User Authentication

FortiOS™ Handbook v2
for FortiOS 4.0 MR2
Contents

Introduction 9
Before you begin ........................................... 9
   How this guide is organized ............................ 9
Document conventions ..................................... 11
   IP addresses ............................................ 11
   Example Network configuration ......................... 13
Cautions, Notes and Tips ................................ 14
Typographical conventions ............................. 15
CLI command syntax conventions ..................... 15
Entering FortiOS configuration data ..................... 17
   Entering text strings (names) ......................... 17
   Entering numeric values .............................. 18
   Selecting options from a list ....................... 18
   Enabling or disabling options ...................... 18
Registering your Fortinet product ..................... 18
Fortinet products End User License Agreement ......... 18
Training .................................................. 19
Documentation ........................................... 19
   Fortinet Tools and Documentation CD ................. 19
   Fortinet Knowledge Base ............................ 19
   Comments on Fortinet technical documentation ...... 19
Customer service and technical support ............... 19

Introduction to authentication 21
What is authentication? ................................ 21
Means of authentication ................................ 21
   Local password authentication ...................... 21
   Server-based password authentication ............... 21
      Single Sign On authentication using FSAE ....... 22
   Certificate-based authentication .................... 22
      Certificate authorities ........................... 23
      Certificates for users ........................... 23
   Two-factor authentication ........................... 23
Types of authentication ................................ 23
   Firewall authentication (or Identity-based policies) 23
# Contents

FortiGuard Web Filter override authentication ........................................... 24
VPN authentication ..................................................................................... 24
Authenticating IPsec VPN peers (devices) .................................................... 24
Authenticating IPsec VPN users .................................................................. 24
Authenticating SSL VPN users .................................................................... 24
Authenticating PPTP and L2TP VPN users .................................................. 25

USER’S view of authentication .................................................................... 25
Web-based user authentication ...................................................................... 25
VPN client-based authentication .................................................................. 26

FortiGate administrator’s view of authentication ........................................ 26

## Authentication servers

<table>
<thead>
<tr>
<th>Server Type</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>RADIUS servers</td>
<td>29</td>
</tr>
<tr>
<td>Configuring the Fortinet unit to use a RADIUS server</td>
<td>30</td>
</tr>
<tr>
<td>LDAP servers</td>
<td>31</td>
</tr>
<tr>
<td>Configuring the Fortinet unit to use an LDAP server</td>
<td>33</td>
</tr>
<tr>
<td>Using the Query icon.</td>
<td>34</td>
</tr>
<tr>
<td>TACACS+ servers</td>
<td>35</td>
</tr>
<tr>
<td>Configuring the Fortinet unit to use a TACACS+ authentication server</td>
<td>36</td>
</tr>
<tr>
<td>Directory Service servers</td>
<td>37</td>
</tr>
<tr>
<td>RSA/ACE (SecurID) servers</td>
<td>37</td>
</tr>
<tr>
<td>Using the SecurID user group for authentication.</td>
<td>38</td>
</tr>
<tr>
<td>Firewall policy</td>
<td>38</td>
</tr>
<tr>
<td>IPsec VPN XAuth</td>
<td>38</td>
</tr>
<tr>
<td>PPTP VPN</td>
<td>38</td>
</tr>
<tr>
<td>SSL VPN</td>
<td>38</td>
</tr>
</tbody>
</table>

## Users and user groups

<table>
<thead>
<tr>
<th>User Group Type</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users</td>
<td>39</td>
</tr>
<tr>
<td>Creating local users</td>
<td>40</td>
</tr>
<tr>
<td>Creating PKI or peer users</td>
<td>41</td>
</tr>
<tr>
<td>Two-factor authentication</td>
<td>42</td>
</tr>
<tr>
<td>User groups</td>
<td>43</td>
</tr>
<tr>
<td>Firewall user groups</td>
<td>43</td>
</tr>
<tr>
<td>SSL VPN access</td>
<td>43</td>
</tr>
<tr>
<td>IPsec VPN access</td>
<td>43</td>
</tr>
<tr>
<td>Configuring a firewall user group</td>
<td>44</td>
</tr>
<tr>
<td>Directory Service user groups</td>
<td>45</td>
</tr>
<tr>
<td>Configuring Peer user groups</td>
<td>45</td>
</tr>
<tr>
<td>Viewing, editing and deleting user groups</td>
<td>46</td>
</tr>
</tbody>
</table>
## Configuring authenticated access

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication timeout</td>
<td>47</td>
</tr>
<tr>
<td>Password policy</td>
<td>47</td>
</tr>
<tr>
<td>Authentication protocols</td>
<td>48</td>
</tr>
<tr>
<td>Authentication in firewall policies</td>
<td>49</td>
</tr>
<tr>
<td>Configuring authentication for a firewall policy</td>
<td>49</td>
</tr>
<tr>
<td>Configuring authenticated access to the Internet</td>
<td>51</td>
</tr>
<tr>
<td>VPN authentication</td>
<td>51</td>
</tr>
<tr>
<td>Configuring authentication of SSL VPN users</td>
<td>51</td>
</tr>
<tr>
<td>Configuring authentication timeout</td>
<td>51</td>
</tr>
<tr>
<td>Configuring authentication of remote IPsec VPN users</td>
<td>52</td>
</tr>
<tr>
<td>Configuring XAuth authentication</td>
<td>53</td>
</tr>
<tr>
<td>Configuring authentication of PPTP VPN users and user groups</td>
<td>54</td>
</tr>
<tr>
<td>Configuring authentication of L2TP VPN users/user groups</td>
<td>55</td>
</tr>
</tbody>
</table>

## FSAE for integration with Windows AD or Novell

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction to FSAE</td>
<td>57</td>
</tr>
<tr>
<td>Using FSAE in a Windows AD environment</td>
<td>57</td>
</tr>
<tr>
<td>FSAE user logon monitoring</td>
<td>58</td>
</tr>
<tr>
<td>NTLM authentication with FSAE</td>
<td>59</td>
</tr>
<tr>
<td>Using FSAE in a Novell eDirectory environment</td>
<td>61</td>
</tr>
<tr>
<td>Operating system requirements</td>
<td>61</td>
</tr>
<tr>
<td>Installing FSAE</td>
<td>61</td>
</tr>
<tr>
<td>FSAE components for Windows AD</td>
<td>61</td>
</tr>
<tr>
<td>FSAE components for Novell eDirectory</td>
<td>62</td>
</tr>
<tr>
<td>Installing FSAE for Windows AD</td>
<td>62</td>
</tr>
<tr>
<td>Installing FSAE for Novell</td>
<td>63</td>
</tr>
<tr>
<td>Configuring FSAE on Windows AD</td>
<td>64</td>
</tr>
<tr>
<td>Configuring Windows AD server user groups</td>
<td>64</td>
</tr>
<tr>
<td>Configuring collector agent settings</td>
<td>65</td>
</tr>
<tr>
<td>Configuring Directory Access settings</td>
<td>67</td>
</tr>
<tr>
<td>Configuring the Ignore User List</td>
<td>67</td>
</tr>
<tr>
<td>Configuring FortiGate group filters</td>
<td>68</td>
</tr>
<tr>
<td>Configuring TCP ports for FSAE on client computers</td>
<td>70</td>
</tr>
<tr>
<td>Configuring ports on the collector agent computer</td>
<td>70</td>
</tr>
<tr>
<td>Configuring alternate user IP address tracking</td>
<td>70</td>
</tr>
<tr>
<td>Viewing collector agent status</td>
<td>70</td>
</tr>
<tr>
<td>Viewing DC agent status</td>
<td>71</td>
</tr>
<tr>
<td>Selecting Domain Controllers and working mode for monitoring</td>
<td>72</td>
</tr>
<tr>
<td>Configuring FSAE on Novell networks</td>
<td>73</td>
</tr>
<tr>
<td>Configuring a group filter</td>
<td>75</td>
</tr>
</tbody>
</table>
Contents

Configuring FSAE on FortiGate units ........................................................... 76
Configuring LDAP server access ................................................................. 76
Specifying your collector agents or Novell eDirectory agents ..................... 78
Selecting Windows user groups (LDAP only) .............................................. 79
Viewing information imported from the Windows AD server ......................... 79
Creating Directory Service user groups ..................................................... 81
Creating firewall policies ........................................................................ 81
Enabling guests to access FSAE policies ..................................................... 82
Testing the configuration ........................................................................ 83

Certificate-based authentication .................................................................. 85
Certificates overview .............................................................................. 85
SSL, HTTPS, and certificates ................................................................... 85
IPsec VPNs and certificates ..................................................................... 86
Managing X.509 certificates ...................................................................... 86
Generating a certificate signing request .................................................... 86
Generating certificates with CA software .................................................. 88
  Server certificate ................................................................................. 88
  CA certificate ..................................................................................... 88
  PKI certificate ................................................................................... 88
Obtaining a signed server certificate from an external CA ......................... 89
Installing a CA root certificate and CRL to authenticate remote clients ....... 89
Online updates to certificates and CRLs .................................................... 90
  Local certificates .............................................................................. 91
  CA certificates .................................................................................. 91
  Certificate Revocation Lists ............................................................... 91
Backing up and restoring local certificates ............................................... 92
Configuring certificate-based authentication ............................................. 94
  Authenticating administrators with security certificates ....................... 94
  Authenticating SSL VPN users with security certificates ..................... 94
  Authenticating IPsec VPN users with security certificates ................... 95

Monitoring authenticated users ................................................................. 97
Monitoring firewall users ....................................................................... 97
Monitoring SSL VPN users ................................................................... 97
Monitoring IPsec VPN users ................................................................... 98
Example

Firewall authentication example .................................................. 99
  Overview ................................................................................. 99
Creating a locally-authenticated user account .................................. 100
Creating a RADIUS-authenticated user account ................................. 100
Creating user groups ................................................................... 101
  Creating the Directory Services user group .................................. 101
  Creating the Firewall user group .................................................. 103
Defining firewall addresses ............................................................. 103
Creating firewall policies ............................................................... 103

Index

107
Introduction

Welcome and thank you for selecting Fortinet products for your network protection. This chapter contains the following topics:

- Before you begin
- Document conventions
- Entering FortiOS configuration data
- Registering your Fortinet product
- Fortinet products End User License Agreement
- Training
- Documentation
- Customer service and technical support

Before you begin

Before you begin using this guide, please ensure that:

- You have administrative access to the web-based manager and/or CLI.
- The FortiGate unit is integrated into your network.
- The operation mode has been configured.
- The system time, DNS settings, administrator password, and network interfaces have been configured.
- Firmware, FortiGuard Antivirus and FortiGuard Antispam updates are completed.

While using the instructions in this guide, note that administrators are assumed to be super_admin administrators unless otherwise specified. Some restrictions will apply to other administrators.

How this guide is organized

This FortiOS Handbook chapter contains the following sections:

“Introduction to authentication” describes some basic elements and concepts of authentication.

“Authentication servers” describes external authentication servers and how to configure a FortiGate unit to use them.

“Users and user groups” describes the different types of user accounts and user groups. Authenticated access to resources is based on user identities and user groups.

“Configuring authenticated access” provides detailed procedures for setting up authenticated access in firewall policies and authenticated access to VPNs.

“FSAE for integration with Windows AD or Novell” describes how to install and configure the Fortinet Server Authentication Extension (FSAE) on network domain controllers and the FortiGate unit. On the FortiGate unit, Windows AD or Novell network user groups can be made members of Directory Services user groups. With FSAE, network users have single sign-on access to resources through the FortiGate unit.

“Monitoring authenticated users” describes the FortiGate unit authenticated user monitoring screens.

“Example” provides a configuration example in which Windows AD and other network users are provided authenticated access to the Internet.
Document conventions

Fortinet technical documentation uses the conventions described below.

IP addresses

To avoid publication of public IP addresses that belong to Fortinet or any other organization, the IP addresses used in Fortinet technical documentation are fictional and follow the documentation guidelines specific to Fortinet. The addresses used are from the private IP address ranges defined in RFC 1918: Address Allocation for Private Internets, available at http://ietf.org/rfc/rfc1918.txt?number-1918.

Most of the examples in this document use the following IP addressing:

- IP addresses are made up of A.B.C.D
- A - can be one of 192, 172, or 10 - the non-public addresses covered in RFC 1918.
- B - 168, or the branch / device / virtual device number.
  - Branch number can be 0xx, 1xx, 2xx - 0 is Head office, 1 is remote, 2 is other.
  - Device or virtual device - allows multiple FortiGate units in this address space (VDOMs).
  - Devices can be from x01 to x99.
- C - interface - FortiGate units can have up to 40 interfaces, potentially more than one on the same subnet
  - 001 - 099 - physical address ports, and non-virtual interfaces
  - 100-255 - VLANs, tunnels, aggregate links, redundant links, vdom-links, etc.
- D - usage based addresses, this part is determined by what device is doing
  - The following gives 16 reserved, 140 users, and 100 servers in the subnet.
  - 001 - 009 - reserved for networking hardware, like routers, gateways, etc.
  - 010 - 099 - DHCP range - users
  - 100 - 109 - FortiGate devices - typically only use 100
  - 110 - 199 - servers in general (see later for details)
  - 200 - 249 - static range - users
  - 250 - 255 - reserved (255 is broadcast, 000 not used)
  - The D segment servers can be farther broken down into:
    - 110 - 119 - Email servers
    - 120 - 129 - Web servers
    - 130 - 139 - Syslog servers
    - 140 - 149 - Authentication (RADIUS, LDAP, TACACS+, FSAE, etc)
    - 150 - 159 - VoIP / SIP servers / managers
    - 160 - 169 - FortiAnalyzers
    - 170 - 179 - FortiManagers
    - 180 - 189 - Other Fortinet products (FortiScan, FortiDB, etc.)
    - 190 - 199 - Other non-Fortinet servers (NAS, SQL, DNS, DDNS, etc.)
    - Fortinet products, non-FortiGate, are found from 160 - 189.
The following table shows some examples of how to choose an IP number for a device based on the information given. For internal and dmz, it is assumed in this case there is only one interface being used.

### Table 1: Examples of the IP numbering

<table>
<thead>
<tr>
<th>Location and device</th>
<th>Internal</th>
<th>Dmz</th>
<th>External</th>
</tr>
</thead>
<tbody>
<tr>
<td>Head Office, one FortiGate</td>
<td>10.011.101.100</td>
<td>10.011.201.100</td>
<td>172.20.120.191</td>
</tr>
<tr>
<td>Head Office, second FortiGate</td>
<td>10.012.101.100</td>
<td>10.012.201.100</td>
<td>172.20.120.192</td>
</tr>
<tr>
<td>Branch Office, one FortiGate</td>
<td>10.021.101.100</td>
<td>10.021.201.100</td>
<td>172.20.120.193</td>
</tr>
<tr>
<td>Office 7, one FortiGate with 9 VDOMs</td>
<td>10.079.101.100</td>
<td>10.079.101.100</td>
<td>172.20.120.194</td>
</tr>
<tr>
<td>Office 3, one FortiGate, web server</td>
<td>n/a</td>
<td>10.031.201.110</td>
<td>n/a</td>
</tr>
<tr>
<td>Bob in accounting on the corporate user network (dhcp) at Head Office, one FortiGate</td>
<td>10.0.11.101.200</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Router outside the FortiGate</td>
<td>n/a</td>
<td>n/a</td>
<td>172.20.120.195</td>
</tr>
</tbody>
</table>
Example Network configuration

The network configuration shown in Figure 1 or variations on it is used for many of the examples in this document. In this example, the 172.20.120.0 network is equivalent to the Internet. The network consists of a head office and two branch offices.

Figure 1: Example network configuration
Cautions, Notes and Tips

Fortinet technical documentation uses the following guidance and styles for cautions, notes and tips.

**Caution:** Warns you about commands or procedures that could have unexpected or undesirable results including loss of data or damage to equipment.

**Note:** Presents useful information, but usually focused on an alternative, optional method, such as a shortcut, to perform a step.

**Tip:** Highlights useful additional information, often tailored to your workplace activity.
## Typographical conventions

Fortinet documentation uses the following typographical conventions:

### Table 2: Typographical conventions in Fortinet technical documentation

<table>
<thead>
<tr>
<th>Convention</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Button, menu, text box, field,</td>
<td>From Minimum log level, select Notification.</td>
</tr>
<tr>
<td>or check box label</td>
<td>config system dns</td>
</tr>
<tr>
<td></td>
<td>set primary &lt;address_ipv4&gt;</td>
</tr>
<tr>
<td></td>
<td>end</td>
</tr>
<tr>
<td>CLI input</td>
<td>FGT-602803030703 # get system settings</td>
</tr>
<tr>
<td></td>
<td>comments : (null)</td>
</tr>
<tr>
<td></td>
<td>opmode : nat</td>
</tr>
<tr>
<td>Emphasis</td>
<td>HTTP connections are not secure and can be intercepted by a third party.</td>
</tr>
<tr>
<td>File content</td>
<td>&lt;HTML&gt;&lt;HEAD&gt;&lt;TITLE&gt;Firewall Authentication&lt;/TITLE&gt;&lt;/HEAD&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;BODY&gt;&lt;H4&gt;You must authenticate to use this service.&lt;/H4&gt;</td>
</tr>
<tr>
<td>Keyboard entry</td>
<td>Type a name for the remote VPN peer or client, such as Central_Office_1.</td>
</tr>
<tr>
<td>Navigation</td>
<td>Go to VPN &gt; IPSEC &gt; Auto Key (IKE).</td>
</tr>
<tr>
<td>Publication</td>
<td>For details, see the FortiOS Handbook.</td>
</tr>
</tbody>
</table>

### CLI command syntax conventions

This guide uses the following conventions to describe the syntax to use when entering commands in the Command Line Interface (CLI).

Brackets, braces, and pipes are used to denote valid permutations of the syntax.

Constraint notations, such as `<address_ipv4>`, indicate which data types or string patterns are acceptable value input.

### Table 3: Command syntax notation

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Square brackets</td>
<td>A non-required word or series of words. For example: [verbose {1</td>
</tr>
</tbody>
</table>
Table 3: Command syntax notation  (Continued)

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Angle brackets < >** | A word constrained by data type. To define acceptable input, the angled brackets contain a descriptive name followed by an underscore (_) and suffix that indicates the valid data type. For example:  
  `<retries_int>` indicates that you should enter a number of retries, such as 5. Data types include:  
  • `<xxx_name>`: A name referring to another part of the configuration, such as `policy_A`.  
  • `<xxx_index>`: An index number referring to another part of the configuration, such as 0 for the first static route.  
  • `<xxx_pattern>`: A regular expression or word with wild cards that matches possible variations, such as `*@example.com` to match all email addresses ending in `@example.com`.  
  • `<xxx_fqdn>`: A fully qualified domain name (FQDN), such as `mail.example.com`.  
  • `<xxx_email>`: An email address, such as `admin@mail.example.com`.  
  • `<xxx_url>`: A uniform resource locator (URL) and its associated protocol and host name prefix, which together form a uniform resource identifier (URI), such as `http://www.fortinet.com/`.  
  • `<xxx_ipv4>`: An IPv4 address, such as `192.168.1.99`.  
  • `<xxx_v4mask>`: A dotted decimal IPv4 netmask, such as `255.255.255.0`.  
  • `<xxx_ipv4mask>`: A dotted decimal IPv4 address and netmask separated by a space, such as `192.168.1.99 255.255.255.0`.  
  • `<xxx_ipv4/mask>`: A dotted decimal IPv4 address and CIDR-notation netmask separated by a slash, such as `192.168.1.99/24`.  
  • `<xxx_ipv6>`: A colon(:)-delimited hexadecimal IPv6 address, such as `3f2e:6a8b:78a3:0d82:1725:6a2f:0370:6234`.  
  • `<xxx_v6mask>`: An IPv6 netmask, such as `/96`.  
  • `<xxx_ipv6mask>`: An IPv6 address and netmask separated by a space.  
  • `<xxx_str>`: A string of characters that is not another data type, such as `P@ssw0rd`. Strings containing spaces or special characters must be surrounded in quotes or use escape sequences.  
  • `<xxx_int>`: An integer number that is not another data type, such as 15 for the number of minutes. |
### Entering FortiOS configuration data

The configuration of a FortiGate unit is stored as a series of configuration settings in the FortiOS configuration database. To change the configuration you can use the web-based manager or CLI to add, delete or change configuration settings. These configuration changes are stored in the configuration database as they are made.

