WatchGuard Certified Training

Fireware XTM
Advanced Active Directory Authentication

Courseware: Fireware XTM and WatchGuard System Manager v11.7

Revised: January 2013
Updated for: Fireware XTM v11.7
Disclaimer

Information in this guide is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of WatchGuard Technologies, Inc.

Copyright and Patent Information

Copyright © 2013 WatchGuard Technologies, Inc. All rights reserved.

WatchGuard, Firebox, Fireware, LiveSecurity, and spamBlocker are either registered trademarks or trademarks of WatchGuard Technologies, Inc. in the United States and other countries. This product is covered by one or more pending patent applications.

All other trademarks and tradenames are the property of their respective owners.

Printed in the United States.
# Table of Contents

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Active Directory Authentication</strong></td>
<td>1</td>
</tr>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>What You Will Learn</td>
<td>1</td>
</tr>
<tr>
<td>Exercises</td>
<td>1</td>
</tr>
<tr>
<td>What Active Directory Authentication Can Do For You</td>
<td>2</td>
</tr>
<tr>
<td>Related Information</td>
<td>2</td>
</tr>
<tr>
<td>What You Should Know</td>
<td>2</td>
</tr>
<tr>
<td>How Authentication Works in Fireware XTM</td>
<td>2</td>
</tr>
<tr>
<td>How Authorization Works in Fireware XTM</td>
<td>5</td>
</tr>
<tr>
<td>Authorization by Clientless Single Sign-On (SSO)</td>
<td>15</td>
</tr>
<tr>
<td><strong>Active Directory Authentication Process Details</strong></td>
<td>15</td>
</tr>
<tr>
<td>Understanding the LDAP Framework of Active Directory</td>
<td>16</td>
</tr>
<tr>
<td>How Fireware XTM Authenticates Users with Active Directory</td>
<td>20</td>
</tr>
<tr>
<td>Detailed Steps in the Authentication Process</td>
<td>20</td>
</tr>
<tr>
<td>Optional Data that Active Directory Can Give Fireware XTM</td>
<td>26</td>
</tr>
<tr>
<td><strong>Before You Begin</strong></td>
<td>29</td>
</tr>
<tr>
<td>Necessary Equipment and Services</td>
<td>29</td>
</tr>
<tr>
<td>Management Computer Configuration</td>
<td>29</td>
</tr>
<tr>
<td>Firewall Configuration</td>
<td>30</td>
</tr>
<tr>
<td>Physically Connect the Devices</td>
<td>30</td>
</tr>
<tr>
<td><strong>Exercise 1: Allow Authenticated Users on the External Network to Manage the XTM Device</strong></td>
<td>31</td>
</tr>
<tr>
<td>When to Use Authentication for Access to the XTM Device</td>
<td>31</td>
</tr>
<tr>
<td>Network Topology</td>
<td>31</td>
</tr>
<tr>
<td>Configure the Active Directory Server</td>
<td>32</td>
</tr>
<tr>
<td>Configure the XTM Device</td>
<td>32</td>
</tr>
<tr>
<td>Demonstrate It: Authenticate to Your Partner’s XTM Device to Manage It</td>
<td>41</td>
</tr>
<tr>
<td><strong>Exercise 2: Use Active Directory to Authenticate Mobile VPN with SSL Clients</strong></td>
<td>43</td>
</tr>
<tr>
<td>When to Use Active Directory for Mobile VPN Authentication</td>
<td>43</td>
</tr>
<tr>
<td>Network Topology</td>
<td>43</td>
</tr>
<tr>
<td>Configure the XTM Device</td>
<td>44</td>
</tr>
<tr>
<td>Download the Mobile VPN with SSL Client Software</td>
<td>52</td>
</tr>
<tr>
<td>Install the SSLVPN Client Software</td>
<td>52</td>
</tr>
<tr>
<td>Make an SSLVPN Connection to Your Partner’s XTM Device</td>
<td>52</td>
</tr>
<tr>
<td><strong>Exercise 3: Use Clientless Single Sign-On to Authorize Domain Users</strong></td>
<td>54</td>
</tr>
<tr>
<td>Active Directory for Clientless SSO</td>
<td>54</td>
</tr>
<tr>
<td>Default Domain Policy</td>
<td>55</td>
</tr>
<tr>
<td>Install the SSO Agent</td>
<td>55</td>
</tr>
<tr>
<td>Configure the XTM Device</td>
<td>58</td>
</tr>
<tr>
<td>Demonstrate Clientless SSO</td>
<td>60</td>
</tr>
<tr>
<td><strong>Frequently Asked Questions</strong></td>
<td>63</td>
</tr>
<tr>
<td><strong>What You Have Learned</strong></td>
<td>64</td>
</tr>
</tbody>
</table>
Active Directory Authentication
Restrict Access with Active Directory Users or Groups

This training is for:

<table>
<thead>
<tr>
<th>Device</th>
<th>WatchGuard XTM Devices with Fireware XTM OS v11.7 and later</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device OS versions</td>
<td>Fireware XTM v11.7 with a Pro Upgrade</td>
</tr>
<tr>
<td>Management Software versions</td>
<td>WatchGuard System Manager v11.7</td>
</tr>
<tr>
<td>Category</td>
<td>Authentication / Active Directory</td>
</tr>
</tbody>
</table>

Introduction

What You Will Learn
Authentication is an effective way to limit access to your network resources. This training course shows you how authentication works, and how to configure your Fireware XTM to use your existing Active Directory users and groups to give your users access network resources.

Exercises
This course demonstrates two examples of Active Directory authentication. Each step-by-step exercise illustrates a use case that might apply in your network. The exercises are:

- Allow AD authenticated users on the external network to manage the XTM device
- Use Active Directory to authenticate Mobile VPN clients
- (Optional) Use Clientless Single Sign-On to authorize domain users

Before you begin the exercises, make sure to read the section “Before You Begin,” on page 29. This section includes a list of the equipment and software you must have for the exercises, and basic information about how to prepare your XTM device and your Active Directory server.

Note
This module includes exercises related to firewall authentication (over port 4100), Mobile VPN, and Clientless Single Sign-On (SSO) in a single domain environment. Clientless SSO on a multi-domain environment is not included in this training.
What Active Directory Authentication Can Do For You

Because of the dynamic nature of the IP addresses of today’s highly mobile workforce, you can no longer rely only on IP addresses to control access to your network resources. If you select an access control method that forces your users to authenticate before they can connect to resources, you can use your firewall policies to have better control over resource access when you don’t know the IP addresses of your users’ IP addresses.

Active Directory authentication provides these benefits:

- Restricts access to network resources by user name or group name
- Enforces user accountability based on user name
- Centralizes maintenance of user accounts

Related Information

For more information about Active Directory and LDAP, see these additional resources:

- *How Active Directory Searches Work* from Microsoft:  
- LDAP RFCs:
  - RFC 1777 defines what is now called version 2 of the Lightweight Directory Access Protocol (or LDAP v2):  
  - The core specifications of LDAP v3 are defined in RFC 2251:  

What You Should Know

When you want to restrict access to resources by user name or group name, consider these two distinct concepts: *Authentication* and *Authorization*.

- **Authentication** proves the identity of the user.  
  The XTM device can authenticate users against your Active Directory server for Firewall Authentication and for Mobile VPN connections.
- **Authorization** grants the user permission to do something.  
  You enable access to networks by adding user names or group names in the source field (the From list) of a policy in Policy Manager.

How Authentication Works in Fireware XTM

The XTM device can authenticate a user with your Active Directory server in three ways: Firewall Authentication, Mobile VPN with IPSec, and Mobile VPN with SSL.

In this training module, we discuss how to use Active Directory to authenticate your users with Firewall Authentication and Mobile VPN with SSL.

You can also use Active Directory to authenticate Mobile VPN with IPSec clients (iOS, the WatchGuard Mobile VPN with IPSec client, and the Shrew Soft VPN client), but we do not discuss these methods in this module. For more information, see the WatchGuard System Manager Help.
**Firewall Authentication**

A user with an Active Directory account must establish an HTTPS connection to the XTM device over TCP port 4100. To do this, the user opens a web browser and types the DNS name or IP address of the XTM device interface that protects network resources in the address list.

For example:

```
https://my.xtm_device.net:4100
https://10.0.1.1:4100
```

After the user is authenticated, the XTM device knows the user name and the groups of which the user is a member. Traffic from that user is allowed through a firewall policy if the policy’s **From** list has a user name or group name that matches the user’s identity or group membership.

The XTM device configuration must include a firewall policy that allows traffic to pass to the XTM device over port 4100. Policy Manager automatically adds the WatchGuard Authentication policy, which allows port 4100 connections to the XTM device from only trusted and optional networks. If you want users to authenticate from external networks, you must edit this policy (or add another policy) to also allow connections to the XTM device over port 4100 from external networks. For more information, see the subsequent exercises in this module.

To service the connection requests, a web server in the XTM device listens on TCP port 4100. To authenticate, users type a user name and a password, and select a domain.

