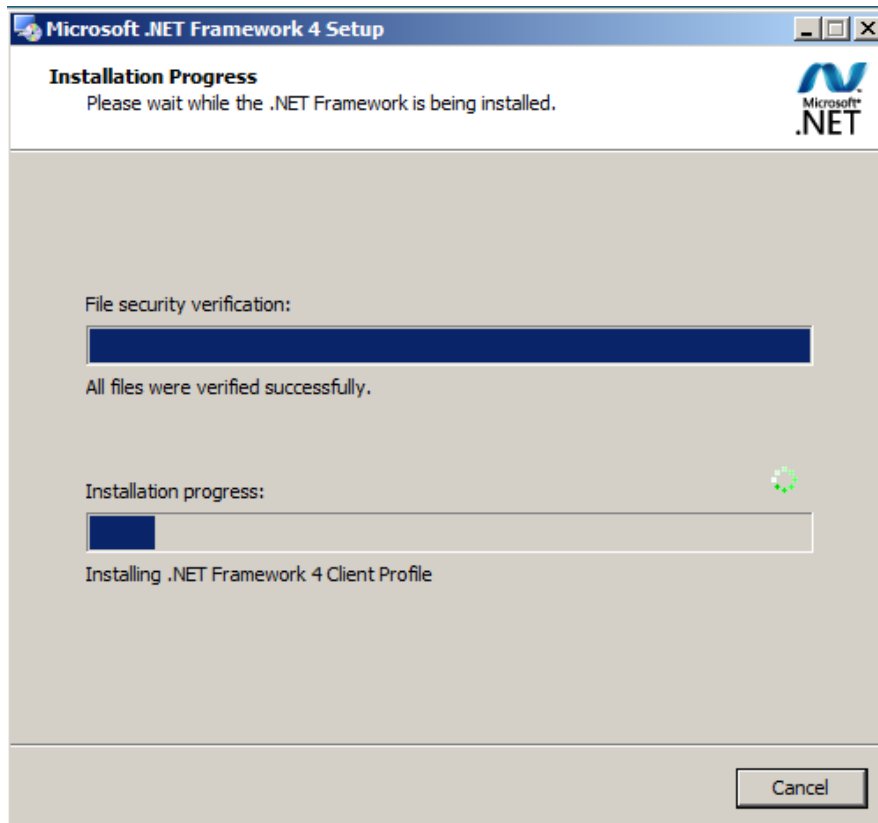
- △ Install .NET Framework 4.0
- △ Install VC++ 2012 Redistributable
- △ Install pGina

Install .NET Framework 4.0

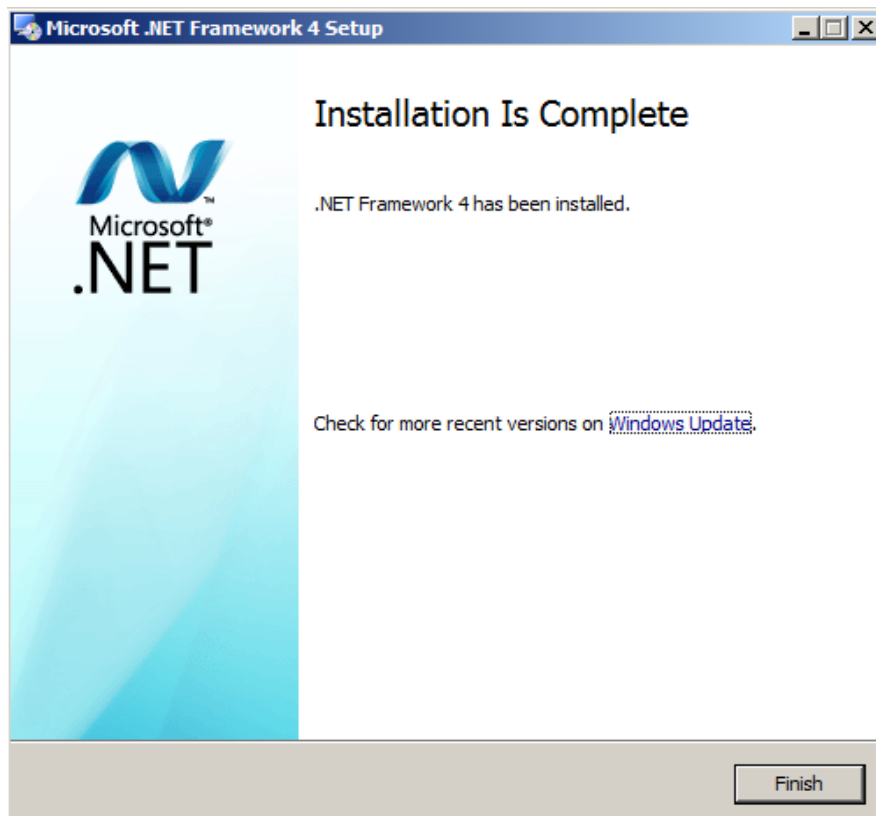
- Double click on your .NET Framework 4 file to launch the installation process



- On the **.NET Framework 4 Setup** page, select I have read and accept the license terms and click Install
- The installation progress starts

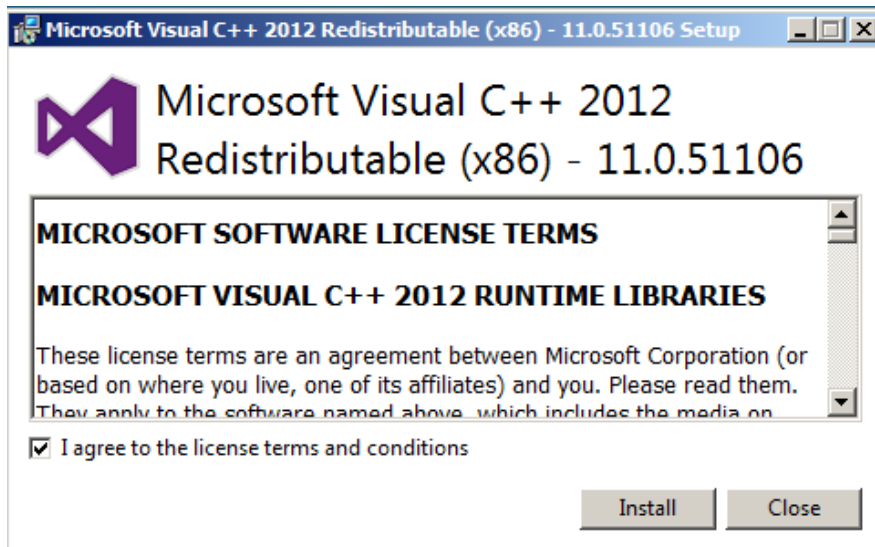


- On the **Installation Is Complete** page, click Finish

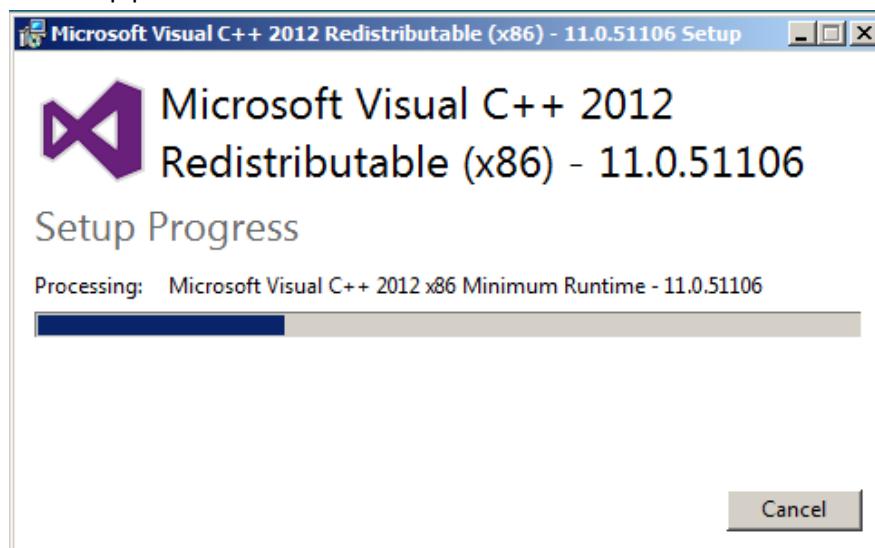


Install VC++ 2012 Redistributable

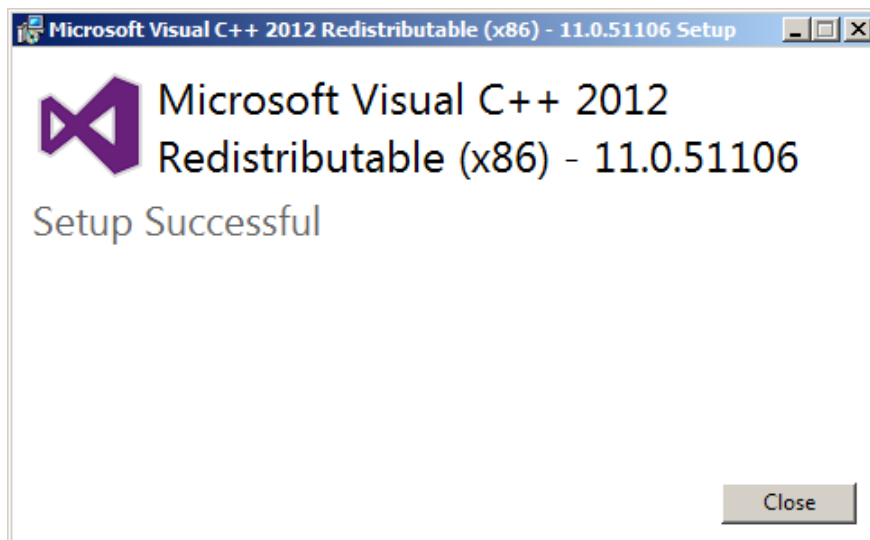
- Double click on your Visual C++ 2012 Redistributable File to launch to installation process



- Select I agree to the license terms and conditions and click Install
- The Setup process starts

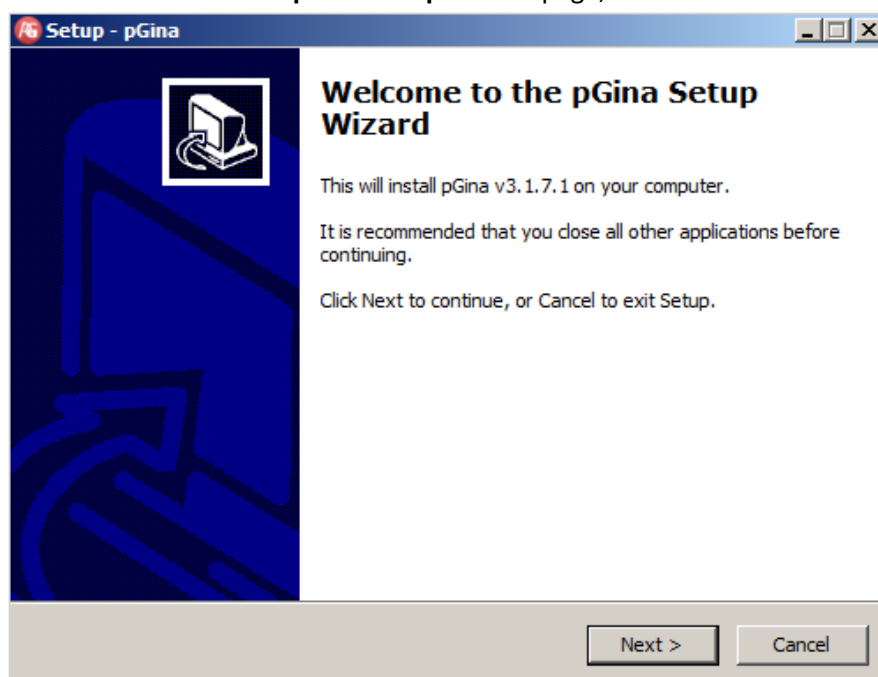


- On the **Setup Successful** page click Close

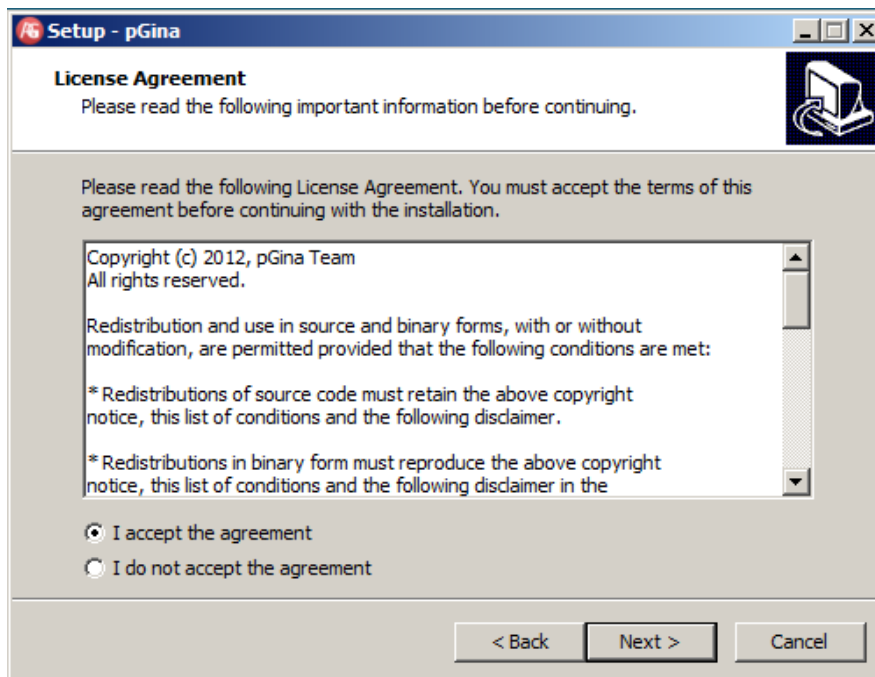


Install pGina

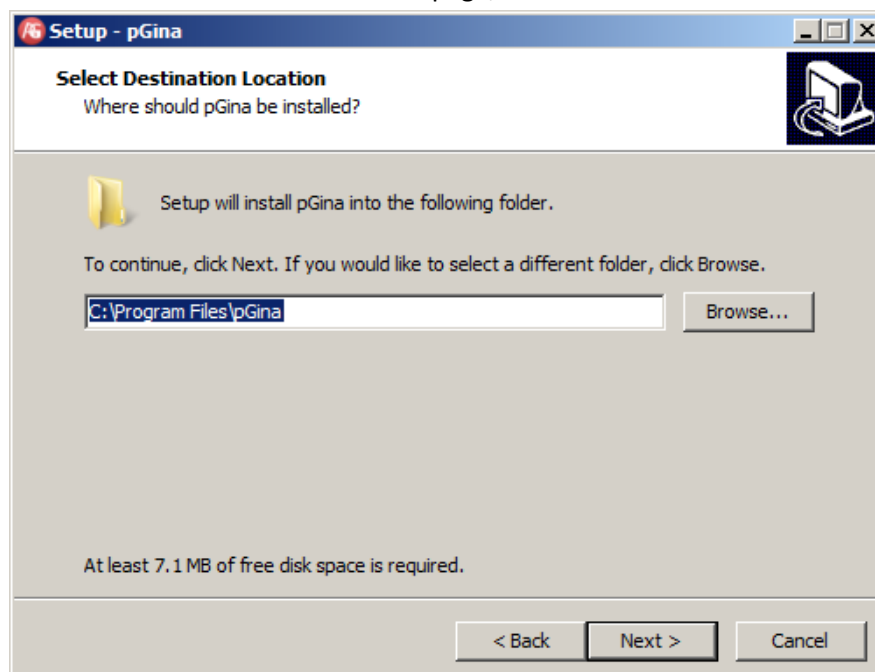
- Double click on your pGina installation file to launch the process
- On the **Welcome to the pGina Setup Wizard** page, click Next



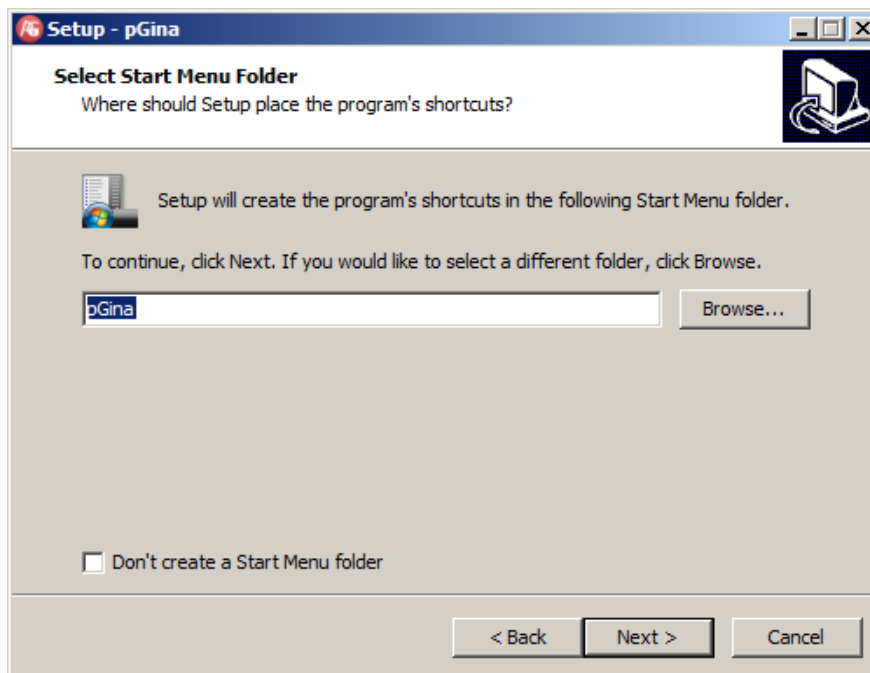
- On the **License Agreement** page, select I accept the agreement and click Next



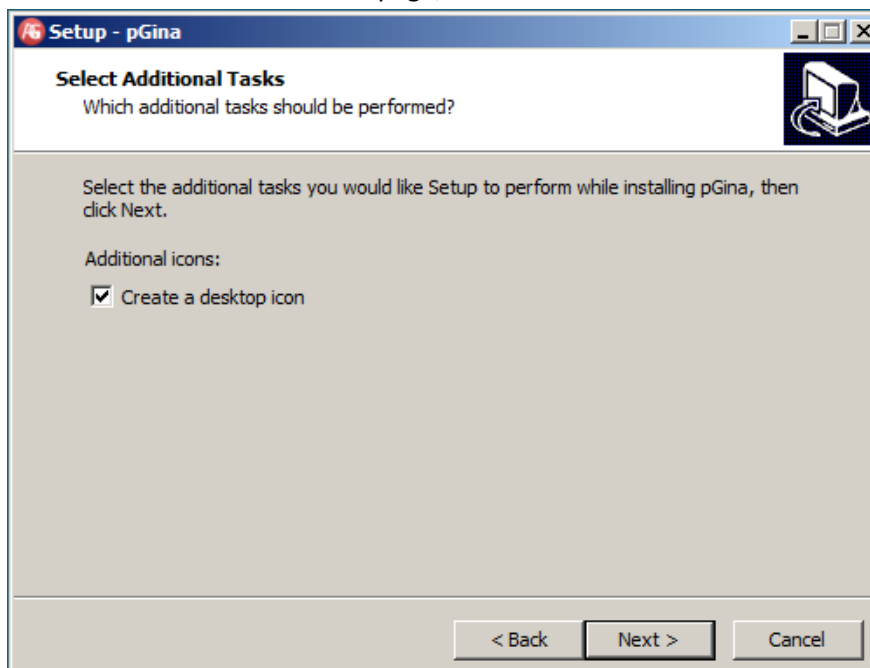
- On the **Select Destination Location** page, click Next