Individual settings in the configuration database can be text strings, numeric values, selections from a list of allowed options, or on/off (enable/disable).

#### Entering text strings (names)

Text strings are used to name entities in the configuration. For example, the name of a firewall address, administrative user, and so on. You can enter any character in a FortiGate configuration text string except, to prevent Cross-Site Scripting (XSS) vulnerabilities, text strings in FortiGate configuration names cannot include the following characters:

- " (double quote), & (ampersand), ' (single quote), < (less than) and > (greater than)

You can determine the limit to the number of characters that are allowed in a text string by determining how many characters the web-based manager or CLI allows for a given name field. From the CLI, you can also use the `tree` command to view the number of characters that are allowed. For example, firewall address names can contain up to 64 characters. When you add a firewall address to the web-based manager you are limited to entering 64 characters in the firewall address name field. From the CLI you can do the following to confirm that the firewall address name field allows 64 characters.

```
config firewall address
tree
  -- [address]  **name (64)**
      | - subnet
      | - type
      | - start-ip
      | - end-ip
```

#### Table 3: Command syntax notation (Continued)

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Curly braces { }</td>
<td>A word or series of words that is constrained to a set of options delimited by either vertical bars or spaces. You must enter at least one of the options, unless the set of options is surrounded by square brackets [ ].</td>
</tr>
<tr>
<td>Options delimited by vertical bars</td>
<td>Mutually exclusive options. For example: {enable</td>
</tr>
<tr>
<td>Options delimited by spaces</td>
<td>Non-mutually exclusive options. For example: {http https ping snmp ssh telnet} indicates that you may enter all or a subset of those options, in any order, in a space-delimited list, such as: ping https ssh. <strong>Note:</strong> To change the options, you must re-type the entire list. For example, to add snmp to the previous example, you would type: ping https snmp ssh. If the option adds to or subtracts from the existing list of options, instead of replacing it, or if the list is comma-delimited, the exception will be noted.</td>
</tr>
</tbody>
</table>
|- fqdn (256)
|- cache-ttl (0,86400)
|- wildcard
|- comment (64 xss)
|- associated-interface (16)
  + color (0,32)

Note that the tree command output also shows the number of characters allowed for other firewall address name settings. For example, the fully-qualified domain name (fqdn) field can contain up to 256 characters.

**Entering numeric values**

Numeric values are used to configure various sizes, rates, numeric addresses, or other numeric values. For example, a static routing priority of 10, a port number of 8080, or an IP address of 10.10.10.1. Numeric values can be entered as a series of digits without spaces or commas (for example, 10 or 64400), in dotted decimal format (for example the IP address 10.10.10.1) or as in the case of MAC or IPv6 addresses separated by colons (for example, the MAC address 00:09:0F:B7:37:00). Most numeric values are standard base-10 numbers, but some fields (again such as MAC addresses) require hexadecimal numbers.

Most web-based manager numeric value configuration fields limit the number of numeric digits that you can add or contain extra information to make it easier to add the acceptable number of digits and to add numbers in the allowed range. CLI help includes information about allowed numeric value ranges. Both the web-based manager and the CLI prevent you from entering invalid numbers.

**Selecting options from a list**

If a configuration field can only contain one of a number of selected options, the web-based manager and CLI present you a list of acceptable options and you can select one from the list. No other input is allowed. From the CLI you must spell the selection name correctly.

**Enabling or disabling options**

If a configuration field can only be on or off (enabled or disabled) the web-based manager presents a check box or other control that can only be enabled or disabled. From the CLI you can set the option to enable or disable.

**Registering your Fortinet product**

Before you begin configuring and customizing features, take a moment to register your Fortinet product at the Fortinet Technical Support web site, https://support.fortinet.com.

Many Fortinet customer services, such as firmware updates, technical support, and FortiGuard Antivirus and other FortiGuard services, require product registration.

For more information, see the Fortinet Knowledge Center article [Registration Frequently Asked Questions](https://support.fortinet.com).

**Fortinet products End User License Agreement**

See the [Fortinet products End User License Agreement](https://support.fortinet.com)
Training

Fortinet Training Services provides courses that orient you quickly to your new equipment, and certifications to verify your knowledge level. Fortinet provides a variety of training programs to serve the needs of our customers and partners world-wide.

To learn about the training services that Fortinet provides, visit the Fortinet Training Services web site at http://campus.training.fortinet.com, or email training@fortinet.com.

Documentation

The Fortinet Technical Documentation web site, http://docs.fortinet.com, provides the most up-to-date versions of Fortinet publications, as well as additional technical documentation such as technical notes.

In addition to the Fortinet Technical Documentation web site, you can find Fortinet technical documentation on the Fortinet Tools and Documentation CD, and on the Fortinet Knowledge Center.

Fortinet Tools and Documentation CD

Many Fortinet publications are available on the Fortinet Tools and Documentation CD shipped with your Fortinet product. The documents on this CD are current at shipping time. For current versions of Fortinet documentation, visit the Fortinet Technical Documentation web site, http://docs.fortinet.com.

Fortinet Knowledge Base

The Fortinet Knowledge Base provides additional Fortinet technical documentation, such as troubleshooting and how-to-articles, examples, FAQs, technical notes, a glossary, and more. Visit the Fortinet Knowledge Base at http://kb.fortinet.com.

Comments on Fortinet technical documentation

Please send information about any errors or omissions in this or any Fortinet technical document to techdoc@fortinet.com.

Customer service and technical support

Fortinet Technical Support provides services designed to make sure that your Fortinet products install quickly, configure easily, and operate reliably in your network.

To learn about the technical support services that Fortinet provides, visit the Fortinet Technical Support web site at https://support.fortinet.com.

You can dramatically improve the time that it takes to resolve your technical support ticket by providing your configuration file, a network diagram, and other specific information. For a list of required information, see the Fortinet Knowledge Base article FortiGate Troubleshooting Guide - Technical Support Requirements.
Introduction to authentication

Identifying users and other computers—authentication—is a key part of network security. This section describes some basic elements and concepts of authentication.

The following topics are included in this section:

- What is authentication?
- Means of authentication
- Types of authentication
- User’s view of authentication
- FortiGate administrator’s view of authentication

What is authentication?

Authentication is the act of confirming the identity of a person or other entity. In the context of a private computer network, the identities of users or host computers must be established to ensure that only authorized parties can access the network. The FortiGate unit provides network access control and applies authentication to users of firewall policies and VPN clients.

Means of authentication

FortiGate unit authentication is divided into two basic types: password authentication for people and certificate authentication for hosts or endpoints. An exception to this is that FortiGate units in an HA cluster and FortiManager units use password authentication.

Password authentication verifies individual user identities, but access to network resources is based on membership in user groups. For example, a firewall policy can be configured to permit access only to the members of one or more user groups. Any user who attempts network access through that policy is then authenticated through a request for their user name and password.

Local password authentication

The simplest authentication is based on user accounts stored locally on the FortiGate unit. For each account, a user name and password is stored. The account also has a disable option so that you can suspend the account without deleting it.

Local user accounts work well for a single-FortiGate installation. If your network has multiple FortiGate units that will use the same accounts, the use of an external authentication server can simplify account configuration and maintenance.

You create local user accounts in the web-based manager under User > User. This page is also used to create accounts where an external authentication server stores and verifies the password.

Server-based password authentication

Using external LDAP, RADIUS, or TACACS+ authentication servers is desirable when multiple FortiGate units need to authenticate the same users, or where the FortiGate unit is added to a network that already contains an authentication server.
When you use an external authentication server to authenticate users, the FortiGate unit sends the user’s entered credentials to the external server. The password is encrypted. The server’s response indicates whether the supplied credentials are valid or not.

You must configure the FortiGate unit to access the external authentication servers that you want to use. The configuration includes the parameters that authenticate the FortiGate unit to the authentication server.

You can use external authentication servers in two ways:

- Create user accounts on the FortiGate unit, but instead of storing each user’s password, specify the server used to authenticate that user. As with accounts that store the password locally, you add these users to appropriate user groups.

- Add the authentication server to user groups. Any user who has an account on the server can be authenticated and have the access privileges of the FortiGate user group. Optionally, when an LDAP server is a FortiGate user group member, you can limit access to users who belong to specific groups defined on the LDAP server.

**Single Sign On authentication using FSAE**

“Single sign on” means that users logged on to a computer network are authenticated for access to network resources through the FortiGate unit without having to enter their user name and password again. The Fortinet Server Authentication Extension (FSAE) provides Single Sign On capability for:

- Microsoft Windows networks using either Active Directory or NTLM authentication
- Novell networks, using eDirectory

FSAE monitors user logons and sends the FortiGate unit the user name, IP address, and the list of Windows AD user groups to which the user belongs. When the user tries to access network resources, the FortiGate unit selects the appropriate firewall policy for the destination. If the user belongs to one of the permitted user groups, the connection is allowed.

For detailed information about FSAE, see “FSAE for integration with Windows AD or Novell” on page 57.

**Certificate-based authentication**

An RSA X.509 server certificate is a small file issued by a Certificate Authority (CA) that is installed on a computer or FortiGate unit to authenticate itself to other devices on the network. When one party on a network presents the certificate as authentication, the other party can validate that the certificate was issued by the CA. The identification is therefore as trustworthy as the Certificate Authority (CA) that issued the certificate.

To protect against compromised or misused certificates, CAs can revoke any certificate by adding it to a Certificate Revocation List (CRL). Certificate status can also be checked online using Online Certificate Status Protocol (OCSP).

RSA X.509 certificates are based on public-key cryptography, in which there are two keys: the private key and the public key. Data encrypted with the private key can be decrypted only with the public key and vice versa. As the names suggest, the private key is never revealed to anyone and the public key can be freely distributed. Encryption with the recipient’s public key creates a message that only the intended recipient can read. Encryption with the sender’s private key creates a message whose authenticity is proven because it can be decrypted only with the sender’s public key.

Server certificates contain a signature string encrypted with the CA’s private key. The CA’s public key is contained in a CA root certificate. If the signature string can be decrypted with the CA’s public key, the certificate is genuine.
Certificate authorities

A certificate authority can be:

- an organization, such as VeriSign Inc., that provides certificate services
- a software application, such as Microsoft Certificate Services or OpenSSH

For a company web portal or customer-facing SSL VPN, a third-party certificate service has some advantages. The CA certificates are already included in popular web browsers and customers trust the third-party. On the other hand, third-party services have a cost.

For administrators and for employee VPN users, the local CA based on a software application provides the required security at low cost. You can generate and distribute certificates as needed. If an employee leaves the organization, you can simply revoke their certificate.

Certificates for users

FortiGate unit administrators and SSL VPN users can install certificates in their web browsers to authenticate themselves. If the FortiGate unit uses a CA-issued certificate to authenticate itself to the clients, the browser will also need the appropriate CA certificate.

FortiGate IPsec VPN users can install server and CA certificates according to the instructions for their IPsec VPN client software. The FortiClient Endpoint Security application, for example, can import and store the certificates required by VPN connections.

FortiGate units are also compatible with some Public Key Infrastructure systems. For an example of this type of system, see “RSA/ACE (SecurID) servers” on page 37.

Two-factor authentication

Optionally, you can require both a certificate and user name/password authentication. Certificates are installed on the user’s computer. Also requiring a password protects against unauthorized use of that computer. Two-factor authentication is available for PKI users. For more information, see “Two-factor authentication” on page 42.

Types of authentication

Authentication applies to several FortiGate features:

- firewall policies (identity-based policies)
- VPNs

Firewall authentication (or Identity-based policies)

Firewall policies enable traffic to flow between network interfaces. If you want to limit which users have access to particular resources, you create identity-based firewall policies that allow access only to members of specific user groups. Authentication, a request for user name and password, is triggered when a user attempts to access a resource for which data must pass through an identity-based firewall policy.

The user’s authentication expires if the connection is idle for too long. The Authentication Timeout setting is in User > Authentication. It has a default timeout of 30 minutes.
FortiGuard Web Filter override authentication

Optionally, users can be allowed the privilege of overriding FortiGuard Web Filtering to view blocked web sites. Depending on the override settings, the override can apply to the user who requested it, the entire user group to which the user belongs, or all users who share the same web filter profile. As with other FortiGate features, access to FortiGuard overrides is controlled through user groups. Firewall and Directory Services user groups are eligible for the override privilege. For more information about web filtering and overrides, see the UTM chapter of this FortiOS Handbook.

VPN authentication

In IPsec VPNs, there is authentication of the peer device and optionally of the peer user.

Authenticating IPsec VPN peers (devices)

The simplest way for IPsec VPN peers to authenticate each other is through the use of a preshared key, sometimes also called a shared secret. The preshared key is a text string used to encrypt the data exchanges that establish the VPN tunnel. The tunnel cannot be established if the two peers do not use the same key. The disadvantage of preshared key authentication is that it can be difficult to securely distribute and update the preshared keys.

RSA X.509 certificates are a better way for VPN peers to authenticate each other. Each peer offers a certificate signed by a Certificate Authority (CA) which the other peer can validate with the appropriate CA root certificate. For more information about certificates, see “Certificate-based authentication” on page 85.

You can supplement either preshared key or certificate authentication by requiring the other peer to provide a specific peer ID value. The peer ID is a text string configured on the peer device. On a FortiGate peer or FortiClient Endpoint Security peer, the peer ID provided to the remote peer is called the Local ID.

Authenticating IPsec VPN users

An IPsec VPN can be configured to accept connections from multiple dynamically addressed peers. You would do this to enable employees to connect to the corporate network while traveling or from home. On a FortiGate unit, you create this configuration by setting the Remote Gateway to Dialup User.

It is possible to have an IPsec VPN in which remote peer devices authenticate using a common preshared key or a certificate, but there is no attempt to identify the user at the remote peer. To add user authentication, you can do one of the following:

• require a unique preshared key for each peer
• require a unique peer ID for each peer
• require a unique peer certificate for each peer
• require additional user authentication (XAuth)

The peer ID is a text string configured on the peer device. On a FortiGate peer or FortiClient Endpoint Security peer, the peer ID provided to the remote peer is called the Local ID.

Authenticating SSL VPN users

SSL VPN users can be

• user accounts with passwords stored on the FortiGate unit
• user accounts authenticated by an external RADIUS, LDAP or TACACS+ server
• PKI users authenticated by certificate

You need to create a user group for your SSL VPN. Simply create a firewall user group, enable SSL VPN access for the group, and select the web portal the users will access. SSL VPN access requires an SSL VPN firewall policy that permits access to members of your user group.

Authenticating PPTP and L2TP VPN users

PPTP and L2TP are older VPN tunneling protocols that do not provide authentication themselves. FortiGate units restrict PPTP and L2TP access to users who belong to one specified user group. Users authenticate themselves to the FortiGate unit by username/password. You can configure PPTP and L2TP VPNs only in the CLI. Before you configure the VPN, create a firewall user group and add to it the users who are permitted to use the VPN. Users are authenticated when they attempt to connect to the VPN. For more information about configuring PPTP or L2TP VPNs, see the FortiGate CLI Reference.

User’s view of authentication

The user sees a request for authentication when they try to access a protected resource. The way in which the request is presented to the user depends on the method of access to that resource.

VPN authentication usually controls remote access to a private network.

Web-based user authentication

Firewall policies usually control browsing access to an external network that provides connection to the Internet. In this case, the Fortinet unit requests authentication through the web browser:

Figure 2: Authentication challenge through a web browser

The user types a user name and password and then selects Continue or Login. If the credentials are incorrect, the authentication screen is redisplayed with blank fields so that the user can try again. When the user enters valid credentials, they get access to the required resource. In some cases, if a user tries to authenticate several times without success, a message appears, such as: “Too many bad login attempts. Please try again in a few minutes.”
VPN client-based authentication

A VPN provides remote clients with access to a private network for a variety of services that include web browsing, email, and file sharing. A client program such as FortiClient negotiates the connection to the VPN and manages the user authentication challenge from the Fortinet unit.

FortiClient can store the user name and password for a VPN as part of the configuration for the VPN connection and pass them to the FortiGate unit as needed. Or, FortiClient can request the user name and password from the user when the FortiGate unit requests them.

Figure 3: FortiClient application request for user name and password

SSL VPN is a form of VPN that can be used with a standard Web browser. There are two modes of SSL VPN operation (supported in NAT/Route mode only):

- web-only mode, for remote clients equipped with a web-browser only
- tunnel mode, for remote computers that run a variety of client and server applications.

Note: After a defined period of user inactivity on the VPN connection (the idle timeout, defined by the FortiGate administrator), the user’s access expires. The default is 30 minutes. To access the resource, the user will have to authenticate again.

FortiGate administrator’s view of authentication

Authentication is based on user groups. The FortiGate administrator configures authentication for firewall policies and VPN tunnels by specifying the user groups whose members can use the resource. Some planning is required to determine how many different user groups need to be created. Individual user accounts can belong to multiple groups, making allocation of user privileges very flexible.

A member of a user group can be:

- a user whose user name and password are stored on the Fortinet unit
- a user whose name is stored on the Fortinet unit and whose password is stored on a remote or external authentication server

Note: After a defined period of user inactivity (the authentication timeout, defined by the FortiGate administrator), the user’s access expires. The default is 5 minutes. To access the resource, the user will have to authenticate again.
a remote or external authentication server with a database that contains the user name and password of each person who is permitted access

The general process of setting up authentication is as follows:

1. If remote or external authentication is needed, configure the required servers.
2. Configure local and peer (PKI) user identities. For each local user, you can choose whether the Fortinet unit or a remote authentication server verifies the password. Peer members can be included in user groups for use in firewall policies.
3. Create user groups.
   Add local/peer user members to each user group as appropriate. You can also add an authentication server to a user group. In this case, all users in the server’s database can authenticate. You can only configure peer user groups through the CLI.
4. Configure firewall policies and VPN tunnels that require authenticated access.
Authentication servers

Fortinet units support the use of external authentication servers. An authentication server can provide password checking for selected Fortinet users or it can be added as a member of a Fortinet user group. If you are going to use authentication servers, you must configure the servers before you configure Fortinet users or user groups that require them.

This section includes the following topics:

• RADIUS servers
• LDAP servers
• TACACS+ servers
• Directory Service servers
• RSA/ACE (SecurID) servers

RADIUS servers

Remote Authentication and Dial-in User Service (RADIUS) servers provide authentication, authorization, and accounting functions. Fortinet units use the authentication and accounting functions of the RADIUS server.

Your RADIUS server listens on either port 1812 or port 1645 for authentication requests. You must configure it to accept the Fortinet unit as a client.

The RADIUS server user database can be any combination of:

• user names and passwords defined in a configuration file
• an SQL database
• user account names and passwords configured on the computer where the RADIUS server is installed.