![Login](image)

*Figure 1:* The Firewall Authentication web page

If the authentication is successful, the success message appears.

*Figure 2:* Firewall Authentication success message

If authentication fails, a failure message appears. The content of the failure message depends on where in the authentication process the failure occurred.
Mobile VPN with SSL Authentication

To use Mobile VPN with SSL to authenticate:

1. Launch the Mobile VPN with SSL client.

![Figure 3: Mobile VPN with SSL connection dialog box](image)

2. Type the IP address of the XTM device, your user name, and password.

3. Click **Connect**.

   When the connection is successful, a connection message appears, and the WatchGuard SSL icon in the system tray changes from black to green.

![Figure 4: Mobile VPN with SSL successful connection](image)

Information the XTM Device Gets From the Authentication Process

When a user authenticates to an XTM device, the device collects information to match traffic flows to users. To track the authenticated user's session, the XTM device keeps these items in memory:

- The type of authentication server that authenticated the user.
  
  *For this training, we use Active Directory.*

- The user name the user typed to authenticate.

- The IP address for the XTM device that is the source of the authentication (the user’s IP address).

- The groups to which the user belongs.
  
  *The XTM device gets this information from a query it sends to the Active Directory server.*

  *Group information must come from the authentication server. If group information is not in the server’s authentication response message, you can add a firewall policy to restrict the user’s access only by user name.*

- The session timeout and idle timeout values for this user or group.

- The virtual IP address assigned to the Mobile VPN user. (This applies only to Mobile VPN with IPSec connections and Mobile VPN with SSL connections.)
How Authorization Works in Fireware XTM

To authorize users to connect to resources, you add their user names, or the names of their groups, to a policy in Policy Manager. Users are authorized to pass traffic through a policy if their user names appear in the policy’s From list, or if they are members of a group that appears in the policy’s From list.

To make sure that your policies do not allow traffic you did not intend, do not configure your policies with aliases that include a wide range of addresses. Such aliases can include Any, Any-Trusted, Any-Optional, Any-External, or an alias that is the name of an XTM device interface. Before you use one of these aliases in a policy, carefully consider the purpose of the policy. These aliases can allow access to users that do not authenticate.

Make a List of Authorized Users and Groups

Policy Manager keeps a list of user and group objects so that you can easily get access to them when you manage your firewall policies. Before you can add an Active Directory user or group to a policy, you must add it to the Authorized Users and Groups list in Policy Manager.

To add users or groups to this list:


![Figure 5: Open the Authorized Users and Groups dialog box](image)
The **Authorized Users and Groups** dialog box appears.

![Authorized Users and Groups dialog box](image)

**Figure 6:** Authorized Users and Groups dialog box

2. Click **Add**.

   The **Define New Authorized User or Group** dialog box appears.

![Define New Authorized User or Group dialog box](image)

**Figure 7:** Define a new user or group

3. Type the **Name** for this user, or the name of an Active Directory group.

4. (Optional) Type a **Description** of the user or group.

5. Select **Group** or **User**.

6. From the **Auth Server** drop-down list, select **Active Directory**.

7. Select the **Enable login limits for each user or group** check box.

8. To limit the number of times the user, or users in the group, can log in with the same credentials to no more than three concurrent user sessions, select **Limit concurrent users sessions to** and type or select 3 in the adjacent text box.

9. From the **When the limit is reached** drop-down list, select an option:
   - Reject subsequent login attempts
   - Allow subsequent login attempts and log off the first session.
10. Click **OK**.
   The new user or group appears in the **Authorized Users and Groups** dialog box.

![Figure 8: New Active Directory user account in Authorized Users and Groups](image)

**Use Firewall Policies to Restrict Access By User or Group**

To limit access to firewall policies, you add a policy on the **Firewall** tab of Policy Manager. To get access, users authenticate to the firewall, which is also known as **Firewall Authentication**.

![Figure 9: The Policy Manager Firewall tab](image)
This policy allows a user and a group.

![Edit Policy Properties](image)

Figure 10: A policy that allows access only for a user and a group

To limit access to a Firewall policy by user or group:

1. On the **Firewall** tab, double-click a policy to edit it.
2. In the **From** list, select the **Any-Trusted** and **Any-Optional** aliases, and any other addresses or aliases that could allow access to a user who has not authenticated, and click **Remove**.
3. In the **From** section, click **Add**.

![Add Address](image)

Figure 11: Add to the **From** list of a policy

The **Add Address** dialog box appears.
4. Click **Add User**.

![Add Address dialog box](image)

**Figure 12:** Add Address dialog box

The **Add Authorized Users or Groups** dialog box appears with the users and groups you added to the **Authorized Users and Groups** list.

![Add Authorized Users or Groups dialog box](image)

**Figure 13:** Select a user or group to add to the policy

5. From the left **Type** drop-down list, select **Firewall**.
6. From the right **Type** drop-down list, select **Group** to see the available groups, or select **User** to see the available users.

If the user or group you want to add does not appear in this list, click **Add** to add it to the list.

---

If you use PPTP to authenticate your mobile users, select **PPTP** from the **Type** drop-down list.

You cannot use Active Directory to authenticate PPTP users.
7. Select the user or group you want to add to the policy and click Select. The user or group appears in the **Selected Members and Addresses** list.

![Image of Selected Members and Addresses]

*Figure 14: The user or group appears in **Selected Members and Addresses** list*

8. Click **OK**. The user or group appears in the **From** list.

![Image of Edit Policy Properties]

*Figure 15: This policy allows traffic from only authenticated members of the group*
Custom Addresses and Tunnel Addresses

To restrict whether traffic is allowed from an authenticated user, you can add a custom address or a tunnel address. These address types let you specify the user or group, and set two other conditions that traffic must meet in order to match the address.

Note

Custom addresses and tunnel addresses apply only to firewall policies. They do not apply to Mobile VPN with IPSec policies.

With a custom address, you can specify these conditions for traffic:

• A user or a group member
• An IP address. This can be a host IP address, a network IP address, or an IP address range.
• The interface where the traffic passes through the XTM device.
  - If the custom address is in the From list, this is the interface where the traffic enters the XTM device.
  - If the custom address is in the To list, this is the interface where the traffic exits the XTM device.

With a tunnel address, you can specify these conditions for traffic:

• User or member of a group.
• IP address. This can be a host IP address, a network IP address, or an IP address range.
• Branch Office VPN tunnel that the traffic goes through.

If you use one of these address types in a firewall policy, traffic must match all three conditions of either address type.

For example, suppose you want to grant FTP access to an Active Directory user. You want users to authenticate first, but you do not want users to get access to FTP sites when they are authenticated from the optional or external network, only from the trusted network. Also, you want the user to have access only if the user’s traffic comes from a small segment of the trusted network, the 10.0.1.64/28 subnet.

To do this, add a custom address:

1. Double-click the policy to edit it. The Edit Policy Properties dialog box appears, with the Policy tab selected.
2. In the From list, select the Any-Trusted and Any-Optional aliases, along with any other addresses or aliases that could match this user’s IP address, and click Remove.
3. In the From section, click Add. The Add Address dialog box appears.
You cannot add users or groups to the Authorized Users and Groups list from the Add Member dialog box. You must add objects to the Authorized Users and Groups list before you can use them in a custom address or a tunnel address.

You cannot use a Mobile VPN Group name in a custom address or tunnel address.

The 10.0.1.64/28 subnet includes host addresses from 10.0.1.65 through 10.0.1.78. You could use an address range for this instead of a network IP address.

4. Click Add Other. The Add Member dialog box appears.

![Add Member dialog box](image1)

Figure 16: The Add Member dialog box

5. From the Choose Type drop-down list, select Custom Address.
6. From the User/Group drop-down list, select a user or group object you already added to the Authorized Users and Groups list.
7. From the Address drop-down list, select Specify. A new text box appears.
8. In the text box that appears, type the IP address 10.0.1.64/26.
9. From the Interface drop-down list, select Trusted.
10. Click OK.

The custom address appears in the Selected Members and Addresses list.

![Add Address dialog box](image2)

Figure 17: Custom address in the Add Address dialog box
11. To see the details of this address, place your cursor over it. A tool tip appears.

*Figure 18:* The details of the custom address appear in the tool tip
Use Mobile VPN with SSL Policies to Restrict Access by User or Group

For Mobile VPN with SSL users, you control access with policies on the Firewall tab of Policy Manager. When you create a Mobile VPN with SSL group, Policy Manager automatically adds policies that allow access to the resources you specify, over any port or protocol. These Mobile VPN with SSL policies allow traffic only from users that are members of the SSLVPN-Users group.

Figure 19: The Firewall tab with the automatically generated Mobile VPN with SSL policies

At the top of the Edit Policy Properties dialog box, in the From list, you can see the name of the Mobile VPN with SSL group from which the policy allows traffic.