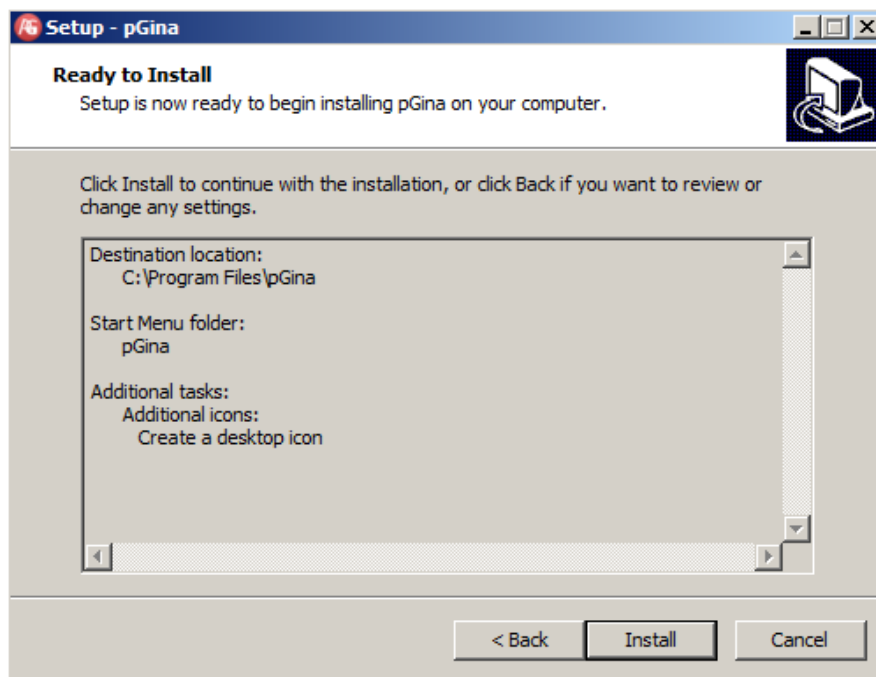
- On the **Select Start Menu Folder** page, click Next



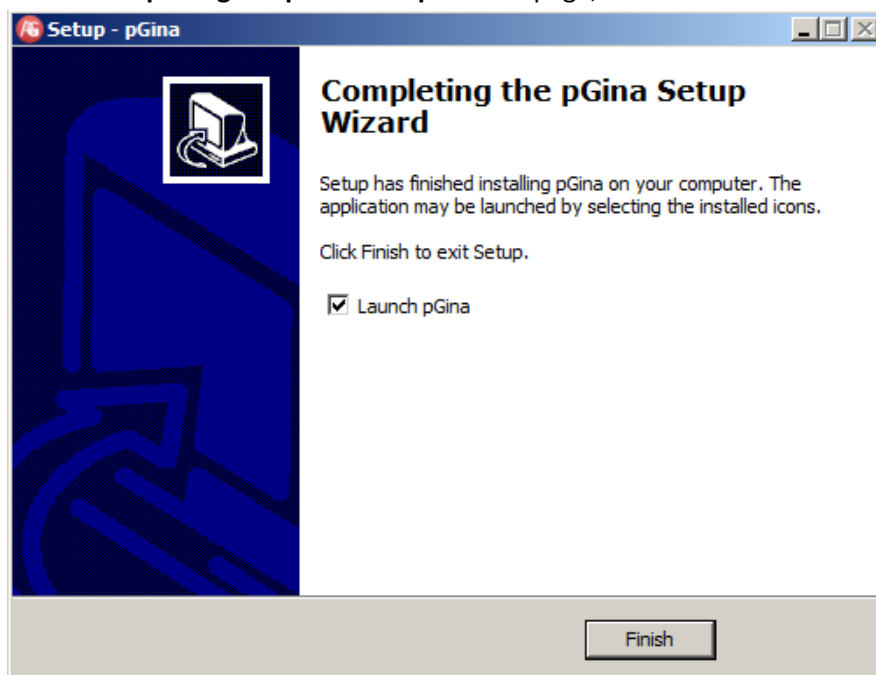
- On the **Select Additional Tasks** page, select Next



- On the **Ready to Install** page, click Install



- On the **Completing the pGina Setup Wizard** page, click Finish



After installation, a pGina service is created and runs under System account.

LDAP Authentication

How it works

pGina captures the user his credentials, makes a connection to your LDAP server and verifies if the user exists in Active Directory and that the password is correct. pGina also verifies if the user is a member of a specific group. This group can be specified in the authorization process. If authentication is successful, pGina creates a local user account on the workgroup server with the same username/password as your domain user and adds the user account into a security group

defined in the gateway process. When the user logs off, the local user account and his profile are deleted from your workgroup server.

LDAP Authentication Task List

- △ Create a LDAP user account
- △ Create and configure your LDAP Administrators group in Active Directory
- △ Configure pGina
- △ Configure LDAP plugin
- △ Configure Local Machine plugin
- △ Simulate your connection
- △ Logon
- △ LDAP Authentication Debug

Create a LDAP user account

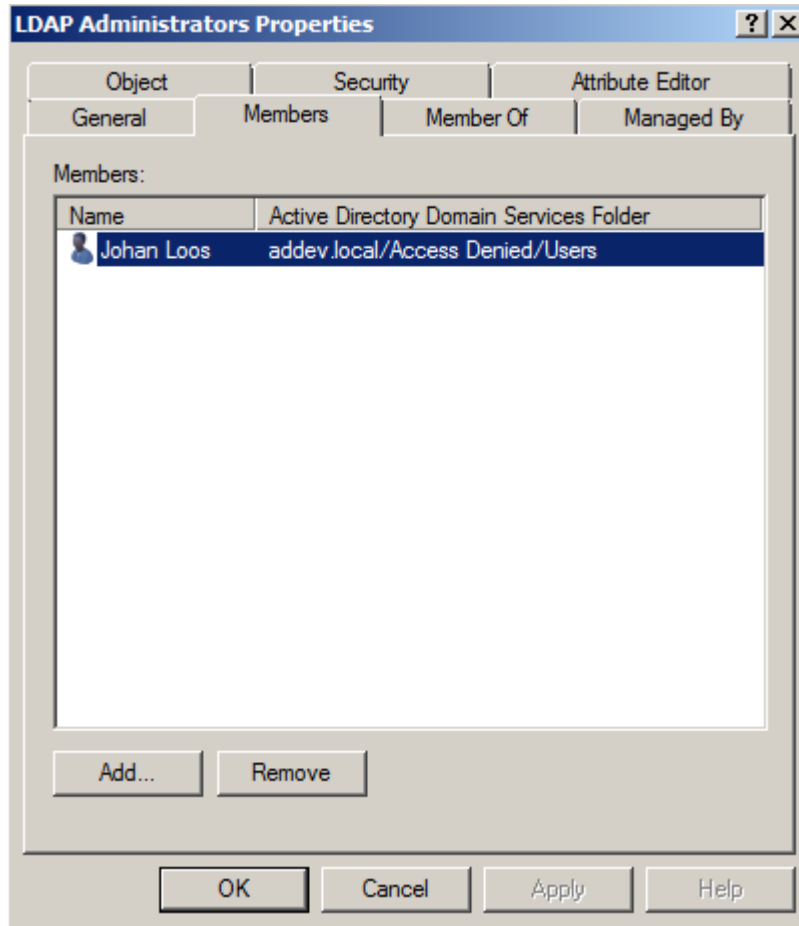
- Open **Active Directory User and Computers** from **Administrative Tools**
- Create a new user account which can be used to perform LDAP queries

The screenshot shows the 'ldapuser Properties' dialog box with the 'Account' tab selected. The 'User logon name' is 'ldapuser' and the domain is '@addev.local'. The 'User logon name (pre-Windows 2000)' is 'ADDEV\ldapuser'. The 'Logon Hours...' and 'Log On To...' buttons are visible. The 'Unlock account' checkbox is unchecked. The 'Account options' section shows 'Password never expires' selected. The 'Account expires' section shows 'Never' selected.

Create and configure your LDAP Administrators group in Active Directory

All members of this group are allowed to login into a server in a workgroup via LDAP.

- Open **Active Directory Users and Computers** from **Administrative Tools**
- Create a new group and add to required users on the Members tab



Configure pGina

Before you can logon with your domain credentials, you need to configure some plugins. pGina delegates the logon process to plugins. Depending on the type of backend you choose. In our example the backend server is a LDAP server. The process is done in three stages:

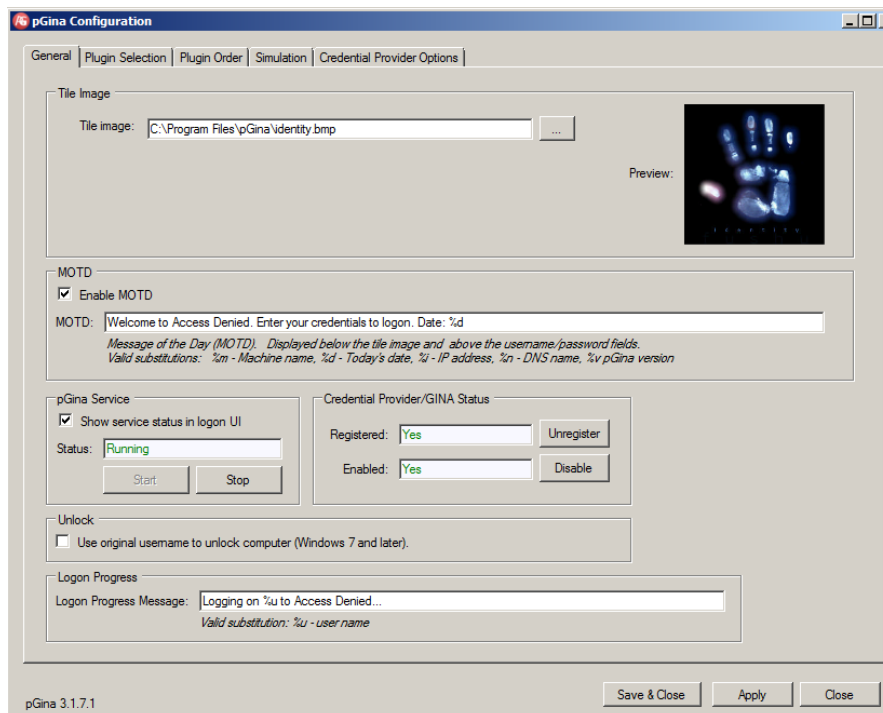
Authentication: This process validates the credentials of the user account

Authorization: This process determines if the user is allowed to access resources. This is done via group membership

Gateway: This process can be used to provide account management

- On the **General** page, configure the following settings
 - You can select a bitmap Tile Image which is displayed in the logon screen
 - You can enable the Message of the Day (MOTD). This message is displayed in the logon screen

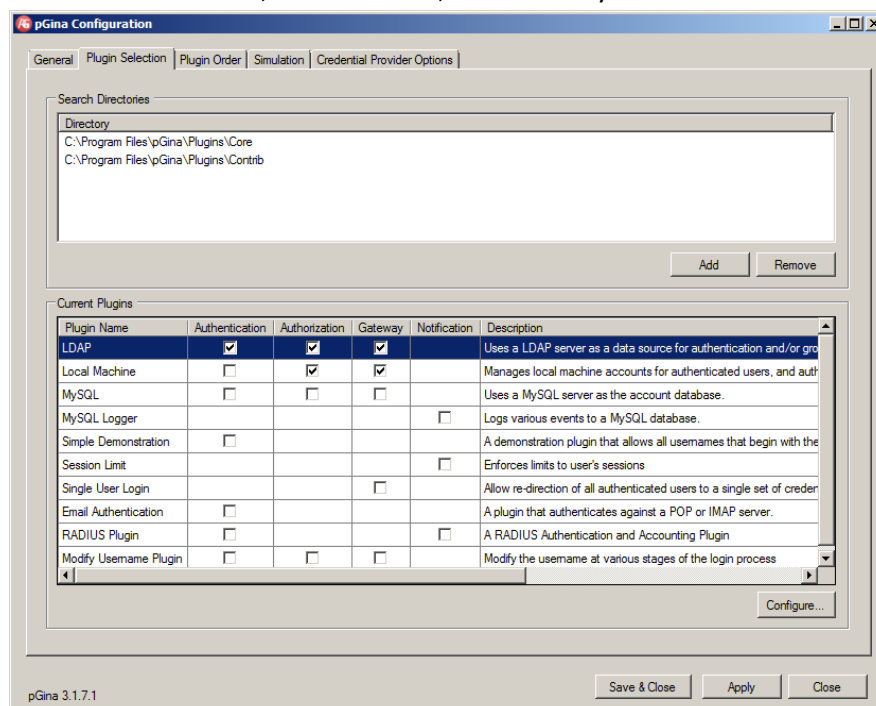
- You can also specify a Logon Progress Message which is displayed when the user is successful authenticated



- Click Apply and click Save & Close

Configure LDAP plugin

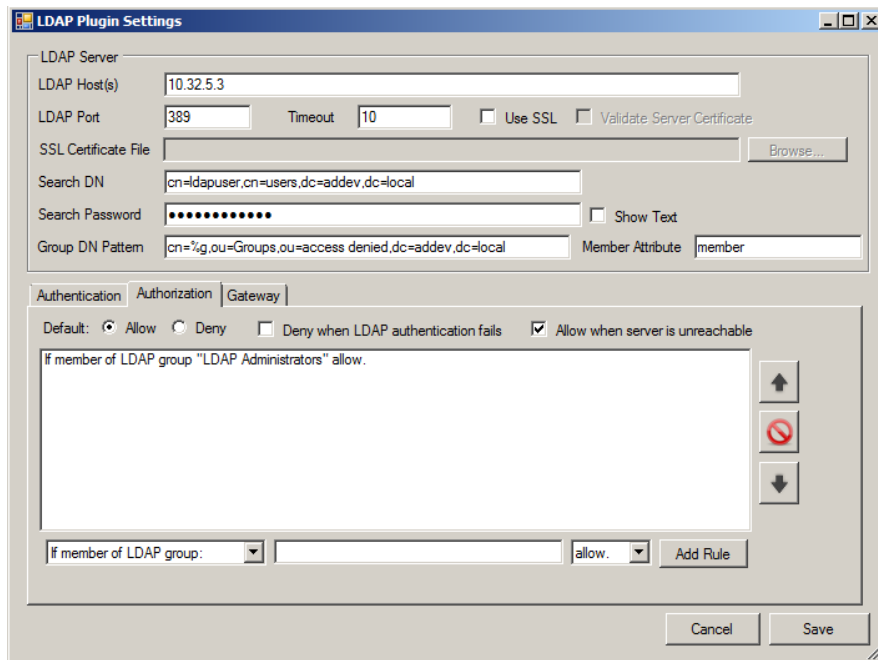
- On the **Plugin Selection** page, select the LDAP Plugin
- Select Authentication, Authorization, and Gateway checkbox and click on Configure



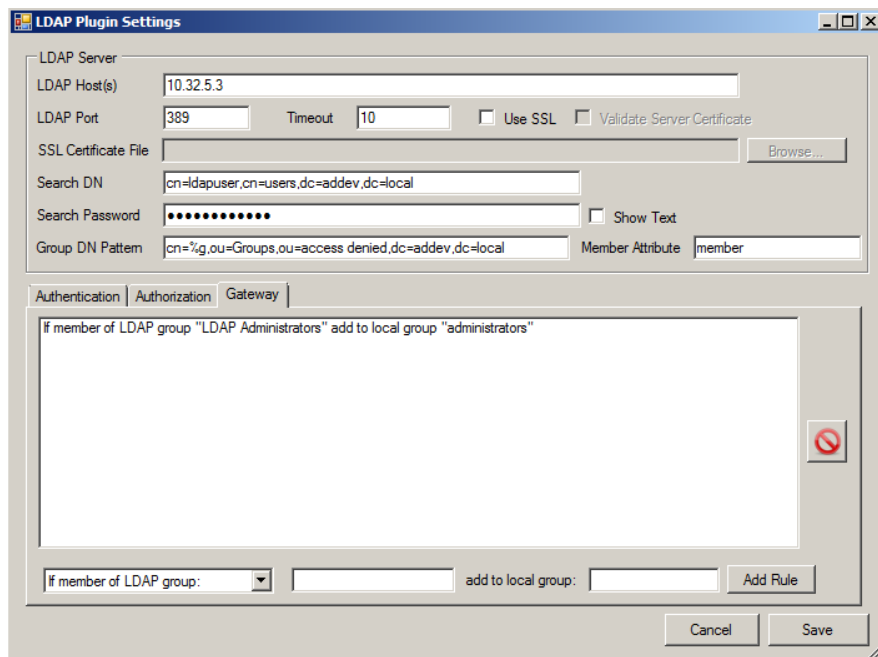
- On the **Authentication** page, select the following

- In the LDAP Hosts field, type the IP address or FQDN of your LDAP Servers (Active Directory Domain Controllers)
- In the LDAP Port field, type the port where your LDAP server is listening on (389, or 636 for SSL)
- You can check the Use SSL field to perform authentication over SSL. Be sure that your domain controller has a trusted certificate and that the certificate of the Root CA is available on this server
- In the Search DN field, type the Distinguish name of the account which is used to bind/connect to your LDAP server. This account is also used to search in Active Directory when you launch a LDAP query
- In the Search Password field, type the password of your Search DN account
- In the Group DN Pattern field, type the Distinguish Name of the location when converting a group name to a LDAP DN
- In the Member Attribute field, type the LAP attribute used to store group members. If you are using the object class groupOfNames ,then type member
- Search for DN and Search Contexts to look for an account in the location you specify. In my case, I look for the samaccountname username for the location specified in Context value. You can add more contexts if you want to search in several locations in Active Directory

- On the **Authorization** page, select the following
 - If member of LDAP Group: Type a group which currently exists in Active Directory to authorize users from Active Directory. If the user is a member of the security group LDAP Administrators (which is available in Active Directory) then access is allowed.



