



ADMINISTRATION GUIDE

Fortinet Server Authentication Extension™ Version 3.0 MR7

Visit <http://support.fortinet.com> to register your Fortinet Server Authentication Extension product. By registering you can receive product updates, technical support, and FortiGuard services.

FORTINET®

www.fortinet.com

Fortinet Server Authentication Extension™ Administration Guide
Version 3.0 MR7 (Build 031)
18 July 2008
01-30007-0373-20080718

© Copyright 2008 Fortinet, Inc. All rights reserved. No part of this publication including text, examples, diagrams or illustrations may be reproduced, transmitted, or translated in any form or by any means, electronic, mechanical, manual, optical or otherwise, for any purpose, without prior written permission of Fortinet, Inc.

Trademarks

Fortinet, FortiGate and FortiGuard are registered trademarks and Dynamic Threat Prevention System (DTPS), APSecure, FortiASIC, FortiBIOS, FortiBridge, FortiClient, FortiDB, FortiGate, FortiGate Unified Threat Management System, FortiGuard-Antispam, FortiGuard-Antivirus, FortiGuard-Intrusion, FortiGuard-Web, FortiLog, FortiAnalyzer, FortiManager, FortiOS, FortiPartner, FortiProtect, FortiReporter, FortiResponse, FortiShield, and FortiVoIP, are trademarks of Fortinet, Inc. in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Contents

Introduction	5
About FSAE.....	5
About this document.....	5
Document conventions.....	5
Typographic conventions.....	6
Fortinet documentation	6
Fortinet Tools and Documentation CD.....	7
Fortinet Knowledge Center	7
Comments on Fortinet technical documentation	7
Customer service and technical support	7
FSAE overview	9
Introduction.....	9
Operating system requirements.....	11
Understanding NTLM authentication.....	11
Understanding the NTLM authentication process.....	11
Installing FSAE on your network.....	13
FSAE components.....	13
FSAE components for Windows AD	13
FSAE components for Novell eDirectory.....	13
Installing FSAE for Windows AD.....	14
To install the FSAE collector agent.....	14
To install the DC Agent.....	14
Installing FSAE for Novell.....	15
To install the FSAE Novell agent	15
Configuring FSAE	17
Configuring FSAE on Windows AD	17
Configuring Windows AD server user groups	17
Configuring collector agent settings	18
To configure the FSAE collector agent	18
Configuring AD settings	20
Configuring the Ignore User List	20
To configure the Ignore User List	20
Configuring FortiGate group filters	20
To configure a FortiGate group filter.....	21
Configuring TCP ports for FSAE	23
Configuring alternate user IP address tracking	23
To configure alternate user IP address tracking	23

Configuring FSAE on Novell networks.....	24
To configure the eDirectory agent	24
To add an eDirectory server	25
Configuring FSAE on FortiGate units.....	26
Configuring the LDAP server	26
To configure LDAP server access	26
Specifying your collector agents or Novell eDirectory agents	27
To specify collector agents	27
Selecting Windows user groups (LDAP only)	27
To select Windows user groups	27
Viewing information imported from the Windows AD server	28
Creating user groups	30
To create a user group for FSAE authentication	30
Creating firewall policies	31
To create a firewall policy for FSAE authentication	31
Allowing guests to access FSAE policies	31
Testing the configuration	32
Index.....	33

Introduction

This chapter introduces you to the Fortinet Server Authentication Extension (FSAE) and the following topics:

- [About FSAE](#)
- [About this document](#)
- [Fortinet documentation](#)
- [Customer service and technical support](#)

About FSAE

The Fortinet Server Authentication Extension (FSAE) provides seamless authentication of Microsoft Windows Active Directory users on FortiGate units.



Fortinet Server Authentication Extension (FSAE) version 3.5 is Microsoft Certified for Windows Server 2003 Standard Edition (32-bit and 64-bit).

About this document

This document explains how to install and configure FSAE.

This document contains the following chapters:

- [“FSAE overview”](#) describes the purpose and operation of FSAE.
- [“Configuring FSAE”](#) describes how to configure FSAE agents on Windows and Novell networks and how to configure FortiGate unit to obtain authentication information from FSAE.