Figure 20: The Edit Policy Properties dialog box for the Allow SSLVPN-Users policy that enables users in the SSLVPN-Users group to get network access through this policy

The To list includes the host IP addresses or network IP addresses that the Mobile VPN with SSL user can use to connect to the VPN.
Authorization by Clientless Single Sign-On (SSO)

Another method of authorization in a domain-controlled environment is to use the same credentials used to log in to the user's computer. For this method, users do not need to authenticate manually to the firewall to submit their user credentials. This method is called Single Sign-On (SSO).

Clientless SSO Components

- **XTM device** — Where the authorization takes place
- **Active Directory** — Where user credentials such as the user name and groups are stored
- **SSO Agent** — Queries the Event Log Monitor on the domain controller
- **Event Log Monitor** — Polls the logon and logoff events from the domain client computer and retrieves group membership information from the domain controller

Traffic Driven In Passive Mode

When a client computer on your domain connects to the Internet with a web browser, the XTM device captures the traffic and notes the source IP address used for that session. If the device does not find an existing authenticated session for the IP address, it contacts the SSO Agent for the user credentials on the client computer. The SSO Agent forwards the request to the Event Log Monitor, which contacts the domain client IP address for the logon event details. It tries to get the user name and domain information that the user logged on with, which should be the same user credentials that are stored in your Active Directory server. The Event Log Monitor also gets the name of each group the user belongs to from the domain controller. Once it has collected all the available information, the Event Log Monitor sends it back to the SSO Agent. The SSO Agent then sends the user credentials to the XTM device. The XTM checks the user information to determine if the traffic can be allowed, or if it must be denied, based on the configured policy rules.

Active Directory Authentication Process Details

Terms and Definitions

The items in this list appear throughout the remainder of this training course.

**Active Directory**
Microsoft's directory service. It stores information about objects on a network and makes this information available to users through an LDAP interface.

**Attribute**
A characteristic of an object in the directory. The schema defines whether the attribute can have only one value (single-valued) or multiple values (multi-valued).

**Base DN**
The start of the directory tree. The Base DN holds all objects in the domain.

**Container**
An object in the directory that can contain other objects. This is similar to a folder on your computer that can contain other folders or files.

**Directory**
A store of information. This is similar to an address book, which stores names and phone numbers.

**Directory Object**
An entry in the directory. An object has a list of attributes that describes it.

**Directory Server**
A computer, such as a domain controller, that provides access to an LDAP-based directory.
**Directory Service**
A service that runs on a directory server to give access to the directory.

**Directory Tree**
The hierarchical organization of information that starts from a single point (the root, or Base DN) and branches out. It is analogous to a tree and similar in structure to a computer file system. The structure of the tree is determined by the schema.

**Distinguished Name (DN)**
The globally-unique name of an object in the directory. It defines the object’s location in the directory tree.
The DN starts with the friendly name for the object, followed by the name of the container that holds the object, and continues with the name of the container that holds that container, and so on, all the way to the Base DN.

**Firewall Authentication**
One method of authentication. Users make an HTTPS connection with a web browser to the XTM device over port 4100, and supply their user names and passwords.

**LDAP**
LDAP (Lightweight Directory Access Protocol) is a protocol used to get access to an information directory.

**Leaf**
An object in the directory that cannot contain other objects. Similar to a file on your computer, a leaf represents the end of the branch for that object in the directory tree. User objects and group objects are leaf objects.

**Mobile VPN Authentication**
An authentication method that uses the WatchGuard Mobile VPN with IPSec software. For this method, users type their credentials to log in.

**Schema**
The set of rules that controls all aspects of what can be stored in the directory.

**User Principal Name (UPN)**
A naming convention used by Active Directory to identify a user and the domain to which the user belongs. The UPN is almost always identical to the user’s email address: it includes the user’s logon name, followed by @ and the name of the domain. For example, the UPN for the user student20 in the training.net domain is student20@training.net.

**Understanding the LDAP Framework of Active Directory**

**What Active Directory Has In Common with LDAP**
LDAP is a protocol. It defines methods to access information in a directory. A directory is simply a store of information, like an address book that stores names and phone numbers. A directory server runs a directory service to provide the access for clients. In your Active Directory domain, a domain controller runs the directory service.

Active Directory uses an LDAP-compliant directory for storing information about every object and resource in your domain: users, computers, file shares, applications, organizational units, groups, security policies, and so on. Because Active Directory implements LDAP, you can use standard LDAP operations to get information about the directory’s objects.
Structure of the LDAP Directory

Information in an LDAP directory is stored in a tree-like hierarchy. It begins with one container that holds everything, and branches out in a way that is similar to how files and folders are organized on your computer. The start of the tree, the container that holds everything, is called the Base DN. It represents your Active Directory domain.

The Base DN can hold container objects, leaf objects, or both. Container objects can hold other objects including other container objects, leaf objects, or both. You can have many containers within containers. Leaf objects are different from container objects in one major respect: leaf objects cannot contain other objects. Leaf objects can exist anywhere in the directory tree. The diagram in Figure 21 shows a simple representation of a directory tree.

Do not confuse a container object with an Active Directory group. A group in Active Directory is a leaf object; it cannot hold other objects. Members of an Active Directory group are not contained within the group, they are only members of the group.

Microsoft provides an interface into the directory with a tool called ADSI Edit. This GUI tool is a Microsoft Management Console (MMC) snap-in that acts as a low-level editor for Active Directory and illustrates the tree structure of the directory. It is included when you install Windows Server 2000 or 2003 Support Tools from the product CD. The subsequent image of the ADSI Edit tool shows the training.net domain with two user objects (circled).

Figure 21: Simple view of LDAP structure

Figure 22: ADSI Edit tool for the training.net domain with two user objects in the Sales OU
Objects and Attributes

Every object in an LDAP directory is described by a list of attributes. Some attributes, such as sAMAccountName, must be assigned a value, while others can be null. These requirements are defined in the schema. An attribute can be either single-valued (there can be only one value assigned to the attribute) or multi-valued (the attribute can have more than one value).

Figure 23 shows a sample list of some of the attributes for the student20 user object:

```
<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>cn</td>
<td>student20</td>
</tr>
<tr>
<td>sn</td>
<td>20</td>
</tr>
<tr>
<td>givenName</td>
<td>student</td>
</tr>
<tr>
<td>distinguishedName</td>
<td></td>
</tr>
<tr>
<td>cn</td>
<td>student20,OU=Sales,OU=Accounts,DC=training,DC=net</td>
</tr>
<tr>
<td>displayName</td>
<td>student20</td>
</tr>
<tr>
<td>memberOf</td>
<td>CN=Some Universal Group,DC=training,DC=net</td>
</tr>
<tr>
<td>memberOf</td>
<td>CN=Some Local Group, CN=Users, DC=training, DC=net</td>
</tr>
<tr>
<td>memberOf</td>
<td>CN=Firebox Restricted,OU=Accounts,DC=training,DC=net</td>
</tr>
<tr>
<td>name</td>
<td>student20</td>
</tr>
<tr>
<td>objectGUID</td>
<td>bGh5jCbsmUS9a5PDKjw1NQ==</td>
</tr>
<tr>
<td>sAMAccountName</td>
<td>student20</td>
</tr>
</tbody>
</table>
```

When you add a user to a group, Active Directory automatically adds another value to the user object’s memberOf attribute to indicate the user’s membership in the group. Because the Fireware XTM LDAP query finds the user object and all of its attributes, Fireware XTM can tell what groups the user belongs to by reading the user object’s memberOf attribute.

Identifying Objects in the Directory

**Base DN**

The name of the Base DN uses the DNS components of your domain name, called Domain Components (DC). Active Directory domains must have at least two DNS domain components: a friendly name such as mycompany, and a top-level domain suffix such as .net or .com. In our examples, we use the domain name training.net. The DNS domain components of this name are training and net. (The domain name can also have a local component, as in classroom.training.net.)

If the training.net domain had a child domain called “classroom”, the DN would be: DC=classroom, DC=training, DC=net

To construct the Base DN name, you write DC=<domain component>,, DC=<domain component> with one such entry for each domain component. You start with the first part of your domain name and end with the top-level domain suffix. Separate each part with a comma and no space. There are no dots between each part of the name or at the end. Thus, the name of the Base DN for the training.net domain is: DC=training, DC=net
Object's Friendly Name
Every object in the directory has a simple name, or friendly name. It starts with an abbreviation for the type of attribute used for the friendly name, followed by =, followed by the object’s name. The objects you most often work with use well-defined attributes for the friendly name:

- For a user object or group object, the friendly name starts with CN=
- For an organizational unit, the friendly name starts with OU=

Here are some examples:

- A user object's friendly name is usually the user’s first and last name, and possibly a middle initial. For example, CN=student30 or CN=student20.
- A group object’s friendly name is the name of the group. For example, CN=XTM device Restricted or CN=MUVPN Group.
- An organizational unit’s friendly name is the name you give the OU. For example, OU=Sales or OU=Accounting.

The technical term for the object’s friendly name is the Relative Distinguished Name or RDN. An objects' RDN must be unique within the branch of the tree where the object is; no other object in that branch, all the way to the root, can use that RDN. This ensures that the DN for any object is globally unique even if two objects have the same RDN. The DNS for objects with identical RDNs remain globally unique because an object’s Distinguished Name specifies not only the object’s RDN, but also its location in the directory.