The RADIUS server uses a “shared secret” key to encrypt information passed between it and clients such as the Fortinet unit.

The Fortinet unit sends the following RADIUS attributes:

1. Acct-Session-ID
2. User Name
3. NAS-Identifier (FGT hostname)
4. Framed-IP-Address (IP address assigned to the client)
5. Fortinet-VSA (IP address client is connecting from)
6. Acct-Input-Octets
7. Acct-Output-Octets

Table 4 describes the supported authentication events and the RADIUS attributes that are sent in the RADIUS accounting message.
In order to support vendor-specific attributes (VSA), the RADIUS server requires a dictionary to define what the VSAs are. Fortinet’s dictionary is configured this way:

```plaintext
##
Fortinet’s VSA’s
#
VENDOR fortinet 12356
BEGIN-VENDOR fortinet
ATTRIBUTE Fortinet-Group-Name 1 string
ATTRIBUTE Fortinet-Client-IP-Address 2 ipaddr
ATTRIBUTE Fortinet-Vdom-Name 3 string
#
# Integer Translations
#
END-VENDOR Fortinet
```

See the documentation provided with your RADIUS server for configuration details.

### Configuring the Fortinet unit to use a RADIUS server

To configure the Fortinet unit to use a RADIUS server, you need to know the server’s domain name or IP address and its shared secret key. The maximum number of remote RADIUS servers that can be configured for authentication is 10.

On the Fortinet unit, the default port for RADIUS traffic is 1812. If your RADIUS server is using port 1645, you can either:

- Reconfigure the RADIUS server to use port 1812. See your RADIUS server documentation for more information.
- Change the Fortinet unit default RADIUS port to 1645 using the CLI:

  ```
  config system global
  set radius_port 1645
  end
  ```

To configure the Fortinet unit for RADIUS authentication - web-based manager

1. Go to `User > Remote > RADIUS` and select `Create New.`
2. Enter a name for the RADIUS server.
3. In `Primary Server Name/IP`, enter the domain name or IP address of the RADIUS server.

### Table 4: RADIUS attributes sent in RADIUS accounting message

<table>
<thead>
<tr>
<th>AUTHENTICATION METHOD</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>XAuth of IPsec (without DHCP)</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>XAuth of IPsec (with DHCP)</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PPTP/L2TP (in PPP)</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>SSL-VPN</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

In order to support vendor-specific attributes (VSA), the RADIUS server requires a dictionary to define what the VSAs are.
4  In **Primary Server Secret**, enter the server secret key.

5  Optionally, enter the information for a secondary RADIUS server in the **Secondary Server Name/IP** and **Secondary Server Secret** fields.

6  Select the **Authentication Scheme**.

   *Use Default Authentication Scheme* will usually work. Or, you can select **Specify Authentication Protocol** and select the protocol your RADIUS server requires.

7  Select **OK**.

To configure the Fortinet unit for RADIUS authentication - CLI example

```
config user radius
edit ourRADIUS
   set auth-type auto
   set server 10.11.102.100
   set secret aoewmntiasf
end
```

For more information about RADIUS server options, refer to the *FortiGate CLI Reference*.

## LDAP servers

Lightweight Directory Access Protocol (LDAP) is an Internet protocol used to maintain authentication data that may include departments, people, groups of people, passwords, email addresses, and printers. An LDAP consists of a data-representation scheme, a set of defined operations, and a request/response network.

The scale of LDAP servers ranges from big public servers such as BigFoot and Infospace, to large organizational servers at universities and corporations, to small LDAP servers for workgroups. This document focuses on the institutional and workgroup applications of LDAP.

A directory is a set of objects with similar attributes organized in a logical and hierarchical way. Generally, an LDAP directory tree reflects geographic and/or organizational boundaries, with the Domain name system (DNS) names to structure the top level of the hierarchy. The common name identifier for most LDAP servers is **cn**, however some servers use other common name identifiers such as **uid**.

If you have configured LDAP support and a user is required to authenticate using an LDAP server, the Fortinet unit contacts the LDAP server for authentication. To authenticate with the Fortinet unit, the user enters a user name and password. The Fortinet unit sends this user name and password to the LDAP server. If the LDAP server can authenticate the user, the user is successfully authenticated with the Fortinet unit. If the LDAP server cannot authenticate the user, the connection is refused by the Fortinet unit.

Binding is the step where the LDAP server authenticates the user, and if the user is successfully authenticated, allows the user access to the LDAP server based on that user's permissions.

The Fortinet unit can be configured to use one of three types of binding:

- anonymous - bind using anonymous user search
- regular - bind using user name/password and then search
- simple - bind using a simple password authentication without a search
You can use simple authentication if the user records all fall under one dn. If the users are under more than one dn, use the anonymous or regular type, which can search the entire LDAP database for the required user name.

If your LDAP server requires authentication to perform searches, use the regular type and provide values for user name and password.

The Fortinet unit supports LDAP protocol functionality defined in RFC 2251: Lightweight Directory Access Protocol v3, for looking up and validating user names and passwords. Fortinet LDAP supports all LDAP servers compliant with LDAP v3. In addition, Fortinet LDAP supports LDAP over SSL/TLS, which can be configured only in the CLI. To configure SSL/TLS authentication, refer to the Fortinet CLI Reference.

Fortinet LDAP does not support proprietary functionality, such as notification of password expiration, which is available from some LDAP servers. Fortinet LDAP does not supply information to the user about why authentication failed.

To configure your Fortinet unit to work with an LDAP server, you need to understand the organization of the information on the server.

The top of the hierarchy is the organization itself. Usually this is defined as Domain Component (DC), a DNS domain. If the name contains a dot, such as “example.com”, it is written as two parts: “dc=example,dc=com”.

In this example, Common Name (CN) identifiers reside at the Organization Unit (OU) level, just below DC. The Distinguished Name (DN) is ou=People,dc=example,dc=com.

**Figure 4: LDAP object hierarchy**

```
  dc=example,dc=com
     ou=People
       cn=Alex User
         uid:auser
       cn:user2
         uid:userid2
       cn:usern
         uid:useridn
```

In addition to the DN, the Fortinet unit needs an identifier for the individual person. Although the Fortinet unit GUI calls this the Common Name (CN), the identifier you use is not necessarily CN. On some servers, CN is the full name of a person. It might be more convenient to use the same identifier used on the local computer network. In this example, User ID (UID) is used.

You need to determine the levels of the hierarchy from the top to the level that contains the identifier you want to use. This defines the DN that the Fortinet unit uses to search the LDAP database. Frequently used distinguished name elements include:

- pw (password)
- cn (common name)
- ou (organizational unit)
- o (organization)
- c (country)
One way to test this is with a text-based LDAP client program. For example, OpenLDAP includes a client, `ldapsearch`, that you can use for this purpose.

Enter the following at the command line:

```
ldapsearch -x '(objectclass=*)'
```

The output is lengthy, but the information you need is in the first few lines:

```
version: 2
#
# filter: (objectclass=*)
# requesting: ALL
#

dn: dc=example,dc=com
dc: example
objectClass: top
objectClass: domain

dn: ou=People,dc=example,dc=com
ou: People
objectClass: top
objectClass: organizationalUnit
...
dn: uid=auser,ou=People,dc=example,dc=com
uid: auser
cn: Alex User
```

**Configuring the Fortinet unit to use an LDAP server**

After you determine the common name and distinguished name identifiers and the domain name or IP address of the LDAP server, you can configure the server on the Fortinet unit. The maximum number of remote LDAP servers that can be configured for authentication is 10.

**To configure the Fortinet unit for LDAP authentication - web-based manager**

1. Go to User > Remote > LDAP and select Create New.

   ![Figure 5: Configure Fortinet unit for LDAP authentication](image)

2. Enter a name for the LDAP server.

3. In Server Name/IP enter the server’s FQDN or IP address.

4. If the server does not use port 389, enter the port number in the Server Port field.
5 Enter the Common Name Identifier (20 characters maximum).
   \textit{cn} is the default, and is used by most LDAP servers.

6 In the Distinguished Name field, enter the base distinguished name for the server using the correct X.500 or LDAP format.
   The FortiGate unit passes this distinguished name unchanged to the server. The maximum number of characters is 512.
   If you don’t know the distinguished name, leave the field blank and select the Query icon to the right of the field. For more information, see the “Using the Query icon” on page 29.

7 In \textit{Bind Type}, select \textit{Regular}.

8 In \textit{User DN}, enter the LDAP administrator’s distinguished name.

9 In \textit{Password}, enter the LDAP administrator’s password.

10 Select \textit{OK}.
   For detailed information about configuration options for LDAP servers, see the online Help on your FortiGate unit.

To configure the Fortinet unit for LDAP authentication - CLI example

\begin{verbatim}
config user ldap
edit ourLDAPsrv
   set server 10.11.101.160
   set cnid cn
   set dn cn=users,dc=office,dc=example,dc=com
   set type regular
   set username cn=administrator,cn=users,dc=office,dc=example,dc=com
   set password w5AiGVMLkgPQ
end
\end{verbatim}

Using the Query icon

The LDAP Distinguished Name Query list displays the LDAP directory tree for the LDAP server connected to the FortiGate unit. This helps you to determine the appropriate entry for the DN field. To see the distinguished name associated with the Common Name identifier, select the Expand icon next to the CN identifier. Select the DN from the list. The DN you select is displayed in the Distinguished Name field. Select OK and the Distinguished Name you selected will be saved in the Distinguished Name field of the LDAP Server configuration.

To see the users within the LDAP Server user group for the selected Distinguished Name, expand the Distinguished Name in the LDAP Distinguished Name Query tree.
In recent years, remote network access has shifted from terminal access to LAN access. Users are now connecting to their corporate network remotely with computers that utilize complete network connections. Remote node technology allows users the same level of access to the corporate network resources as they would have if they were physically in the office. When users connect to their corporate network remotely, they do so through a remote access server. As remote access technology has evolved, the need for network access security has become increasingly important. This need can be filled using a Terminal Access Controller Access-Control System (TACACS+) server.

Terminal Access Controller Access-Control System (TACACS+) is a remote authentication protocol that provides access control for routers, network access servers, and other networked computing devices via one or more centralized servers. TACACS+ allows a client to accept a user name and password and send a query to a TACACS+ authentication server. The server host determines whether to accept or deny the request and sends a response back that allows or denies network access to the user.
There are several different authentication protocols that TACACS+ can use during the authentication process:

- **ASCII**
  Machine-independent technique that uses representations of English characters. Requires user to type a user name and password that are sent in clear text (unencrypted) and matched with an entry in the user database stored in ASCII format.

- **PAP (password authentication protocol)**
  Used to authenticate PPP connections. Transmits passwords and other user information in clear text.

- **CHAP (challenge-handshake authentication protocol)**
  Provides the same functionality as PAP, but is more secure as it does not send the password and other user information over the network to the security server.

- **MS-CHAP (Microsoft challenge-handshake authentication protocol v1)**
  Microsoft-specific version of CHAP.

The default protocol configuration, Auto, uses PAP, MS-CHAP, and CHAP, in that order.

### Configuring the Fortinet unit to use a TACACS+ authentication server

The maximum number of remote TACACS+ servers that can be configured for authentication is 10.

**To configure the Fortinet unit for TACACS+ authentication - web-based manager**

1. Go to *User > Remote > TACACS* and select *Create New*.
2. Enter the following information, and select *OK*.

### Figure 7: TACACS+ server configuration

<table>
<thead>
<tr>
<th>Name</th>
<th>Enter the name of the TACACS+ server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Name/IP</td>
<td>Enter the server domain name or IP address of the TACACS+ server.</td>
</tr>
<tr>
<td>Server Key</td>
<td>Enter the key to access the TACACS+ server.</td>
</tr>
<tr>
<td>Authentication Type</td>
<td>Select the authentication type to use for the TACACS+ server. <em>Auto</em> tries PAP, MSCHAP, and CHAP (in that order).</td>
</tr>
</tbody>
</table>

### To configure the Fortinet unit for TACACS+ authentication - CLI

```bash
config user tacacs+
edit <server_name>
  set auth-type {ascii | auto | chap | ms_chap | pap}
  set key <server_key>
  set tacacs+-port <tacacs+_port_num>
  set server <domain>
end
```
Directory Service servers

Novell and Microsoft Windows networks provide user authentication based on directory services: eDirectory for Novell, Active Directory for Windows. Users can log on at any computer in the domain and have access to resources as defined in their user account. The Fortinet Server Authentication Extension (FSAE) enables FortiGate units to authenticate these network users for firewall policy or VPN access without asking them for their user name and password.

When a user logs in to the Windows or Novell domain, FSAE sends the FortiGate unit the user’s IP address and the names of the user groups to which the user belongs. The FortiGate unit uses this information to maintain a copy of the domain controller user group database. Because the domain controller authenticates users, the FortiGate unit does not perform authentication. It recognizes group members by their IP address.

In the FortiGate Directory Services configuration, you specify the network computers where the FSAE collector agent is installed. The FortiGate unit retrieves the names of the Novell or Active Directory user groups. You cannot use these groups directly. You must define FortiGate user groups of the Directory Services type and then add the Novell or Active Directory user groups to them. The Directory Services user groups that you created can used in firewall policies and VPN configurations.

For more information about Directory Services and FSAE, see “FSAE for integration with Windows AD or Novell” on page 57.

RSA/ACE (SecurID) servers

SecurID is a one-time password system. The user carries a small device, a “token”, that generates and displays a password. The token is time-synchronized with the SecurID authentication server and the password changes about once per minute. To authenticate, users enter their User ID and the password currently displayed on the token.

To use SecurID with a FortiGate unit, you need to:

- configure the RSA ACE/Server and the RADIUS server to work with each other (refer to the RSA ACE/Server documentation)
- configure the FortiGate unit as an Agent Host within the RSA ACE/Server database
- configure the FortiGate unit to access the RADIUS server
- create a FortiGate user group for SecurID users

The instructions provide here are based on RSA ACE/Server version 5.1.

To configure the FortiGate unit as an Agent Host on the RSA ACE/Server

1. On the RSA ACE/Server computer, go to Start > Programs > RSA ACE/Server, and then Database Administration - Host Mode.
2. On the Agent Host menu, select Add Agent Host.
3. In the Name field, enter a name for the FortiGate unit.
4. In the Network address field, enter the FortiGate unit IP address.
5. Select Secondary Nodes and define all hostname/IP addresses that resolve to the FortiGate unit.
If needed, refer to the RSA ACE/Server documentation for more information.

**To configure the FortiGate unit to use the RADIUS server**

1. Go to User > Remote > RADIUS and select Create New.
2. In the Name field, enter a name for the RADIUS server.
3. In the Primary Server Name/IP and Primary Server Secret fields, enter the appropriate information about the RADIUS server you configured for use with SecurID.
4. Select OK.

**To create a SecurID user group**

2. Select Create New.
3. In the Name field, enter a name for the group.
4. In the Available Users/Groups list, select the RADIUS server you configured for use with SecurID.
5. Select the right arrow button to move the selected server to the Members list.
6. Select OK.

**Using the SecurID user group for authentication**

You can use the SecurID user group in several FortiGate features that authenticate by user group:

**Firewall policy**

Select Enable Identity Based Policy and then select Add. Add the SecurID user group to the Selected User Groups list. Set other options as desired and select OK.

**IPsec VPN XAuth**

In the Phase 1 Advanced settings, in the XAuth section, select Enable as Server and choose the SecurID user group.

**PPTP VPN**

PPTP VPN is configured in the CLI. In the PPTP configuration (config vpn pptp), set usrgrp to the SecurID user group.

**SSL VPN**

In the SecurID user group, select the appropriate web portal for these users. In the firewall policy for the SSL VPN, include the SecurID user group in the list of selected user groups.
Users and user groups

FortiGate authentication controls system access by user group. By assigning individual users to the appropriate user groups you can control each user’s access to network resources. The members of user groups are user accounts, of which there are several types. Local users and peer users are defined on the FortiGate unit. User accounts can also be defined on external authentication servers.

This section describes how to configure local users and peer users and then how to configure user groups. For information about configuration of authentication servers see “Authentication servers” on page 29.

This section contains the following topics:

- Users
- User groups

Users

A user is a user account consisting of user name, password, and in some cases other information, configured on the Fortinet unit or on an external authentication server. Users can access resources that require authentication only if they are members of an allowed user group. There are several different types of user accounts with slightly different methods of authentication:

Table 5: How the FortiGate unit authenticates different types of users

<table>
<thead>
<tr>
<th>User type</th>
<th>Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local user with password stored on the Fortinet unit</td>
<td>The user name and password must match a user account stored on the Fortinet unit.</td>
</tr>
<tr>
<td>Local user with password stored on an authentication server</td>
<td>The user name must match a user account stored on the Fortinet unit and the user name and password must match a user account stored on the authentication server. On the external authentication server, there may be user groups to which users can be assigned. These groups exist independently of FortiGate unit user groups.</td>
</tr>
<tr>
<td>Authentication server user</td>
<td>A FortiGate user group can include user accounts that exist on an external authentication server or particular user groups on that server. Any of the included users can authenticate and get access to the resources permitted to the FortiGate user group.</td>
</tr>
<tr>
<td>Directory Services user</td>
<td>By using the Fortinet Server Authentication Extension (FSAE), users on a Microsoft Windows or Novell network can use their network authentication to access resources through the FortiGate unit. Access is controlled through Directory Services user groups which contain Windows or Novell user groups as their members.</td>
</tr>
<tr>
<td>Peer user with certificate authentication</td>
<td>A peer user is a digital certificate holder that authenticates using a client certificate. No password is required, unless two-factor authentication is enabled.</td>
</tr>
</tbody>
</table>
Creating local users

To define a local user you need:

- a user name
- a password or the name of the authentication server that contains the user account

If the user is authenticated externally, the user name on the Fortinet unit must be identical to the user name on the authentication server.

To create a local user - web-based manager

1. Go to User > User and select Create New.

2. Enter the user name in the User Name field.

3. Do one of the following:
   - To authenticate this user locally, select Password and type a password. The password should be at least six characters long.
   - To authenticate this user using an external authentication server, select the Match user option for the appropriate type of server and select the server name.

   If you want to use an authentication server, you must configure access to it first. See “Authentication servers” on page 29.

4. Select OK.

To create a local user - CLI examples

Locally authenticated user

```
config user local
edit user1
   set type password
   set passwd ljt_pj2gpepfdw
end
```

User authenticated on an LDAP server

```
config user local
edit user2
   set type ldap
   set ldap_server ourLDAPsrv
end
```

User authenticated on a RADIUS server

```
config user local
edit user3
   set type radius
```
Users and user groups

```
set radius_server ourRADIUSsrv
end
```

User authenticated on a TACACS+ server
```
config user local
edit user4
    set type tacacs+
    set tacacs+_server ourTACACS+srv
end
```

To remove a user from the Fortinet unit configuration - web-based manager
1. Go to User > User.

Figure 9: Local user list

<table>
<thead>
<tr>
<th></th>
<th>User Name</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>user2</td>
<td>LOCAL</td>
</tr>
<tr>
<td>2</td>
<td>user3</td>
<td>LOCAL</td>
</tr>
<tr>
<td>3</td>
<td>user4</td>
<td>LOCAL</td>
</tr>
</tbody>
</table>

2. Select the check box of the user that you want to remove.
3. Select Delete.
4. Select OK.

Note: You cannot remove a user that belongs to a user group. Remove the user from the user group first.