Document conventions

The following document conventions are used in this guide:

- 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>.

- Notes and Cautions are used to provide important information:



Note: Highlights useful additional information.



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

Typographic conventions

Fortinet documentation uses the following typographical conventions:

Convention	Example
Keyboard input	In the Gateway Name field, type a name for the remote VPN peer or client (for example, <code>Central_Office_1</code>).
Code examples	<pre>config sys global set ips-open enable end</pre>
CLI command syntax	<pre>config firewall policy edit id_integer set http_retry_count <retry_integer> set natip <address_ipv4mask> end</pre>
Document names	<i>FortiGate Administration Guide</i>
File content	<pre><HTML><HEAD><TITLE>Firewall Authentication</TITLE></HEAD> <BODY><H4>You must authenticate to use this service.</H4></pre>
Menu commands	Go to VPN > IPSEC > Phase 1 and select Create New.
Program output	Welcome!
Variables	<address_ipv4>

Fortinet documentation

The most up-to-date publications and previous releases of Fortinet product documentation are available from the Fortinet Technical Documentation web site at <http://docs.forticare.com>.

The following [FortiGate product documentation](#) is available:

- *FortiGate QuickStart Guide*
Provides basic information about connecting and installing a FortiGate unit.
- *FortiGate Installation Guide*
Describes how to install a FortiGate unit. Includes a hardware reference, default configuration information, installation procedures, connection procedures, and basic configuration procedures. Choose the guide for your product model number.

- *FortiGate Administration Guide*
Provides basic information about how to configure a FortiGate unit, including how to define FortiGate protection profiles and firewall policies; how to apply intrusion prevention, antivirus protection, web content filtering, and spam filtering; and how to configure a VPN.
- *FortiGate online help*
Provides a context-sensitive and searchable version of the *Administration Guide* in HTML format. You can access online help from the web-based manager as you work.
- *FortiGate CLI Reference*
Describes how to use the FortiGate CLI and contains a reference to all FortiGate CLI commands.
- *FortiGate Log Message Reference*
Available exclusively from the [Fortinet Knowledge Center](#), the FortiGate Log Message Reference describes the structure of FortiGate log messages and provides information about the log messages that are generated by FortiGate units.
- *FortiGate High Availability User Guide*
Contains in-depth information about the FortiGate high availability feature and the FortiGate clustering protocol.
- *FortiGate VLANs and VDOMs User Guide*
Describes how to configure VLANs and VDOMS in both NAT/Route and Transparent mode. Includes detailed examples.

Fortinet Tools and Documentation CD

All Fortinet documentation is available on the Fortinet Tools and Documentation CD shipped with your Fortinet product. The documents on this CD are current at shipping time. For up-to-date versions of Fortinet documentation visit the Fortinet Technical Documentation web site at <http://docs.forticare.com>.

Fortinet Knowledge Center

Additional Fortinet technical documentation is available from the Fortinet Knowledge Center. The knowledge center contains troubleshooting and how-to articles, FAQs, technical notes, a glossary, and more. Visit the Fortinet Knowledge Center at <http://kc.forticare.com>.

Comments on Fortinet technical documentation

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

Customer service and technical support

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

Please visit the Fortinet Technical Support web site at <http://support.fortinet.com> to learn about the technical support services that Fortinet provides.

FSAE overview

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

- [Introduction](#)
- [Operating system requirements](#)
- [Understanding NTLM authentication](#)

Introduction

On a Microsoft Windows or Novell network, users authenticate 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.

FortiGate units control access to resources based on user groups. Through FSAE, you can make Novell or Windows Active Directory (AD) groups known to the FortiGate unit and include them as members of FortiGate user groups.