Object's Distinguished Name
Every object in the directory is uniquely identified by its Distinguished Name (DN). The DN for an object starts with its friendly name, followed by a list of each container above the object. Each part of the DN is separated by only a comma. Thus, the DN shows how the object relates to its parent objects, all the way to the Base DN.

The friendly name for the student20 object in Figure 23 is CN=student20, so the DN is: CN=student20,OU=Sales,OU=Accounts,DC=training,DC=net

The DN for the OU called Accounts, just within the root of the tree, is: OU=Accounts,DC=training,DC=net

The DN for the Administrators group in the Builtin container is: CN=Administrators,CN=Builtin,DC=training,DC=net

Active Directory Groups and LDAP
Some people confuse a group with a container. This is natural, because we often think of groups containing things. However it is important to keep these two concepts separate. The confusion can be an obstacle to understanding how groups fit into the LDAP structure of Active Directory.

A user’s group membership in Active Directory is not determined by the container the user is in. Instead, group membership is based on the values of an object’s group membership attribute, `memberOf`.

An administrator can use any attribute to define group membership, even a custom attribute added by extending the schema. The value of the attribute is what the XTM device considers to be the group the user belongs to. Use the attribute's name in the `Group String` text box when you configure Active Directory authentication in Policy Manager. Use the attribute's value as the group name in XTM device policies.

An Active Directory group can have members, but membership in a group is not the same thing as being contained in a parent object of the directory tree. A user object can be contained only in an Organizational Unit or other container. Do not confuse membership in a group with the container that holds the user.

Remember that Fireware XTM tells what groups a user is a member of by looking at the user object’s attributes, not by where in the directory the user is located.
How Fireware XTM Authenticates Users with Active Directory

To successfully authenticate a user, the XTM device must do these things:

- **Bind to the LDAP database**
  Fireware XTM does this using the LDAP *bind* operation. The XTM device sends credentials to the directory server to establish permissions to search the directory. These can be the credentials of the user trying to authenticate, or credentials that you specify.

- **Search for the user object to verify it exists in the directory**
  Fireware XTM does this using the LDAP *search* operation. For a search, the only permission required is read access. Active Directory domains grant this permission to all domain user accounts by default.

- **Get the user's information from the search results**
  The search operation finds the user object in the directory and gets all the object's attributes. The object's attributes tell Fireware XTM the user's distinguished name, the groups of which the user is a member, and possibly other optional information.

- **Authenticate the user**
  Fireware XTM completes one final bind operation with the user's credentials to verify the user's password.

**Detailed Steps in the Authentication Process**

The events that make up the Active Directory authentication process include:

**Step 1 — User Attempts to Authenticate**

This can be an attempt to use Firewall Authentication or an attempt to make a Mobile VPN connection. The following steps are the same for either type of authentication.

When the XTM device gets the user credentials, it starts a TCP session with the directory server to start the process.

**Step 2 — Fireware XTM Attempts to Bind to Active Directory**

This first bind request tells the directory server which account Fireware XTM wants to use for the Search operation. For this bind request, Fireware XTM uses one of two different accounts:

- The credentials of the user attempting to authenticate.
- The credentials of an account that you specify.
The account the XTM device uses for this bind is determined by whether you specify a Searching User.

The simplest way to complete the selected area in Figure 24 is as shown:

- **DN of Searching User** and **Password of Searching User** are empty
- **Login Attribute** is set to the default value `sAMAccountName`

When you configure the highlighted area as suggested, Fireware XTM constructs the User Principal Name (UPN) from the user name that the user typed into the authentication dialog box, the @ character, and the domain components in DNS form. The XTM device sends this as identification for this first bind request.

When you use these default settings, the user attempting to authenticate enters the Windows logon name (without domain information) for the **Username**. Thus, if a user with logon name `student20` attempts to authenticate, the user types `student20` in the **Username** text box when prompted. The XTM device sends `student20@training.net` as identification for this bind. (In our examples, the domain components are DC=training,DC=net.)

*Figure 24:* The items that determine the credentials used for the first bind

It is not necessary to provide a Searching User if you keep the default value of `sAMAccountName` for the **Login Attribute**. However, you must specify a Searching User if you use any other value for the **Login Attribute**. The **Login Attribute** is used as a search filter to find the user in the directory.
Active Directory does not require that the User logon name (pre-Windows 2000) value match the User logon name at the top of the Account tab in Figure 25. In most cases the network administrator keeps them the same, but you should make sure you do not confuse the two. Active Directory uses only the User logon name (pre-Windows 2000) value for the sAMAccountName attribute. It uses the User logon name value only for the userPrincipalName attribute.

Figure 25 shows the student20 user account in Active Directory Users and Computers. The circled area shows what Active Directory uses for the sAMAccountName attribute.

If this first bind request in Step 2 fails, this error message appears in the browser:

Authentication Failed: 'LDAP binding failed, credentials are not correct, please try again'

How to Use a Different Login Attribute

If you want the user to type something else in the authentication dialog box instead of the standard Windows logon name, select (or manually type) a different value in the Login Attribute drop-down list in Figure 24.

For example, if you want users to type their Common Name in the Username text box, select cn for the Login Attribute in Figure 24. In this case student20 types student20 or student20 in the Username text box when he authenticates (Windows user names are not case-sensitive).

If you select an attribute that is not sAMAccountName, you must specify a Searching User in Figure 24. This is because Fireware XTM cannot construct the user's UPN if the user types something other than the simple logon name in the Username text box.

For an account that has permission to read the directory, type the full Distinguished Name in the DN of Searching User text box and type the account password in the Password of Searching User text box.
Step 3 — Fireware XTM Searches the Directory for the Login Attribute

When the bind is successful, Fireware XTM sends a search request. An LDAP search request can include many different parameters and filters. The Fireware XTM search request includes these parameters and search filter:

- **Search Base**
  A search request must indicate where in the database hierarchy the directory service should start the search.

  The *Search Base* you specify indicates where in this container (the Search Base) Active Directory begins the search. The search will include the container you specify, and possibly the subcontainers, but not the parent container of this container.

- **Scope**
  The scope of the search indicates whether the directory service searches only in the Search Base but not inside any containers in the Search Base, only one container within this container (one level lower in the search base), or in all containers inside other containers (in all containers to the end of the tree).

  Fireware XTM uses the *scope: subtree* parameter to specify that Active Directory searches in the selected Search Base container, and every container and subcontainer in it, to the end of this branch of the directory tree.

- **Attributes Only**
  This parameter specifies whether the directory server should return only the names of attributes tied to the object, or if it should send the attribute names and the value of each attribute. The search parameter takes a boolean value of *true* or *false*.

  Fireware XTM uses a value of *false* for the parameter to specify that Active Directory returns all the attributes for the object, and the value of each attribute.

- **Search Filter**
  The search filter specifies that the directory server returns only objects that match certain conditions. If a filter is not specified, the search returns every object and attribute in the database.

  Fireware XTM uses an equality match filter to specify that the server:
  
  - Search only for objects that have the specified attribute (this is the Login Attribute value in Figure 24 on page 21).
  
  - Return an object as a match only if the value for that attribute matches the Username that was specified when the user authenticated.

  For example, if you use the default settings in the Active Directory setup area of Policy Manager (Figure 24), and student20 tries to authenticate, the filter reads: *sAMAccountName=student20*

  For the search result, the server looks only for an object with the *sAMAccountName* attribute AND the *student20* attribute value.
Step 4 — The Server Sends the Search Result to the XTM Device

The server searches its database using the parameters and filter described above. If no such object exists with an attribute that matches the filter, Active Directory still returns a search result, but the result is <null>, meaning that the search did not find any matches. The authentication fails if this happens because the server cannot find the user.

If the server finds an object that matches the filter, it sends Fireware XTM all the attributes and their values for that object.

If the search result is null, this error appears in the browser for the user attempting Firewall Authentication:

   Authentication Failed: 'Specified username or password is not correct, please try again'

Step 5 — Fireware XTM Extracts the Information It Needs From the Search Result

Fireware XTM reads all of the attribute/value pairs for the user object and searches for the DN (distinguishedName) attribute. Fireware XTM then searches again to find the groups of which the user is a member.

If you specify additional attributes for the Optional Settings in the Active Directory setup in Policy Manager, Fireware XTM also extracts the values for those attributes.

Step 6 — Fireware XTM Unbinds and Binds Again to the Database

To run a new search, the XTM device unbinds and completes a new bind operation. The XTM device uses the full distinguished name of the user attempting to authenticate for this new bind and all subsequent bind operations.

Step 7 — Fireware XTM Searches the tokenGroups Attribute For the User Object

Now, Fireware XTM searches to find a special attribute called tokenGroups. This is a calculated attribute, so it does not appear in the list of attributes that Active Directory returned in the previous search.
Step 8 — The Server Sends the Search Result to the XTM Device
The tokenGroups attribute is a multi-valued attribute. The attribute’s values represent the SIDs (security identifiers) for each group of which the user is a member.