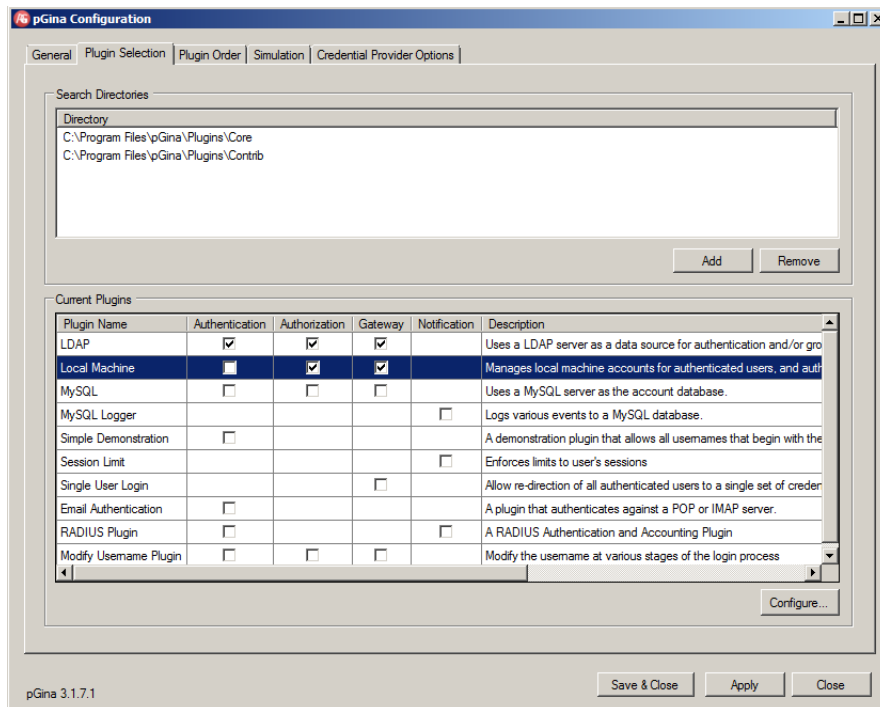
- On the **Gateway** page, select the following
 - If member of LDAP group: Verify if the user is a member of this group and add this user into a local group which exists on the local machine



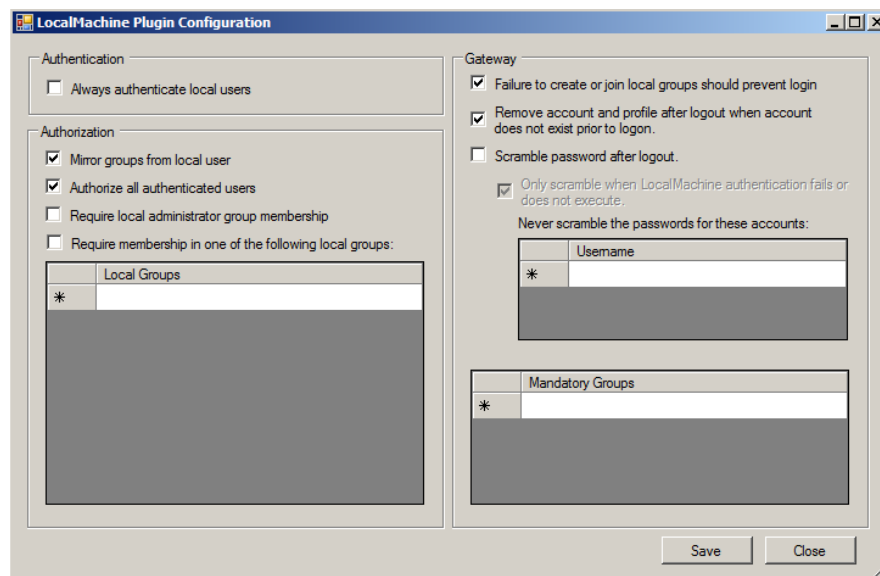
- Click Save

Configure Local Machine plugin

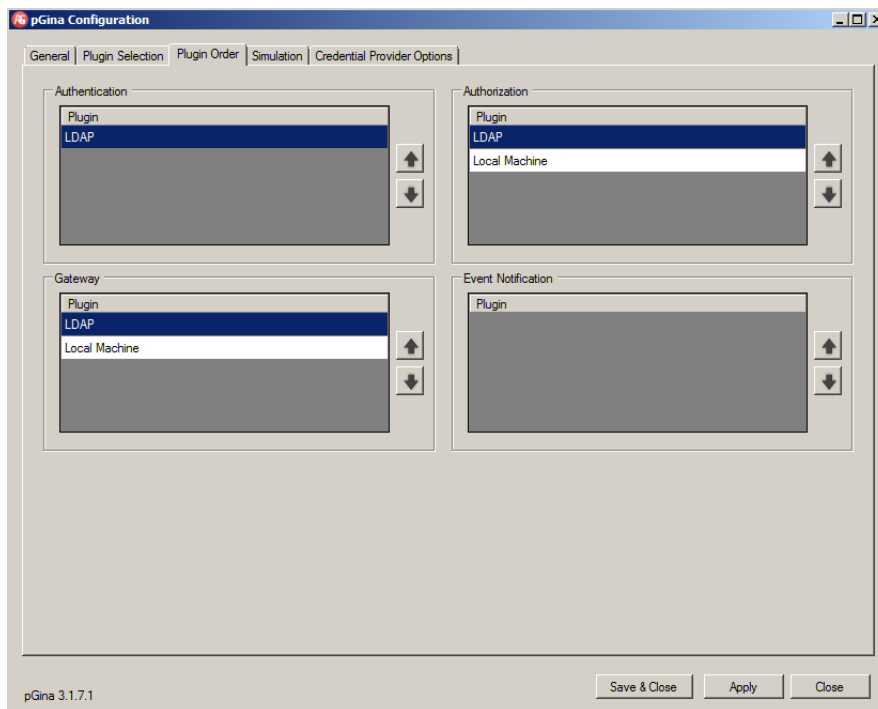
- On the **Plugin Selection** page, Select the Local Machine Plugin
- Select Authorization, Gateway, and click on Configure



- On the **LocalMachine Plugin Configuration** page, select the following
 - Authorize all authenticated users: All authenticated users will be authorized
 - Remove account and profile after logout: When the user logs off, the plugin deletes the user account and the profile from that server

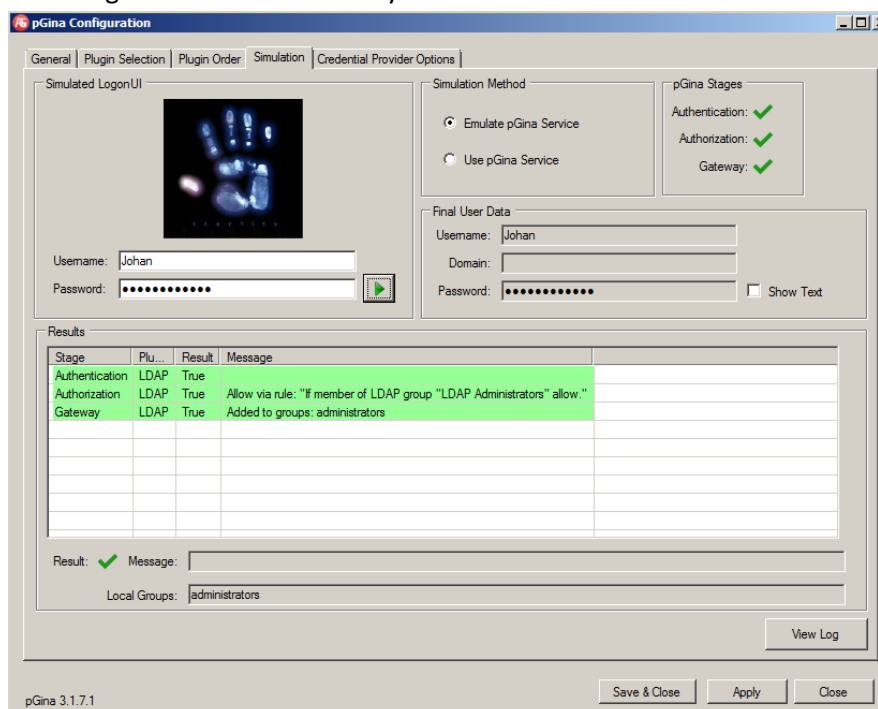


- Click Save
- On the **Plugin Order** page, move the plugins in the correct order



Simulate your connection

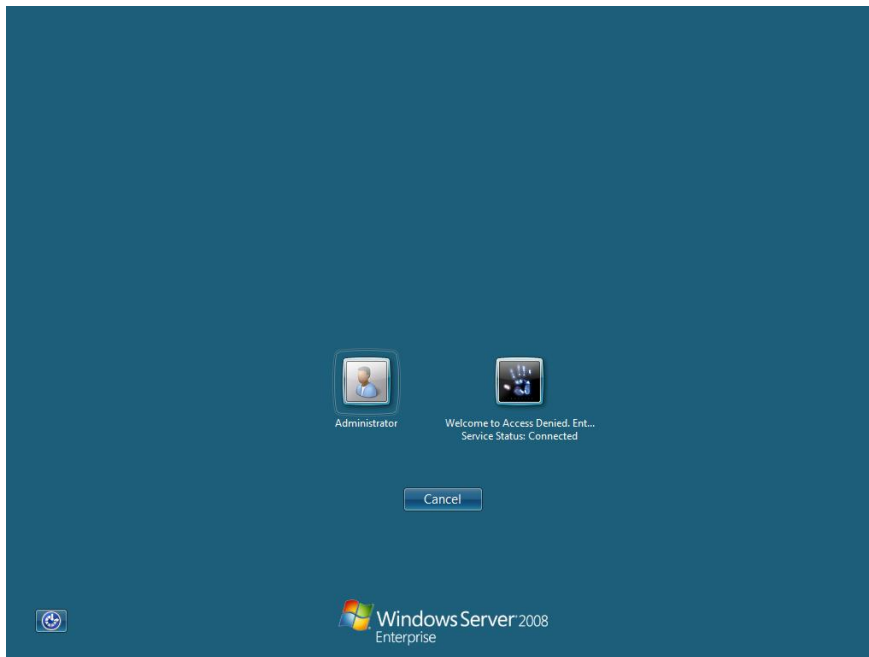
- On the **Simulation** page, type a username and password of the account which you want to use to logon and click on the Play button



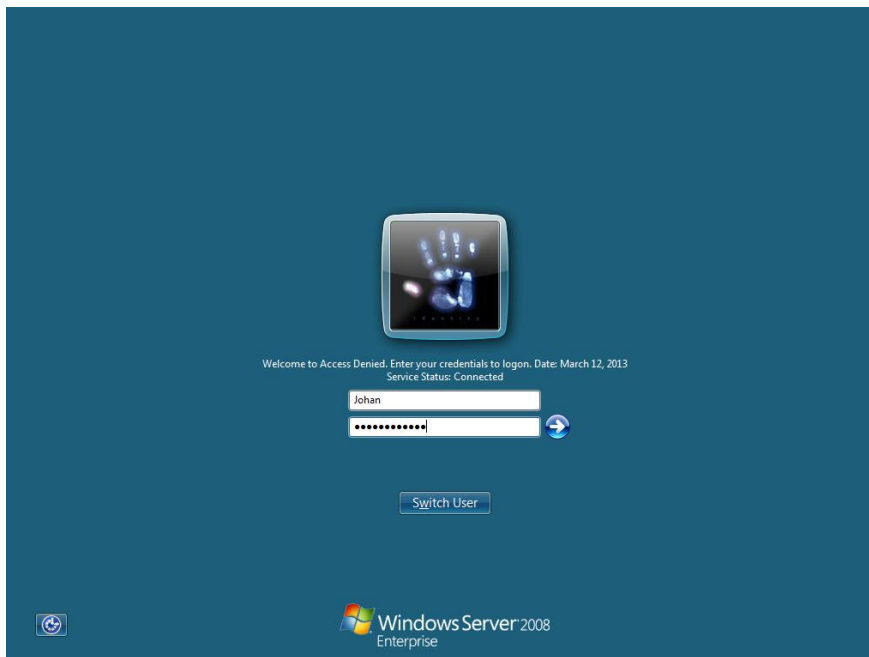
- The result are displayed in the Result pane
- Click Save & Close

Logon

- On your logon screen press CTRL+ALT+DEL and select switch user



- Type your domain credentials to logon



- Press Enter to logon
- You are now logged on the your workgroup server and member of the local administrators group

LDAP Authentication Debug

- pGina binds a LDAP connection to our LDAP server using our user Idapuser


```

Frame 8: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on interface 0
Ethernet II, Src: Vmware_65:25:d3 (00:0c:29:65:25:d3), Dst: Vmware_16:09:96 (00:0c:29:65:25:d3)
Internet Protocol Version 4, Src: 10.32.5.11 (10.32.5.11), Dst: 10.32.5.3 (10.32.5.3)
Transmission Control Protocol, Src Port: 49178 (49178), Dst Port: ldap (389), Seq: 1, Ack: 1, Len: 72
Lightweight Directory Access Protocol
  LDAPMessage bindRequest(121) "cn=ldapuser,cn=users,dc=addev,dc=local" simple
    messageID: 121
    protocolOp: bindRequest (0)
    bindRequest
      version: 3
      name: cn=ldapuser,cn=users,dc=addev,dc=local
      authentication: simple (0)
        simple: 61636365737364656e696564
[Response In: 9]

```

- Bind connection successfully

```

Frame 9: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface 0
Ethernet II, Src: Vmware_16:09:96 (00:0c:29:65:25:d3), Dst: Vmware_65:25:d3 (00:0c:29:65:25:d3)
Internet Protocol Version 4, Src: 10.32.5.3 (10.32.5.3), Dst: 10.32.5.11 (10.32.5.11)
Transmission Control Protocol, Src Port: ldap (389), Dst Port: 49178 (49178), Seq: 1, Ack: 73, Len: 22
Lightweight Directory Access Protocol
  LDAPMessage bindResponse(121) success
    messageID: 121
    protocolOp: bindResponse (1)
    bindResponse
      resultCode: success (0)
      matchedDN:
      errorMessage:
[Response To: 8]
[Time: 0.000702000 seconds]

```

- Lookup for the user (Johan) who is logging on

```

Frame 13: 5162 bytes on wire (41296 bits), 5162 bytes captured (41296 bits) on interface 0
Ethernet II, Src: Vmware_16:09:96 (00:0c:29:65:25:d3), Dst: Vmware_65:25:d3 (00:0c:29:65:25:d3)
Internet Protocol Version 4, Src: 10.32.5.3 (10.32.5.3), Dst: 10.32.5.11 (10.32.5.11)
Transmission Control Protocol, Src Port: ldap (389), Dst Port: 49178 (49178), Seq: 2943, Ack: 183, Len: 5108
[2 Reassembled TCP Segments (8006 bytes): #11(2920), #13(5086)]
Lightweight Directory Access Protocol
  LDAPMessage searchResEntry(122) "CN=Johan Loos,OU=Users,OU=Access Denied,DC=addev,DC=local" [1 result]
    messageID: 122
    protocolOp: searchResEntry (4)
    searchResEntry
      objectName: CN=Johan Loos,OU=Users,OU=Access Denied,DC=addev,DC=local
      attributes: 34 items
[Response To: 10]
[Time: 0.000867000 seconds]
Lightweight Directory Access Protocol
  LDAPMessage searchResDone(122) success [1 result]
    messageID: 122
    protocolOp: searchResDone (5)
    searchResDone
      resultCode: success (0)
      matchedDN:
      errorMessage:
[Response To: 10]
[Time: 0.000867000 seconds]

```

- User found

```

Frame 16: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface 0
Ethernet II, Src: Vmware_16:09:96 (00:0c:29:65:25:d3), Dst: Vmware_65:25:d3 (00:0c:29:65:25:d3)
Internet Protocol Version 4, Src: 10.32.5.3 (10.32.5.3), Dst: 10.32.5.11 (10.32.5.11)
Transmission Control Protocol, Src Port: ldap (389), Dst Port: 49178 (49178), Seq: 8051, Ack: 274, Len: 22
Lightweight Directory Access Protocol
  LDAPMessage bindResponse(123) success
    messageID: 123
    protocolOp: bindResponse (1)
    bindResponse
      resultCode: success (0)
      matchedDN:
      errorMessage:
[Response To: 15]
[Time: 0.000721000 seconds]

```

- Verify if the group exists in Active Directory

```

Frame 25: 995 bytes on wire (7960 bits), 995 bytes captured (7960 bits) on interface 0
Ethernet II, Src: Vmware_16:09:96 (00:0c:29:65:25:d3), Dst: Vmware_65:25:d3 (00:0c:29:65:25:d3)
Internet Protocol Version 4, Src: 10.32.5.3 (10.32.5.3), Dst: 10.32.5.11 (10.32.5.11)
Transmission Control Protocol, Src Port: ldap (389), Dst Port: 49178 (49178), Seq: 16145, Ack: 706, Len: 941
Lightweight Directory Access Protocol
  LDAPMessage searchResEntry(127) "CN=LDAP Administrators,OU=Groups,OU=Access Denied,DC=addev,DC=local" [1 result]
    messageID: 127
    protocolOp: searchResEntry (4)
    searchResEntry
      objectName: CN=LDAP Administrators,OU=Groups,OU=Access Denied,DC=addev,DC=local
      attributes: 17 items
[Response To: 24]
[Time: 0.000234000 seconds]
Lightweight Directory Access Protocol
  LDAPMessage searchResDone(127) success [1 result]
    messageID: 127
    protocolOp: searchResDone (5)
    searchResDone
      resultCode: success (0)
      matchedDN:
      errorMessage:
[Response To: 24]
[Time: 0.000234000 seconds]

```

- Group found

```

Frame 27: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface 0
Ethernet II, Src: Vmware_16:09:96 (00:0c:29:16:09:96), Dst: Vmware_65:25:d3 (00:0c:29:65:25:d3)
Internet Protocol Version 4, Src: 10.32.5.3 (10.32.5.3), Dst: 10.32.5.11 (10.32.5.11)
Transmission Control Protocol, Src Port: ldap (389), Dst Port: 49178 (49178), Seq: 17086, Ack: 779, Len: 23
Lightweight Directory Access Protocol
  LDAPMessage bindResponse(128) success
    messageID: 128
    protocolOp: bindResponse (1)
    bindResponse
      resultCode: success (0)
      matchedDN:
      errorMessage:
      [Response To: 261]
    [Time: 0.000751000 seconds]

```

- Verify if the user is a member of the LDAP Administrators group

```

Frame 33: 233 bytes on wire (1864 bits), 233 bytes captured (1864 bits) on interface 0
Ethernet II, Src: Vmware_65:25:d3 (00:0c:29:65:25:d3), Dst: Vmware_16:09:96 (00:0c:29:16:09:96)
Internet Protocol Version 4, Src: 10.32.5.11 (10.32.5.11), Dst: 10.32.5.3 (10.32.5.3)
Transmission Control Protocol, Src Port: 49178 (49178), Dst Port: ldap (389), Seq: 963, Ack: 25162, Len: 179
Lightweight Directory Access Protocol
  LDAPMessage searchRequest(131) "cn=LDAP Administrators,ou=Groups,ou=access denied,dc=addev,dc=local" baseObject
    messageID: 131
    protocolOp: searchRequest (3)
    searchRequest
      baseObject: cn=LDAP Administrators,ou=Groups,ou=access denied,dc=addev,dc=local
      scope: baseObject (0)
      derefAliases: neverDerefAliases (0)
      sizeLimit: 0
      timeLimit: 0
      typesOnly: False
      filter: (member=CN=Johan Loos,OU=Users,OU=Access Denied,DC=addev,DC=local)
      filter: equalityMatch (3)
        equalityMatch
          attributeDesc: member
          assertionValue: CN=Johan Loos,OU=Users,OU=Access Denied,DC=addev,DC=local
          attributes: 0 items
      [Response In: 341]

```

- User is member of this group

```

Frame 35: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
Ethernet II, Src: Vmware_65:25:d3 (00:0c:29:65:25:d3), Dst: Vmware_16:09:96 (00:0c:29:16:09:96)
Internet Protocol Version 4, Src: 10.32.5.3 (10.32.5.3), Dst: 10.32.5.11 (10.32.5.11)
Transmission Control Protocol, Src Port: ldap (389), Dst Port: 49178 (49178), Seq: 17086, Ack: 779, Len: 23
Lightweight Directory Access Protocol
  LDAPMessage bindResponse(128) success
    messageID: 128
    protocolOp: bindResponse (1)
    bindResponse
      resultCode: success (0)
      matchedDN:
      errorMessage:
      [Response To: 261]
    [Time: 0.000751000 seconds]

```

- Unbind the connection with the LDAP server

```

Frame 35: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
Ethernet II, Src: Vmware_65:25:d3 (00:0c:29:65:25:d3), Dst: Vmware_16:09:96 (00:0c:29:16:09:96)
Internet Protocol Version 4, Src: 10.32.5.11 (10.32.5.11), Dst: 10.32.5.3 (10.32.5.3)
Transmission Control Protocol, Src Port: 49178 (49178), Dst Port: ldap (389), Seq: 1142, Ack: 26105, Len: 12
Lightweight Directory Access Protocol
  LDAPMessage unbindRequest(132)
    messageID: 132
    protocolOp: unbindRequest (2)
    unbindRequest

```

RADIUS Authentication

How it works

pGina captures the user his credentials, and verifies if the password is correct. If authentication is successful, pGina creates a local user account on the server and adds the user account into a security group specified in the gateway process. When the user logs off, the local user account and profile are deleted from that server.