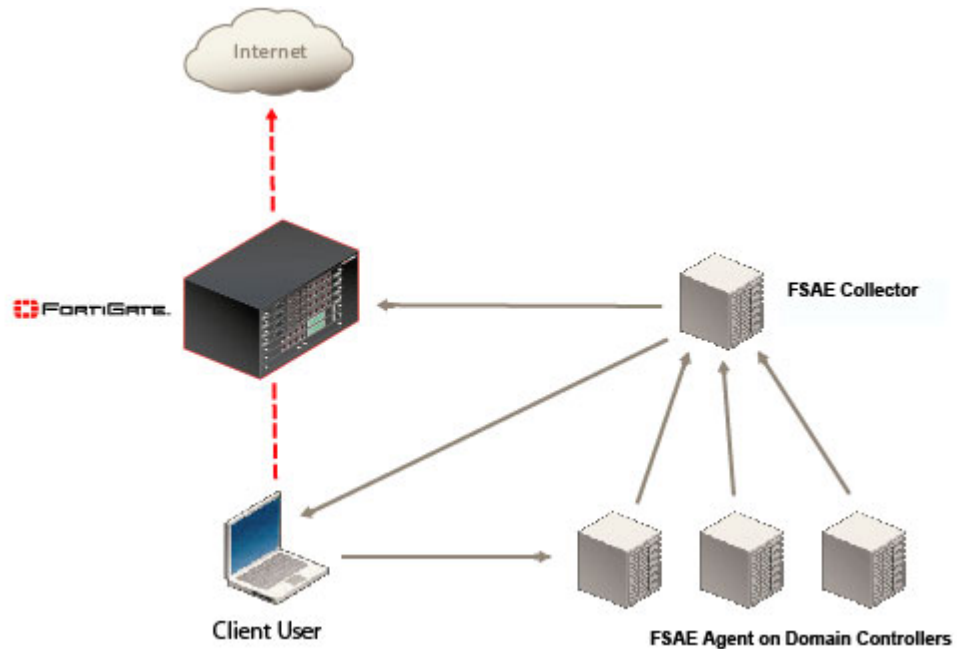
There are several mechanisms for passing user authentication information to the FortiGate unit:

- FSAE software installed on a Novell network monitors user logons and sends the required information directly 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 directly to the FortiGate unit. 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) access.
- Using the NTLM protocol, the FortiGate unit requests information from the Windows network to verify user authentication. This is used where it is not possible to install dc agents on every domain controller. The user must use the Internet Explorer (IE) browser.

FSAE has components that you must install on your network:

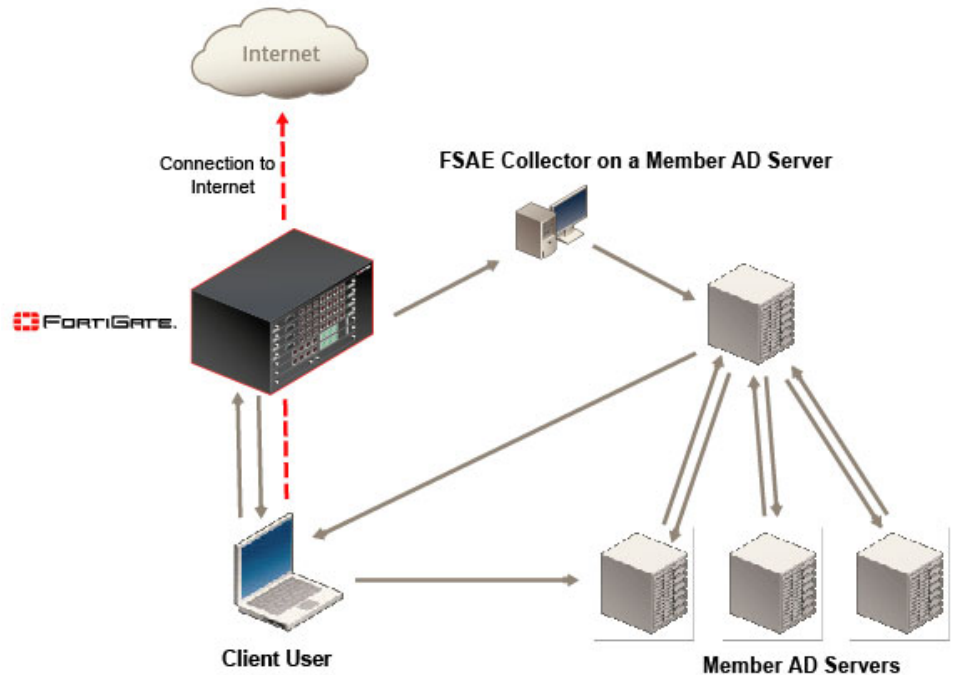
- On a Windows AD network, the domain controller (DC) agent must be installed on every domain controller to monitor user logons and send information about them to the collector agent.
- On a Windows AD network, the collector agent must be installed on at least one computer on the Windows network. The collector agent computer does not need to be a domain controller. The collector agent sends information received from the DC agents to the FortiGate unit.
- On a Novell network, the Novell eDirectory agent must be installed on at least one computer on the network.