The values for this attribute are in a binary format that does not directly represent group names. However, Fireware XTM can convert the binary values to values that it can use in a subsequent search.

Step 9 — Fireware XTM Calculates SID Values
Based on well-known algorithms, the XTM device calculates the SIDs associated with each value of the tokenGroups attribute. After it determines which SIDs to find, it does a new search against the Active Directory LDAP database.

Step 10 — Fireware XTM Completes a Final Search to Find the Groups
This last search asks the Active Directory server to find the group object associated with each of the SIDs. The search looks for any object in Active Directory that has an attributed called objectSid, where the attribute’s value matches one of the SIDs the XTM device obtained from the calculation it did in the previous step.

The search asks Active Directory to tell the XTM device the Common Name of each object it finds from this search.

Step 11 — Active Directory Sends the Search Result
The Common Names for all groups that the user is a member of appear in the search result.

Step 12 — Fireware XTM Attempts a Bind with the User’s Distinguished Name
Finally, the XTM device can authenticate the user. To verify that the user is who he or she claims to be, Fireware XTM sends a bind request with the user’s credentials. It uses the Distinguished Name it got from the previous step for the bind name, and it sends the password that the user typed into the authentication dialog box. If this succeeds, the user is authenticated.

If the password the user typed for Firewall Authentication is incorrect, the user sees this error:

Authentication Failed: 'Specified username or password is not correct, please try again'

For all Mobile VPN with IPSec authentication failures, the remote client sees this in the client-side Log Viewer:

My Connections\50.50.50.1-10.0.1.0 - User Authentication failed
Optional Data that Active Directory Can Give Fireware XTM

Fireware XTM can get additional information from Active Directory when it reads the list of attributes in
the server’s search response. This lets you use Active Directory to assign extra parameters to the
authenticated user’s session, such as timeouts and Mobile VPN address assignments. Because the data
comes from LDAP attributes tied to individual user objects, you can set these parameters for each
individual user instead of being limited to global settings in Policy Manager.

However, Microsoft does not provide ready-made attributes you can use for these items, and you
cannot assign values to these attributes with Active Directory Users and Computers.

To use these optional settings, you must:

• Extend the Active Directory schema to add new attributes for these items.
• Make the new attributes available to the user object class.
• Give values to the attributes for the user objects that should use them.

Before you extend your Active Directory schema, you should thoroughly test and plan. Additions to the
schema are generally permanent and cannot be undone. To find resources to help you plan, test, and
implement changes to the schema, go to the Microsoft web site.

Microsoft provides two main methods to extend the schema. Both of these tools enable you to add
attributes to the schema and make them available to an object class:

• The Active Directory Schema MMC snap-in
  This is a GUI (graphical user interface) you can add as a snap-in to the Microsoft Management
  Console. It enables you to access and edit the schema.

• The ldifde (LDIF Data Exchange) command-line tool
  This is a scriptable command-line interface to import or export LDIF files. LDIF is the LDAP Data
  Interchange Format. It specifies the format used to represent LDAP entries in a text file, to import
  and export directory data between directory servers.

After you add attributes to the schema, you must give them values. You cannot do this with Active
Directory Users and Computers. Microsoft provides several different tools to assign values to the new
attributes. Two commonly used tools are:

• The ldifde tool
  Use this to import an LDIF file that specifies a value for the new attributes of each user object that
  should use them.

• The ADSI Edit snap-in to Microsoft Management Console
  Use this tool to edit raw LDAP attributes. It enables you to access individual directory objects and
  edit the value of each object attribute.
Optional Attributes

To specify additional attributes for Fireware XTM to find in the Active Directory search response, in the Add Active Directory Domain dialog box click Optional Settings. (See Figure 24.) The Active Directory Server Optional Settings dialog box appears.

![Active Directory Server Optional Settings](image)

Figure 26: Optional settings for Active Directory authentication

You can type the name of an LDAP attribute in each text box in Figure 26. Fireware XTM searches for these attributes in the list of attributes it gets from the search result, and uses the value of the attributes as follows:

- **IP Attribute String**
  
  Type the name of the attribute Fireware XTM should use to assign the Mobile VPN client a virtual IP address. This should be a single-valued attribute. The value of the attribute should be a normal dotted-decimal IP address. The IP address must be within the pool of virtual IP addresses you specify when you create the Mobile VPN group.

  This applies only to Mobile VPN clients.

  If the XTM device does not find the IP attribute in the search response, or if you do not specify an attribute in Policy Manager, it assigns the Mobile VPN client a virtual IP address from the virtual IP address pool you create when you make the Mobile VPN Group.

- **Netmask Attribute String**
  
  Type the name of the attribute Fireware XTM should use to assign a subnet mask to the Mobile VPN client's virtual IP address. This should be a single-valued attribute. The value of the attribute should be a normal dotted-decimal subnet mask.

  This applies only to Mobile VPN clients.

  The Mobile VPN software automatically assigns a netmask if the XTM device does not see the netmask attribute in the search response, or if you do not specify one in Policy Manager.

- **DNS Attribute String**
  
  Type the name of the attribute Fireware XTM should use to assign the Mobile VPN client one or more DNS addresses for the duration of the Mobile VPN session. This can be a multi-valued attribute. Each value for the attribute should be a normal dotted-decimal IP address.

  This applies only to Mobile VPN clients.

  If the XTM device does not see the DNS attribute in the search response, or if you do not specify an attribute in Policy Manager, it uses the DNS addresses you specify in Policy Manager in the Network Configuration dialog box on the WINS/DNS tab.
• **WINS Attribute String**
Type the name of the attribute Fireware XTM should use to assign the Mobile VPN client one or more WINS addresses for the duration of the Mobile VPN session. This can be a multi-valued attribute. Each value for the attribute should be a normal dotted-decimal IP address.

This applies only to Mobile VPN clients.

If the XTM device does not see the WINS attribute in the search response or if you do not specify an attribute in Policy Manager, it uses the WINS addresses you specify in Policy Manager in the **Network Configuration** dialog box on the **WINS/DNS** tab.

• **Lease Time Attribute String**
Type the name of the attribute Fireware XTM should use to control the absolute amount of time a user can stay authenticated (session timeout). After this amount of time, Fireware XTM removes the user from the list of authenticated users. This should be a single-valued attribute. Fireware XTM interprets the value of the attribute as a decimal number of seconds. It interprets zero as *never time out*.

This can apply to Mobile VPN clients and to clients that use Firewall Authentication.

- For Mobile VPN clients, when the timeout is reached, Fireware XTM sends an *SA Delete* message to tell the client to delete its IKE and IPSec security associations.
- For Firewall Authenticated users, this message appears on the web authentication page when the session timeout is reached:

  **Authentication Failed:** ‘Session timed out by session limit’

If the XTM device does not find session timeout attributes in the search response, or if you do not specify session timeout attributes for session timeout in Policy Manager, it uses these values:

- For Mobile VPN clients, select **VPN > Mobile VPN > IPSec**, select a Mobile VPN group to edit, and set the session timeout values on the **General** tab.
- For Firewall Authentication, select **Setup > Global Settings** and set the session timeouts.

• **Idle Timeout Attribute String**
Type the name of the attribute Fireware XTM should use to control the amount of time a user can stay authenticated, when traffic does not pass from the user to the XTM device. If traffic does not pass to the XTM device for the specified amount of time, Fireware XTM removes the user from the list of authenticated users. This should be a single-valued attribute. Fireware XTM interprets the value of the attribute as a decimal number of seconds. It interprets zero as *never time out*.

This applies to Mobile VPN clients and to clients that use Firewall Authentication.

- For Mobile VPN clients, when the timeout is reached Fireware XTM sends an *SA Delete* message to tell the client to delete IKE and IPSec security associations.
- For Firewall Authenticated users, this message appears on the web authentication page when the idle timeout is reached:

  **Authentication Failed:** ‘Session timed out by idle limit’

If the XTM device does not find idle timeout attributes in the search response, or if you do not specify attributes for idle timeout in Policy Manager, it uses these values:

- For Mobile VPN clients, select **VPN > Mobile VPN > IPSec**, select a Mobile VPN group to edit, and set the idle timeout values on the **General** tab.
- For Firewall Authentication, select **Setup > Global Settings** and set the idle timeouts.
Before You Begin

Necessary Equipment and Services

To complete these exercises you must have:

- **Windows 2003 or Windows 2008 Server**
  This must be a domain controller for an Active Directory domain.
  The instructor should provide an Active Directory domain controller for the classroom domain. This is the authentication server for all students.
  The domain for the exercises in this module is *training.net*.

- **Management computer**
  See the subsequent section for configuration information

- **WSM version 11.7 software / Fireware XTM OS version 11.7 software**
  Your instructor provides this software, or you can download it from the WatchGuard web site with a valid LiveSecurity login.