Authentication between the RADIUS client and RADIUS server is done via PAP. The RADIUS client (our server) uses the shared key to encrypt the password of the user account and sends it to the RADIUS server.

You can also use IPSec to secure authentication traffic between the RADIUS client and RADIUS server.

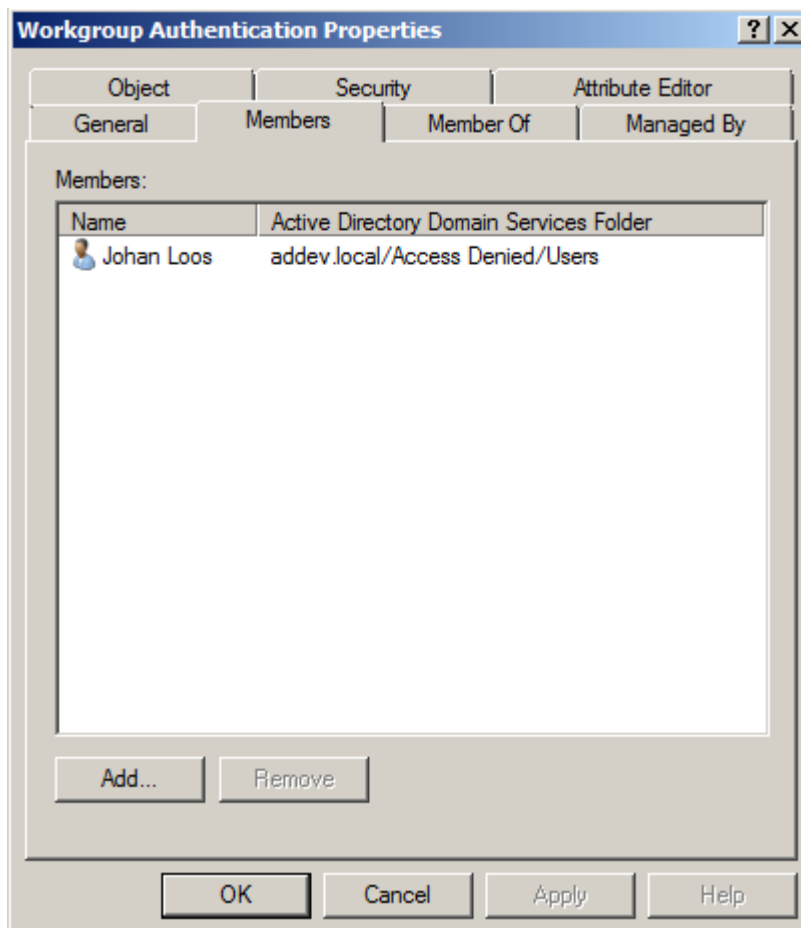
RADIUS Authentication Task List

- △ Create and configure your RADIUS Authentication group in Active Directory
- △ Configure pGina
- △ Configure LDAP plugin
- △ Configure LocalMachine plugin
- △ Configure your server as a RADIUS client on Windows Server 2012 NPS
- △ Create a Network Policy on Windows Server 2012 NPS
- △ Logon
- △ RADIUS Authentication Debug

Create and configure your RADIUS Authentication group in Active Directory

All members of this group are allowed to logon into a server in a workgroup via RADIUS.

- Open **Active Directory Users and Computers** from **Administrative Tools**

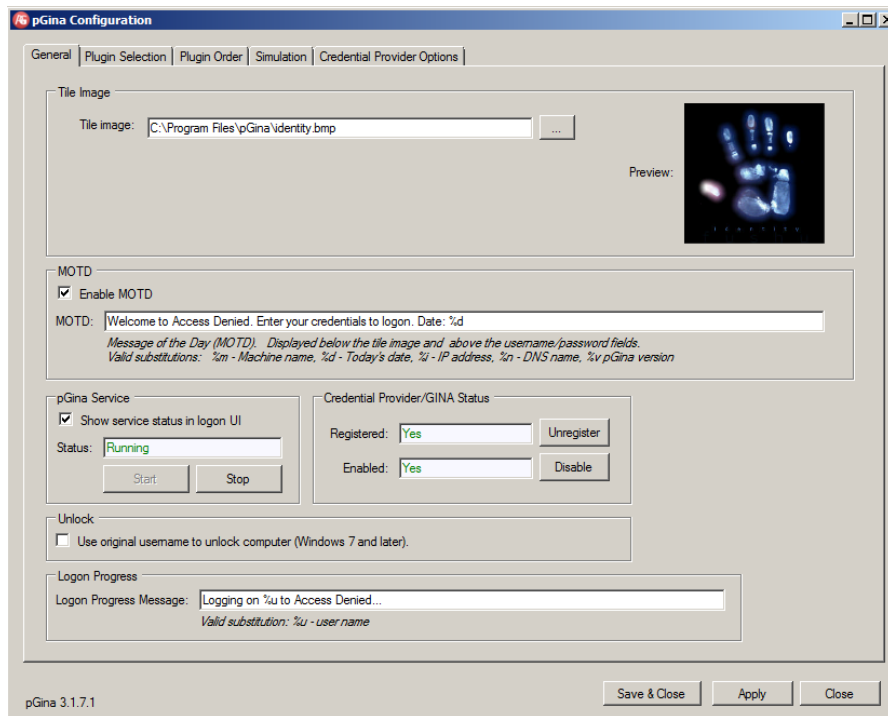


- Click OK

Configure pGina

Before you can logon with your domain credentials, you need to configure some plugins. pGina delegates the logon process to plugins. Depending on the type of backend you choose. In our example the backend server is a RADIUS server.

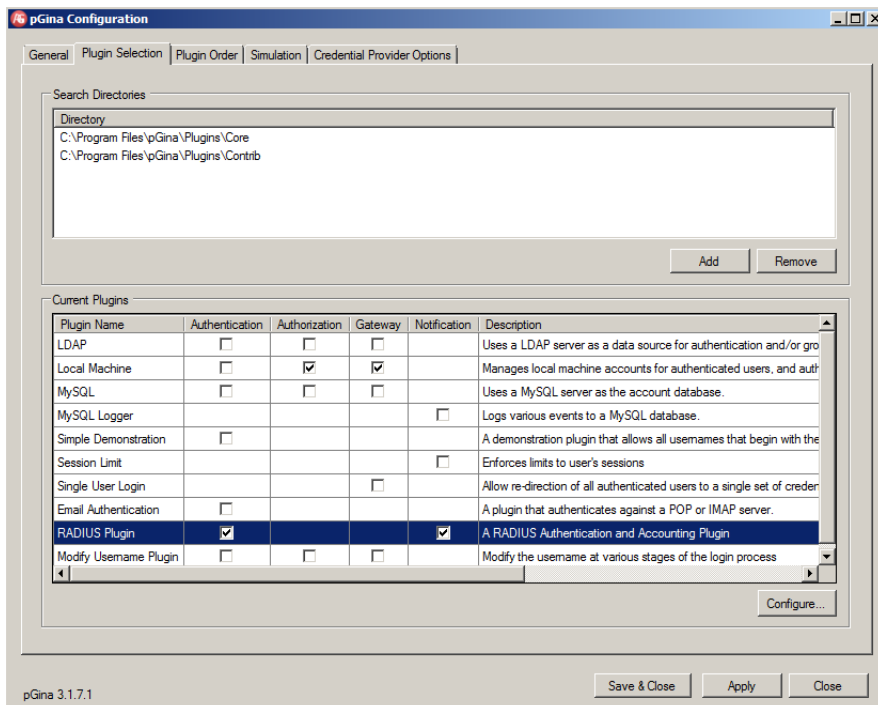
- On the **General** page, configure the following settings
 - You can select a bitmap Tile Image which is displayed in the logon screen
 - You can enable the Message of the Day (MOTD). This message is displayed in the logon screen
 - You can also specify a Logon Progress Message which is displayed when the user is successful authenticated



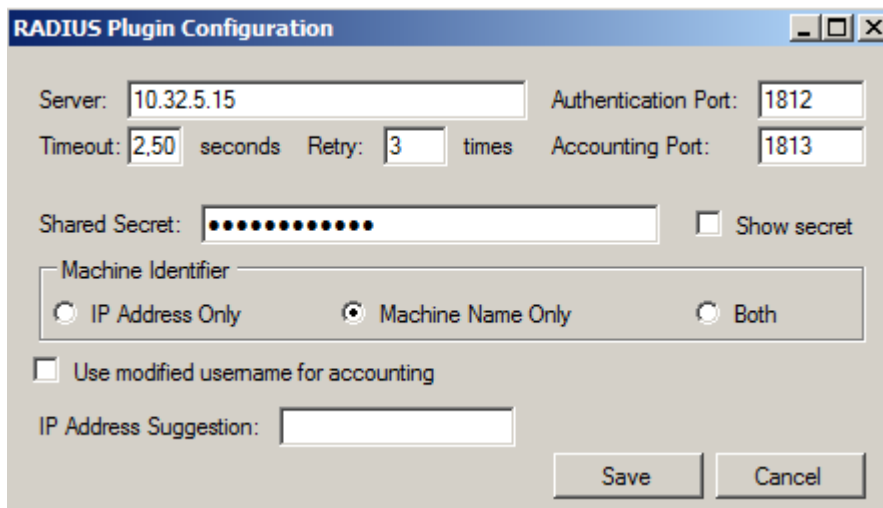
- Click Apply and click Save & Close

Configure RADIUS plugin

- On the **Plugin Selection** page, select the RADIUS Plugin
- Select Authentication, Notification, and click on Configure



- On the **RADIUS Plugin Configuration** page, configure the following:
 - Server: The IP address of your RADIUS Server
 - Shared Secret: Secret used to communicate with the RADIUS Server
 - Machine Identifier: Select an identifier, for example Machine Name Only



RADIUS Plugin Configuration

Server: Authentication Port:

Timeout: seconds Retry: times Accounting Port:

Shared Secret: ☐ Show secret

Machine Identifier

☐ IP Address Only ☒ Machine Name Only ☐ Both

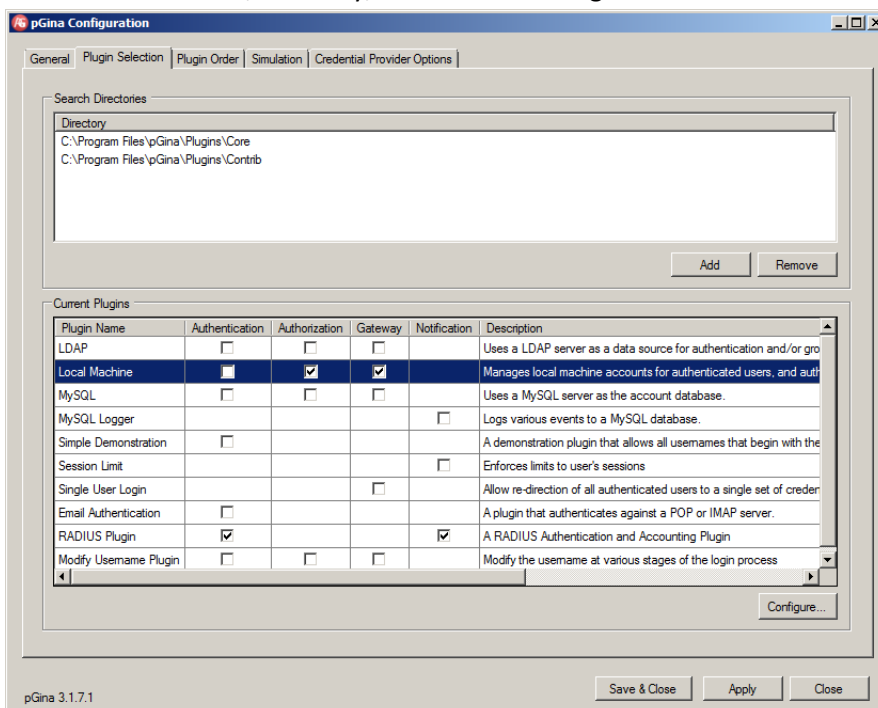
☐ Use modified username for accounting

IP Address Suggestion:

- Click Save

Configure LocalMachine plugin

- On the **Plugin Selection** page, select the Local Machine Plugin
- Select Authorization, Gateway, and click on Configure



pGina Configuration

General | **Plugin Selection** | Plugin Order | Simulation | Credential Provider Options

Search Directories

Directory

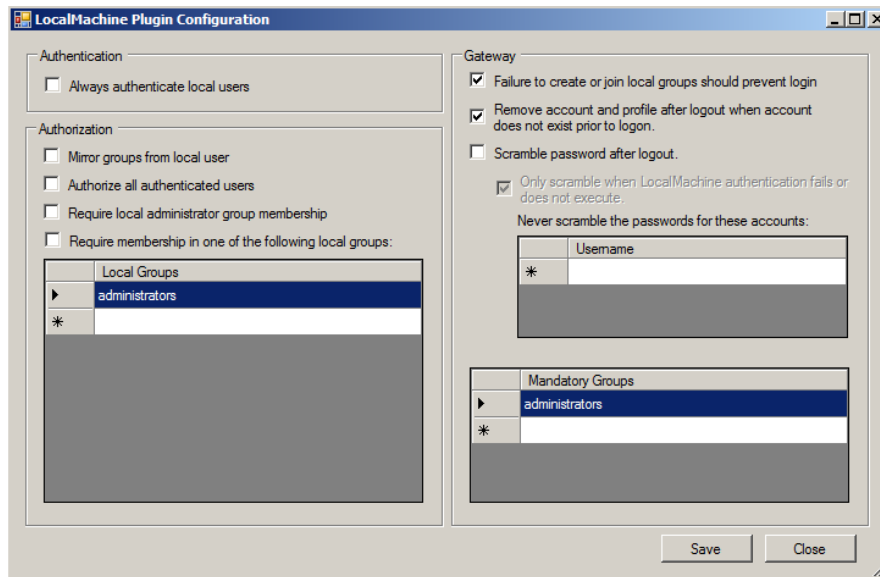
C:\Program Files\pGina\Plugins\Core
C:\Program Files\pGina\Plugins\Contrib

Current Plugins

Plugin Name	Authentication	Authorization	Gateway	Notification	Description
LDAP	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Uses a LDAP server as a data source for authentication and/or group membership.
Local Machine	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Manages local machine accounts for authenticated users, and authenticates users against local machine accounts.
MySQL	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Uses a MySQL server as the account database.
MySQL Logger	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Logs various events to a MySQL database.
Simple Demonstration	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	A demonstration plugin that allows all usernames that begin with the letter 'A'.
Session Limit	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Enforces limits to user's sessions.
Single User Login	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Allow re-direction of all authenticated users to a single set of credentials.
Email Authentication	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	A plugin that authenticates against a POP or IMAP server.
RADIUS Plugin	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	A RADIUS Authentication and Accounting Plugin.
Modify Username Plugin	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Modify the username at various stages of the login process.

pGina 3.1.7.1

- On the **LocalMachine Plugin Configuration** page, select the following
 - Remove account and profile after logout: When the user logs off, the plugin removes the user account from the group below, deletes the user account and the profile from the server
 - Mandatory Groups: The user account is added to the groups in the list



- Click Save

Configure your server as RADIUS client on Windows Server 2012 NPS

- Open **Network Policy Server** from **Administrative Tools**
- Expand RADIUS Clients and Servers, right click on **RADIUS Clients** and select **New RADIUS Client**
- On the **New RADIUS Client** dialog box, specify a friendly name and IP address

addevsrv01 Properties

Settings Advanced

☒ Enable this RADIUS client

☐ Select an existing template:

Name and Address

Friendly name:
addevsrv01

Address (IP or DNS):
10.32.5.11 Verify...