Figure 1: FSAE with DC agent



In [Figure 1](#), the Client User logs on to the Windows domain, information is forwarded to the FSAE collector agent by the FSAE agent on the domain controller and, if authentication is successful, is then sent through the collector agent to the FortiGate unit.

Figure 2: NTLM FSAE implementation



In [Figure 2](#), the Client User logs on to the Windows domain. The FortiGate unit intercepts the request, and requests information about the user login details. The returned values are compared to the stored values on the FortiGate unit that have been received from the domain controller.

Operating system requirements

Note the following operating system requirements:

Server: Microsoft Windows 2000 or Microsoft Windows 2003 (32-bit and 64-bit)

- FSAE DC Agent is implemented as a Windows Subauthentication Package. On Windows 2000/2003 servers, installing a Windows Subauthentication Package requires a reboot.
- The FSAE DC Agent DLL, `dcagent.dll`, is installed in the Windows system directory (e.g. `c:\windows\system32\`).

Client: Microsoft Windows 2000 Professional or Microsoft Windows XP Professional

Understanding NTLM authentication

In system configurations where it is not possible to install FSAE clients on all AD servers, the FortiGate unit must be able to query the AD servers to find out if a user has been properly authenticated. This is achieved through the NTLM messaging features of Active Directory and the web browser. 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-Authenticate: 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 The FortiGate unit checks with the FSAE client (over port 8000) to see if the authentication hash matches the one on the domain controller. The FortiGate unit will deny the authentication by issuing a 401 return code and prompt for a username and password, or return an “OK” response and the Window’s group name(s) for the client.

Unless the TCP connection is broken, no further credentials are sent from the client to the proxy.

- 7 The FortiGate unit uses the group name(s) to match a protection profile for the client, and establishes a temporary firewall policy that allows future traffic to pass through the FortiGate unit.



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

Installing FSAE on your network

This chapter explains how to install FSAE on your network. The following topics are included:

- [FSAE components](#)
- [Installing FSAE for Windows AD](#)
- [Installing FSAE for Novell](#)

FSAE components

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 that you must install on your network:

- The domain controller (DC) agent, which must be installed on every domain controller
- The collector agent, which must be installed on at least one network computer

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 Novell agent.

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 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 check box.
 - Select the Serve NTLM authentication requests check box.If you do not want to support NTLM authentication
 - Clear the Serve NTLM authentication requests check box.
 - Select the Monitor user logon events check box.You can also change these options after installation.
- 7 Select Next and then select Install.
- 8 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.
- 9 Select Next and then select Install.
- 10 When the FSAE InstallShield Wizard completes FSAE collector agent installation, ensure that Launch DC Agent Install Wizard is selected and 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 Verify the list of trusted domains 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 17](#).
- 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 Next.
- 9 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 14](#) 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 26](#).

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 Novell eDirectory 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 Novell 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 FSAE 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 24.

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

This chapter explains how to configure FSAE on your network and how to configure a FortiGate unit to receive authentication information from FSAE.

- [Configuring FSAE on Windows AD](#)
- [Configuring FSAE on Novell networks](#)
- [Configuring FSAE on FortiGate units](#)
- [Testing the configuration](#)

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 23](#).