To remove a user from the FortiGate unit configuration - CLI example
```
config user local
    delete user4444
end
```

Creating PKI or peer users

A PKI or peer user is a digital certificate holder. A PKI user account on the FortiGate unit contains the information required to determine which CA certificate to use to validate the user’s certificate. Peer users can be included in firewall user groups or peer certificate groups used in IPsec VPNs.

To define a peer user you need:

- a peer user name
- the text from the subject field of the user’s certificate, or the name of the CA certificate used to validate the user’s certificate

Note: The configuration page for PKI users in the web-based manager is not available unless there is at least one peer user defined. Follow the CLI-based instructions to create the first peer user. Optionally, you can then log into the web-based manager to configure additional PKI (peer) users.
To create a peer user for PKI authentication - CLI example

```
config user peer
  edit peer1
    set subject E=peer1@mail.example.com
    set ca CA_Cert_1
  end
```

**Note:** If you create a PKI user in the CLI with no values in `subject` or `ca`, you will not be able to open the user’s record in the web-based manager. The CLI will prompt you to add a value in `Subject` (`subject`) or `CA` (`ca`).

To create a peer user for PKI authentication - web-based manager

1. Go to `User > PKI` and select `Create New`.

   ![Figure 10: PKI peer user configuration]

2. Enter the user name.
3. Fill in at least one of the following fields:
   - **Subject** The text string that appears in the Subject field of the user’s certificate.
   - **CA** Select the CA certificate that must be used to authenticate this peer user.
4. Select **OK**.

   There are other configuration settings that can be added or modified for PKI authentication. For example, you can configure the use of an LDAP server to check access rights for client certificates. For information about the detailed PKI configuration settings only available through the CLI, see the *FortiGate CLI Reference*.

**Two-factor authentication**

You can increase security by requiring both certificate and password authentication for PKI users. Certificates are installed on the user’s computer. Also requiring a password protects against unauthorized use of that computer.

To create a peer user with two-factor authentication - web-based manager

While configuring a peer user (see Figure 10, above), select **Require two-factor authentication** and enter a password.

To create a peer user with two-factor authentication - CLI example

```
config user peer
  edit peer1
    set subject E=peer1@mail.example.com
    set ca CA_Cert_1
  end
```
User groups

A user group is a list of user identities. An identity can be:

- a local user account (user name/password) stored on the Fortinet unit
- a local user account with the password stored on a RADIUS, LDAP, or TACACS+ server
- a PKI user account with digital client authentication certificate stored on the FortiGate unit
- a RADIUS, LDAP, or TACACS+ server, optionally specifying particular user groups on that server
- a user group defined on a Directory Service server.

Identity-based firewall policies and some types of VPN configurations allow access only to specified user groups.

In most cases, the Fortinet unit authenticates users by requesting their user name and password. The Fortinet unit checks local user accounts first. If a match is not found, the Fortinet unit checks the RADIUS, LDAP, or TACACS+ servers that belong to the user group. Authentication succeeds when a matching user name and password are found.

There are two types of FortiGate user group: Firewall and Directory Services.

Firewall user groups

A firewall user group can contain any type of user identity except a Directory Services group. When a user attempts to access resources controlled by an identity-based firewall policy, the FortiGate unit requests authentication. If the user authenticates successfully and is a member of one of the permitted groups, the user’s session is allowed to proceed.

SSL VPN access

In any firewall user group, you can enable SSL VPN access and select the web-portal that the users can access. When the user connects to the FortiGate unit via HTTPS on the SSL VPN port (default 10443), the FortiGate unit requests a user name and password.

SSL VPN access also requires an SSL VPN firewall policy (Action is SSL VPN) with an identity-based rule enabling access for the user group. For more information, see the SSL VPN chapter of the FortiOS Handbook.

IPsec VPN access

A firewall user group can provide access for dialup users of an IPsec VPN. In this case, the IPsec VPN phase 1 configuration uses the Accept peer ID in dialup group peer option. The user’s VPN client is configured with the user name as peer ID and the password as pre-shared key. The user can connect successfully to the IPsec VPN only if the user name is a member of the allowed user group and the password matches the one stored on the Fortinet unit.

Note: A user group cannot be a dialup group if any member is authenticated using an external authentication server.
Configuring a firewall user group

A user group can contain:

- local users, whether authenticated by the FortiGate unit or an authentication server
- PKI users
- authentication servers, optionally specifying particular user groups on the server

To create a Firewall user group - web-based manager

1. Go to User > User Group and select Create New.

2. Enter a name for the user group.

3. In Type, select Firewall.

4. From the Available Users/Groups list, select users and then select the right arrow button to move the names to the Members list.

   If you select an authentication server as a group member, by default all user accounts on the authentication server are members of this FortiGate user group. Follow steps 5 through 8 if you want to include only specific user groups from the authentication server. Otherwise, select OK.

5. Select Add.

6. From the Remote Server list, select the authentication server.

   Only servers that are already members of this user group are available.

7. In the Group Name field, enter the group name in the appropriate format for the type of server.

   For example, an LDAP server requires LDAP format, such as:
   
   cn=users, dn=office, dn=example, dn=com

8. Repeat steps 5 through 7 to add all the authentication server user groups that are required.

9. Select OK.
To create a firewall user group - CLI example

In this example, the members of group01 are User1 and all of the members of usergroup1 on RADIUSsrvr2.

```
config user group
edit group01
    set group-type firewall
    set member User1 RADIUSsrvr2
config match
edit 0
    set server-name RADIUSsrvr2
    set group-name usergroup1
end
end
```

**Note:** Matching user group names from an external authentication server might not work if the list of group memberships for the user is longer than 8000 bytes. Group names beyond this limit are ignored.

For more information about user group CLI commands, see the *Fortinet CLI Guide*.

**Directory Service user groups**

A Directory Service user group contains only Windows or Novell network user groups. No other user types are permitted as members. Information about the Windows or Novell user groups and the logon activities of their members is provided by the Fortinet Server Authentication Extension (FSAE) which is installed on the network domain controllers.

You can specify Directory Service user groups in identity-based firewall policies in the same way as you specify firewall user groups. Directory Service user groups cannot have SSL VPN or dialup IPsec VPN access.

For information about configuring Directory Services user groups, see “Creating Directory Service user groups” on page 81. For complete information about installing and configuring FSAE, see “FSAE for integration with Windows AD or Novell” on page 57.

**Configuring Peer user groups**

Peer user groups can only be configured using the CLI. Peers are digital certificate holders defined using the `config user peer` command. The peer groups you define here are used in dialup IPsec VPN configurations that accept RSA certificate authentication from members of a peer certificate group. For more information, see “Authenticating IPsec VPN users with security certificates” on page 95.

To create a peer group - CLI example

```
config user peergroup
edit vpn_peergroup1
    set member pki_user1 pki_user2 pki_user3
end
```
Viewing, editing and deleting user groups

To view the list of FortiGate user groups, go to User > User Group.

Figure 12: Example User group list

To edit a user group - web-based manager

2. Select the check box for the user group that you want to edit.
3. Select the Edit button.
4. Modify the user group as needed.
5. Select OK.

To edit a user group - CLI example

This example adds user3 to Group1. Note that you must re-specify the full list of users:

```
config user group
edit Group1
  set member user2 user4 user3
end
```

To remove a user group - web-based manager

2. Select the check box for the user group that you want to remove.
3. Select the Delete button.
4. Select OK.

To remove a user group - CLI example

```
config user group
delete Group2
end
```

Note: You cannot remove a user group that is part of a firewall policy. Remove it from the firewall policy first.
Configuring authenticated access

When you have configured authentication servers, users, and user groups, you are ready to configure firewall policies and certain types of VPNs to require user authentication. This section describes:

- Authentication timeout
- Authentication protocols
- Authentication in firewall policies
- VPN authentication

Authentication timeout

You set the firewall user authentication timeout to control how long an authenticated connection can be idle before the user must authenticate again. The maximum timeout is 480 minutes (8 hours).

To set the firewall authentication timeout
1. Go to User > User > Authentication.
2. Enter the Authentication Timeout value in minutes.
   - The default authentication timeout is 5 minutes.
3. Select Apply.

You set the SSL VPN user authentication timeout (Idle Timeout) to control how long an authenticated connection can be idle before the user must authenticate again. The maximum timeout is 28800 seconds. The default timeout is 300 seconds.

To set the SSL VPN authentication timeout
1. Go to VPN > SSL > Config.
2. Enter the Idle Timeout value (seconds).
3. Select Apply.

Password policy

Password authentication is effective only if the password is sufficiently strong and is changed periodically. By default, the FortiGate unit requires only that passwords be at least eight characters in length. You can set a password policy to enforce higher standards for both length and complexity of passwords. Password policies can apply to administrator passwords or IPsec VPN preshared keys.

To set a password policy in the web-based manager, go to System > Admin > Settings. In the CLI, use the config system password-policy command.

Password length

The default minimum password length on the FortiGate unit is eight characters, but up to 32 characters is permitted. Security experts suggest a minimum length of 14 characters.
Password complexity

Users usually create passwords composed of alphabetic characters and perhaps some numbers. Password policy can require the inclusion of upper case letters, lower case letters, numerals or punctuation characters.

Suggestions for users

In addition to length and complexity, there are security factors that cannot be enforced in a policy but should be encouraged through guidelines issued to users:

Avoid:
- words found in a dictionary of any language
- numeric sequences, such as "12345"
- sequences of adjacent keyboard characters, such as "qwerty"
- repeated characters
- personal information, such as your name, birthday, or telephone number

Include:
- one or more upper case characters
- one or more of the numerals
- one or more non alpha-numeric characters, such as punctuation marks

Authentication protocols

When user authentication is enabled on a firewall policy, the authentication challenge is normally issued for any of the four protocols, HTTP, HTTPS, FTP, and Telnet, which are dependent on the connection protocol. By making selections in the Protocol Support list, the user controls which protocols support the authentication challenge. The user must connect with a supported protocol first, so that they can subsequently connect with other protocols.

For example, if you have selected HTTP, FTP, or Telnet, a user name and password-based authentication occurs. The FortiGate unit then prompts network users to input their firewall user name and password. If you have selected HTTPS, certificate-based authentication (HTTPS, or HTTP redirected to HTTPS only) occurs.

For certificate-based authentication, you must install customized certificates on the FortiGate unit and on the browsers of network users. If you do not install certificates on the network user’s web browser, the network users may see an SSL certificate warning message and have to manually accept the default FortiGate certificate. The network user’s web browser may deem the default certificate as invalid.

When you use certificate authentication, if you do not specify any certificate when you create the firewall policy, the global settings are used. If you specify a certificate, the per-policy setting will overwrite the global setting. For more information about the use of certification authentication see "Certificate-based authentication" on page 85.

To set the authentication protocols

1. Go to User > User > Authentication.
2. In Protocol Support, select the required authentication protocols.
3. If using HTTPS protocol support, in Certificate, select a Local certificate from the drop-down list.
4. Select Apply.
Authenticating in firewall policies

Firewall policies control traffic between Fortinet interfaces, both physical interfaces and VLAN subinterfaces. Without authentication, a firewall policy enables access from one network to another for all users on the source network. Authentication enables you to allow access only for users who are members of selected user groups. To include authentication in a firewall policy, you must create an identity-based policy.

The style of the authentication method varies by the authentication protocol. If you have selected HTTP, FTP or Telnet, a user name and password-based authentication occurs. The Fortinet unit prompts network users to input their firewall user name and password. If you have selected HTTPS, certificate-based authentication (HTTPS or HTTP redirected to HTTPS only) occurs. You must install customized certificates on the Fortinet unit and on the browsers of network users, which the Fortinet unit matches.

**Note:** You can configure user authentication for firewall policies only when **Action** is set to **Accept**.

Configuring authentication for a firewall policy

To create an identity-based firewall policy,

1. Create users and one or more Firewall user groups.
   For more information, see "Users and user groups" on page 39.
2. Go to **Firewall > Policy > Policy**.
3. Select **Create New** to create a new policy or select an existing policy and the select the **Edit** icon.
4. Make sure that the **Action** for the policy is **ACCEPT**.
5. Select **Enable Identity Based Policy** and then select **Add**.
6 In the Available User Groups list, select the user groups that will be allowed to use this policy and then select the right arrow button to move them to the Selected User Groups list.

7 From from the Available Services list, select the services users will be allowed to access and then select the right arrow button to move them to the Selected Services list.

To enable use of all services, select the ANY service.

8 Set other options as required and then select OK.

Figure 15: Identity Based Policy list and options in firewall policy

9 If users will use a certificate for authentication, from the Certificate list select the CA certificate to use to validate the users’ certificates.
10 To require the user to accept a disclaimer to connect to the destination, select *Enable Disclaimer*. If the user is to be redirected after accepting the disclaimer, enter the URL in the *Redirect URL to* field.

You can edit the User Authentication Disclaimer replacement message text in *System > Config > Replacement Messages*.

11 Select *OK*.

### Configuring authenticated access to the Internet

A policy for accessing the Internet is similar to a policy for accessing a specific network, but the destination address is set to *all*. The destination interface is the one that connects to the Internet service provider. For general purpose Internet access, the Service is set to *ANY*.

Access to HTTP, HTTPS, FTP and Telnet sites may require access to a domain name service. DNS requests do not trigger authentication. You must configure a policy to permit unauthenticated access to the appropriate DNS server, and this policy must precede the policy for Internet access.

### VPN authentication

All VPN configurations require users to authenticate. Authentication based on user groups applies to:

- SSL VPNs
- PPTP and L2TP VPNs
- an IPsec VPN that authenticates users using dialup groups
- a dialup IPsec VPN that uses XAUTH authentication (Phase 1)

You must create user accounts and user groups before performing the procedures in this section. If you create a user group for dialup IPsec clients or peers that have unique peer IDs, their user accounts must be stored locally on the Fortinet unit. You cannot authenticate these types of users using a RADIUS or LDAP server.

### Configuring authentication of SSL VPN users

The general procedure for authenticating SSL VPN users is:

1. Configure user accounts.
2. Create one or more firewall user groups for SSL VPN users.
   
   See “Configuring user accounts and user groups for SSL VPN” in the SSL VPN chapter of this FortiOS Handbook.
3. Enable SSL VPN.
4. Optionally, set inactivity and authentication timeouts.
5. Configure a firewall policy with SSL VPN action. Add an identity-based rule to allow access for the user groups you created for SSL VPN users.
   
   See “Configuring firewall policies” in the SSL VPN chapter of this FortiOS Handbook.

### Configuring authentication timeout

By default, the SSL VPN authentication expires after 8 hours (28800 seconds). You can change it only in the CLI, and the time entered must be in seconds. For example, to change the timeout to one hour, you would enter:

```bash
config vpn ssl settings
```
When you configure the timeout settings, if you set the authentication timeout (auth-timeout) to 0, then the remote client does not have to re-authenticate again unless they log out of the system. To fully take advantage of this setting, the value for idle-timeout has to be set to 0 also, so that the client does not time out if the maximum idle time is reached. If the idle-timeout is not set to the infinite value, the system will log out if it reaches the limit set, regardless of the auth-timeout setting.

Configuring authentication of remote IPsec VPN users

An IPsec VPN on a Fortinet unit can authenticate remote users through a dialup group. The user account name is the peer ID and the password is the pre-shared key. For information about authentication using peer IDs and peer groups, see the Fortinet IPsec VPN User Guide.

Authentication through user groups is supported for groups containing only local users. To authenticate users using a RADIUS or LDAP server, you must configure XAUTH settings. See “Configuring XAuth authentication” on page 53.

To configure user group authentication for dialup IPsec - web-based manager

1. Configure the dialup users who are permitted to use this VPN. Create a user group with Type: Firewall and add them to it.
   
   For more information, see “Users and user groups” on page 39.

2. Go to VPN > IPsec > Auto Key (IKE), select Create Phase 1 and enter the following information.

   Figure 16: Configure VPN IPsec dialup authentication

<table>
<thead>
<tr>
<th>Name</th>
<th>Name for group of dialup users using the VPN for authentication.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Gateway</td>
<td>List of the types of remote gateways for VPN. Select Dialup User.</td>
</tr>
</tbody>
</table>
Configuring authenticated access

VPN authentication

Authentication Method
List of authentication methods available for users. Select Preshared Key and enter the preshared key.

Peer Options
Select Accept peer ID in dialup group. Select the user group that is to be allowed access to the VPN. The listed user groups contain only users with passwords on the Fortinet unit.

Note: The Accept peer ID in dialup group option does not support authentication of users through an authentication server. The user accounts must exist on the FortiGate unit.

3 Select Advanced to reveal additional parameters and configure other VPN gateway parameters as needed.

4 Select OK.

To configure user group authentication for dialup IPsec - CLI example

The peertype and usgrgp options configure user group based authentication.

```
config vpn ipsec phase1
edit office_vpn
set interface port1
set type dynamic
set psksecret yORRAzltNGhzgtV32jend
set proposal 3des-sha1 aes128-sha1
set peertype dialup
set usgrgp Group1
end
```

Configuring XAuth authentication

Extended Authentication (XAuth) increases security by requiring additional user authentication information in a separate exchange at the end of the VPN Phase 1 negotiation. The FortiGate unit asks the user for a user name and password. It then forwards the user's credentials (the password is encrypted) to an external RADIUS or LDAP server for verification.

XAuth can be used in addition to or in place of IPsec phase 1 peer options to provide access security through an LDAP or RADIUS authentication server. You must configure a dialup user group whose members are all externally authenticated. None of these users can have their passwords stored on the Fortinet unit.

To configure authentication for a dialup IPsec VPN - web-based manager

1 Configure the users who are permitted to use this VPN. Create a user group and add them to it.
   For more information, see "Users and user groups" on page 39.

2 Go to VPN > IPsec > Auto Key (IKE).

3 Select Create Phase 1 and configure the basic VPN phase1 settings.
   Remote Gateway must be Dialup User.

4 Select Advanced to reveal additional parameters and enter the following information.
   XAuth      Select Enable as Server.
Server Type

Select PAP, CHAP, or AUTO. Use CHAP whenever possible. Use PAP with all implementations of LDAP and with other authentication servers that do not support CHAP, including some implementations of Microsoft RADIUS. Use AUTO with the Fortinet Remote VPN Client and where the authentication server supports CHAP but the XAuth client does not.

User Group

Select the user group that is to have access to the VPN. The list of user groups does not include any group that has members whose password is stored on the Fortinet unit.

5 Select OK.

For more information about XAUTH configuration, see the IPsec VPN chapter of this FortiOS Handbook.

To configure authentication for a dialup IPsec VPN - CLI example

The xauthtype and authusrgrp fields configure XAuth authentication.

```fortigate-config
config vpn ipsec phase1
edit office_vpn
set interface port1
set type dynamic
set psksecret yORRAzltNGhzgtV32jend
set proposal 3des-sha1 aes128-sha1
set peertype dialup
set xauthtype pap
set authusrgrp Group1
end
```

Some parameters specific to setting up the VPN itself are not shown here. For detailed information about configuring an IPsec VPN, see the IPsec VPN chapter of this FortiOS Handbook.

Configuring authentication of PPTP VPN users and user groups

Configuration of a PPTP VPN is possible only through the CLI. You can configure user groups and firewall policies using either CLI or web-based manager.

To configure authentication for a PPTP VPN

1 Configure the users who are permitted to use this VPN. Create a firewall user group and add them to it.
   For more information, see "Users and user groups" on page 39.

2 Configure the PPTP VPN in the CLI as in this example.

```fortigate-config
config vpn pptp
set status enable
set sip 192.168.0.100
set eip 192.168.0.110
set usurgrp PPTP_Group
end
```

The sip and eip fields define a range of virtual IP addresses assigned to PPTP clients.