- **WatchGuard XTM device — 2 Series, 3 Series, 5 Series, 8 Series, 1050, or 2050**

- **Feature key**
  Your instructor will provide a feature key to enable the features the XTM device must have for these exercises. You use the feature key toward the end of the Quick Setup Wizard when you configure the XTM device.

- **Ethernet cables**
  At a minimum, to complete these exercises you must have:
  - One crossover Ethernet cable to connect your computer to the trusted interface on your student XTM device.
  - One straight-through Ethernet cable to connect the external interface from your XTM device to a hub or switch that connects all student XTM devices to the central XTM device or Internet gateway.

- **Optional Windows 2008 Server Virtual Machine**
  This must be a domain controller for an Active Directory domain.
  The instructor should provide an Active Directory domain controller for the classroom domain. This is the authentication server for all students.
  The domain for the optional Clientless SSO exercise is *apac.wgtraining.net*.

- **Optional Windows XP Virtual Machine for Domain Client Computer**
  This will be used for the optional Clientless SSO as a domain client in an Active Directory domain environment. Your Instructor provides this Virtual Machine (VM) as an optional training item.

Management Computer Configuration

Before you begin these exercises, make sure your management computer is configured correctly.

- Install the WSM v11.7 client software and the Fireware XTM OS v11.7. You do not have to install the WSM server components.
- Connect the management computer directly to the trusted Interface 1 on the XTM device with a crossover Ethernet cable.
- Make sure your management computer has an IP address in the same subnet as the trusted interface with the correct subnet mask. Use the XTM device trusted interface IP address as the default gateway of the computer.
Firewall Configuration

If your XTM device is not yet configured, run the Quick Setup Wizard, and select routed mode. Routed mode has these defaults:

- The external Interface 0 is configured and enabled with a static IP address. Your instructor will tell you what IP address to assign to the external interface.
- The trusted Interface 1 is configured and enabled with IP address 10.0.1.1/24. Your instructor will give you an IP address to use for the trusted interface and for your management computer.

The exercises are designed so that all students can use the same IP address range for their trusted networks.
- None of the other interfaces are configured (they are all set to Disabled).
- The configuration file you open in Policy Manager includes these five policies: FTP, Ping, DNS, WatchGuard, and Outgoing.

Physically Connect the Devices

Because these exercises are designed for a classroom environment, the external interfaces of all student XTM devices should be connected to the same network segment that terminates at the instructor’s XTM device. Your management computer should be connected directly to Interface 1 on your XTM device.
Exercise 1: Allow Authenticated Users on the External Network to Manage the XTM Device

When to Use Authentication for Access to the XTM Device
There are many situations where it is useful to be able manage the XTM device from external locations. When you force users to authenticate before they can manage the XTM device, you can use WSM tools to track who can access the XTM device. You can also restrict access to any resource protected by the XTM device.

Network Topology
This exercise shows how to configure the XTM device for Active Directory authentication to a Windows server on the external network.

This diagram shows how your equipment is connected.

![Network topology for Exercise 1](image)

*Figure 27: Network topology for Exercise 1*
Configure the Active Directory Server

Your instructor has the Active Directory domain information for your classroom. For this exercise, we use these details:

- The training.net domain contains the organizational unit **Accounts** that is not in another container.
- The user account **student** is included somewhere in this organizational unit.
- The user is a member of the **Firebox Admins** Active Directory group.

Configure the XTM Device

Specify an Active Directory Authentication Server

Use Policy Manager to configure the XTM device to use an Active Directory server for authentication.

1. Click ↓
   Or, select **Setup > Authentication > Authentication Servers**. The **Authentication Servers** dialog box appears.
2. Select the **Active Directory** tab.
3. Select the **Enable Active Directory server** check box.
4. In the **IP Address** text box, type `50.50.50.2`.
5. In the **Search Base** text box, type `OU=accounts,DC=training,DC=net`.
6. For all other options, keep the default settings

![Figure 28: The Active Directory configuration for this exercise](image)

7. Click **OK**.

*In this training configuration, the Active Directory server is on the external network. In a typical installation the server would be on a trusted or optional network, protected by the XTM device.*
Add a Group to the Authorized Users and Groups List

1. Select **Setup > Authentication > Authorized Users/Groups**. The **Authorized Users and Groups** dialog box appears.
2. Click **Add**. The **Define New Authorized User or Group** dialog box appears.
3. In the **Name** text box, type the name of the Active Directory group your instructor gives you. For this exercise, type **Firebox Admins**.
4. For the **Type**, select **Group**.
5. From the **Auth Server** drop-down list, select **Active Directory**.

![Define New Authorized User or Group](image)

*Figure 29: Define the Active Directory group Firebox Admins*

6. Click **OK**. The new group appears in the **Authorized Users and Groups** dialog box.

![Authorized Users and Groups](image)

*Figure 30: The new Active Directory group appears in the Authorized Users and Groups list.*

7. Click **OK**.
Edit the WatchGuard Policy to Allow Access for the Active Directory Group

1. Double-click the **WatchGuard** policy to edit it.

   ![Figure 31: Edit the WatchGuard policy](image.png)

   The **Edit Policy Properties** dialog box appears.
2. In the **From** section, click **Add**.

![Edit Policy Properties dialog box](image)

- **Figure 32**: The **Edit Policy Properties** dialog box.

The **Add Address** dialog box appears.

---

**Do not remove the other aliases from the From list. The Any-Trusted alias allows you to manage your XTM device from the trusted network.**
3. Click **Add User**.

![Add Address dialog box](image1)

*Figure 33: The Add Address dialog box*

The **Add Authorized Users or Groups** dialog box appears.

4. From the right **Type** drop-down list, select **Group**.

![Add Authorized Users or Groups dialog box](image2)

*Figure 34: The new Active Directory group in the Add Authorized Users or Groups dialog box*

The new group you added appears in the **Groups** list.
5. Double-click the group. 
The group appears in the **Selected Members and Addresses** list.

![Figure 35: The new group in the Selected Members and Addresses list](image)
6. Click **OK**.
The **Edit Policy Properties** dialog box appears, with the changes to the WatchGuard policy.

![Edit Policy Properties dialog box](image)

Figure 36: The finished WatchGuard policy

7. Click **OK**.
Policy Manager automatically adds a new policy, the **WatchGuard-Authentication** policy, when you first add a user or group to a policy.

![Fireware XTM Policy Manager](image)

**Figure 37:** The **WatchGuard-Authentication** policy is added automatically

8. Double-click the **WatchGuard-Authentication** policy to edit it. A warning message appears.

![Warning Message](image)

9. Click **Yes**.

10. In the **From** section, click **Add**.

11. Double-click the **Any-External** alias to add it to the **Selected Members and Addresses** list.
12. Click **OK**.

The **Edit Policy Properties** dialog box appears with the changes to the **WatchGuard-Authentication** policy. It allows external users to connect to the XTM device over port 4100 for Firewall Authentication.

![Edit Policy Properties](image)

**Figure 38:** The updated **WatchGuard-Authentication** policy

13. Click **Save** and save this configuration to the XTM device.

Or, select **File > Save > To Firebox**.
Demonstrate It: Authenticate to Your Partner’s XTM Device to Manage It

Before you begin:

- Give your partner your XTM device external IP address, the status (read-only) password, and the configuration (read-write) password.
- Get the same information about your partner’s XTM device from your partner.

Try to Connect to Your Partner’s XTM Device Without Authenticating First

1. From WatchGuard System Manager, select File > Connect to Device.
2. Type the external IP address and status passphrase for your partner’s XTM device and click Login. Because you did not authenticate first, you cannot connect. An error message appears.

![Figure 39: Unable to connect](image)

Authenticate to Your Partner’s XTM Device and Try to Connect Again

1. Use a browser to make an HTTPS connection to your partner’s XTM device over port 4100. Type https://<IP address of your partner’s XTM device>:4100. For this example, type https://100.100.100.10:4100
   A browser warning message appears because the XTM device’s web server uses a self-signed certificate. The browser warning message you receive will be different depending on the browser you use. Some browsers have multiple warning pages.
2. In the browser warning message, select to continue to the web site. If your browser has multiple warning message pages, click through the messages to import and accept the XTM device certificate, and proceed to the web site.
3. In the Username and Password text boxes, type the user credentials your instructor gives you. For this exercise, type student.
4. From the Domain drop-down list, select Active Directory.

![Figure 40: Firewall Authentication screen](image)

5. Click Login.
When authentication is successful, this message appears.

![Successful authentication message](image)

*Figure 41: Successful authentication*

6. Try to connect to your partner’s XTM device again. You should now be able to connect.

![Device status screen](image)

*Figure 42: Connected to your partner’s XTM device*

Make sure you do not click the **Logout** button on the authentication web page. You must be able to connect to your partner’s XTM device in the next exercise.
Exercise 2: Use Active Directory to Authenticate Mobile VPN with SSL Clients

In this exercise you make a Mobile VPN connect to your partner’s XTM device. This presents a problem for the classroom setup, because each student’s XTM device uses the same trusted network address range (10.0.1.0/24), so the IP address on your computer is in the same subnet as your partner’s computer. You cannot test the Mobile VPN connection by attempting to pass traffic to an IP address in your own subnet. Because of basic IP routing, traffic that goes to an address in your own subnet stays in your own subnet; it does not route through the Mobile VPN tunnel.