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 and 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.
AD access mode	Determines how FSAE obtains user group information and the format in which the information is displayed: NT-style Domain Mode - receive information from collector agent. Available on all releases of FortiOS 3.0. Group information is in the form domain/group. Active Directory Native Mode - obtain user group information using LDAP. Compatible with FortiOS 3.0 MR6 or later. Group information is in LDAP format.
AD Settings	If AD access mode is Active Directory native mode, you need to configure LDAP access to the domain global catalog. See "Configuring AD settings" on page 20 .
Domain controller monitored by this collector agent	Lists domain controllers. Checkmarks indicate where the FSAE domain controller agent is installed. Use the Select Domain button to remove unwanted domains from this list.

Select Domains	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.
Group Filter	Configure group filtering for each FortiGate unit. See “Configuring FortiGate group filters” on page 20.
Ignore User List	Exclude users such as system accounts that do not authenticate to any FortiGate unit. See “Configuring the Ignore User List” on page 20.
Sync Configuration	Copy this collector agent's Ignore User List and Group Filters to the other collector agents to synchronize the configuration. You are asked to confirm synchronization for each collector agent.
Listening ports	You can change port numbers if necessary.
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.
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 page 23.
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.
Save & Close	Save the modified settings and exit.
Apply	Apply changes now.
Default	Change all settings to the default values.
Help	View the online Help.



Note: To view the version and build number information for your FSAE configuration, click the Fortinet icon in the upper left corner of the Fortinet Collector Agent Configuration screen and select “About FSAE configuration”.

Configuring AD settings

If you selected Active Directory native mode, you need to configure LDAP access for user group information. For the domain where FSAE is installed, select AD Settings. For other domains, select Select Domains, select the domain and then select Setting. Enter the following information, select OK, and repeat for each required domain:

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 Select 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.

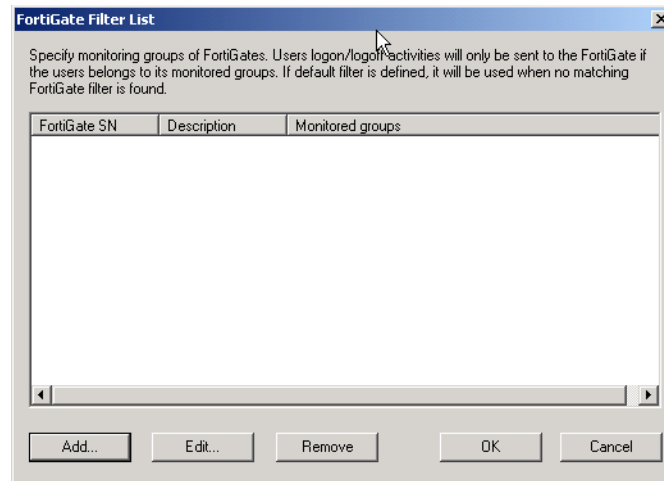


Note: If no filter is defined for a FortiGate unit and there is no default filter, the collector agent sends all Windows AD group and user logon events to the FortiGate unit. While this normally is not a problem, limiting the amount of data sent to the FortiGate unit improves performance by reducing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

The FortiGate Filter List opens. It has the following columns:



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	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 the FortiGate unit 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 "AD access mode" on page 18): <ul style="list-style-type: none"> • NT-style Domain mode: Domain/Group • Active Directory native mode: cn=group, ou=corp, dc=domain
Advanced	Select Advanced, select the user groups from the list, and then select Add.
Remove	Remove the user groups selected in the monitor list.

Configuring TCP ports for FSAE

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 19](#) in the [Configuring FSAE](#) section.

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.
The Registry Editor opens.
- 3 Find the registry key
HKEY_LOCAL_MACHINE\SOFTWARE\Fortinet\FSAE\collectoragent.
- 4 Set the supportFSAEauth value (dword) to 00000001.
- 5 Close the Registry Editor.
- 6 From the Start menu select **Programs > Fortinet > Fortinet Server Authentication Extension > Configure FSAE**.
- 7 Select Apply.

The FSAE service restarts with the updated registry settings.