3 Configure a firewall policy. The source interface is the one through which the clients will connect. The source address is the PPTP virtual IP address range. The destination interface and address depend on the network to which the clients will connect. The policy action is ACCEPT.
Configuring authentication of L2TP VPN users/user groups

Configuration of a L2TP VPN is possible only through the CLI. You can configure user groups and firewall policies using either CLI or web-based manager.

To configure authentication for a PPTP VPN

1 Configure the users who are permitted to use this VPN. Create a firewall user group and add them to it.
   For more information, see "Users and user groups" on page 39.
2 Configure the L2TP VPN in the CLI as in this example.
   ```
   config vpn l2tp
   set status enable
   set sip 192.168.0.100
   set eip 192.168.0.110
   set usgrp L2TP_Group
   end
   ```
   The `sip` and `eip` fields define a range of virtual IP addresses assigned to L2TP clients.
3 Configure a firewall policy. The source interface is the one through which the clients will connect. The source address is the L2TP virtual IP address range. The destination interface and address depend on the network to which the clients will connect. The policy action is ACCEPT.
FSAE for integration with Windows AD or Novell

This chapter provides an overview of the Fortinet Server Authentication Extension (FSAE). The following topics are included:

- Introduction to FSAE
- Installing FSAE
- Configuring FSAE on Windows AD
- Configuring FSAE on FortiGate units
- Testing the configuration

Introduction to FSAE

The Fortinet Server Authentication Extension (FSAE) provides seamless authentication support for Microsoft Windows Active Directory and Novell eDirectory users in a FortiGate environment.

On a Microsoft Windows or Novell network, users authenticate with the Active Directory or Novell eDirectory at logon. It would be inconvenient if users then had to enter another user name and password for network access through the FortiGate unit. FSAE provides authentication information to the FortiGate unit so that users automatically get access to permitted resources.

There are several mechanisms for passing user authentication information to the FortiGate unit:

- FSAE software installed on a Novell network monitors user logons and sends the required information to the FortiGate unit. The FSAE software can obtain information from the Novell eDirectory using either the Novell API or LDAP.
- FSAE software installed on a Windows AD network monitors user logons and sends the required information to the FortiGate unit. The FSAE software can obtain this information by polling the domain controllers or by using an agent on each domain controller that monitors user logons in real time. Optionally, a FortiGate unit running FortiOS 3.0 MR6 or later can obtain group information directly from the AD using Lightweight Directory Access Protocol (LDAP).
- On a Windows AD network, the FSAE software can also serve NTLM requests coming from client browsers (forwarded by the FortiGate unit).

Using FSAE in a Windows AD environment

FSAE installed in a Windows AD environment can provide two kinds of services:

- Monitor user logon activity and send the information to FortiGate unit so that the FortiGate unit can support Single Sign On (SSO).
- Provide NTLM authentication service for requests coming from FortiGate.
FSAE user logon monitoring

FSAE installed in a Windows Active Directory environment can monitor which user is logged on to which workstation and pass that information to the FortiGate unit which can use that information to apply its firewall policies.

When a Windows AD user logs in at a workstation, FSAE

• detects the logon event and records workstation name, domain, and user,
• resolves the workstation name to an IP address,
• uses Active Directory to determine which groups the user belongs to,
• sends the user logon information, including IP address and groups list, to the FortiGate unit.

When the user tries to access network resources, the FortiGate unit selects the appropriate firewall policy for the destination. If the user belongs to one of the permitted user groups, the connection is allowed.

FSAE can use either of two different methods to monitor user logon activity: DC Agent mode or Polling mode.

DC Agent mode

In DC Agent mode (see Figure 17), an agent is installed on each domain controller to monitor user logon events and pass the information to the FSAE collector agent, which forwards the information to the FortiGate unit.

Figure 17: FSAE in DC agent mode

DC Agent mode provides reliable user logon information, however you must install a DC agent on every domain controller in the domain. A reboot is needed after the agent is installed.
Polling mode

In Polling mode (see Figure 18), the FSAE collector agent polls each domain controller for user logon information and forwards it to the FortiGate unit.

Figure 18: FSAE in Polling mode

The polling mode provides logon information less reliably. For example, under heavy system load a poll might miss some user logon events. However, you do not need to install a DC agent on each domain controller.

NTLM authentication with FSAE

In a Windows AD network, FSAE can also provide NTLM authentication service to the FortiGate unit (see Figure 19). When the user makes a request that requires authentication, the FortiGate unit initiates NTLM negotiation with the client browser. The FortiGate unit does not process the NTLM packets itself. Instead, it forwards all the NTLM packets to the FSAE service to process.

If the NTLM authentication with the Windows AD network is successful, and the user belongs to one of the groups permitted in the relevant firewall policy, the FortiGate unit allows the connection. Fortinet has tested NTLM authentication on Internet Explorer and Firefox browsers.
Understanding the NTLM authentication process

1. The user attempts to connect to an external (internet) HTTP resource. The client application (browser) on the user’s computer issues an unauthenticated request through the FortiGate unit.

2. The FortiGate is aware that this client has not authenticated previously, so responds with a 401 Unauthenticated status code, and tells the client which authentication method to reply with in the header: Proxy-Authenticated: NTLM. The session is dismantled.

3. The client application connects again, and issues a GET-request, with a Proxy-Authorization: NTLM <negotiate string> header. <negotiate-string> is a base64-encoded NTLM Type 1 negotiation packet.

4. The FortiGate unit replies with a 401 “proxy auth required” status code, and a Proxy-Authenticate: NTLM <challenge string> (a base 64-encoded NTLM Type 2 challenge packet). In this packet is the challenge nonce, a random number chosen for this negotiation that is used once and prevents replay attacks.

   Note: The TCP connection must be kept alive, as all subsequent authentication-related information is tied to the TCP connection. If it is dropped, the authentication process must start again from the beginning.

5. The client sends a new GET-request with a header: Proxy-Authenticate: NTLM <authenticate string>, where <authenticate string> is a NTLM Type 3 Authentication packet that contains:
   - user name and domain
   - the challenge nonce encoded with the client password (it may contain the challenge nonce twice using different algorithms).
6 If the negotiation is successful and the user belongs to one of the groups permitted in the firewall policy, the connection is allowed. Otherwise, the FortiGate unit denies the authentication by issuing a 401 return code and prompts for a username and password. Unless the TCP connection is broken, no further credentials are sent from the client to the proxy.

Note: If the authentication policy reaches the authentication timeout period, a new NTLM handshake occurs.

Using FSAE in a Novell eDirectory environment

FSAE in a Novell eDirectory environment works similar to the FSAE Polling mode in the Windows AD environment. The FSAE eDirectory agent polls the eDirectory servers for user logon information and forwards it to the FortiGate unit.

When a user logs on at a workstation, FSAE
• detects the logon event by polling the eDirectory server and records the IP address and user ID;
• looks up in the eDirectory which groups this user belongs to,
• sends the IP address and user groups information to the FortiGate unit.

When the user tries to access network resources, the FortiGate unit selects the appropriate firewall policy for the destination. If the user belongs to one of the permitted user groups, the connection is allowed.

Operating system requirements

Consult the FortiOS v4.0 MR2 Release Notes for operating system compatibility information.

Installing FSAE

The components you need to install depend on whether you are installing FSAE on Windows AD or Novell eDirectory.

FSAE components for Windows AD

FSAE has two components to install on your network:
• the collector agent must be installed on at least one network computer
• the domain controller (DC) agent must be installed on every domain controller if you will use DC Agent mode, but is not required if you use Polling mode.

The FSAE installer first installs the collector agent. You can then continue with installation of the DC agent, or install it later by going to Start > Programs > Fortinet > Fortinet Server Authentication Extension > Install DC Agent. The installer installs a DC agent on the domain controllers of all of the trusted domains in your network.

If you install the collector agent on two or more computers, you can create a redundant configuration on the FortiGate unit for greater reliability. If the current collector agent fails, the FortiGate unit switches to the next one in its list of up to five collector agents.

You must install FSAE using an account that has administrator privileges. You can use the default Administrator account, but then you must re-configure FSAE each time the account password changes. Fortinet recommends that you create a dedicated account with administrator privileges and a password that does not expire.
FSAE components for Novell eDirectory

For a Novell network, there is only one FSAE component to install, the FSAE eDirectory agent. In some cases, you also need to install the Novell Client.

Installing FSAE for Windows AD

To install FSAE, you must obtain the FSAE Setup file from the Fortinet Support web site. Perform the following installation procedure on the computer that will run the Collector Agent. This can be any server or domain controller that is part of your network. The procedure also installs the DC Agent on all of the domain controllers in your network.

To install the FSAE collector agent

1 Create an account with administrator privileges and a password that does not expire. See Microsoft Advanced Server documentation for more information.

2 Log in to the account that you created in Step 1.

3 Double-click the FSAESetup.exe file.
   The FSAE InstallShield Wizard starts.

4 Select Next. Optionally, you can change the FSAE installation location.

5 Select Next.

6 In the Password field, enter the password for the account listed in the User Name field. This is the account you are logged into currently.

7 Select Next.

8 By default, FSAE authenticates users both by monitoring logons and by accepting authentication requests using the NTLM protocol.
   If you want to support only NTLM authentication
   • Clear the Monitor user logon events and send the information to Fortinet check box.
   • Select the Serve NTLM authentication requests coming from FortiGate check box.
   If you do not want to support NTLM authentication
   • Clear the Serve NTLM authentication requests coming from FortiGate check box.
   • Select the Monitor user logon events and send the information to Fortinet check box.
   You can also change these options after installation.

9 Select the access method to use for Windows Directory:
   • Select Standard to use Windows domain and user name credentials.
   • Select Advanced if you will set up LDAP access to Windows Directory.

10 Select Next and then select Install.

11 For DC Agent mode, when the FSAE InstallShield Wizard completes FSAE collector agent installation, ensure that Launch DC Agent Install Wizard is selected and then select Finish.

To install the DC Agent

1 If you have just installed the FSAE collector agent, the FSAE - Install DC Agent wizard starts automatically. Otherwise, go to Start > Programs > Fortinet > Fortinet Server Authentication Extension > Install DC Agent.
2 Verify the Collector Agent IP address.
   If the Collector Agent computer has multiple network interfaces, ensure that the one
   that is listed is on your network. The listed Collector Agent listening port is the default.
   You should change this only if the port is already used by some other service.

3 Select Next.

4 Select the domains to monitor and select Next.
   If any of your required domains are not listed, cancel the wizard and set up the proper
   trusted relationship with the domain controller. Then run the wizard again by going to
   Start > Programs > Fortinet > Fortinet Server Authentication Extension >
   Install DC Agent.

5 Optionally, select users that you do not want monitored. These users will not be able to
   authenticate to FortiGate units using FSAE. You can also do this later. See
   “Configuring FSAE on Windows AD” on page 64.

6 Select Next.

7 Optionally, clear the check boxes of domain controllers on which you do not want to
   install the FSAE DC Agent.

8 Select the Working Mode: DC Agent Mode or Polling Mode. For more information, see
   “DC Agent mode” on page 58 and “Polling mode” on page 59.

9 Select Next.

10 Select Yes when the wizard requests that you reboot the computer.

   Note: If you reinstall the FSAE software on this computer, your FSAE configuration is
   replaced with default settings.

If you want to create a redundant configuration, repeat the procedure “To install the FSAE
   collector agent” on page 62 on at least one other Windows AD server.

   Note: When you start to install a second collector agent, when the Install Wizard dialog
   appears the second time, cancel it. From the configuration GUI, the monitored domain
   controller list should show your domain controllers unselected. Select the ones you wish to
   monitor with this collector agent, and click Apply.

Before you can use FSAE, you need to configure it on both Windows AD and on the
FortiGate units. See the next section, “Configuring FSAE on Windows AD”, and
“Configuring FSAE on FortiGate units” on page 76.

Installing FSAE for Novell

To install FSAE, you must obtain the FSAE_Setup_eDirectory file from the Fortinet
Support web site. Perform the following installation procedure on the computer that will
run the FSAE eDirectory agent. This can be any server or domain controller that is part of
your network.

To install the FSAE eDirectory agent

1 Create an account with administrator privileges and a password that does not expire.
   See Novell documentation for more information.

2 Log in to the account that you created in Step 1.

3 Double-click the FSAE_Setup_eDirectory.exe file.
   The Fortinet eDirectory Agent InstallShield Wizard starts.
4 Optionally, fill in the User Name and Organization fields.
5 Select the Anyone who uses this computer (all users) option.
6 Select Next.
7 Optionally, enter any of the following information:
   You can also enter or modify this information after installation. See “Configuring FSAE on Novell networks” on page 73.

**eDirectory Server**

| Server Address | Enter the IP address of the eDirectory server. |
| Use secure connection (SSL) | Select to connect to the eDirectory server using SSL security. |
| Search Base DN | Enter the base Distinguished Name for the user search. |

**eDirectory Authentication**

| User name | Enter a user name that has access to the eDirectory, using LDAP format. |
| User password | Enter the password. |

8 Select Next.
9 Select Install.

**Configuring FSAE on Windows AD**

On the FortiGate unit, firewall policies control access to network resources based on user groups. Each FortiGate user group is associated with one or more Windows AD user groups.

FSAE sends information about Windows user logons to FortiGate units. If there are many users on your Windows AD domains, the large amount of information might affect the performance of the FortiGate units. To avoid this problem, you can configure the FSAE collector agent to send logon information only for groups named in the FortiGate unit’s firewall policies.

On each computer that runs a collector agent, you need to configure

- Windows AD user groups
- collector agent settings, including the domain controllers to be monitored
- the collector agent Ignore User list
- the collector agent FortiGate Group Filter for each FortiGate unit
- LDAP access settings, if LDAP is used to obtain group information

**Note:** In some environments where user IP addresses change frequently, it might be necessary to configure the alternate IP address tracking method. For more information, see “Configuring alternate user IP address tracking” on page 70.

**Configuring Windows AD server user groups**

FortiGate units control access at the group level. All members of a group have the same network access as defined in FortiGate firewall policies. You can use existing Windows AD user groups for authentication to FortiGate units if you intend that all members within each group have the same network access privileges. Otherwise, you need to create new user groups for this purpose.
If you change a user’s group membership, the change does not take effect until the user logs off and then logs on again.

FSAE sends only Domain Local Security Group and Global Security Group information to FortiGate units. You cannot use Distribution group types for FortiGate access. No information is sent for empty groups.

Refer to Microsoft documentation for information about creating groups.

Configuring collector agent settings

You need to configure which domain controllers you use and which domains you monitor for user logons. You can also alter default settings and settings you made during installation.

To configure the FSAE collector agent

1. From the Start menu select Programs > Fortinet > Fortinet Server Authentication Extension > Configure FSAE.

2. Enter the following information and then select Save&Close.

- **Monitoring user logon events**: Select to automatically authenticate users as they log on to the Windows domain.
- **Support NTLM authentication**: Select to facilitate logon of users who are connected to a domain that does not have the DC Agent installed.
- **Collector Agent Status**: Shows RUNNING when collector agent is active.
- **Listening ports**
  - **FortiGate**: TCP port for FortiGate units. Default 8000.
  - **DC Agent**: UDP port that DC Agents use. Default 8002.

Logging

- **Log level**: Select the minimum severity level of logged messages.
- **Log file size limit (MB)**: Enter the maximum size for the log file in MB.
- **View Log**: View all FSAE logs.
### Log logon events in separate logs
Record user login-related information separately from other logs. The information in this log includes:
- data received from DC agents
- user logon/logoff information
- workstation IP change information
- data sent to FortiGate units

### View Logon Events
If Log logon events in separate logs is enabled, you can view user login-related information.

### Authentication
- **Require authenticated connection from FortiGate**
  - Select to require the FortiGate unit to authenticate before connecting to the Collector Agent.

### Password
Enter the password that FortiGate units must use to authenticate. The maximum password length is 16 characters. The default password is “fortinetcanada”.

### Timers
- **Workstation verify interval (minutes)**
  - Enter the interval in minutes at which FSAE checks whether the user is still logged in. The default is every 5 minutes. If ports 139 or 445 cannot be opened on your network, set the interval to 0 to prevent checking. See “Configuring TCP ports for FSAE on client computers” on page 70.

- **Dead entry timeout interval**
  - Enter the interval in minutes after which FSAE purges information for user logons that it cannot verify. The default is 480 minutes (8 hours).
  - Dead entries usually occur because the computer is unreachable (in standby mode or disconnected, for example) but the user has not logged off.
  - You can also prevent dead entry checking by setting the interval to 0.

- **IP address change verify interval**
  - FSAE periodically checks the IP addresses of logged-in users and updates the FortiGate unit when user IP addresses change. This does not apply to users authenticated through NTLM. Enter the verification interval in seconds. IP address verification prevents users from being locked out if they change IP addresses. You can enter 0 to prevent IP address checking if you use static IP addresses.

### Cache user group lookup result
Enable caching.

### Cache expire in (minutes)
FSAE caches group information for logged-in users. Enter the duration in minutes after which the cache entry expires. If you enter 0, the cache never expires.

### Clear Group Cache
Clear group information of logged-in users.

### Common Tasks
- **Show Service Status**
  - View information about the status of the collector agent and connected FortiGate units. See “Viewing collector agent status” on page 70.

- **Show Monitored DCs**
  - Shows detailed information about connected DC agents.
  - Use the Select DC to Monitor button to select domain controllers to monitor and choose Working Mode. See “Selecting Domain Controllers and working mode for monitoring” on page 72.

- **Show Logon Users**
  - View a list of currently logged-in users. Select the column headers to sort the list.

- **Select Domains to Monitor**
  - Select this button to remove domains that you do not want to monitor. From the Domain Filter dialog box that displays, clear check boxes for unwanted domains and select OK.

- **Set Directory Access Information**
Configuring Directory Access settings

FSAE can access Windows Active Directory in one of two modes:

- **Standard** — FSAE receives group information from the collector agent in the form `domain\group`. This is available on FortiOS 3.0 and later.
- **Advanced** — FSAE obtains user group information using LDAP. This is compatible with FortiOS 3.0 MR6 and later. Group information is in LDAP format.

If you change AD access mode, you must reconfigure your group filters to ensure that the group information is in the correct format.

**To configure Directory Access settings**

1. From the Start menu select *Programs* > *Fortinet* > *Fortinet Server Authentication Extension* > *Configure FSAE*.
2. In the *Common Tasks* section, select *Set Directory Access Information*.
   - The *Set Directory Access Information* dialog box opens.
3. From the *AD access mode* list, select either *Standard* or *Advanced*.
4. If you selected Advanced AD access mode, select *Advanced Setting* and configure the following settings and then select *OK*:
   - **AD server address**
     - Enter the address of your network’s global catalog server.
   - **AD server port**
     - The default AD server port is 3268. Change this only if your server uses a different port.
   - **BaseDN**
     - Enter the Base distinguished name for the global catalog.
   - **User name**
     - If the global catalog accepts your FSAE agent’s credentials, you can leave these fields blank. Otherwise, enter credentials for an account that can access the global catalog.
   - **Password**

**Configuring the Ignore User List**

The Ignore User List excludes users such as system accounts that do not authenticate to any FortiGate unit. The logons of these users are not reported to FortiGate units.
To configure the Ignore User List
1. From the Start menu select Programs > Fortinet > Fortinet Server Authentication Extension > Configure FSAE.
2. In the Common Tasks section, select Set Ignore User List.
   The current list of ignored users is displayed. You can expand each domain to view the names of ignored users.
3. Do any of the following:
   - To remove a user from the list, select the check box beside the user name and then select Remove. The user’s login is no longer ignored.
   - To add users to be ignored, select Add, select the check box beside each required user name, and then select Add.
4. Select OK.