Shared Secret

Select an existing Shared Secrets template:
None

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

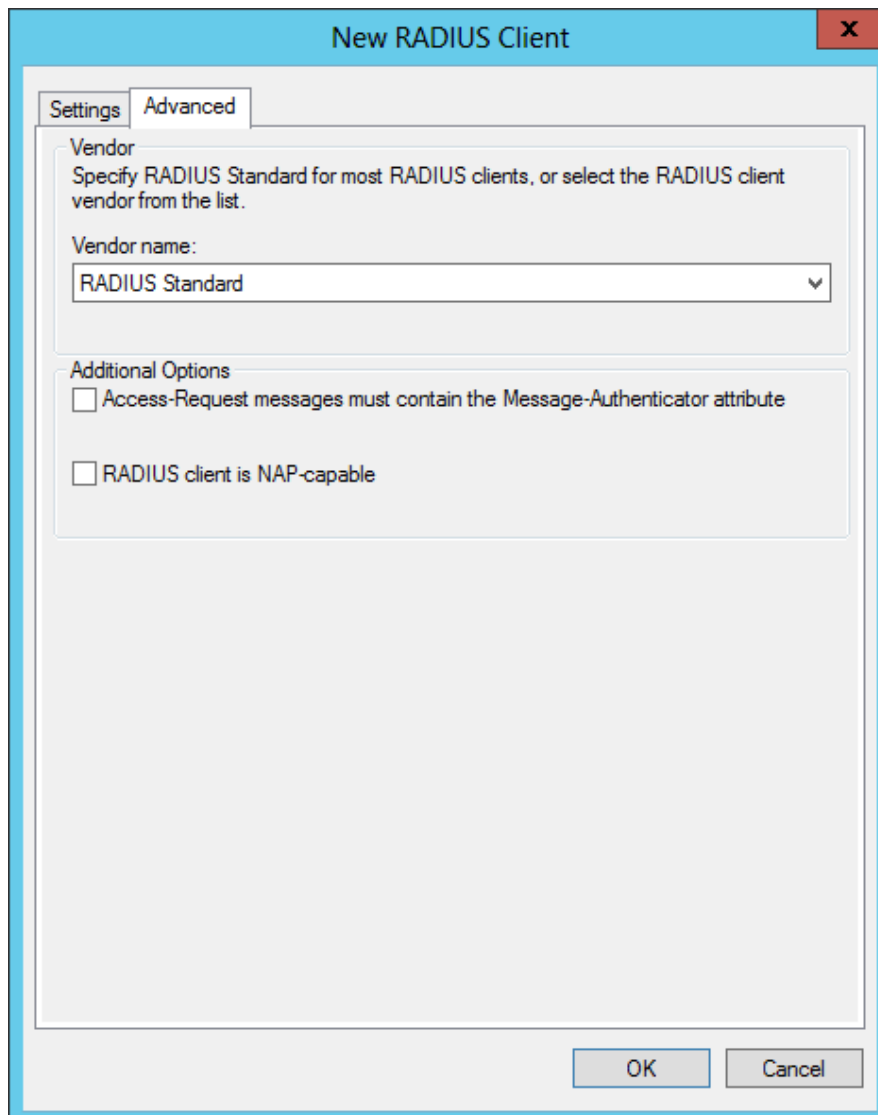
☒ Manual ☐ Generate

Shared secret:
.....

Confirm shared secret:
.....

OK Cancel Apply

- Click on **Advanced**, uncheck or check the required options



- Click **OK**

Create a Network Policy on Windows Server 2012 NPS

- From the **Network Policy Server Console**, right click on **Network Policies** and select **New**
- On the **Specify Network Policy Name and Connection Type** page, type a name for your policy and click **Next**

New Network Policy

Specify Network Policy Name and Connection Type

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

Policy name:

Network connection method
 Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.

☒ Type of network access server:

☐ Vendor specific:

Previous Next Finish Cancel

- On the **Specify Conditions** page, click **Add**
- From the **Select Condition** dialog box, add the following Windows Groups *Workgroup Authentication*, and click **Next**

New Network Policy

Specify Conditions

Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required.

Conditions:

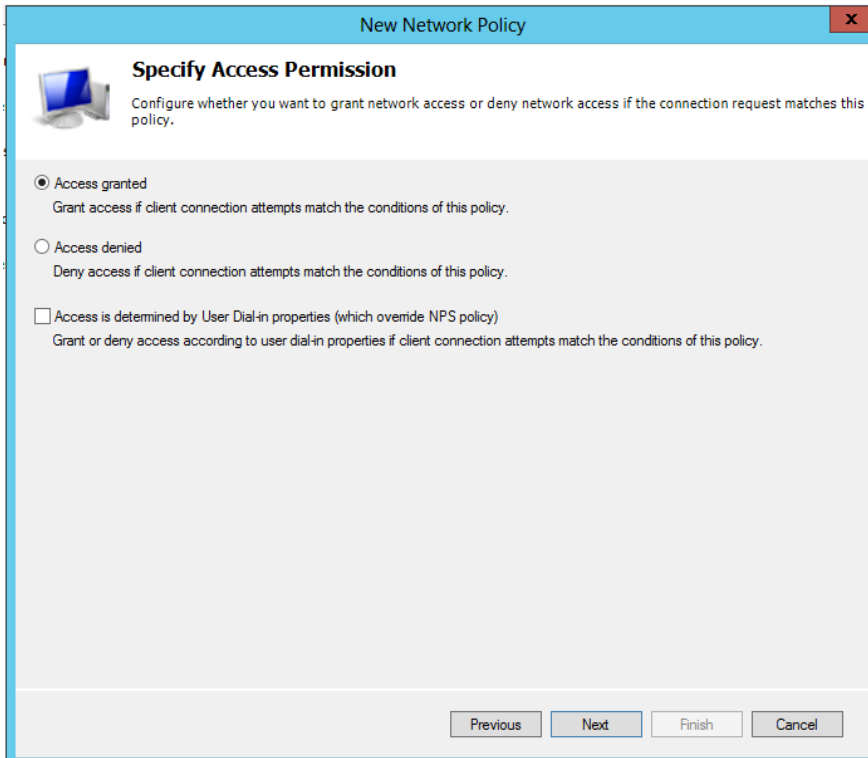
Condition	Value
Windows Groups	ADDEV\Workgroup Authentication

Condition description:
 The Windows Groups condition specifies that the connecting user or computer must belong to one of the selected groups.

Add... Edit... Remove

Previous Next Finish Cancel

- On the **Specify Access Permissions** page, select **Access Granted** and click **Next**



New Network Policy

Specify Access Permission

Configure whether you want to grant network access or deny network access if the connection request matches this policy.

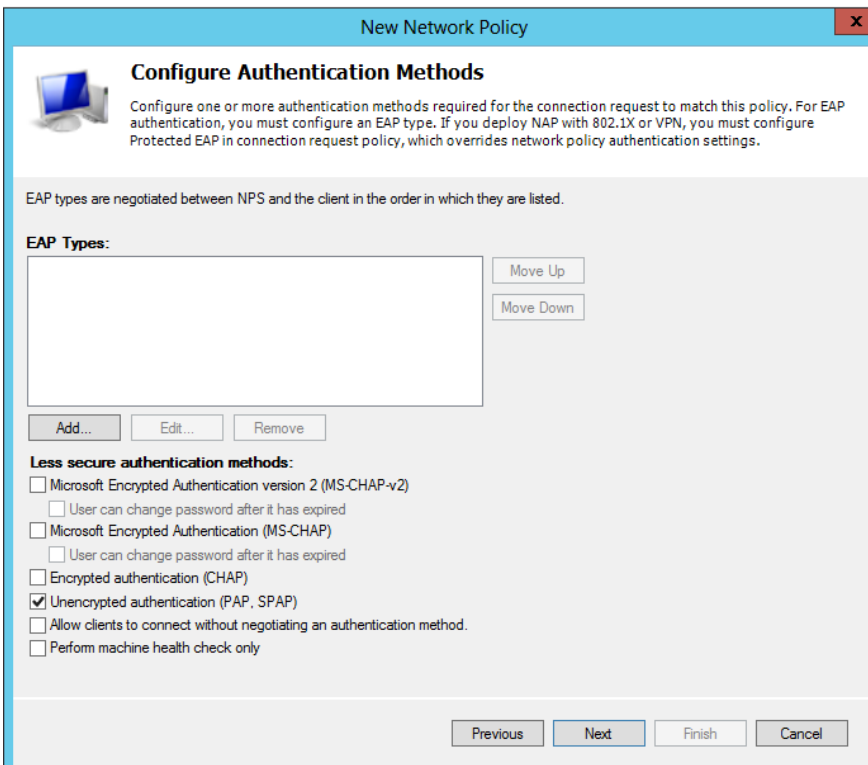
☒ Access granted
 Grant access if client connection attempts match the conditions of this policy.

☐ Access denied
 Deny access if client connection attempts match the conditions of this policy.

☐ Access is determined by User Dial-in properties (which override NPS policy)
 Grant or deny access according to user dial-in properties if client connection attempts match the conditions of this policy.

Previous Next Finish Cancel

- On the **Configure Authentication Methods** page, clear all authentications methods and select only **Unencrypted Authentication (PAP,SPAP)** and click **Add**



New Network Policy

Configure Authentication Methods

Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type. If you deploy NAP with 802.1X or VPN, you must configure Protected EAP in connection request policy, which overrides network policy authentication settings.

EAP types are negotiated between NPS and the client in the order in which they are listed.

EAP Types:

Move Up Move Down

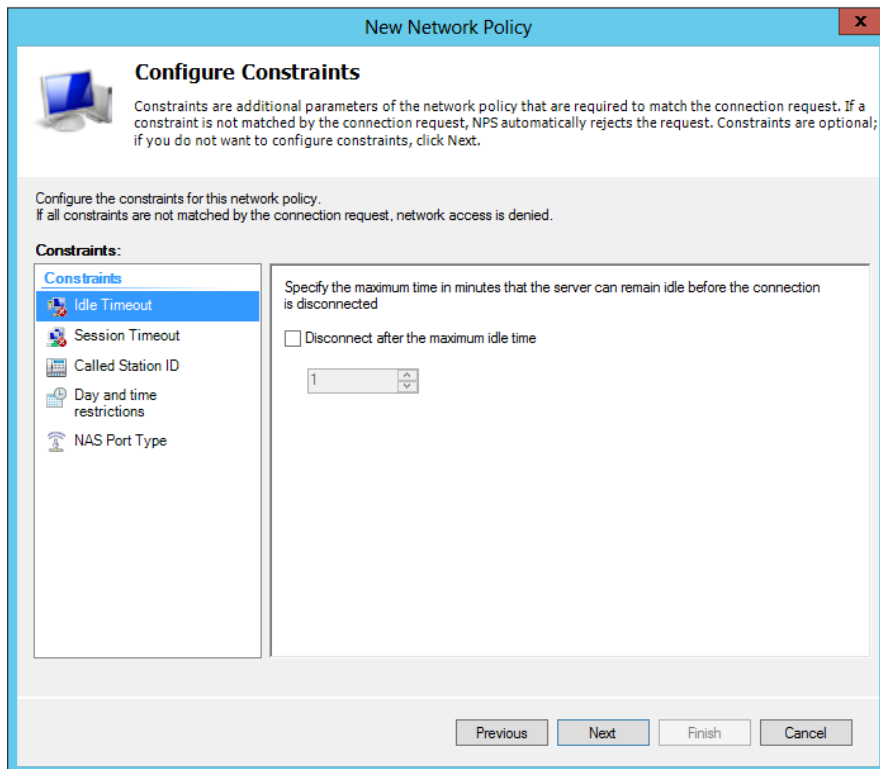
Add... Edit... Remove

Less secure authentication methods:

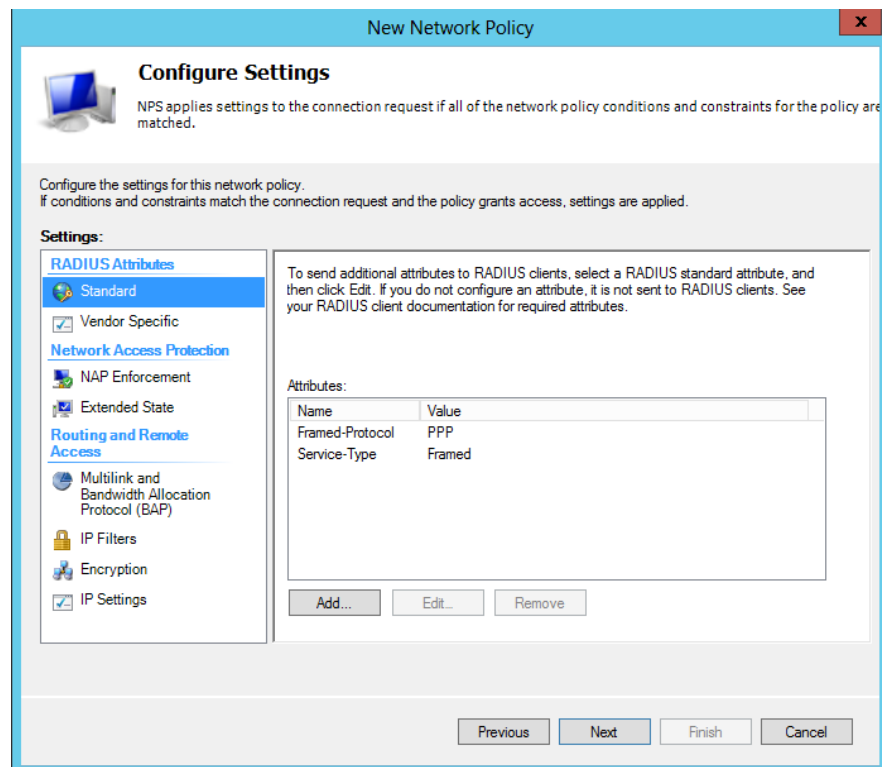
☐ Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
☐ User can change password after it has expired
☐ Microsoft Encrypted Authentication (MS-CHAP)
☐ User can change password after it has expired
☐ Encrypted authentication (CHAP)
☒ Unencrypted authentication (PAP, SPAP)
☐ Allow clients to connect without negotiating an authentication method.
☐ Perform machine health check only

Previous Next Finish Cancel

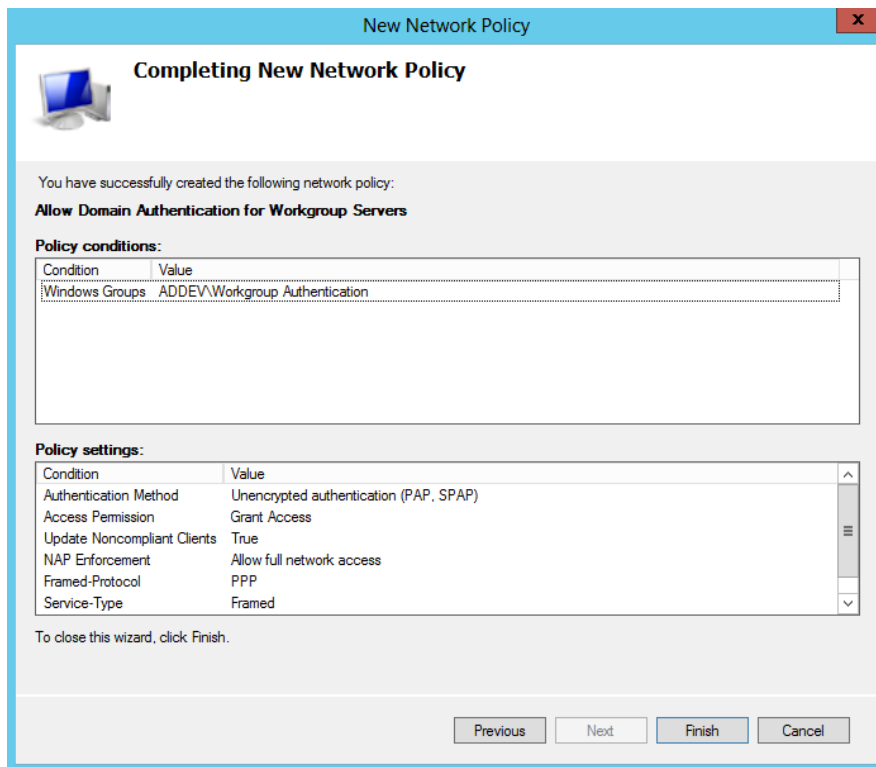
- On the **Configure Constraints** page, click **Next**



- On the **Configure Settings** page, click **Next**

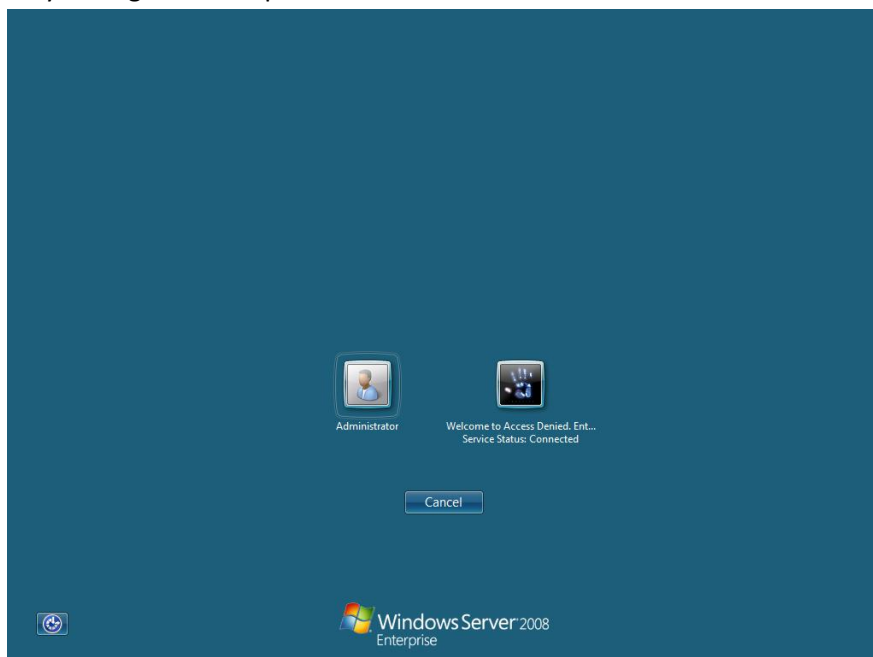


- On the **Completing New Network Policy** page, click **Finish**

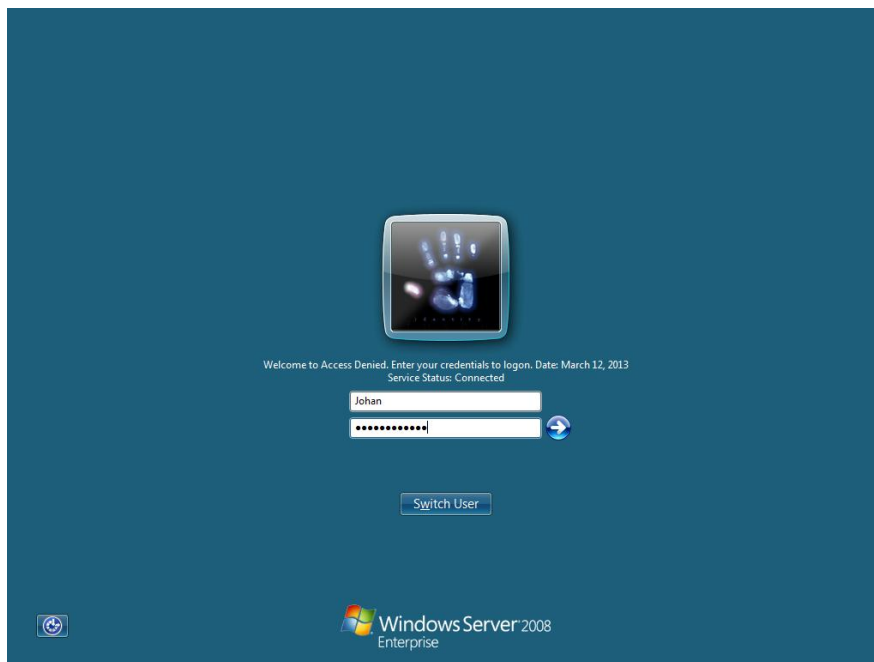


Logon

- On your logon screen press CTRL+ALT+DEL and select switch user



- Type your domain credentials to logon



- Press Enter to login
- You are now logged on the workgroup server and member of the local administrators group

RADIUS Authentication Debug

- RADIUS client sends Accept-Request authentication request

```

Frame 1: 99 bytes on wire (792 bits), 99 bytes captured (792 bits) on interface 0
Ethernet II, Src: Vmware_65:25:d3 (00:0c:29:65:25:d3), Dst: Vmware_98:b6:2c (00:0c:29:98:b6:2c)
Internet Protocol Version 4, Src: 10.32.5.11 (10.32.5.11), Dst: 10.32.5.15 (10.32.5.15)
User Datagram Protocol, Src Port: 65107 (65107), Dst Port: radius (1812)
Radius Protocol
  Code: Access-Request (1)
  Packet identifier: 0xef (239)
  Length: 57
  Authenticator: 37c01e1252d7882df4c7338cfffde8f9
  [The response to this request is in frame 15]
  Attribute Value Pairs
    AVP: l=7 t=User-Name(1): johan
      User-Name: johan
    AVP: l=18 t=User-Password(2): Encrypted
      User-Password (encrypted): cad797f6e9f69a404cad3672006a042d
    AVP: l=12 t=NAS-Identifier(32): ADDEVSRV01
      NAS-Identifier: ADDEVSRV01

```

- RADIUS server sends Accept-Accept request

```

Frame 15: 120 bytes on wire (960 bits), 120 bytes captured (960 bits) on interface 0
Ethernet II, Src: Vmware_98:b6:2c (00:0c:29:98:b6:2c), Dst: Vmware_65:25:d3 (00:0c:29:65:25:d3)
Internet Protocol Version 4, Src: 10.32.5.15 (10.32.5.15), Dst: 10.32.5.11 (10.32.5.11)
User Datagram Protocol, Src Port: radius (1812), Dst Port: 65107 (65107)
Radius Protocol
  Code: Access-Accept (2)
  Packet identifier: 0xef (239)
  Length: 78
  Authenticator: e832bad3141462d58a317189a753bc99
  [This is a response to a request in frame 1]
  [Time from request: 0.004139000 seconds]
  Attribute Value Pairs
    AVP: l=6 t=Framed-Protocol(7): PPP(1)
    AVP: l=6 t=Service-Type(6): Framed(2)
    AVP: l=46 t=Class(25): 3b32043800000137000102000a20050f0000000000000000...