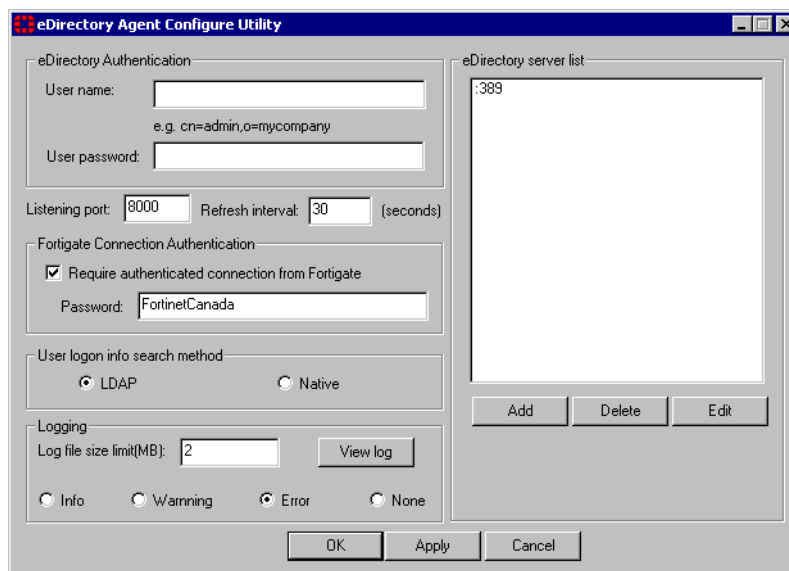
Configuring FSAE on Novell networks

You need to configure the 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 eDirectory agent accesses user logon information: LDAP or native Novell API. LDAP is the default. If you select native Novell API, you must also have the Novell Client installed on the PC.

Logging

- Log level** Select Info, Warning or Error as the minimum severity level of message to log or select None to disable logging.
- Log file size limit (MB)** Enter the maximum size for the log file in MB.
- View Log** View the current log file.

eDirectory server list

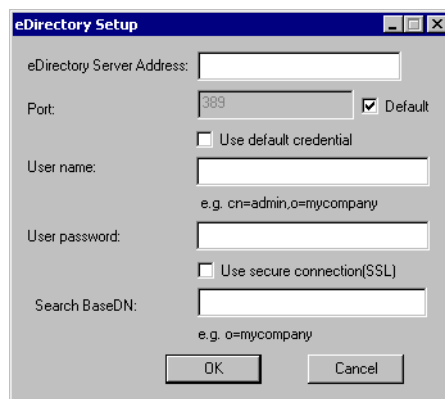
If you specified an eDirectory server during installation, it appears in this list.

- Add** Add an eDirectory server. See [“To add an eDirectory server”](#), next.
- Delete** Delete the selected eDirectory server.
- Edit** Modify the settings for the selected server.

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.



- 2 Enter the following information and select OK:

- eDirectory Server Address** Enter the IP address of the eDirectory server.
- Port** If the eDirectory server does not use the default port 389, clear the Default check box and enter port number.
- Use default credential** Select to use the credentials specified in the eDirectory Configuration Utility. See [“To configure the eDirectory agent” on page 24](#). Otherwise, leave the check box clear and enter a User name and Password below.
- User name** Enter a user name that has access to the eDirectory, using LDAP format.
- User password** Enter the password.
- 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.

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,
- specify Windows AD servers that contain an FSAE collector agent or the server on the Novell network that contains the Novell eDirectory agent,
- add Active Directory user groups to new or existing FortiGate user groups,
- create firewall policies for Windows AD Server groups,
- optionally, specify a guest protection profile to allow guest access,

Configuring the LDAP server

LDAP access is required if your network has a Novell eDirectory agent or a collector agent using Windows AD native mode.