Configuring FortiGate group filters
FortiGate filters control the user logon information sent to each FortiGate unit. You need to configure the list so that each FortiGate unit receives user logon information for the user groups that are named in its firewall policies.

You do not need to configure a group filter on the collector agent if the FortiGate unit retrieves group information from Windows AD using LDAP. In that case, the collector agent uses as its filter the list of groups you selected on the FortiGate unit.

The filter list is initially empty. You need to configure filters for your FortiGate units using the Add function. At minimum, you should create a default filter that applies to all FortiGate units that do not have a specific filter defined for them.

Note: If no filter is defined for a FortiGate unit and there is no default filter, the collector agent sends all Windows AD group and user logon events to the FortiGate unit. While this normally is not a problem, limiting the amount of data sent to the FortiGate unit improves performance by reducing the amount of memory the unit uses to store the group list.

To configure a FortiGate group filter
1. From the Start menu select Programs > Fortinet > Fortinet Server Authentication Extension > Configure FSAE.
2. In the Common Tasks section, select Set Group Filters.
   The FortiGate Filter List opens. It has the following columns:
FSAE for integration with Windows AD or Novell

Configuring FSAE on Windows AD

FortiGate SN  
The serial number of the FortiGate unit to which this filter applies.

Description  
An optional description of the role of this FortiGate unit.

Monitored Groups  
The Windows AD user groups that are relevant to the firewall policies on this FortiGate unit.

Add  
Create a new filter.

Edit  
Modify the filter selected in the list.

Remove  
Remove the filter selected in the list.

OK  
Save the filter list and exit.

Cancel  
Cancel changes and exit.

3 Select Add to create a new filter. If you want to modify an existing filter, select it in the list and then select Edit.

4 Enter the following information and then select OK.

Default filter  
Select to create the default filter. The default filter applies to any FortiGate unit that does not have a specific filter defined in the list.

FortiGate Serial Number  
Enter the serial number of the FortiGate unit to which this filter applies. This field is not available if Default is selected.

Description  
Enter a description of this FortiGate unit's role in your network. For example, you could list the resources accessed through this unit. This field is not available if Default is selected.

Monitor the following groups  
The collector agent sends to the FortiGate unit the user logon information for the Windows AD user groups in this list. Edit this list using the Add, Advanced and Remove buttons.

Add  
In the preceding single-line field, enter the Windows AD domain name and user group name, and then select Add. If you don’t know the exact name, use the Advanced button instead.

The format of the entry depends on the AD access mode (see “Configuring Directory Access settings” on page 67):
Standard: Domain\Group
Advanced: cn=group, ou=corp, dc=domain
Configuring FSAE on Windows AD

Windows AD records when users log on but not when they log off. For best performance, FSAE monitors when users log off. To do this, FSAE needs read-only access to each client computer’s registry over TCP port 139 or 445. At least one of these ports should be open and not blocked by firewall policies.

If it is not feasible or acceptable to open TCP port 139 or 445, you can turn off FSAE logoff detection. To do this, set the collector agent workstation verify interval to 0. FSAE assumes that the logged on computer remains logged on for the duration of the collector agent dead entry timeout interval. By default this is eight hours. For more information about both interval settings, see “Timers” on page 66.

Configuring ports on the collector agent computer

On the computer where you install the collector agent, you must make sure that the firewall does not block the listening ports for the FortiGate unit and the DC Agent. By default, these are TCP port 8000 and UDP port 8002. For more information about setting these ports, see “To configure the FSAE collector agent” on page 65.

Configuring alternate user IP address tracking

In environments where user IP addresses change frequently, you can configure FSAE to use an alternate method to track user IP address changes. Using this method, FSAE responds more quickly to user IP address changes because it directly queries workstation IP addresses to match users and IP addresses. You need to have FSAE version 3.5.27 or later and FortiOS 3.0 MR7 or later.

To configure alternate user IP address tracking

1. On the computer where the collector agent is installed, go to Start > Run.
2. Enter regedit or regedt32 and select OK.
3. The Registry Editor opens.
4. Find the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Fortinet\FSAE\collectoragent.
5. Set the supportFSAEauth value (dword) to 00000001.
6. Close the Registry Editor.
7. From the Start menu select Programs > Fortinet > Fortinet Server Authentication Extension > Configure FSAE.
8. Select Apply.
   The FSAE service restarts with the updated registry settings.

Viewing collector agent status

Use the Show Service Status function to view your collector agents.

To view collector agent status

1. From the Start menu select Programs > Fortinet > Fortinet Server Authentication Extension > Configure FSAE.
2 In the **Common Tasks** section, select **Show Service Status**.

The FSAE Collector Agent Status window opens.

You can see which FortiGate units have a collector agent installed and how long the agent has been connected.

**Viewing DC agent status**

Use the Show Monitored DCs function to view the status of DC agents.

**To view domain controller agent status**

1 From the Start menu select **Programs > Fortinet > Fortinet Server Authentication Extension > Configure FSAE**.

2 In the **Common Tasks** section, select **Show Monitored DCs**.

For each DC Agent, you can view the IP address, number of logon events received, the last logon event and when it was received.

3 If you want to change which DC agents are monitored or change the working mode for logon event monitoring, select **Select DC to Monitor**. For more information see "Selecting Domain Controllers and working mode for monitoring" on page 72.
Selecting Domain Controllers and working mode for monitoring

You can change which DC agents are monitored or change the working mode for logon event monitoring.

1. From the Start menu select Programs > Fortinet > Fortinet Server Authentication Extension > Configure FSAE.
2. In the Common Tasks section, select Show Service Status.
3. Select Select DC to Monitor.

Working Mode

**DC Agent mode** — a Domain Controller agent monitors user logon events and passes the information to the FSAE collector agent. This provides reliable user logon information, however you must install a DC agent on every domain controller in the domain.

**Polling mode** — the FSAE collector agent polls each domain controller for user logon information. Under heavy system load this might provide information less reliably, but you do not need to install a DC agent on each domain controller.
Configuring FSAE on Novell networks

You need to configure the FSAE eDirectory agent to communicate with eDirectory servers. You may have provided some of this information during installation.

To configure the eDirectory agent

1. From the Start menu select Programs > Fortinet > eDirectory Agent > eDirectory Config Utility.

The eDirectory Agent Configuration Utility dialog opens.

2. Enter the following information and select OK.

**eDirectory Authentication**
- **User name**: Enter a user name that has access to the eDirectory, using LDAP format.
- **User password**: Enter the password.
- **Listening port**: Enter the TCP port on which FSAE listens for connections from FortiGate units. The default is 8000. You can change the port if necessary.
- **Refresh interval**: Enter the interval in seconds between polls of the eDirectory server to check for new logins. The default is 30 seconds.

**FortiGate Connection Authentication**
- **Require authenticated connection from FortiGate**: Select to require the FortiGate unit to authenticate before connecting to the eDirectory Agent.
- **Password**: Enter the password that FortiGate units must use to authenticate. The maximum password length is 16 characters. The default password is “FortinetCanada”.

**User logon info search method**: Select how the FSAE eDirectory agent accesses user logon information: LDAP or Native (Novell API). LDAP is the default. If you select Native, you must also have the Novell Client installed on the PC.

**Logging**
- **Log level**: Select Debug, Info, Warning or Error as the minimum severity level of message to log or select None to disable logging.
To add an eDirectory server

1. In the eDirectory Agent Configuration Utility dialog box (see the preceding procedure, “To configure the eDirectory agent”), select Add.
   
The eDirectory Setup dialog box opens.

   ![eDirectory Setup](Image)

2. Enter the following information and select OK:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>eDirectory Server Address</strong></td>
<td>Enter the IP address of the eDirectory server.</td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td>If the eDirectory server does not use the default port 389, clear the Default check box and enter port number.</td>
</tr>
<tr>
<td><strong>User name</strong></td>
<td>Enter a user name that has access to the eDirectory, using LDAP format.</td>
</tr>
<tr>
<td><strong>User password</strong></td>
<td>Enter the password.</td>
</tr>
<tr>
<td><strong>Search Base DN</strong></td>
<td>Enter the base Distinguished Name for the user search.</td>
</tr>
<tr>
<td><strong>Use secure connection (SSL)</strong></td>
<td>Select to connect to the eDirectory server using SSL security.</td>
</tr>
</tbody>
</table>
Configuring a group filter

The FSAE eDirectory agent sends user logon information to the FortiGate unit for all user groups unless you either

- configure an LDAP server entry for the eDirectory on the FortiGate unit and select the groups that you want to monitor (see “Configuring LDAP server access” on page 76), or
- configure the group filter on the eDirectory agent (see “To configure the group filter”, below).

If both the FortiGate LDAP configuration and the FSAE eDirectory agent group filter are present, the FortiGate user group selections are used.

To configure the group filter

1. From the Start menu select Programs > Fortinet > eDirectory Agent > eDirectory Config Utility.
2. Select Group Filter.
3. Do one of the following:
   - Enter group names, then select Add.
   - Select Advanced, select groups, and then select Add.
4. Select OK.
Configuring FSAE on FortiGate units

To configure your FortiGate unit to operate with FSAE, you

- Configure LDAP access to the Novell eDirectory or Windows AD global catalog. Skip this step if you are using FSAE Standard mode.
- Specify the FSAE collector agent or Novell eDirectory agent that will provide user logon information.
- Add Active Directory user groups to FortiGate user groups,
- Create firewall policies for FSAE-authenticated groups,
- optionally, specify a guest protection profile to allow guest access.

Configuring LDAP server access

LDAP access is required if your network has a Novell eDirectory agent or a collector agent using Advanced AD access mode. If you are using FSAE Standard mode, go to “Specifying your collector agents or Novell eDirectory agents” on page 78.

The LDAP configuration on the FortiGate unit not only provides access to the LDAP server, it sets up the retrieval of Windows AD user groups for you to select in Directory Services. The LDAP Server configuration (in User > Remote > LDAP) includes a function to preview the LDAP server’s response to your distinguished name query. If you already know the appropriate Distinguished Name (DN) and User DN settings, you may be able to skip some of the following steps.

1. Go to User > Remote > LDAP and select Create New.
2. Select the Query distinguished name button to the right of the Distinguished Name field.
   A new window opens, like this:

   **Figure 20: Result of initial DN query**

   ![LDAP Distinguished Name Query](image)

   If more than one name is listed, you might need to explore each name following the steps below to determine which one is relevant to your needs.

3. Copy the name string to the Distinguished Name field and select OK.
   This closes the window and copies the name string to the Distinguished Name field of the LDAP Server configuration.

4. Set Bind Type to Regular.

5. In the User DN field, enter the administrative account name that you created for FSAE.
   For example, if the account is FSAE_Admin, enter “cn=FSAE_Admin,cn=users”.

6. Make sure that the User DN entry ends with a comma and append the string from the Distinguished Name field to the end of it.
   Example: cn=FSAE_Admin,cn=users,dc=office,dc=example,dc=com

7. Enter the administrative account password in the Password field.
8 Select the *Query distinguished name* button again.

The LDAP Distinguished Name Query window opens again and looks like this:

**Figure 21: Authenticated DN query**

![LDAP Distinguished Name Query](https://example.com/figure21.png)

You can expand any of the DNs that contain entries. When you select an expandable DN, the *Distinguished Name* field is updated. Look for the DN that contains the users or groups whose logon you want to monitor.

9 Select the DN that you want to monitor and then select *OK*.

This closes the window and updates the *Distinguished Name* field of the LDAP Server configuration.

10 Check the following fields and select *OK*:

- **Name**: Enter a name to identify the LDAP server.
- **Common Name Identifier**: The default common name identifier is `cn`. This is correct for most LDAP servers. However, some servers use other identifiers such as `uid`.
- **Secure Connection**: Do not select. The FSAE collector agent does not support secure connection.

**To configure LDAP for Directory Services - CLI example**

```bash
config user ldap
edit "ADserver"
    set server "10.11.101.160"
    set cnid "cn"
    set dn "cn=users,dc=office,dc=example,dc=com"
    set type regular
    set username
        "cn=administrator,cn=users,dc=office,dc=example,dc=com"
    set password set_a_secure_password
next
end
```
Specifying your collector agents or Novell eDirectory agents

You need to configure the FortiGate unit to access at least one FSAE collector agent or Novell eDirectory agent. You can specify up to five servers on which you have installed a collector or eDirectory agent. The FortiGate unit accesses these servers in the order that they appear in the list. If a server becomes unavailable, the unit accesses the next one in the list.

To specify collector agents


2. Enter the following information and select OK:

   - **Name**: Enter a name for the Windows AD server. This name appears in the list of Windows AD servers when you create user groups.

   Enter the following information for up to five collector agents.

   - **FSAE Collector IP/Name**: Enter the IP address or the name of the server where this agent is installed. Maximum name length is 63 characters.
   - **Port**: Enter the TCP port used for FSAE. This must be the same as the FortiGate listening port specified in the Novell eDirectory or FSAE collector agent configuration. See “Configuring collector agent settings” on page 65 or “Configuring FSAE on Novell networks” on page 73.
   - **Password**: Enter the password for the collector agent or eDirectory agent. For the FSAE collector agent, this is required only if you configured the agent to require authenticated access.
   - **LDAP Server**: For Novell eDirectory, enable. For Windows AD, enable if the collector agent is configured to use Advanced AD access mode. Select the LDAP server you configured previously. See “Configuring LDAP server access” on page 76.

   **To specify the collector agent for Directory Services - CLI example**

   ```
   config user fsae
   edit WinGroups
   set ldap-server ADserver
   set password ENC G7QV7NEq11Cm9jKmVmJFVhQ2+wtNEe9T0iYA5Sa+EqT2J8zhOrbkJPD0RmY3c4LaorDs0BczAldONmcGfthTxwwGsigzGpbJdC71spFLQYtj
   set server 10.11.101.160
   end
   ```
Selecting Windows user groups (LDAP only)

If the collector agent uses Advanced AD access mode, the FortiGate unit obtains user group information using LDAP. You need to select the Windows user groups that you want to monitor. These user group names are then available to add to FortiGate Directory Service user groups.

To select Windows user groups

   The list of Directory Service servers is displayed.

   **Figure 23: List of Directory Service servers**

<table>
<thead>
<tr>
<th>Name</th>
<th>FSAE Collector IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>WinGroups</td>
<td>10.11.101.160:8900</td>
</tr>
</tbody>
</table>

2. Select the Edit Users/Groups icon.
   The FortiGate unit performs an LDAP query and displays the result.

   **Figure 24: Result of Directory Service LDAP query**

3. Select the check boxes of the user groups that you want to monitor and then select OK.
   You can also use the Add User/Group icon to select a group by entering its distinguished name.

Viewing information imported from the Windows AD server

You can view the domain and group information that the FortiGate unit receives from the AD Server. Go to User > Directory Service. The display differs for Standard and Advanced AD access mode.
Figure 25: List of groups from Active Directory server (Standard AD access mode)

Directory Service Server

Domain

Groups

Figure 26: List of monitored groups (Advanced AD access mode)

Directory Service Server

Domain and groups in LDAP format

Remove group

Create New
Add a new Directory Service server.

Name

Server
The name defined for the Directory Service server.

Domain
Domain name imported from the Directory Service server.

Groups
The group names imported from the Directory Service server.

FSAE Collector IP
The IP address of the FSAE agent on the Directory Service server

Delete icon
Delete this server definition.

Edit icon
Edit this server definition.

Refresh icon
Get user group information from the Directory Service server.

Add User/Group
Add a user or group to the list. You must know the distinguished name for the user or group. This is available for Windows AD in Advanced AD access mode only.

Edit Users/Groups
Select users and groups to add to the list. See “Selecting Windows user groups (LDAP only)” on page 79. This is available in Advanced AD access mode only.
Creating Directory Service user groups

You cannot use Windows or Novell groups directly in FortiGate firewall policies. You must create FortiGate user groups of the Directory Service type and add Windows or Novell groups to them.

To create a user group for FSAE authentication

2. Select Create New.

The New User Group dialog box opens.

3. In the Name box, enter a name for the group, FSAE_Internet_users for example.
4. In Type, select Directory Service.
5. From the Available Members list, select the required Directory Service groups.
   Using the CTRL or SHIFT keys, you can select multiple groups.
6. Select the green right arrow button to move the selected groups to the Members list.
7. Select OK.

To create the FSAE_Internet-users user group - CLI example

```
config user group
  edit FSAE_Internet_users
    set group-type directory-service
    set member
      CN=Engineering,cn=users,dc=office,dc=example,dc=com
      CN=Sales,cn=users,dc=office,dc=example,dc=com
  end
```

Creating firewall policies

Policies that require FSAE authentication are very similar to other firewall policies. Using identity-based policies, you can configure access that depends on the Directory Service user group.

To create a firewall policy for FSAE authentication

1. Go to Firewall > Policy and select Create New.
2. Enter the following information:
3 Select Enable Identity Based Policy and then select Add.
   The New Authentication Rule window opens.

4 Select the required user group from the Available User Groups list and then select the right arrow button to move the selected group to the Selected User Groups list.
   You can select multiple groups using the CTRL or SHIFT keys.

5 Select the required service from the Available Services list and then select the right arrow button to move the selected service to the Selected Services list.
   You can select multiple services using the CTRL or SHIFT keys.

6 Select a Schedule from the list as needed.

7 Optionally, select UTM and enable UTM options.

8 Select OK to close the New Authentication Rule window.

9 Select Directory Service (FSAE).

10 Select OK.

To create a firewall policy for FSAE authentication - CLI example

```
config firewall policy
edit 0
   set srcintf port2
   set dstintf port1
   set srcaddr internal_net
   set dstaddr all
   set action accept
   set identity-based enable
   set nat enable
config identity-based-policy
edit 1
   set schedule always
   set groups FSAE_Internet_users
   set service ANY
end
end
```

Enabling guests to access FSAE policies

You can enable guest users to access FSAE firewall policies. Guests are users who are unknown to the Windows AD or Novell network and servers that do not log on to a Windows AD domain.

To enable guest access in your FSAE firewall policy, add an identity-based policy assigned to the built-in user group FSAE_Guest_Users. Specify the services, schedule and protection profile that apply to guest users. For more information, see "Creating firewall policies" on page 81.
Testing the configuration

To verify that you have correctly configured FSAE on your network and on your FortiGate units:

1. From a workstation on your network, log on to your domain using an account that belongs to a group that is configured for authentication on the FortiGate unit.

2. Try to connect to the resource that is protected by the firewall policy requiring authentication through FSAE.
   
   You should be able to connect to the resource without being asked for user name or password.

3. Log off and then log on using an account that does not belong to a group you have configured for authentication on the FortiGate unit.

4. Try to connect to the resource that is protected by the firewall policy requiring authentication through FSAE.
   
   Your attempt to connect to the resource should fail.
Certificate-based authentication

This section provides an overview of how the FortiGate unit verifies the identities of administrators, SSL VPN users, or IPsec VPN peers using security certificates. The FortiGate unit employs a variety of Internet protocols to secure access to the FortiGate unit.

The following topics are included in this section:

- Certificates overview
- Managing X.509 certificates
- Configuring certificate-based authentication

Certificates overview

Certificates always play a role in authentication of clients connecting via HTTPS, either as administrators or SSL VPN users. Certificate authentication is optional for IPsec VPN peers.