To resolve this problem, make sure to enable Interface 2 on each classroom XTM device. The IP address on this interface is outside your computer’s subnet. You can then use the IP address of Interface 2 to connect to your partner’s XTM device.

Before you begin, you must complete Exercise 1 on page 31. Make sure you are connected to your partner’s XTM device with WatchGuard System Manager.

From WatchGuard System Manager, click to open Policy Manager for your partner’s XTM device.

When to Use Active Directory for Mobile VPN Authentication

Use Active Directory to authenticate Mobile VPN connections when the remote users that you allow to connect with Mobile VPN are all in your Active Directory domain.

Network Topology

Your equipment is connected in the same configuration you used for Exercise 1.
Configure the XTM Device

1. Select **Network > Configuration**.
   The **Network Configuration** dialog box appears. Only Interface 0 and Interface 1 are configured. All other interfaces are disabled.

![Network Configuration dialog box](image)

*Figure 43: Beginning network configuration*

2. Double-click **Interface 2** to configure it.
   The **Interface Settings - Interface #2** dialog box appears.
3. From the **Interface Type** drop-down list, select **Optional**.

![Interface Setting - Interface #2](image)

*Figure 44: Set the interface type to Optional.*

4. By default, the **Interface Name** is Optional-1 and the **IP Address** is 10.0.2.1/24. Keep the default settings and click **OK**.

![Interface Settings - Interface #2](image)

*Figure 45: Interface 2 defaults*

5. Click **OK** to return to Policy Manager.

6. Select **VPN > Mobile VPN > SSL**. The Mobile VPN with SSL Configuration dialog box appears.

---

It is not necessary to physically connect interface 2 to an Ethernet cable. You enable it so that you and your partner have an IP address outside your own trusted network to connect after you make the Mobile VPN connection to your partner’s XTM device. The XTM device will respond to pings and management connections on this interface when you enable it.
7. Select the **Activate Mobile VPN with SSL** check box. The fields on the dialog box are enabled, and the IP address of your device automatically appears in the IP address text boxes.

![Mobile VPN with SSL Configuration dialog box General tab](image)

Figure 46: Mobile VPN with SSL Configuration dialog box General tab

8. In the **Primary** text box, type or select a public IP address or domain name.

9. In the **Networking and IP Address Pool** section, the options **Routed VPN traffic** and **Allow access to networks connected through Trusted, Optional, and VLANs** are selected by default. Keep these selections.

10. In the **Virtual IP Address Pool** text box, keep the default setting.
11. Select the **Authentication** tab.

![Mobile VPN with SSL Configuration dialog box Authentication tab](image)

**Figure 47:** Mobile VPN with SSL Configuration dialog box Authentication tab

12. From the **Authentication Server Settings** list, select the check box for the Active Directory server you configured in Figure 24 on page 21. For this exercise, select *training.net*. 
13. To select the **training.net** server as the default server, click **Make Default**.
The training.net Active Directory server is marked with the (Default) designation and moved to the top of the Authentication Server list.

![Mobile VPN with SSL Configuration](image)

*Figure 48: Select the Active Directory server*

14. In the list of users and groups, the **SSLVPN-Users** group was added automatically. Keep this setting.

15. For the **Type** option, keep the default selection of **Group**.

16. In the **Type** text box, type the name of the group on your Active Directory server to use for authentication.
   For this exercise, type **AD-VPN-Users**.

17. From the **Authentication Server** drop-down list, select the authentication server for this group.
   For this exercise, select **training.net**.
18. Click **Add**.
The group appears in the **Users and Groups** list.

![Image](image_url)

*Figure 49: Add the Active Directory group you want to use for authentication to the **Users and Groups** list.*

19. Select the **Advanced** tab and review the settings. For this example, we keep the default settings.
20. Click **OK**.

Policy Manager appears with the new **WatchGuard SSLVPN** and **Allow SSLVPN-Users** policies added to the configuration.

![Policy Manager screenshot](image-url)

**Figure 50:** The automatically generated **WatchGuard SSLVPN**, **WatchGuard Authentication**, and **Allow SSLVPN-Users** policies

When you save the Mobile VPN with SSL configuration, the **Allow SSLVPN-Users** policy is created or updated to apply to the groups and users you configured for authentication. The group and user names you added do not appear in the **From** list in the **Allow SSLVPN-Users** policy. Instead, the single group name **SSLVPN-Users** appears, followed by the authentication method in parentheses.

For example, if you configured Mobile VPN with SSL to use your Active Directory server (training.net), and added two Active Directory groups, **SSLVPN-Users1** and **SSLVPN-Users2**, the group name **SSLVPN-Users (training.net)** appears in the **From** list in the **Allow SSLVPN-Users** policy. The policy does not show the two group names you added in the Mobile VPN with SSL configuration. Even though the group and user names you added do not appear in the From list, this policy does apply to all users and groups you configured in the Mobile VPN with SSL authentication settings.

**Enable Logging for the SSLVPN Policy**

From Policy Manager:

1. Double-click the **WatchGuard SSLVPN** policy to edit it.

   A warning message appears.

   ![Policy Manager warning message](image-url)

   **Figure 51:** Policy Manager warning message for automatically generated policies

2. Click **Yes**.
3. Select the **Properties** tab and click **Logging**.

![Figure 52: Properties tab of the policy](image)

The **Logging and Notification** dialog box appears.

4. Select the **Send log message** check box.

![Figure 53: Enable logging for the policy](image)

5. Click **OK**.

The **Edit Policy Properties** dialog box appears.

6. Repeat Steps 1–5 for the **Allow SSLVPN-Users** policy.

7. Click **OK** to return to Policy Manager.
8. Click and save this configuration to the XTM device.
   Or, select File > Save > To Firebox.
9. After the file has saved to the XTM device, go to your web browser and click Logout on the web authentication page.

![You have been successfully authenticated.](image)

Figure 54: Log out from your partner’s XTM device

**Download the Mobile VPN with SSL Client Software**

1. Open a web browser and connect to your partner’s XTM device at this address:
   https://<IP address of an XTM device interface>/sslvpn.html
2. Type your user name and password to authenticate to the XTM device.
   The Items Available to download page appears.
3. Adjacent to the installer you want to use, click Download.
   Make sure to select the correct versions of the installer. There is one for Windows clients and one for Mac OS X clients.
   For this training module select the Windows installer (WG-MVPN-SSL.exe).
4. Save the file to your computer.

**Install the SSLVPN Client Software**

1. Double-click the WG-MVPN-SSL.exe file.
   The Mobile VPN with SSL Client Setup Wizard starts.
2. On each page of the wizard, keep the default settings.
3. Finish and exit the wizard.

**Make an SSLVPN Connection to Your Partner’s XTM Device**

1. To start the client software, select Start > All Programs > WatchGuard > Mobile VPN with SSL Client > Mobile VPN with SSL Client.
   Or, double-click the Mobile VPN with SSL shortcut on your desktop.
2. Type the IP address of the XTM device you want to connect to, and the username and password for the user.
3. Click Connect.
4. To test the connection, open WatchGuard System Manager and connect to the optional interface of your partner’s XTM device.
Do not use the external IP address of your partner's XTM device. Connect to the optional interface IP address 10.0.2.1 so that the traffic goes through the Mobile VPN tunnel.

5. Click . Firebox System Manager (FSM) appears.

6. On the Front Panel tab, expand Interfaces.

7. Verify that you are connected to your partner's XTM device (not to your own XTM device optional interface) by looking at the external interface IP address. It should be the IP address for your partner's XTM device.

8. Expand Mobile VPN with SSL Tunnels and review your Mobile VPN with SSL connection statistics.

9. Open a command prompt and ping 10.0.2.1 on the optional interface of your partner's XTM device.

10. Watch Traffic Monitor for your partner's XTM device to verify that the ping goes through the VPN tunnel. A message like this should appear:

```
Allow 10.0.2.105 10.0.2.1 icmp-Echo Firebox Admins/SSL Firebox allowed (decrypted packet, SA info: id 0x086632d8) 60 128 (Firebox Admins-Any.in-00) src_user="student@Active Directory"
```

In WSM and FSM, traffic messages like this should appear:

```
Allow 10.0.2.105 10.0.2.1 WG-Management/tcp 2321 4117 Firebox Admins/SSL Firebox allowed (decrypted packet, SA info: id 0x086632d8), mss not exceeding 1376, idle timeout=43205 sec 48 128 (Firebox Admins-Any.in-00) tcpinfo="offset 7 S 2628964518 win 16384" src_user="student@Active Directory"
```
Exercise 3: Use Clientless Single Sign-On to Authorize Domain Users

In this exercise you will simulate an Active Directory (AD) domain environment and have domain client hosts join the domain. This presents a challenge in a classroom setup because everyone will use the same AD server, but with different XTM Devices to resolve the individual domain clients.