To configure LDAP server access

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

Name	Enter the name used to identify the LDAP server.
Server Name/IP	For Novell eDirectory, enter the IP address or name of the Novell eDirectory server. For Windows AD, enter the IP address or name of the Windows AD global catalog LDAP server.
Server Port	Enter the port used to communicate with the LDAP server. By default, LDAP uses port 389. Note: If you use a secure LDAP server, the default port will reflect your selection in Protocol.
Common Name Identifier	Enter the common name identifier for the LDAP server (20 characters maximum). The default common name identifier is <code>cn</code> . This is correct for most LDAP servers. However some servers use other common name identifiers such as <code>uid</code> .
Distinguished Name	Enter the distinguished name used to look up entries on the LDAP server. For example, <code>dc=example,dc=com</code> 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.
Query icon	View the LDAP server Distinguished Name Query tree for the base Distinguished Name. Expand the Common Name identifier to see the associated DNSs. You can copy and paste the DN from the list into the Distinguished Name field. Select OK.
Bind Type	Select Regular. This is the default for Windows LDAP.
Filter	Enter the filter used for group searching. Use <code>(objectclass=*)</code> to search all objects.
User DN	Distinguished name of the user to be authenticated. Available if Bind Type is Regular. For example, <code>cn=administrator, cn=users,dc=sample,dc=com</code>
Password	Password of user to be authenticated. Available if Bind Type is Regular.
Secure Connection	Do not select. The FSAE collector agent does not support secure connection.

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 Windows AD 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

- 1 Go to **User > Directory Service** and select Create New.
- 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.
FSAE Collector IP	Enter the following information for up to five collector agents.
IP Address	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 18 or "Configuring FSAE on Novell networks" on page 24.
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. See "Configuring FSAE" on page 17.
LDAP Server	For Novell eDirectory, enable. For Windows AD, enable if the collector agent is configured to use Active Directory Native Mode. Select the LDAP server you configured previously. See "Configuring the LDAP server" on page 26.

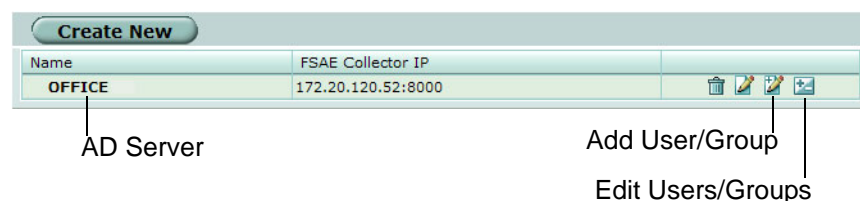
Selecting Windows user groups (LDAP only)

If the collector agent uses Windows AD native 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

- 1 Go to **User > Directory Service**.
The list of Directory Service servers is displayed.

Figure 3: List of Directory Service servers



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

- 3 Select the check boxes of the user groups that you want to monitor and then select OK.

Figure 4: Result of Directory Service LDAP query



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 NT-style Domain mode and Active Directory native mode.

Figure 5: List of groups from Active Directory server (NT-style Domain mode)

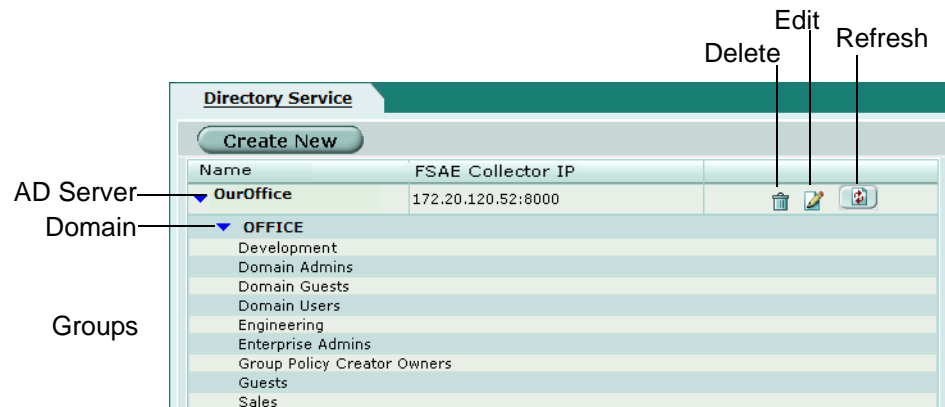
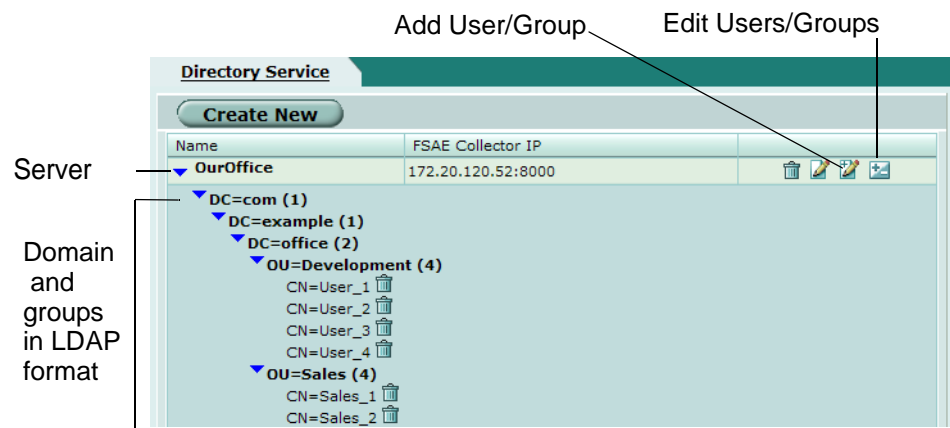