SSL, HTTPS, and certificates

The secure HTTP (HTTPS) protocol uses SSL security. Certificates are an integral part of SSL. When a web browser connects to the FortiGate unit via HTTPS, a certificate is used to verify the FortiGate unit’s identity to the client. Optionally, the FortiGate unit can require the client to authenticate itself in return.

By default, the FortiGate unit uses a self-signed security certificate to authenticate itself to HTTPS clients. When the certificate is offered, the client browser displays two security messages.

- The first message prompts users to accept and optionally install the FortiGate unit’s self-signed security certificate. If the user does not accept the certificate, the FortiGate unit refuses the connection. When the user accepts the certificate, the FortiGate login page is displayed, and the credentials entered by the user are encrypted before they are sent to the FortiGate unit. If the user chooses to install the certificate, the prompt is not displayed again.

- Just before the FortiGate login page is displayed, a second message informs users that the FortiGate certificate distinguished name differs from the original request. This message is displayed because the FortiGate unit redirects the connection (away from the distinguished name recorded in the self-signed certificate) and can be ignored.

Optionally, you can install an X.509 server certificate issued by a certificate authority (CA) on the FortiGate unit. You can then configure the FortiGate unit to identify itself using the server certificate instead of the self-signed certificate.

This feature is supported for SSL VPN operation only and cannot be used to suppress the two security messages during administrative log ins. For more information, see “Authenticating SSL VPN users with security certificates” on page 94.

After successful certificate authentication, communication between the client browser and the FortiGate unit is encrypted using SSL over the HTTPS link.
IPsec VPNs and certificates

Certificate authentication is a more secure alternative to preshared key (shared secret) authentication for IPsec VPN peers. Unlike administrators or SSL VPN users, IPsec peers use HTTP to connect to the VPN gateway configured on the FortiGate unit. The VPN gateway configuration can require certificate authentication before it permits an IPsec tunnel to be established.

Managing X.509 certificates

The general process for handling certificates is as follows:

• Generate a certificate signing request on the FortiGate unit.
• Have the CA sign the server certificate.
• Install the server certificate on the device that must authenticate itself.
• Install the CA certificate and certificate revocation list (CRL) on the device that will validate the certificate of the authenticating device.

This section provides procedures for generating certificate requests, installing signed server certificates, and importing CA root certificates and CRLs at the FortiGate unit. For information about how to install root certificates, CRLs, and personal or group certificates on a remote client browser, refer to the browser documentation.

Generating a certificate signing request

Whether you create certificates locally with a software application or obtain them from an external certificate service, you will need to generate a certificate signing request.

When you generate the request, a private and public key pair is created for the FortiGate unit. The generated request includes the public key of the FortiGate unit and information such as the FortiGate unit’s public static IP address, domain name, or email address. The FortiGate unit’s private key remains confidential on the FortiGate unit.

After you submit the request to a CA, the CA will verify the information and register the contact information on a digital certificate that contains a serial number, an expiration date, and the public key of the CA. The CA will then sign the certificate. You then install the certificate on the FortiGate unit.

To generate the certificate request

1 Go to System > Certificates > Local Certificates.
2 Select Generate.

3 In the Certificate Name field, type a name for the certificate request. Typically, this would be the name of the FortiGate unit.

   Note: To enable the export of a signed certificate as a PKCS12 file later on if required, do not include spaces in the name.

4 Enter values in the Subject Information area to identify the FortiGate unit:
   • If the FortiGate unit has a static IP address, select Host IP and enter the public IP address of the FortiGate unit. If the FortiGate unit does not have a public IP address, use an email address (or domain name if available) instead.
   • If the FortiGate unit has a static IP address and subscribes to a dynamic DNS service, use a domain name if available to identify the FortiGate unit. If you select Domain Name, enter the fully qualified domain name of the FortiGate unit. Do not include the protocol specification (http://) or any port number or path names.

   Note: If a domain name is not available and the FortiGate unit subscribes to a dynamic DNS service, an “unable to verify certificate” type message may be displayed in the user’s browser whenever the public IP address of the FortiGate unit changes.

   • If you select E-Mail, enter the email address of the owner of the FortiGate unit.

5 Enter values in the Optional Information area to further identify the FortiGate unit.

   Organization Unit Name of your department. You can enter a maximum of 5 Organization Units. To add or remove a unit, use the plus (+) or minus (-) icon.

   Organization Legal name of your company or organization.
From the Key Size list, select 1024 Bit, 1536 Bit or 2048 Bit. Larger keys are slower to generate but more secure.

7 In Enrollment Method, you have two methods to choose from. Select File Based to generate the certificate request, or Online SCEP to obtain a signed SCEP-based certificate automatically over the network. For the SCEP method, enter the URL of the SCEP server from which to retrieve the CA certificate, and the CA server challenge password.

8 Select OK.

The request is generated and displayed in the Local Certificates list with a status of PENDING.

9 Select the Download button to download the request to the management computer.

10 In the File Download dialog box, select Save and save the Certificate Signing Request on the local file system of the management computer.

11 Name the file and save it on the local file system of the management computer.

Generating certificates with CA software

1 Install the CA software as a stand-alone root CA.
2 Provide identifying information for your self-administered CA

Server certificate

1 Generate a Certificate Signing Request (CSR) on the FortiGate unit.
2 Copy the CSR base-64 encoded text (PKCS#10 or PKCS#7) into the CA software and generate the certificate.
3 Export the certificate as a X.509 DER encoded binary file with .CER extension
4 Upload the certificate file to the FortiGate unit Local Certificates page (type is Certificate).

CA certificate

1 Retrieve the CA Certificate from the CA software as a DER encoded file.
2 Upload the CA certificate file to the FortiGate unit CA Certificates page.

PKI certificate

1 Generate a Certificate Signing Request (CSR) on the FortiGate unit.
2 Copy the CSR base-64 encoded text (PKCS#10 or PKCS#7) into the CA software and generate the certificate.
3 Export the certificate as a X.509 DER encoded binary file with .CER extension.
4 Install the certificate in the user’s web browser or IPsec VPN client as needed.
Obtaining a signed server certificate from an external CA

To obtain a signed server certificate for a FortiGate unit, you must send a request to a CA that provides digital certificates that adhere to the X.509 standard. The FortiGate unit provides a way for you to generate the request.

To submit the certificate signing request (file-based enrollment)

1. Using the web browser on the management computer, browse to the CA web site.
2. Follow the CA instructions for a base-64 encoded PKCS#10 certificate request and upload your certificate request.
3. Follow the CA instructions to download their root certificate and CRL.

When you receive the signed server certificate from the CA, install the certificate on the FortiGate unit. See “To install the signed server certificate” below.

To install the signed server certificate

1. On the FortiGate unit, go to System > Certificates > Local Certificates.
2. Select Import.
3. From Type, select Local Certificate.
4. Select Browse, browse to the location on the management computer where the certificate was saved, select the certificate, and then select Open.
5. Select OK, and then select Return.

Installing a CA root certificate and CRL to authenticate remote clients

When you apply for a signed personal or group certificate to install on remote clients, you can obtain the corresponding root certificate and CRL from the issuing CA. When you receive the signed personal or group certificate, install the signed certificate on the remote client(s) according to the browser documentation. Install the corresponding root certificate (and CRL) from the issuing CA on the FortiGate unit according to the procedures given below.

To install a CA root certificate

1. After you download the root certificate of the CA, save the certificate on the management computer. Or, you can use online SCEP to retrieve the certificate.
2. On the FortiGate unit, go to System > Certificates > CA Certificates.
3. Select Import.
4 Do one of the following:
   • To import using SCEP, select SCEP. Enter the URL of the SCEP server from which to retrieve the CA certificate. Optionally, enter identifying information of the CA, such as the file name.
   • To import from a file, select Local PC, then select Browse and find the location on the management computer where the certificate has been saved. Select the certificate, and then select Open.

5 Select OK, and then select Return.

The system assigns a unique name to each CA certificate. The names are numbered consecutively (CA_Cert_1, CA_Cert_2, CA_Cert_3, and so on).

To import a certificate revocation list

A Certificate Revocation List (CRL) is a list of the CA certificate subscribers paired with certificate status information. The list contains the revoked certificates and the reason(s) for revocation. It also records the certificate issue dates and the CAs that issued them.

When configured to support SSL VPNs, the FortiGate unit uses the CRL to ensure that the certificates belonging to the CA and remote peers or clients are valid. You must download the CRL from the CA web site on a regular basis.

1 After you download the CRL from the CA web site, save the CRL on the management computer.

2 Go to System > Certificates > CRL.

3 Select Import.

4 Do one of the following:
   • To import using an HTTP server, select HTTP and enter the URL of the HTTP server.
   • To import using an LDAP server, select LDAP and select the LDAP server from the list.
   • To import using an SCEP server, select SCEP and select the Local Certificate from the list. Enter the URL of the SCEP server from which the CRL can be retrieved.
   • To import from a file, select Local PC, then select Browse and find the location on the management computer where the CRL has been saved. Select the CRL and then select Open.

5 Select OK, and then select Return.

Online updates to certificates and CRLs

If you obtained your local or CA certificate using SCEP, you can configure online renewal of the certificate before it expires. Similarly, you can receive online updates to CRLs.
Local certificates

In the `config vpn certificate local` command, you can specify automatic certificate renewal. The relevant fields are:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scep-url &lt;URL_str&gt;</td>
<td>The URL of the SCEP server. This can be HTTP or HTTPS.</td>
</tr>
<tr>
<td>scep-password &lt;password_str&gt;</td>
<td>The password for the SCEP server.</td>
</tr>
<tr>
<td>auto-regenerate-days &lt;days_int&gt;</td>
<td>How many days before expiry the FortiGate unit requests an updated local certificate. The default is 0, no auto-update.</td>
</tr>
<tr>
<td>auto-regenerate-days-warning &lt;days_int&gt;</td>
<td>How many days before local certificate expiry the FortiGate generates a warning message. The default is 0, no warning.</td>
</tr>
</tbody>
</table>

In this example, an updated certificate is requested three days before it expires.
```
config vpn certificate local
  edit mycert
    set scep-url http://scep.example.com/scep
    set scep-server-password my_pass_123
    set auto-regenerate-days 3
    set auto-regenerate-days-warning 2
  end
```

CA certificates

In the `config vpn certificate ca` command, you can specify automatic certificate renewal. The relevant fields are:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scep-url &lt;URL_str&gt;</td>
<td>The URL of the SCEP server. This can be HTTP or HTTPS.</td>
</tr>
<tr>
<td>auto-update-days &lt;days_int&gt;</td>
<td>How many days before expiry the FortiGate unit requests an updated CA certificate. The default is 0, no auto-update.</td>
</tr>
<tr>
<td>auto-update-days-warning &lt;days_int&gt;</td>
<td>How many days before CA certificate expiry the FortiGate generates a warning message. The default is 0, no warning.</td>
</tr>
</tbody>
</table>

In this example, an updated certificate is requested three days before it expires.
```
config vpn certificate ca
  edit mycert
    set scep-url http://scep.example.com/scep
    set auto-update-days 3
    set auto-update-days-warning 2
  end
```

Certificate Revocation Lists

If you obtained your CRL using SCEP, you can configure online updates to the CRL using the `config vpn certificate crl` command. The relevant fields are:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>http-url &lt;http_url&gt;</td>
<td>URL of the server used for automatic CRL certificate updates. This can be HTTP or HTTPS.</td>
</tr>
<tr>
<td>scep-cert &lt;scep_certificate&gt;</td>
<td>Local certificate used for SCEP communication for CRL auto-update.</td>
</tr>
</tbody>
</table>
Managing X.509 certificates

Certificate-based authentication

**In this example, an updated CRL is requested only when it expires.**

```
config vpn certificate crl
  edit cert_crl
    set http-url http://scep.example.com/scep
    set scep-cert my-scep-cert
    set scep-url http://scep.ca.example.com/scep
    set update-interval 0
    set update-vdom root
  end
```

**Backing up and restoring local certificates**

The FortiGate unit provides a way to export a server certificate and the FortiGate unit’s personal key through the CLI. If required (to restore the FortiGate unit configuration), you can import the exported file through the System > Certificates > Local Certificates page of the web-based manager.

**Note:** As an alternative, you can back up and restore the entire FortiGate configuration through the System > Maintenance > Backup & Restore page of the web-based manager. The backup file is created in a FortiGate-proprietary format. For more information, see the “System Maintenance” chapter of the FortiGate Administration Guide.

**To export a server certificate and private key**

This procedure exports a server (local) certificate and private key together as a password protected PKCS12 file. The export file is created through a customer-supplied TFTP server. Ensure that your TFTP server is running and accessible to the FortiGate unit before you enter the command.

1. Connect to the FortiGate unit through the CLI.
2. Type the following command:
   
   ```
   execute vpn certificate local export tftp <cert_name> <exp_filename> <tftp_ip>
   ```
   
   where:
   
   - `<cert_name>` is the name of the server certificate; typing `?` displays a list of installed server certificates.
   - `<exp_filename>` is a name for the output file.
   - `<tftp_ip>` is the IP address assigned to the TFTP server host interface.
3. Move the output file from the TFTP server location to the management computer for future reference.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scep-url</td>
<td>URL of the SCEP CA server used for automatic CRL certificate updates. This can be HTTP or HTTPS.</td>
</tr>
<tr>
<td>scep_url</td>
<td>URL of the SCEP CA server used for automatic CRL certificate updates. This can be HTTP or HTTPS.</td>
</tr>
<tr>
<td>update-interval</td>
<td>How frequently, in seconds, the FortiGate unit checks for an updated CRL. Enter 0 to update the CRL only when it expires.</td>
</tr>
<tr>
<td>seconds</td>
<td>How frequently, in seconds, the FortiGate unit checks for an updated CRL. Enter 0 to update the CRL only when it expires.</td>
</tr>
<tr>
<td>update-vdom</td>
<td>VDOM used to communicate with remote SCEP server for CRL auto-update.</td>
</tr>
<tr>
<td>update_vdom</td>
<td>VDOM used to communicate with remote SCEP server for CRL auto-update.</td>
</tr>
</tbody>
</table>
To import a previously exported server certificate and private key

1. Go to **VPN > Certificates > Local Certificates** and select **Import**.

2. In **Type**, select **PKCS12 Certificate**.

3. Select **Browse**. Browse to the location on the management computer where the exported file has been saved, select the file, and then select **Open**.

4. In the **Password** field, type the password needed to upload the exported file.

5. Select **OK**, and then select **Return**.

To import separate server certificate and private key files

Use the following procedure to import a server certificate and the associated private key file when the server certificate request and private key were not generated by the FortiGate unit. The two files to import must be available on the management computer.

1. Go to **VPN > Certificates > Local Certificates** and select **Import**.

2. In **Type**, select **Certificate**.

3. Select the **Browse** button beside the **Certificate file** field. Browse to the location on the management computer where the certificate file has been saved, select the file, and then select **Open**.

4. Select the **Browse** button beside the **Key file** field. Browse to the location on the management computer where the key file has been saved, select the file, and then select **Open**.

5. If required, in the **Password** field, type the associated password, and then select **OK**.

6. Select **Return**.
Configuring certificate-based authentication

You can configure certificate-based authentication for FortiGate administrators, SSL VPN users, and IPsec VPN users.

Authenticating administrators with security certificates

You can install a certificate on the management computer to support strong authentication for administrators. When a personal certificate is installed on the management computer, the FortiGate unit processes the certificate after the administrator supplies a user name and password.

To enable strong administrative authentication:

- Obtain a signed personal certificate for the administrator from a CA and load the signed personal certificate into the web browser on the management computer according to the browser documentation.
- Install the root certificate and the CRL from the issuing CA on the FortiGate unit (see "Installing a CA root certificate and CRL to authenticate remote clients" on page 89).
- Create a PKI user account for the administrator.
- Add the PKI user account to a firewall user group dedicated to PKI-authenticated administrators.
- In the administrator account configuration, select PKI as the account Type and select the User Group to which the administrator belongs.

Authenticating SSL VPN users with security certificates

X.509 certificates can be used to authenticate IPsec VPN peers or clients, or SSL VPN clients. When configured to authenticate a VPN peer or client, the FortiGate unit prompts the VPN peer or client to authenticate itself using the X.509 certificate. The certificate supplied by the VPN peer or client must be verifiable using the root CA certificate installed on the FortiGate unit in order for a VPN tunnel to be established.

To enable certificate authentication for an SSL VPN user group

1 Install a signed server certificate on the FortiGate unit and install the corresponding root certificate (and CRL) from the issuing CA on the remote peer or client.
2 Obtain a signed group certificate from a CA and load the signed group certificate into the web browser used by each user. Follow the browser documentation to load the certificates.
3 Install the root certificate and the CRL from the issuing CA on the FortiGate unit (see "Installing a CA root certificate and CRL to authenticate remote clients" on page 89).
4 Create a PKI user for each SSL VPN user. For each user, specify the text string that appears in the Subject field of the user’s certificate and then select the corresponding CA certificate.
5 Use the config user peergrp CLI command to create a peer user group. Add to this group all of the SSL VPN users who are authenticated by certificate.
6 Go to VPN > SSL > Config.
7 Select Enable SSL-VPN.
8  Select Require Client Certificate, and then select Apply.
9  Go to Firewall > Policy.
10 Select the Edit icon in the row that corresponds to the SSL-VPN firewall policy for traffic generated by holders of the group certificate.
11 Select SSL Client Certificate Restrictive.
12 Select OK.

Authenticating IPsec VPN users with security certificates

To require VPN peers to authenticate by means of a certificate, the FortiGate unit must offer a certificate to authenticate itself to the peer.

To enable the FortiGate unit to authenticate itself with a certificate:

1  Install a signed server certificate on the FortiGate unit.
   See “To install the signed server certificate” on page 89.
2  Install the corresponding CA root certificate on the remote peer or client. If the remote peer is a FortiGate unit, see “To install a CA root certificate” on page 89.
3  Install the certificate revocation list (CRL) from the issuing CA on the remote peer or client. If the remote peer is a FortiGate unit, see “To import a certificate revocation list” on page 90.
4  In the VPN phase 1 configuration, set Authentication Method to RSA Signature and from the Certificate Name list select the certificate that you installed in Step 1.

To authenticate a VPN peer using a certificate, you must install a signed server certificate on the peer. Then, on the FortiGate unit, the configuration depends on whether there is only one VPN peer or if this is a dialup VPN that can have multiple peers.

To configure certificate authentication of a single peer

1  Install the CA root certificate and CRL.
2  Create a PKI user to represent the peer. Specify the text string that appears in the Subject field of the user’s certificate and then select the corresponding CA certificate.
3  In the VPN phase 1 Peer Options, select Accept this peer certificate only and select the PKI user that you created.

To configure certificate authentication of multiple peers (dialup VPN)

1  Install the corresponding CA root certificate and CRL.
2  Create a PKI user for each remote VPN peer. For each user, specify the text string that appears in the Subject field of the user’s certificate and then select the corresponding CA certificate.
3  Use the config user peergrp CLI command to create a peer user group. Add to this group all of the PKI users who will use the IPsec VPN.
4  In the VPN phase 1 Peer Options, select Accept this peer certificate group only and select the peer group that you created.
Monitoring authenticated users

This section describes how to view lists of currently logged-in firewall and VPN users. It also describes how to disconnect users.

The following topics are included in this section:

- Monitoring firewall users
- Monitoring SSL VPN users
- Monitoring IPsec VPN users

Monitoring firewall users

Go to User > Monitor > Firewall to view current authenticated users.