```

Encrypting RADIUS traffic with IPSec Task List

You can use IPSec to further encrypt authentication traffic.

- △ Create an Inbound rule on your RADIUS server
- △ Create a Connection Security Rule on your RADIUS server (NPS Server)

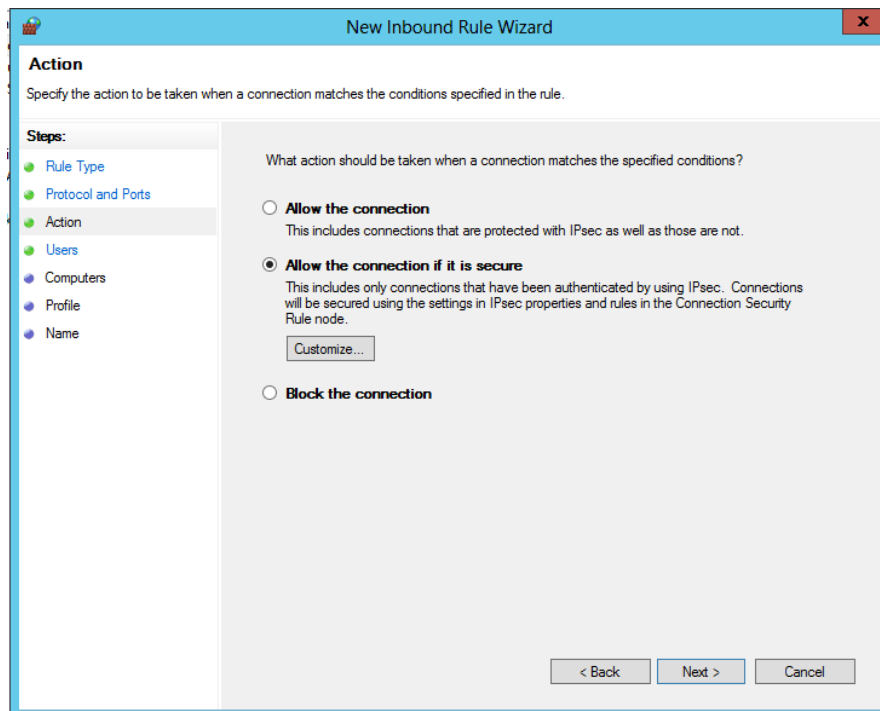
- △ Create a Connection Security Rule on your RADIUS client (workgroup server)
- △ Monitor Security Associations

Create an Inbound rule on your RADIUS server

- Open **Windows Firewall with Advanced Security** from **Administrative Tools**
- Right click on Inbound Rule and select New Rule
- On the **Rule Type** page, select Port and click Next

- On the **Protocols and Port** page, select Specific local ports and type 1812

- On the **Action** page, select Allow the connection if it is secure and click Customize



- On the **Customize Allow if Secure Settings** page, select Require the connection to be encrypted and select Allow the computers to dynamically negotiate encryption and click OK

Customize Allow if Secure Settings

Select one of these options to determine which action Windows Firewall with Advanced Security will take for the incoming or outgoing packets that match the firewall rule criteria.

☐ **Allow the connection if it is authenticated and integrity-protected**

Allow only connections that are both authenticated and integrity-protected by using IPsec. Compatible with Windows Vista and later.

☒ **Require the connections to be encrypted**

Require privacy in addition to integrity and authentication

☒ Allow the computers to dynamically negotiate encryption

This option allows authenticated but unencrypted network packets to be sent while encryption is being negotiated. Compatible with Windows Vista and later.

☐ **Allow the connection to use null encapsulation**

Null encapsulation allows you to require that the connection be authenticated, but does not provide integrity or privacy protection for the packet payload. Compatible with Windows 7 and later.

☐ **Override block rules**

Useful for tools that must always be available, such as remote administration tools. If you specify this option, you must also specify an authorized computer or computer group.

- On the **Users** page, click Next

New Inbound Rule Wizard

Users

Specify the users that are allowed to make the connection specified by this rule.

Steps:

- Rule Type
- Protocol and Ports
- Action
- **Users**
- Computers
- Profile
- Name

Authorized users

☐ Only allow connections from these users

Exceptions

☐ Skip this rule for connections from these users

Note: user identities can only be verified if an authentication method that carries user identity is used.

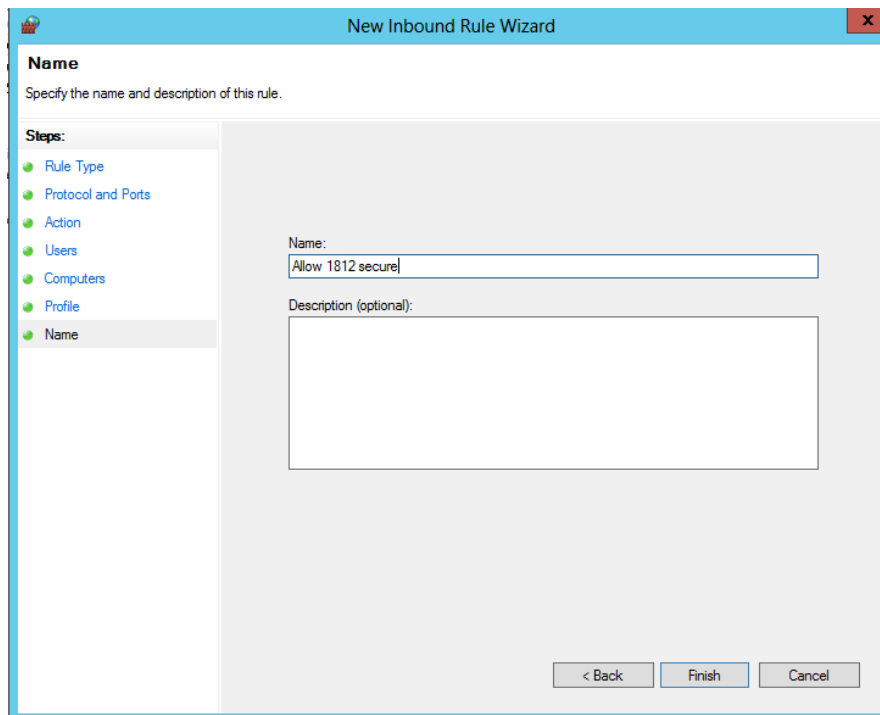
- On the **Computers** page, click Next

The screenshot shows the 'Computers' page of the 'New Inbound Rule Wizard'. The title bar reads 'New Inbound Rule Wizard'. The page title is 'Computers'. Below the title, it says 'Specify the computers that are allowed to make the connection specified by this rule.' On the left, there is a 'Steps:' list with 'Computers' selected. The main area has two sections: 'Authorized computers' and 'Exceptions'. Both sections have a checkbox to 'Only allow connections from these computers' and 'Skip this rule for connections from these computers' respectively, followed by empty list boxes and 'Add...' and 'Remove' buttons. At the bottom, there is a note: 'Note: computer identities can only be verified if an authentication method that carries computer identity is used.' and navigation buttons '< Back', 'Next >', and 'Cancel'.

- On the **Profile** page, click Next

The screenshot shows the 'Profile' page of the 'New Inbound Rule Wizard'. The title bar reads 'New Inbound Rule Wizard'. The page title is 'Profile'. Below the title, it says 'Specify the profiles for which this rule applies.' On the left, there is a 'Steps:' list with 'Profile' selected. The main area has a section titled 'When does this rule apply?' with three checked options: 'Domain' (Applies when a computer is connected to its corporate domain.), 'Private' (Applies when a computer is connected to a private network location, such as a home or work place.), and 'Public' (Applies when a computer is connected to a public network location.). At the bottom, there are navigation buttons '< Back', 'Next >', and 'Cancel'.

- On the **Name** page, type a name for your rule and click Finish



New Inbound Rule Wizard

Name
Specify the name and description of this rule.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Users
- Computers
- Profile
- Name**

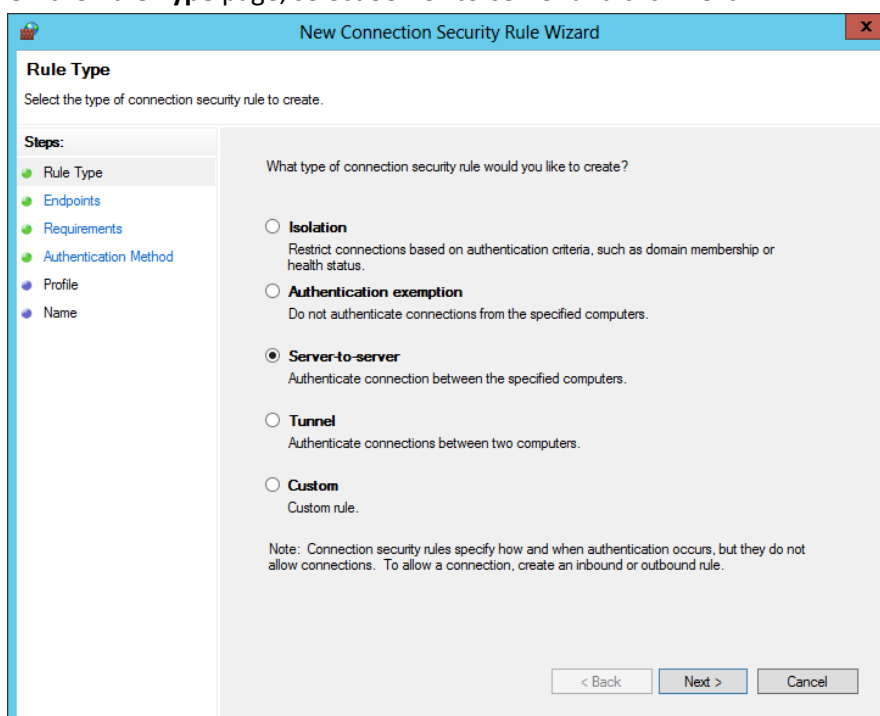
Name:
Allow 1812 secure

Description (optional):

< Back Finish Cancel

Create a Connection Security Rule on your RADIUS server (NPS Server)

- Right click on Connection Security Rules and select New Rule
- On the **Rule Type** page, select Server-to-server and click Next



New Connection Security Rule Wizard

Rule Type
Select the type of connection security rule to create.

Steps:

- Rule Type
- Endpoints
- Requirements
- Authentication Method
- Profile
- Name

What type of connection security rule would you like to create?

☐ **Isolation**
Restrict connections based on authentication criteria, such as domain membership or health status.

☐ **Authentication exemption**
Do not authenticate connections from the specified computers.

☒ **Server-to-server**
Authenticate connection between the specified computers.

☐ **Tunnel**
Authenticate connections between two computers.

☐ **Custom**
Custom rule.

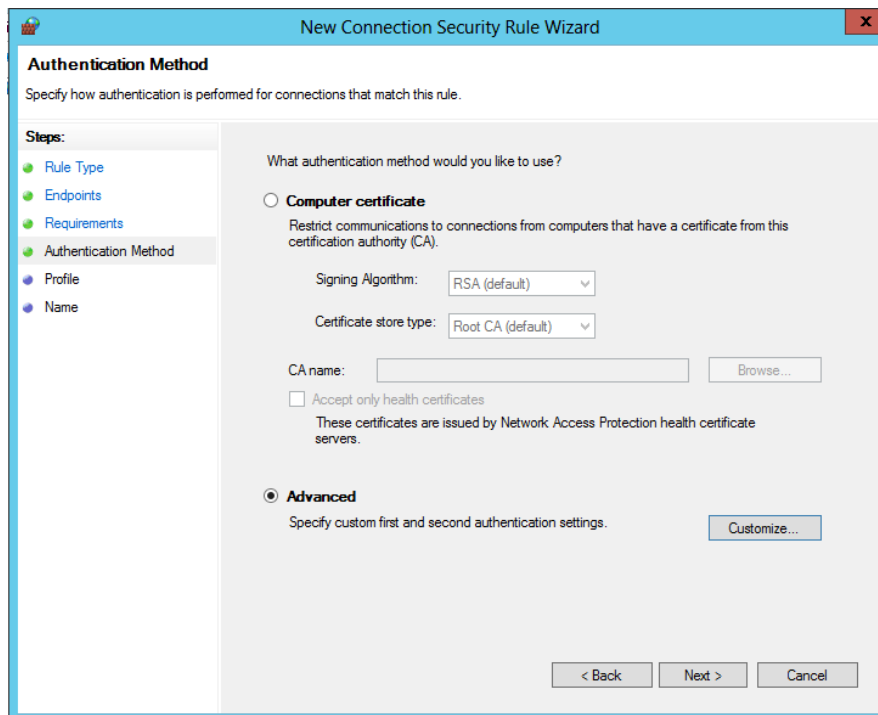
Note: Connection security rules specify how and when authentication occurs, but they do not allow connections. To allow a connection, create an inbound or outbound rule.

< Back Next > Cancel

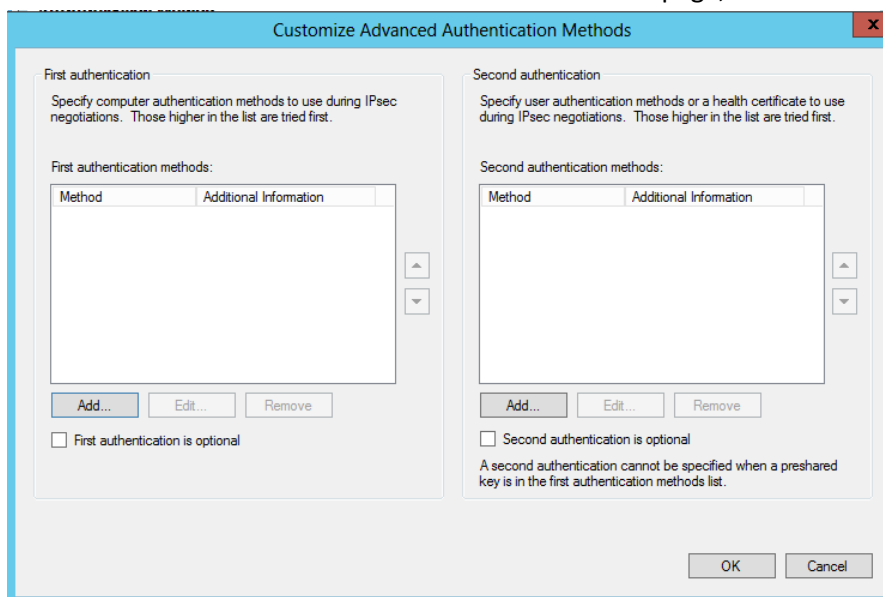
- On the **Endpoints** page, add the IP address of your workgroup server, and click Next

- On the **Requirements** page, select Require authentication for inbound and outbound connections, and click Next

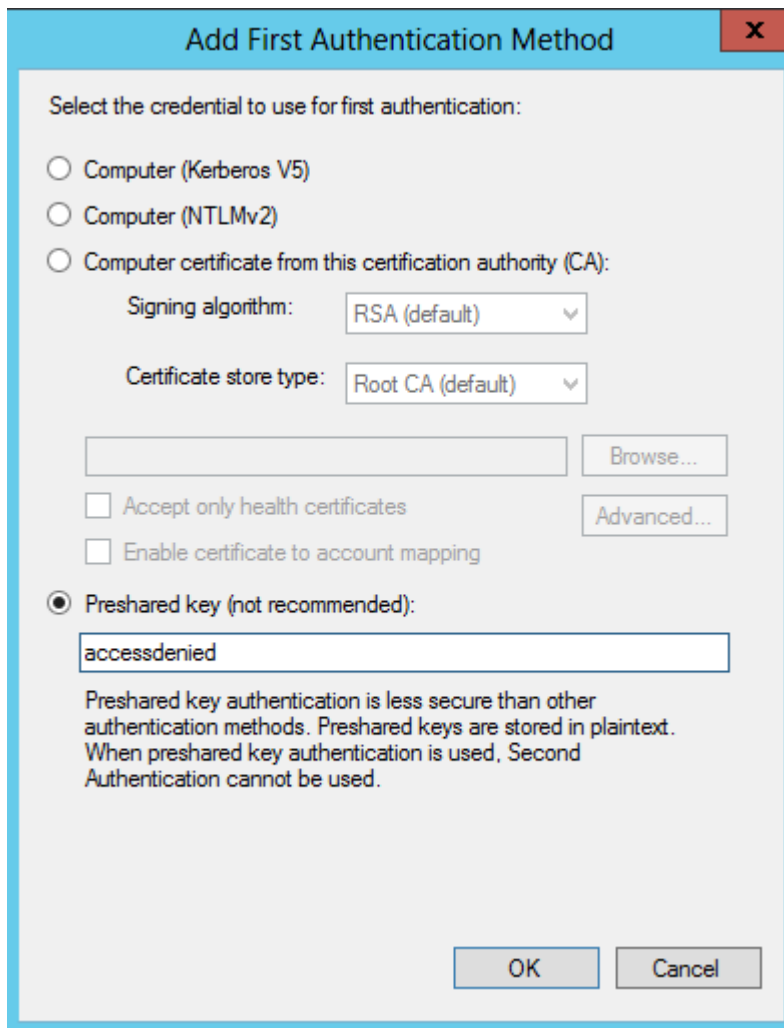
- On the **Authentication Methods** page, select Advanced and click Customize



- On the **Customize Advanced Authentication Methods** page, click Add



- On the **Add First Authentication Method** page, select Preshared key and type a pre-shared key



Add First Authentication Method

Select the credential to use for first authentication:

☐ Computer (Kerberos V5)

☐ Computer (NTLMv2)

☐ Computer certificate from this certification authority (CA):

 Signing algorithm: RSA (default) ▼

 Certificate store type: Root CA (default) ▼

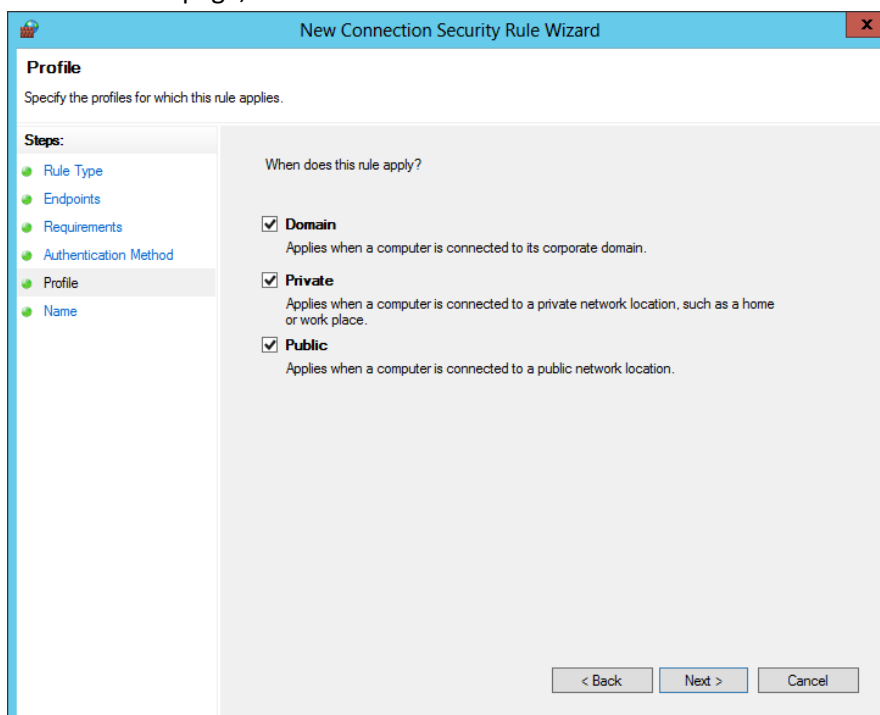
☐ Accept only health certificates

☐ Enable certificate to account mapping

☒ Preshared key (not recommended):

Preshared key authentication is less secure than other authentication methods. Preshared keys are stored in plaintext. When preshared key authentication is used, Second Authentication cannot be used.