Figure 6: List of groups from Active Directory server (AD native mode)



- 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 AD Native mode only.
- Edit Users/Groups** Select users and groups to add to the list. See [“Selecting Windows user groups \(LDAP only\)” on page 27](#). This is available in AD Native mode only.

Creating user groups

You cannot use Directory Service groups directly in FortiGate firewall policies. You must add Directory Service groups to FortiGate user groups.

To create a user group for FSAE authentication

- 1 Go to **User > User Group**.
- 2 Select **Create New**.

The New User Group dialog box opens.

Figure 7: New User Group dialog box

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

Creating firewall policies

Policies that require FSAE authentication are very similar to other firewall policies. Currently, only one single authentication firewall policy can be configured if the source interface/source IP pair is the same.

To create a firewall policy for FSAE authentication

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

Source interface and address	as required
Destination interface and address	as required
Schedule	as required
Service	ANY
Action	ACCEPT
NAT	as needed
- 3 Select Authentication and then select Directory Service (FSAE) from the adjacent list.
- 4 Select the required user group from the Available Groups list and then select the right arrow button to move the selected group to the Allowed list.
You can select multiple groups using the CTRL or SHIFT keys.
- 5 Select OK.

Allowing guests to access FSAE policies

You can allow 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 allow guest access, use the FortiGate web-based manager or CLI to specify a guest protection profile for your FSAE firewall policy. For example

```
config firewall policy
  edit FSAE_policy
    set fsae-guest-profile strict
  end
```

You can specify any existing protection profile or create a custom protection profile to assign to guest users. For more information, see the Firewall Protection Profile chapter of the *FortiGate Administration Guide*.

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 username 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.

Index

A

access
 guest users, 31

C

collector agent, 9
 settings, 18
 specifying, 27
 comments, documentation, 7
 configuration
 collector agent, 18
 collector agent Ignore User list, 20
 collector agent LDAP access, 20
 collector agent TCP ports, 23
 FortiGate firewall policies, 31
 LDAP server, FortiGate unit, 26
 on Windows, 17
 testing, 32
 customer service, 7

D

Dead entry timeout
 collector agent configuration, 19
 documentation
 commenting on, 7
 Fortinet, 6
 domain controller, 9

F

FortiGate documentation
 commenting on, 7
 Fortinet customer service, 7
 Fortinet documentation, 6
 Fortinet Knowledge Center, 7

G

group filters
 FortiGate, on collector agent, 20

groups
 Windows AD, viewing on FortiGate, 28

I

installation
 Windows, 13
 introduction
 Fortinet documentation, 6

L

LDAP
 FortiGate configuration, 26
 LDAP access
 collector agent, 20

N

NTLM implementation, 10
 NTLM mode, 11
 NT-style domain mode implementation, 10

S

system requirements
 Windows, 11

T

TCP ports
 for collector agent, 23
 technical support, 7
 testing configuration, 32

U

user groups
 on FortiGate unit, 30
 Windows AD, 17

W

Workstation verify interval
 collector agent configuration, 19

FORTINET®

www.fortinet.com

FORTINET®

www.fortinet.com