Figure 28: Firewall users listed in monitor

You can de-authenticate a user by selecting their Delete icon.

Monitoring SSL VPN users

You can monitor web-mode and tunnel-mode SSL VPN users by user name and IP address.

To monitor SSL VPN users - web-based manager

1. Go to VPN > SSL > Monitor.
2. To disconnect a user, selecting the user and then select the Delete icon.

Figure 29: Monitoring SSL VPN users

The first line, listing the user name and IP address, is present for a user with either a web-mode or tunnel-mode connection. The Subsession line is present only if the user has a tunnel mode connection. The Description column displays the virtual IP address assigned to the user's tunnel-mode connection.

To monitor SSL VPN users - CLI

To list all of the SSL VPN sessions and their index numbers:

execute vpn sslvpn list
The output looks like this:

SSL-VPN Login Users:

<table>
<thead>
<tr>
<th>Index</th>
<th>User</th>
<th>Auth Type</th>
<th>Timeout</th>
<th>From</th>
<th>HTTPS in/out</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>user1</td>
<td>1</td>
<td>256</td>
<td>172.20.120.51</td>
<td>0/0</td>
</tr>
</tbody>
</table>

SSL-VPN sessions:

<table>
<thead>
<tr>
<th>Index</th>
<th>User</th>
<th>Source IP</th>
<th>Tunnel/Dest IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>user2</td>
<td>172.20.120.51</td>
<td>10.0.0.1</td>
</tr>
</tbody>
</table>

You can use the Index value in the following commands to disconnect user sessions:

To disconnect a tunnel-mode user

```bash
execute vpn sslvpn del-tunnel <index>
```

To disconnect a web-mode user

```bash
execute vpn sslvpn del-web <index>
```

You can also disconnect multiple users:

**To disconnect all tunnel-mode SSL VPN users in this VDOM**

```
execlute vpn ssl del-all tunnel
```

**To disconnect all SSL VPN users in this VDOM**

```
execlute vpn ssl del-all
```

### Monitoring IPsec VPN users

To monitor IPsec VPN tunnels in the web-based manager, go to **VPN > IPsec > Monitor**. User names are available only for users who authenticate with XAuth.

You can close a tunnel by selecting its **Bring Down** link in the **Status** column.

**Figure 30: Monitoring dialup VPN users**

For more information, see the IPsec VPN chapter of this Handbook.
Example

This chapter provides an example of a FortiGate unit providing authenticated access to the Internet for both Windows network users and local users.

The following topics are included in this section:

- Firewall authentication example

Firewall authentication example

Overview

In this example, there is a Windows network connected to Port 2 on the FortiGate unit and another LAN, Network_1, connected to Port 3.

All Windows network users authenticate when they log on to their network. Members of the Engineering and Sales groups can access the Internet without entering their authentication credentials again. The example assumes that the Fortinet Server Authentication Extension (FSAE) has already been installed and configured on the domain controller.

LAN users who belong to the Internet_users group can access the Internet after entering their user name and password to authenticate. This example shows only two users, User1 is authenticated by a password stored on the FortiGate unit, User2 is authenticated on an external authentication server. Both of these users are referred to as local users because the user account is created on the FortiGate unit.
Creating a locally-authenticated user account

User1 is authenticated by a password stored on the FortiGate unit. It is very simple to create this type of account.

To create a local user - web-based manager
1. Go to User > User and select Create New.
2. Enter the following information: User name, Password.
   - **User Name**: User1
   - **Password**: hardtoguess
3. Select OK.

To create a local user - CLI

```bash
config user local
edit user1
   set type password
   set passwd hardtoguess
end
```

Creating a RADIUS-authenticated user account

To authenticate users using an external authentication server, you must first configure the FortiGate unit to access the server.

To configure the remote authentication server - web-based manager
1. Go to User > Remote > RADIUS and select Create New.
2. Enter the following information and select OK:
   - **Name**: OurRADIUSsrv
   - **Primary Server Name/IP**: 10.11.101.15
   - **Primary Server Secret**: OurSecret
   - **Authentication Scheme**: Select Use Default Authentication Scheme.

To configure the remote authentication server - CLI

```bash
config user radius
edit OurRADIUSsrv
   set server 10.11.102.15
   set secret OurSecret
   set auth-type auto
end
```

Creation of the user account is similar to the locally-authenticated account, except that you specify the RADIUS authentication server instead of the user’s password.

To configure a remote user - web-based manager
1. Go to User > User and select Create New.
2. Enter the following information and select OK:
   - **User Name**: User2
   - **RADIUS**: Select Match user on RADIUS server and then select OurRADIUSsrv from the list.
To configure a remote user - CLI

```
config user local
edit User2
  set name User2
  set type radius
  set radius-server OurRADIUSsrv
end
```

Creating user groups

There are two user groups: a Directory Services user group for FSAE users and a firewall user group for other users. It is not possible to combine these two types of users in the same user group.

Creating the Directory Services user group

For this example, assume that FSAE has already been set up on the Windows network and that it uses Advanced mode, meaning that it uses LDAP to access user group information. You need to

- configure LDAP access to the Windows AD global catalog
- specify the collector agent that sends user logon information to the FortiGate unit
- select Windows user groups to monitor
- select and add the Engineering and Sales groups to a Directory Services user group

To configure LDAP for Directory Services - web-based manager

1. Go to User > Remote > LDAP and select Create New.
2. Enter the following information:

<table>
<thead>
<tr>
<th>Name</th>
<th>ADserver</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Name / IP</td>
<td>10.11.101.160</td>
</tr>
<tr>
<td>Distinguished Name</td>
<td>dc=office,dc=example,dc=com</td>
</tr>
<tr>
<td>Bind Type</td>
<td>Regular</td>
</tr>
<tr>
<td>User DN</td>
<td>cn=FSAE_Admin,cn=users,dc=office,dc=example,dc=com</td>
</tr>
<tr>
<td>Password</td>
<td>set_a_secure_password</td>
</tr>
</tbody>
</table>

   Leave other fields at their default values.
3. Select OK.

To configure LDAP for Directory Services - CLI

```
config user ldap
edit "ADserver"
  set server "10.11.101.160"
  set dn "cn=users,dc=office,dc=example,dc=com"
  set type regular
  set username
    "cn=administrator,cn=users,dc=office,dc=example,dc=com"
  set password set_a_secure_password
next
end
```
To specify the collector agent for Directory Services - web-based manager

2. Enter the following information and select OK:

<table>
<thead>
<tr>
<th>Name</th>
<th>WinGroups</th>
</tr>
</thead>
<tbody>
<tr>
<td>FSAS Collector</td>
<td>10.11.101.160</td>
</tr>
<tr>
<td>IP/Name</td>
<td>8000</td>
</tr>
<tr>
<td>Password</td>
<td>fortinet_canada</td>
</tr>
<tr>
<td>LDAP Server</td>
<td>ADserver</td>
</tr>
</tbody>
</table>

To specify the collector agent for Directory Services - CLI

```
config user fsae
  edit "WinGroups"
  set ldap-server "ADserver"
  set password ENC
    G7G7Q7NEqilCM9jKmVmjJFVvhQ2+wtNEe9T0iYA5Sa+EqT2J8zh0rbkJFD
    r0RmY3c4La0Xs0BczAfONmcGfthTxxwGsigzGpbJdC71spF1QYtj
  set server "10.11.101.160"
end
```

To select Windows user groups to monitor - web-based manager

2. Expand WinGroups, then select the Edit Users/Groups icon.
3. Select the Engineering and Sales groups and then select OK.

To create the FSAE_Internet-users user group - web-based manager

1. Go to User > User Group and select Create New.
2. Enter the group name, FSAE_Internet_users.
4. In the Available Members list, select the Engineering and Sales groups and then select the right arrow button to move them to the Members list.
5. Select OK.

To create the FSAE_Internet-users user group - CLI

```
config user group
  edit FSAE_Internet_users
  set group-type directory-service
  set member
    CN=Engineering,cn=users,dc=office,dc=example,dc=com
    CN=Sales,cn=users,dc=office,dc=example,dc=com
end
```
Creating the Firewall user group

The non-FSAE users need a user group too. In this example, only two users are shown, but additional members can be added easily.

To create the firewall user group - web-based manager
1. Go to User > User Group and select Create New.
2. Enter the following information and then select OK:

   Name: Internet_users
   Type: Firewall
   Members: User1, User2

To create the firewall user group - CLI

   config user group
   edit Internet_users
   set group-type firewall
   set member User1 User2
   end

Defining firewall addresses

Go to Firewall > Address and create the following addresses:

   Address Name: Internal_net
   Type: Subnet / IP Range
   Subnet / IP Range: 10.11.102.0/24
   Interface: Port 3

   Address Name: Windows_net
   Type: Subnet / IP Range
   Subnet / IP Range: 10.11.101.0/24
   Interface: Port 2

Creating firewall policies

Two firewall policies are needed: one for firewall group who connect through port3 and one for FSAE group who connect through port2.

To create a firewall policy for FSAE authentication - web-based manager
1. Go to Firewall > Policy and select Create New.
2. Enter the following information:

   Source interface: Port2
   Source address: Windows_net
   Destination interface: Port1
   Destination address: all
   Action: ACCEPT
   NAT: Enable
3 Select Enable Identity Based Policy and then select Add.

In the New Authentication Rule window, enter the following information, and then select OK:

- **User Group**: FSAE_Internet_users
- **Service**: ANY
- **Schedule**: always
- **UTM**: Optionally, enable UTM options.

4 Select OK.

**To create a firewall policy for FSAE authentication - CLI**

```
config firewall policy
edit 0
set srcintf port2
set dstintf port1
set srcaddr Windows_net
set dstaddr all
set action accept
set identity-based enable
set nat enable
config identity-based-policy
edit 1
set schedule always
set groups FSAE_Internet_users
set service ANY
end
end
```

**To create a firewall policy for local user authentication - web-based manager**

1 Go to `Firewall > Policy` and select `Create New`.
2 Enter the following information:

- **Source interface**: Port3
- **Source address**: Internal_net
- **Destination interface**: Port1
- **Destination address**: all
- **Action**: ACCEPT
- **NAT**: Enable

3 Select Enable Identity Based Policy and then select Add.

In the New Authentication Rule window, enter the following information, and then select OK:

- **User Group**: Internet_users
- **Service**: ANY
- **Schedule**: always
- **UTM**: Optionally, enable UTM options.

4 Select OK.
To create a firewall policy for local user authentication - CLI

```plaintext
config firewall policy
edit 0
set srcintf port3
set dstintf port1
set srcaddr internal_net
set dstaddr all
set action accept
set identity-based enable
set nat enable
config identity-based-policy
edit 1
set schedule always
set groups Internet_users
set service ANY
end
end
```
Index

A
access
guest users, 82
Active Directory - see Directory Service
ASCII, 36
attributes
  RADIUS, 29
authenticating access
  configuring, 47
authenticated access
  FortiGate, 39
  with LDAP servers, 40
  with RADIUS servers, 40
  with TACACS+ servers, 40
authentication
  firewall policy, 49
  Internet access, 51
  IPsec VPN, 52
  L2TP, 55
  overview, 85
  PPTP VPN, 54
  protocols, 48
  SSL VPN, 51
  SSL VPN timeout, 52
  timeout, 47
  VPN, 51
  VPN client-based, 26
  web-based user, 25
XAuth, 53
authentication protocols
  ASCII, 36
  CHAP, 36
  MS-CHAP, 36
  PAP, 36
  setting, 48
  TACACS+ servers, 36
authentication servers
  Directory Service, 37
  LDAP, 31
  RADIUS, 29
  TACACS+, 35
authentication timeout
  firewall, 47
  setting, 47
  SSL VPN, 47, 52

B
binding
  LDAP servers, 31

C
certificate request, 87
  generating, 86
certificate revocation list
  importing, 90
certificates
  importing CRL, 90
  installing root CA, 89
  installing signed server, 89
  obtaining signed server, 89
certification, 19
  CHAP, 36
  CLI syntax conventions, 15
collector agent
  settings, 65
  specifying, 78
comments, documentation, 19
common name
  LDAP servers, 32
collection
configuration
  collector agent, 65
  collector agent Ignore User list, 67
  collector agent LDAP access, 67
  collector agent TCP ports, 70
  FortiGate firewall policies, 81
  LDAP server, FortiGate unit, 76
  testing, 83
configuring
  authenticated access, 47
  firewall policy authentication, 49
  Internet access authentication, 51
  IPsec VPN authentication, 52
  L2TP VPN authentication, 55
  local users, 40
  peer user groups, 45
  peer users, 41
  PPTP VPN authentication, 54
  SSL VPN authentication, 51
  XAuth authentication for IPsec dialup users, 53
  XAuth authorization with LDAP servers, 53
  XAuth authentication with RADIUS servers, 53
conventions, 11
creating
  local users, 40
  peer user groups, 45
  peer users, 41
  user groups, 44
Cross-Site Scripting
  protection from, 17
customer service, 19

D
Dead entry timeout
  collector agent configuration, 66
default
  password, 9
default port
RADIUS servers, 30
TACACS+ servers, 35
deleting
local users from FortiGate configuration, 41
user group from FortiGate configuration, 46
dialup users
configuring authentication for, 52
dictionary
RADIUS attributes, 30
directory
LDAP servers, 31
Directory Service
user groups, 45
Directory Service servers, 37
distinguished names
elements, 32
LDAP servers, 32
list of, 34
document conventions
CLI syntax, 15
documentation, 19
commenting on, 19
conventions, 11
Fortinet, 19
domain component
LDAP servers, 32

E
edirectory - see Directory Service
elements
distinguished names, 32

F
FAQ, 19
firewall
configuring user groups, 44
creating user groups, 44
Internet access authentication, 51
IPsec VPN dialup user access, 43
policy authentication, 49
user authentication timeout, 47
user groups, 43
firewall policy and strong authentication, 95
FortiGate
authenticating users, 39
authenticating with XAuth, 53
configuring to use LDAP server, 33
configuring to use RADIUS server, 30
configuring to use TACACS+ server, 36
IPsec VPN, 52
FortiGate documentation
commenting on, 19
FortiGuard
Antispam, 9
Antivirus, 9, 18
services, 18

Fortinet
Knowledge Center, 19
Technical Documentation, 19
Technical Documentation, conventions, 11
Technical Support, 19
Technical Support, registering with, 18
Technical Support, web site, 18
Training Services, 19
Fortinet customer service, 19
Fortinet documentation, 19
Fortinet Knowledge Center, 19

G
glossary, 19
group filters
FortiGate, on collector agent, 68
groups
Windows AD, viewing on FortiGate, 79

H
hierarchy
LDAP servers, 32
how-to, 19

I
Idle timeout
VPN connection, 26
Internet access authentication, 51
introduction
Fortinet documentation, 19
IP address
private network, 11
IP address range
setting for L2TP VPN, 55
setting for PPTP VPN, 54
setting for SSL VPN, 51
IPsec VPN
configuring authentication for, 52
dialup users, access to, 43
dialup users, configuring authentication for, 52

K
Knowledge Center, 19

L
L2TP VPN
configuring authentication for, 55
LDAP
FortiGate configuration, 76
XAuth authentication with, 53
LDAP access
collector agent, 67
LDAP servers, 31
  authenticating users with, 40
  binding, 31
  common name, 32
  configuring FortiGate unit to use, 33
  directory, 31
  Distinguished Name Query list, 34
  distinguished names, 32
  domain component, 32
  hierarchy, 32
  protocols, 32
  RFC compliance, 32
Local certificates
  generating request, 86
  installing signed, 89
local users
  configuring, 40
  creating, 40
  deleting from FortiGate configuration, 41
  removing from FortiGate configuration, 41
  logging in, security messages, 85
M
  mode
    operation, 9
  MS-CHAP, 36
N
  Novell edirectory - see Directory Service
  NTLM implementation, 60
  NTLM mode, 59
  NT-style domain mode implementation, 58
O
  operation mode, 9
P
  PAP, 36
  password
    administrator, 9
  peer user groups
    configuring, 45
    creating, 45
  peer users, 39, 41
    configuring, 41
    creating, 41
  PKI authentication - see peer users
  port
    RADIUS servers, 30
  PPTP VPN
    authentication, 54
    configuring authentication for, 54
    IP address range, 54
  product registration, 18
  protocols
    authentication, 48
    LDAP servers, 32
Q
  Query list
    LDAP Distinguished Name, 34
R
  RADIUS
    XAuth authentication with, 53
  RADIUS attributes, 29
  RADIUS authentication servers, 29
  RADIUS servers
    attribute dictionary, 30
    authenticating users with, 40
    changing default port, 30
    configuring FortiGate unit to use, 33
    default port, 30
    port, 30
    VSA, 30
  registering
    with Fortinet Technical Support, 18
  removing
    local users from FortiGate configuration, 41
    user group from FortiGate configuration, 46
  Require Client Certificate option, 95
  revocation list, importing, 89
  RFC
    1918, 11
  RFC compliance
    LDAP servers, 32
  root certificate, installing, 89
S
  self-signed certificate, installing, 85
  server certificate
    installing signed, 89
    obtaining, 89
  servers
    configuring XAuth authentication using, 53
  setting
    authentication protocols, 48
    firewall policy authentication, 49
    firewall user authentication timeout, 47
    SSL VPN authentication timeout, 47, 52
  SSL Client Certificate Restrictive option, 95
  SSL VPN
    authentication timeout, 47, 52
    user authentication, 51
  SSL VPN user groups, 43
    configuring, 43
    creating, 43
    IPsec VPN dialup users, 43
  strong authentication, 94
    for administrators, 94
    for SSL VPN users, 94
  system requirements
    Windows, 61
T
TACACS+ servers, 35
  ASCII, 36
  authenticating users with, 40
  authentication protocols, 36
  changing default port, 35
  CHAP, 36
  configuring the FortiGate unit to use, 36
  default port, 35
  MS-CHAP, 36
  PAP, 36
  port, 35
TCP ports
  for collector agent, 70
technical
documentation, 19
  documentation conventions, 11
  notes, 19
  support, 19
technical support, 19
testing configuration, 83
Training Services, 19
tunnel mode
  SSL VPN IP range, 51
two-factor authentication, 23, 42
types of user groups, 43
types of users, 39

U
user authentication
  IPsec VPN dialup users, 52
  L2TP VPN, 55
  PPTP VPN, 54
  protocols, 48
  SSL VPN, 51
  timeout, 47
  XAuth, 53
user groups, 43
  creating, 44
  Directory Service, 45
  firewall, 43
  on authentication servers, 44
  on FortiGate unit, 81
  peer, configuring, 45
  peer, creating, 45
types of, 43
  Windows AD, 64
users, 39
  authenticating with LDAP servers, 40
  authenticating with RADIUS servers, 40
  authenticating with TACACS+ servers, 40
  local, creating, 40
  local, deleting from FortiGate configuration, 41
  local, removing from FortiGate configuration, 41
  peer, configuring, 41
  peer, creating, 41
types of, 39

V
vendor-specific attributes - see VSA
VPN
  IPsec, 52
  L2TP, 55
  PPTP, 54
  SSL, 51
VPN authentication, 51
VPN client-based authentication, 26
VPN connection
  idle timeout, 26
VSA
  RADIUS servers, 30
vulnerability
  Cross-Site Scripting, 17
  XSS, 17

W
web-based user authentication, 25
Workstation verify interval
  collector agent configuration, 66

X
X.509 security certificates
  managing, 86
  XAuth, 53
    configuring authentication with, 53
  XSS vulnerability
    protection from, 17