- Click multiple times OK and click Next
- On the **Profile** page, click Next



New Connection Security Rule Wizard

Profile

Specify the profiles for which this rule applies.

Steps:

- Rule Type
- Endpoints
- Requirements
- Authentication Method
- Profile
- Name

When does this rule apply?

☒ **Domain**
Applies when a computer is connected to its corporate domain.

☒ **Private**
Applies when a computer is connected to a private network location, such as a home or work place.

☒ **Public**
Applies when a computer is connected to a public network location.

- On the **Name** page, type a name and click Finish

The screenshot shows the 'New Connection Security Rule Wizard' window with the 'Name' page selected in the 'Steps' list on the left. The main area contains a 'Name' field with the text 'Connection rule for RADIUS' and an empty 'Description (optional)' text box. At the bottom are '< Back', 'Finish', and 'Cancel' buttons.

Create a Connection Security Rule on your RADIUS client (workgroup server)

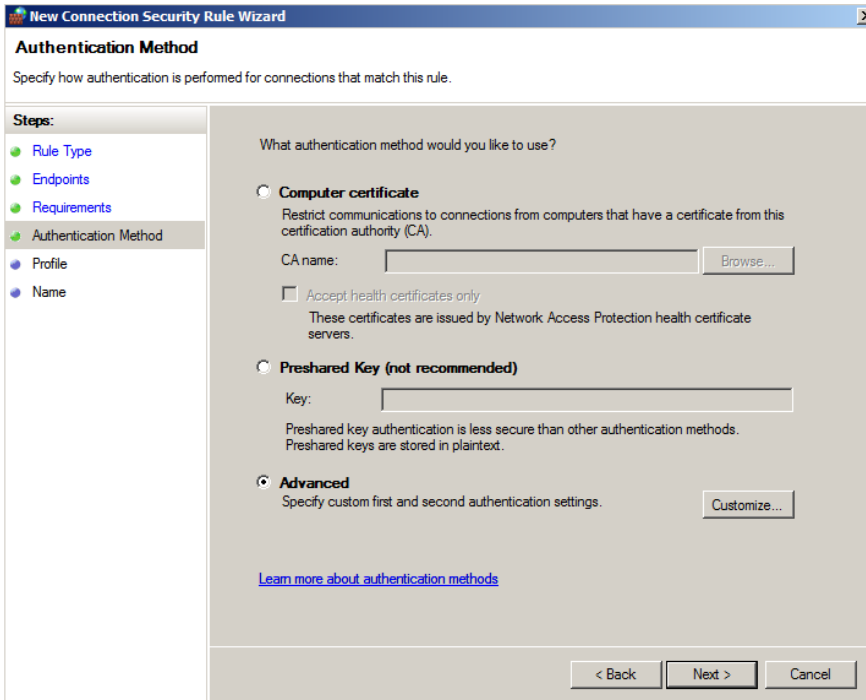
- Right click on Connection Security Rules and select New Rule
- On the **Rule Type** page, select Server-to-server and click Next

The screenshot shows the 'New Connection Security Rule Wizard' window with the 'Rule Type' page selected in the 'Steps' list on the left. The main area asks 'What type of connection security rule would you like to create?' and lists five options: Isolation, Authentication exemption, Server-to-server (selected), Tunnel, and Custom. A note at the bottom states: 'Note: Connection security rules specify how and when authentication occurs, but they do not allow connections. To allow a connection, create an inbound or outbound rule.' and includes a link 'Learn more about rule types'. At the bottom are '< Back', 'Next >', and 'Cancel' buttons.

- On the **Endpoints** page, add the IP address of your workgroup server, and click Next

- On the **Requirements** page, select Require authentication for inbound and outbound connections, and click Next

- On the **Authentication Methods** page, select Advanced and click Customize



New Connection Security Rule Wizard

Authentication Method

Specify how authentication is performed for connections that match this rule.

Steps:

- Rule Type
- Endpoints
- Requirements
- Authentication Method**
- Profile
- Name

What authentication method would you like to use?

☐ **Computer certificate**
 Restrict communications to connections from computers that have a certificate from this certification authority (CA).
 CA name:
☐ *Accept health certificates only*
 These certificates are issued by Network Access Protection health certificate servers.

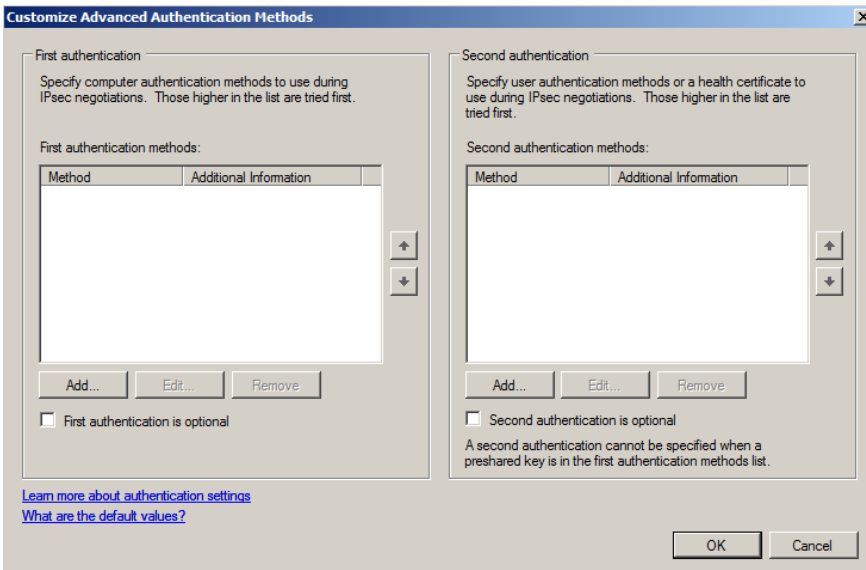
☐ **Preshared Key (not recommended)**
 Key:
 Preshared key authentication is less secure than other authentication methods. Preshared keys are stored in plaintext.

☒ **Advanced**
 Specify custom first and second authentication settings.

[Learn more about authentication methods](#)

< Back Next > Cancel

- On the **Customize Advanced Authentication Methods** page, click Add



Customize Advanced Authentication Methods

First authentication
 Specify computer authentication methods to use during IPsec negotiations. Those higher in the list are tried first.

First authentication methods:

Method	Additional Information

☐ First authentication is optional

Second authentication
 Specify user authentication methods or a health certificate to use during IPsec negotiations. Those higher in the list are tried first.

Second authentication methods:

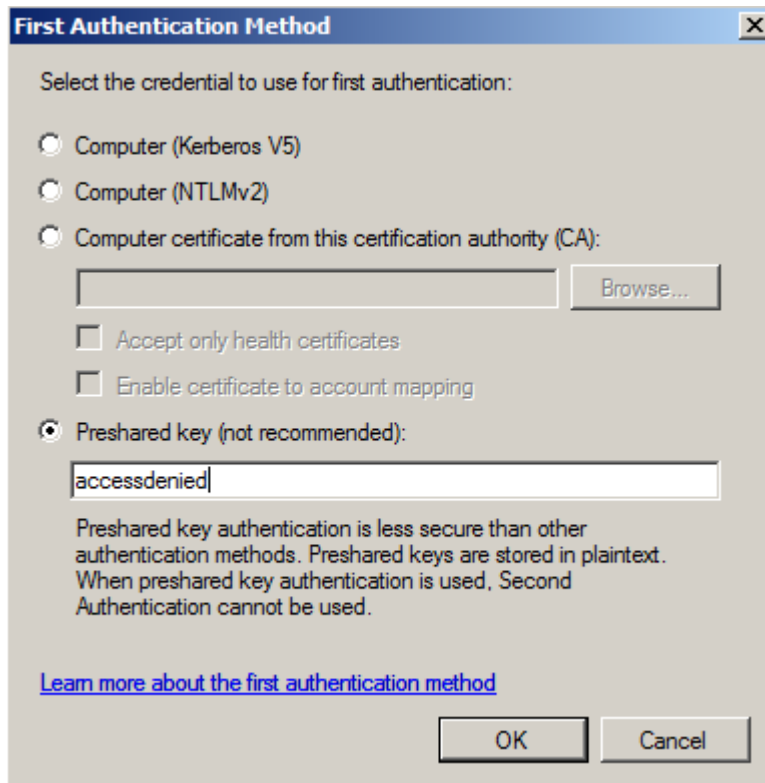
Method	Additional Information

☐ Second authentication is optional
 A second authentication cannot be specified when a preshared key is in the first authentication methods list.

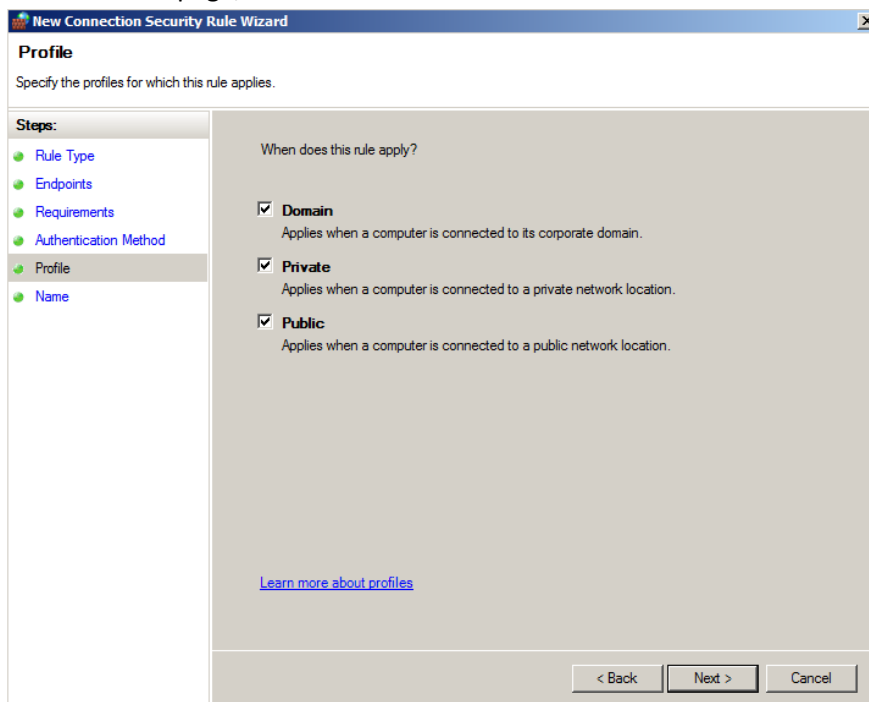
[Learn more about authentication settings](#)
[What are the default values?](#)

OK Cancel

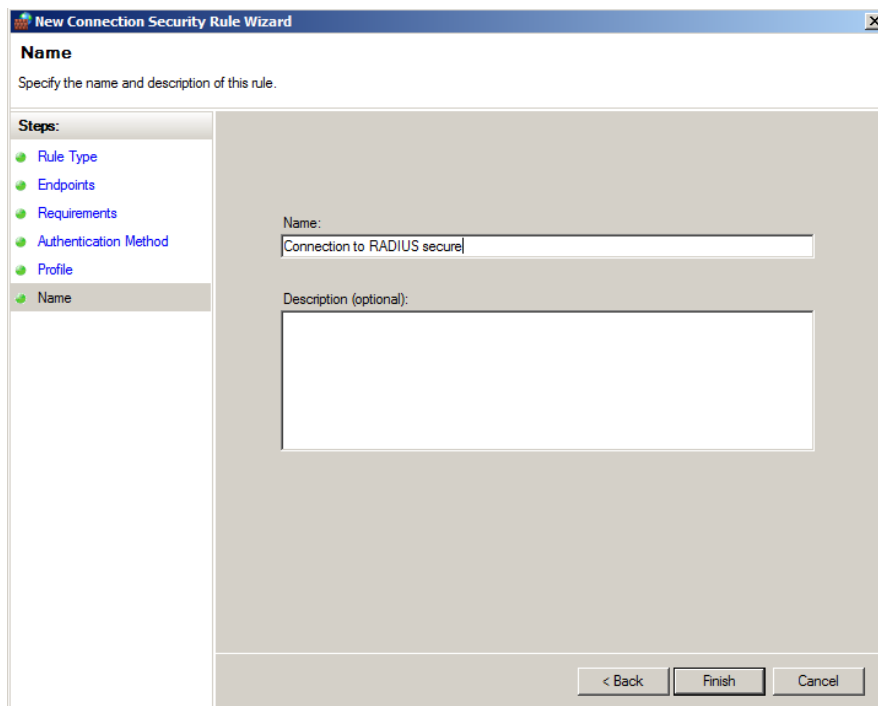
- On the **Add First Authentication Method** page, select Preshared key and type a pre-shared key



- Click multiple times OK and click Next
- On the **Profile** page, click Next



- On the **Name** page, type a name and click Finish



New Connection Security Rule Wizard

Name

Specify the name and description of this rule.

Steps:

- Rule Type
- Endpoints
- Requirements
- Authentication Method
- Profile
- Name**

Name:

Description (optional):

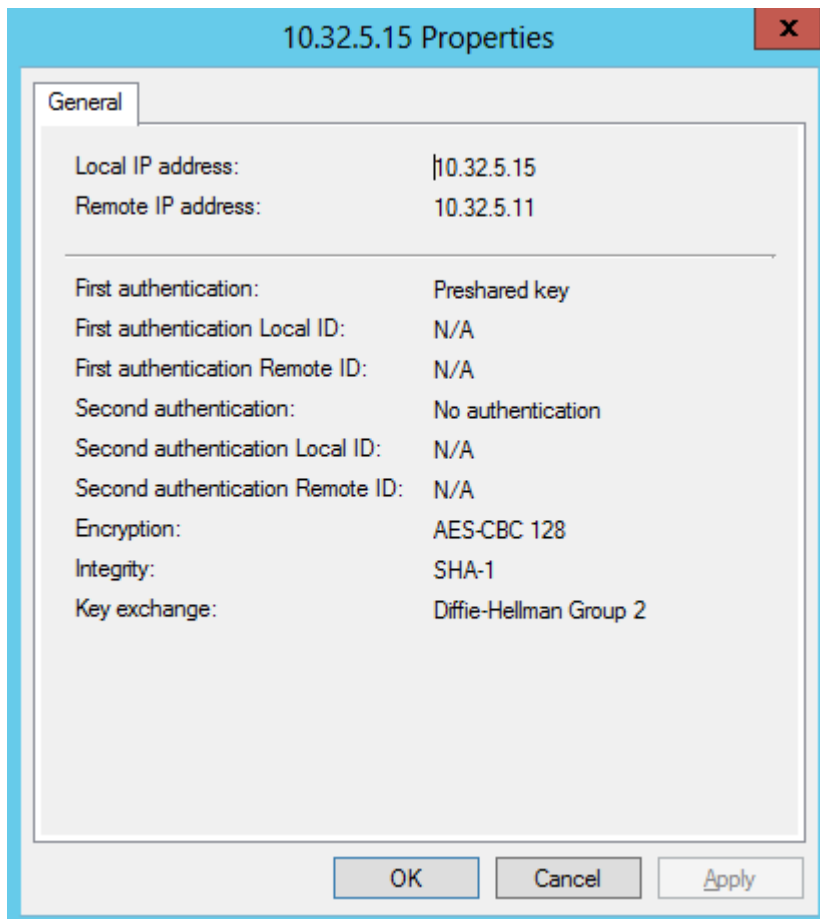
< Back Finish Cancel

Monitor Security Associations

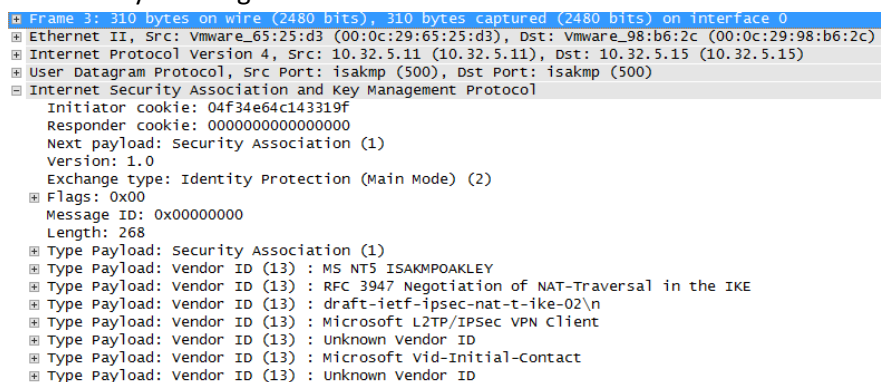
- On your RADIUS server, expand **Monitoring | Security Associations | Main Mode**
- When the RADIUS client initiates a secure connection to the RADIUS server, a security association is created.