To resolve this issue, we use virtual machines (VMs) for the Windows 2008 Active Directory server and the Windows XP domain client. Similarly, you may use this optional exercise in your own laboratory where you can replace the virtual machines with real hardware.

Before you begin, you must install the virtual machines (VMs) to make sure you have an Active Directory (AD) server and a domain client. Because the WatchGuard Authentication Gateway service must run as a user who is a member of the Domain Admins group, we also recommend that you create a new user account for this purpose and then add the new user to the Domain Admins group. For the service to operate correctly, make sure you configure this Domain Admin user account with a password that never expires.

Note
This exercise is optional because it requires the virtual machines (VM) for your Active Directory servers and domain clients to join the domain apac.wgtraining.net.

Active Directory for Clientless SSO
In this image, the domain apac.wgtraining.net (NetBIOS name is APAC) has an OU (organizational unit) named Students where the training users are stored.
Default Domain Policy

Your AD server should have a Default Domain Policy that collects successful *Audit account logon events* and *Audit logon events*.

![Default Domain Policy Diagram](image)

Install the SSO Agent

Make sure you are logged in with a user account with *Domain Admin* permissions.

1. Launch the WatchGuard SSO Agent installer.
   The name of the installer is *WatchGuard Authentication Gateway*.

![WatchGuard Authentication Gateway Installer](image)

2. Click **Next** to continue.

3. Browse to select the installation folder.
   The default installation folder is automatically selected. Though you can select a different location to install the SSO Agent, for this exercise, keep the default location.

4. Click **Next**.
5. **Select the SSO Components to install.**

For this single domain exercise, select to install both the Single Sign-On Agent and Event Log Monitor components on the same AD server.

6. To select a start menu folder other than the default location, click **Browse**. If you do not want to create a start menu folder, select the **Do not create a Start Menu folder** check box.
7. Click **Next**.
The **Domain User Credentials** page appears.

8. Type the **Domain User Name** and **Password** and click **Next**.

9. Review the installation and click **Next**.
The **Installation is Complete** page appears.

10. Click **Finish**.

Your instructor will provide the domain username and password for the SSO Agent installation.
Configure the XTM Device

From Policy Manager:

1. Select **Setup > Authentication > Authentication Servers**.
   The **Authentication Servers** dialog box appears.
2. Select the **Active Directory** tab.
3. Click **Add**.
   The **Add Active Directory Domain** dialog box appears.
4. Add the domain information for your Active Directory server.

5. Click **OK**.
6. Select **Setup > Authentication > Authentication Settings**.
   The **Authentication Settings** dialog box appears.
7. Select the **Single Sign-On** tab.
8. Select the **Enable Single Sign-On (SSO) with Active Directory** check box.
9. In the **SSO Agent IP address** text box, type the IP address where the SSO Agent is installed.

Because the SSO Agent is installed in the same location as the Active Directory server, the IP address of the SSO Agent is the same as that of the Active Directory server.

10. Click **OK**.

11. Save the configuration file to your XTM device.

If there are IP addresses that you do not want to use SSO, you can add them to the SSO Exceptions list.
Demonstrate Clientless SSO

1. Log in to the XP domain client with the *training-admin* user account.
2. Browse to any web page. The *training-admin* user information should appear in Firebox System Manager in the **Authentication List**

![Firebox System Manager](image)

3. Log off the *training-admin* user account from the XP domain client and log in with the *student10* user account.
4. Browse to any web page.

   The *student10* user information should appear in Firebox System Manager in the **Authentication List**.
5. To create a firewall policy to authorize Active Directory users, select **Setup > Authentication > Authorized Users/Groups**.

   The **Authorized Users and Groups** dialog box appears.
6. In the **Name** text box, type *student20*.
7. Select **User**.
8. From the **Auth Server** drop-down list, select your Active Directory server.

![Define New Authorized User or Group](image)

9. Click **OK** to add the authorized user.
10. In Policy Manager, click and add a policy that allows only student20 to browse the web.

![New Policy Properties dialog box](image)

11. In the From section, click Add.
   The Add Address dialog box appears.

12. Click Add User.
   The Add Authorized Users or Groups dialog box appears.

![Add Authorized Users or Groups dialog box](image)

13. In the Users list, select student20 and click Select.
   student20 appears in the From list of the policy.
14. Click **OK**.

The policy now includes student20 as the only user allowed to browse the internet.

15. In the **To** list, make sure the only option is **Any-External**.

16. Click **OK**.

17. Log in to the XP domain client with the student20 user account and try to browse the web.

18. Log off student20 from the domain client and log in as another user. Try to browse the web.
Frequently Asked Questions

- **Why doesn’t Fireware XTM see the user as a member of a universal group x?**

  When Active Directory replicates objects across the forest, it replicates only partial lists of attributes for some objects. In a domain that is not the domain where the universal group was created, a user’s universal group membership only appears on a Global Catalog server. However, a user’s universal group membership information is always present in the primary domain controller in the user’s home domain.

  To summarize, the search results for that user will not appear as universal group membership for that universal group if:

  - Your domain is part of a multi-domain forest.
  - The user is a member of a universal group that was created in a domain that is not the user’s home domain.
  - You specify an Active Directory server in Policy Manager that is neither the primary domain controller for the user’s home domain, nor a Global Catalog server.

  If you want to use universal groups in this situation, you have two options:

  - When you specify the Active Directory server settings in Policy Manager, use the primary domain controller for the home domain of all the users that authenticate to your XTM device.
  - If you cannot specify the primary domain controller as the home domain for the Active Directory server, configure Policy Manager to use a Global Catalog (GC) server. Specify the IP address for the GC server and change the port from 389 to 3268, the port used for GC queries.

- **Is it necessary to allow connections from external locations to the XTM device over TCP port 4100 for Firewall authentication to work?**

  Yes.

  With Firewall Authentication, authenticated users connect to the XTM device web server over TCP port 4100. Although the XTM device listens for connections on port 4100, the XTM device does not allow port 4100 traffic to its interfaces unless a policy specifically allows it. Policy Manager automatically adds a policy to allow these connections from trusted and optional networks when you add a user or group to a policy so that users on those networks can authenticate to the XTM device.

  However, port 4100 is not open by default on the XTM device external interface. You must edit the automatically generated Firebox-Authentication policy to allow connections to the XTM device over port 4100 from external networks.

- **What happens if the user closes the browser after the user is authenticated?**

  After a user successfully authenticates with Firewall Authentication, it is not necessary to keep the browser open to stay authenticated. However, the session timeout or the idle timeout will eventually cause the XTM device to remove the user from the list of authenticated users.

  If your Active Directory server does not return any optional attributes (see in “Optional Data that Active Directory Can Give Fireware XTM” on page 26), select **Setup > Authentication > Authentication Settings** in Policy Manager to set these values.

  When the browser that was used for authentication is closed, a user cannot verify the status of authentication. The user can go to the Firewall Authentication page again to check the status. If the user is currently authenticated, this message appears: *You have been successfully authenticated.*

  If the user is not authenticated, the user is prompted to provide a user name and password.
• **Can I use Active Directory to authenticate PPTP sessions?**
  
  No.
  
The XTM device can authenticate PPTP sessions only with the internal database of Firebox Users or a RADIUS server.

• **What account should I use for the Searching User?**
  
  By default, any user in an Active Directory domain has read access to the directory. You can create a user account with limited privileges for the Searching User.
  
  Users in the Administrators group on a directory server receive answers to their Active Directory queries faster than normal users, but the difference should not be noticeable except on a directory server with an extremely heavy traffic load. It is not recommended to use an account with administrator-level privileges.

• **Is the Users object a container or a group?**
  
  Both:
  
  - The Users folder in Active Directory Users and Computers is a container.
  - Active Directory also has a Users group in the Builtin container.
  
  A user account you add in the Users container is automatically a member of the Users group, because any new user is automatically a member of the Domain Users group. The Domain Users group is a member of the Users group by default. This is an example of transitive group membership.

• **Why does a user lose the ability to authenticate to the XTM device when I set “Log On To” machine restrictions for the user account?**
  
  When you edit a user account in Active Directory Users and Computers, you can click the Log On To button on the Account tab to restrict which domain computers the user can log on to locally. If you set this restriction on the user account, LDAP bind requests with the user’s credentials no longer succeed, even if the bind request is sent from the specified machine. You can resolve this by adding the Active Directory server’s netBIOS name to the list of computers in the Log On To section of the user account. This does not give local logon privileges to the user on the domain controller. Normal users are not allowed to log on to a domain controller.

### What You Have Learned

In this training module you learned how:

• Fireware XTM authenticates users against an Active Directory server
• Fireware XTM authorizes traffic from users
• Active Directory uses LDAP
• To set up the XTM device for Active Directory authentication, and allow users to access XTM device management ports from the external network
• To configure Active Directory authentication for a Mobile VPN with SSL group
• To use clientless SSO in an Active Directory domain environment