Main Mode						
Local Address	Remote Address	1st Authentication Method	2nd Authentication Method	Encryption	Integrity	Key Exchange
10.32.5.15	10.32.5.11	Preshared key	No authentication	AES-CBC...	SHA-1	Diffie-Hellr

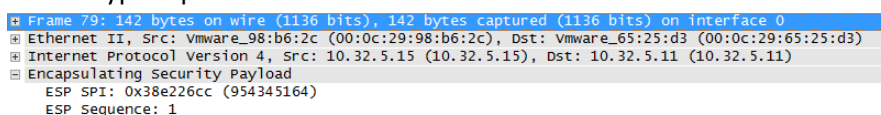
- IPSec Main Mode Security Association between RADIUS server and RADIUS client



- ISAKMP Key Exchange in Wireshark



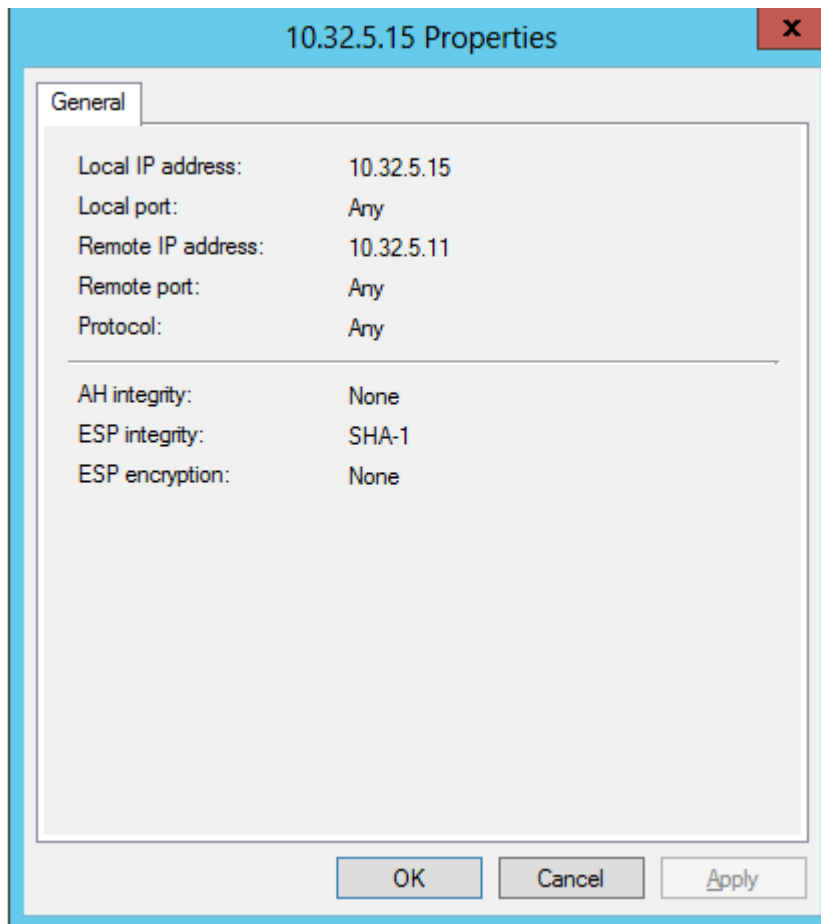
- ESP encrypted packets in Wireshark



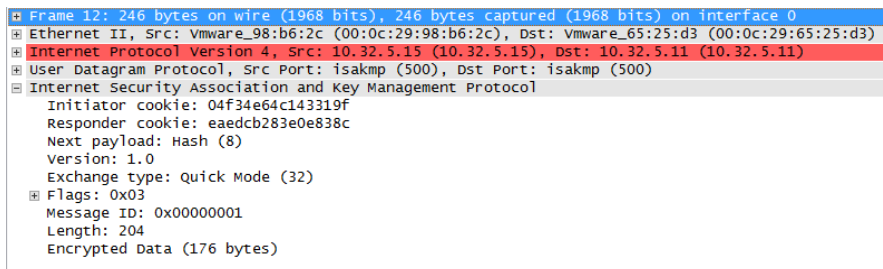
- Expand **Monitoring** | **Security Associations** | **Quick Mode**

Quick Mode							
Local Address	Remote Address	Local Port	Remote ...	Protocol	AH Integrity	ESP Integrity	ESP Encryption
10.32.5.15	10.32.5.11	Any	Any	Any	None	SHA-1	None

- IPSec Quick Mode Security Association between RADIUS server and RADIUS client



- ESP encrypted packets in Wireshark

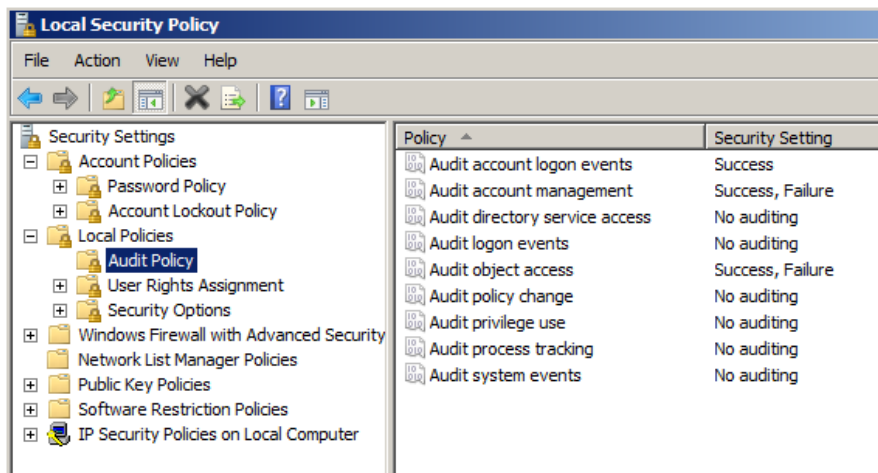


Authentication traffic is now encrypted by IPSec between the RADIUS server and RADIUS client.

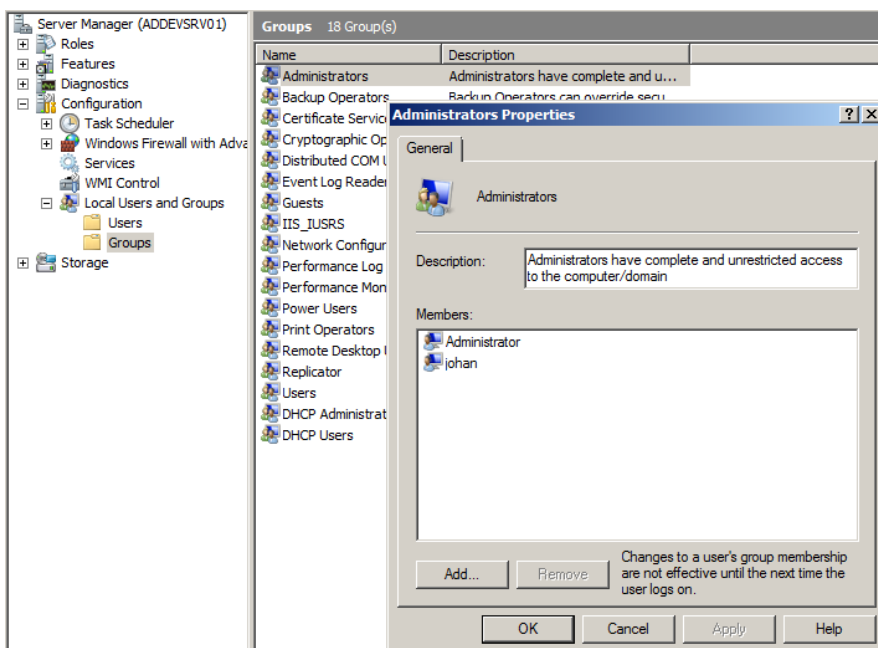
Auditing

To view auditing information on account management (create/delete user account), configure your server via a local group policy to Audit Account Management Events for Success and Failure.

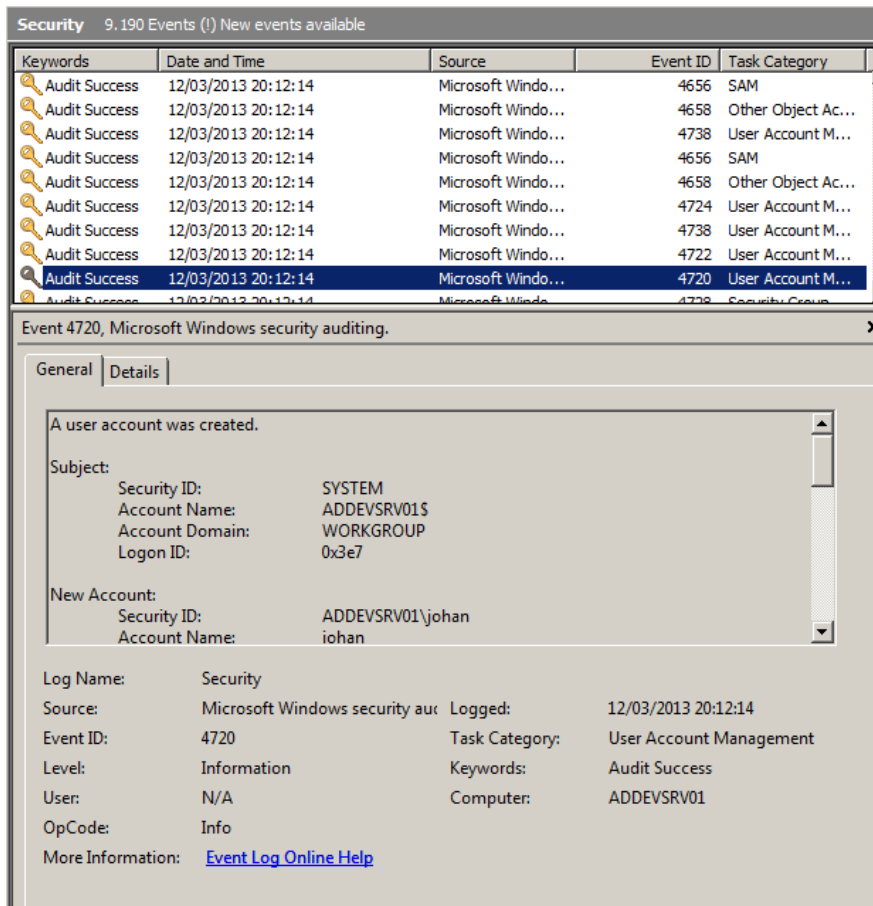
- Open **Local Security Policy** from **Administrative Tools**
- Navigate to **Security Settings | Local Policies | Audit Policy**



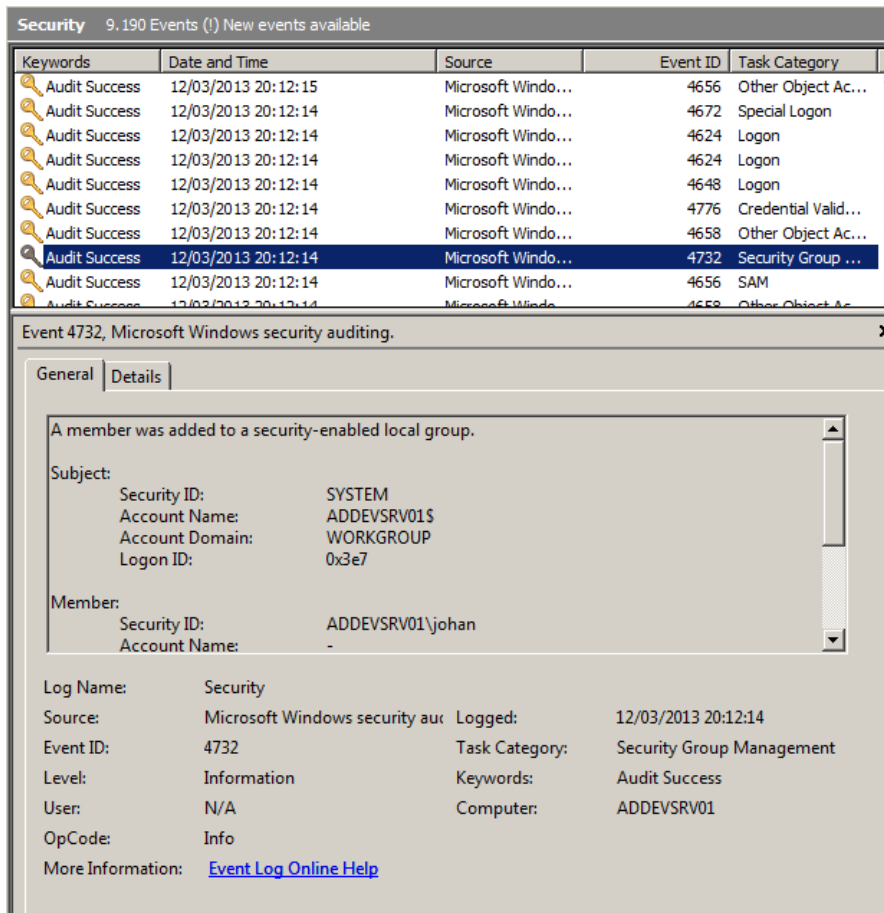
- If your authentication was done via LDAP or RADIUS, the user is added into the local group which you have specified above.



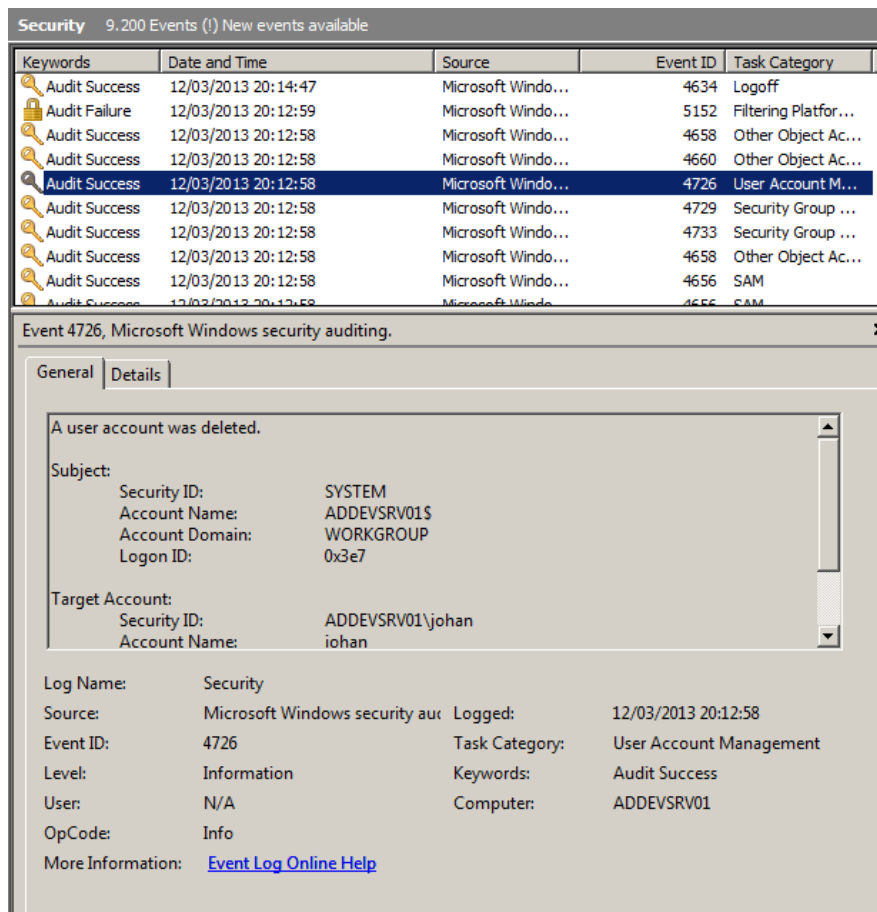
- User account is created on the workgroup server



- User account is added to a local group on the workgroup server



- User account is deleted (when you log off) on the workgroup server



Logging information retrieved from your NPS Server:

- The user has been granted access to the network

Network Policy and Access Services Number of events: 980

Number of events: 980

Level	Date and Time	Source	Event ID	Task Category
Information	12/03/2013 19:55:29	Microsoft Wi...	6278	Network Polic...
Information	12/03/2013 19:55:29	Microsoft Wi...	6272	Network Polic...
Information	12/03/2013 19:55:29	NPS	4400	None
Information	12/03/2013 19:50:50	Microsoft Wi...	6273	Network Polic...
Information	12/03/2013 19:50:40	Microsoft Wi...	6273	Network Polic...

Event 6272, Microsoft Windows security auditing.

General Details

Network Policy Server granted access to a user.

User:

Security ID: ADDEVJohan
Account Name: Johan
Account Domain: ADDEV
Fully Qualified Account Name: addev.local/Access Denied/Users/Johan Loos

Client Machine:

Security ID: NULL SID
Account Name: -
Fully Qualified Account Name: -

Log Name: Security
Source: Microsoft Windows security Logged: 12/03/2013 19:55:29
Event ID: 6272 Task Category: Network Policy Server
Level: Information Keywords: Audit Success
User: N/A Computer: ADDEVDC04.addev.local
OpCode: Info
More Information: [Event Log Online Help](#)

- Authentication is done via the policy we have created above

Network Policy and Access Services Number of events: 980

Number of events: 980

Level	Date and Time	Source	Event ID	Task Category
Information	12/03/2013 19:55:29	Microsoft Wi...	6278	Network Polic...
Information	12/03/2013 19:55:29	Microsoft Wi...	6272	Network Polic...
Information	12/03/2013 19:55:29	NPS	4400	None
Information	12/03/2013 19:50:50	Microsoft Wi...	6273	Network Polic...
Information	12/03/2013 19:50:40	Microsoft Wi...	6273	Network Polic...

Event 6272, Microsoft Windows security auditing.

General Details

Authentication Details:

Connection Request Policy Name: Use Windows authentication for all users
Network Policy Name: Allow Domain Authentication for Workgroup Servers
Authentication Provider: Windows
Authentication Server: ADDEVDC04.addev.local
Authentication Type: PAP
EAP Type: -
Account Session Identifier: -
Logging Results: Accounting information was written to the local log file.

Quarantine Information:

Log Name: Security
Source: Microsoft Windows security Logged: 12/03/2013 19:55:29
Event ID: 6272 Task Category: Network Policy Server
Level: Information Keywords: Audit Success
User: N/A Computer: ADDEVDC04.addev.local
OpCode: Info
More Information: [Event Log Online Help](#)

Appendix A

IP address	Name	Server	Note
10.32.5.3	ADDEVDC01	Domain Controller	Member of Active Directory
10.32.5.15	ADDEVDC04	Network Policy Server	Member of Active Directory
10.32.5.11	ADDEVSRV01		Workgroup

URL: <http://pgina.org/>

Version used: 3.1.7.1 BETA