



**FortiGate™ Certificate Management
Version 4.0**

FORTINET™

www.fortinet.com

FortiGate™ Certificate Management User Guide
Version 4.0
05 October 2007
01-30005-0182-20071005

© Copyright 2007 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

Dynamic Threat Prevention System (DTPS), APSecure, FortiASIC, FortiBIOS, FortiBridge, FortiClient, FortiGate, FortiGate Unified Threat Management System, FortiGuard, FortiGuard Antispam, FortiGuard Antivirus, FortiGuard Intrusion Prevention, FortiGuard Web Filtering, FortiLog, FortiAnalyzer, FortiManager, Fortinet, FortiOS, FortiPartner, FortiProtect, FortiReporter, FortiResponse, FortiShield, FortiVoIP, and FortiWiFi 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
FortiGate certificate management	5
About this document.....	6
Document conventions.....	6
Typographic conventions.....	6
FortiGate documentation	7
Fortinet Tools and Documentation CD.....	8
Fortinet Knowledge Center	8
Comments on Fortinet technical documentation	8
Customer service and technical support	8
Using certificates to verify identity	9
Authentication overview	9
Basic authentication	9
Strong authentication	10
Authenticating VPN peers and clients with security certificates	11
Managing X.509 certificates	11
Obtaining a signed server certificate for the FortiGate unit	11
To generate the certificate request	12
To install the signed server certificate	13
Installing a CA root certificate and CRL to authenticate remote clients	14
To install a CA root certificate	14
To import a certificate revocation list	14
Configuring strong authentication	15
Authenticating SSL VPN user groups through security certificates	15
To enable strong authentication for an SSL VPN user group.....	16
Configuring authentication for VPN peers and clients	16
Backing up and restoring local certificates	16
To export a server certificate and private key.....	16
To import a previously exported server certificate and private key.....	17
To import separate server certificate and private key files	17
Index	19

Introduction

This section introduces you to certificate authentication and the FortiGate certificate management process.

Authentication is the process of determining if a remote host can be trusted, which ultimately controls remote access to network resources. To establish its trustworthiness, the remote host must provide an acceptable authentication certificate by obtaining a certificate from a certification authority (CA). The application can accept or reject any certificate - if the certificate is rejected, the connection is not completed. At a minimum, a certificate should be current, and the identity contained in the certificate should match the CA identity.

The FortiGate unit can use certificate authentication with X.509 security certificates (version 1 or 3) to allow administrative access via HTTPS, and to authenticate IPsec VPN peers or clients and SSL VPN user groups or clients.

The following topics are included in this section:

- [FortiGate certificate management](#)
- [About this document](#)
- [FortiGate documentation](#)
- [Customer service and technical support](#)

FortiGate certificate management

Digital certificates are downloadable files that you can install on FortiGate units. A certificate typically includes:

- the public key being signed
- a name, which can refer to a person, a computer or an organization
- a validity period
- the location (URL) of a revocation center
- the digital signature of the certificate, produced by the CA's private key

An X.509 security certificate consists of a public key, and some identifying information that has been digitally signed by the CA. Because CAs can be trusted, the certificates issued by a CA are deemed to be trustworthy.

You can use X.509 security certificates for authentication purposes when you have the required server/personal/site certificates and root certificates from an issuing CA. When X.509 certificates are not used, the FortiGate unit offers its own self-signed server certificate to client applications when they attempt to connect to the FortiGate unit.

You can back up and restore installed certificates and private keys using the FortiGate unit's built-in backup and import features. The FortiGate unit supports the RSA password-protected PKCS12 (Public Key Cryptography Standard 12) file format to create secure backup files.

About this document

This document explains how to manage certificates using the FortiGate web-based manager. Refer to this document to generate certificate requests, install signed certificates, import CA root certificates and certificate revocation lists, and back up and restore installed certificates and private keys. To define comparable parameters through the CLI, see the *FortiGate CLI Reference*.

Document conventions

The following document conventions are used in this guide:

- In the examples, private IP addresses are used for both private and public IP addresses.
- 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
Menu commands	Go to VPN > IPSEC > Phase 1 and select Create New.
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>
Program output	Welcome!
Variables	<address_ipv4>

FortiGate 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 IPS User Guide*
Describes how to configure the FortiGate Intrusion Prevention System settings and how the FortiGate IPS deals with some common attacks.
- *FortiGate IPSec VPN User Guide*
Provides step-by-step instructions for configuring IPSec VPNs using the web-based manager.
- *FortiGate SSL VPN User Guide*
Compares FortiGate IPSec VPN and FortiGate SSL VPN technology, and describes how to configure web-only mode and tunnel-mode SSL VPN access for remote users through the web-based manager.
- *FortiGate PPTP VPN User Guide*
Explains how to configure a PPTP VPN using the web-based manager.

- *FortiGate Certificate Management User Guide*
Contains procedures for managing digital certificates including generating certificate requests, installing signed certificates, importing CA root certificates and certificate revocation lists, and backing up and restoring installed certificates and private keys.
- *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 from the Fortinet Tools and Documentation CD shipped with your Fortinet product. The documents on this CD are current for your product at shipping time. For the latest versions of all Fortinet documentation see 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, 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.

Using certificates to verify identity

This section provides an overview of how the FortiGate unit verifies the identities of SSL VPN users or VPN peers and clients 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:

- [Authentication overview](#)
- [Managing X.509 certificates](#)
- [Configuring strong authentication](#)
- [Configuring authentication for VPN peers and clients](#)
- [Backing up and restoring local certificates](#)

Authentication overview

The FortiGate unit uses the Secure Sockets Layer (SSL) protocol to secure communications whenever a client application attempts to log in to the system. At the transport layer, SSL provides an end-to-end secure link between the client computer and the FortiGate unit for the purpose of peer entity authentication and encrypted data exchange. SSL enables the client and server to negotiate a symmetric encryption algorithm and session key before any application data is transferred between the client and the FortiGate unit.

The SSL security built into client applications and the FortiGate unit creates a secure connection. For example, when a web browser connects to the FortiGate unit through an HTTPS link, SSL is used to verify the FortiGate unit's identity to the client. If required (according to the FortiGate configuration), the FortiGate unit may prompt the client to authenticate itself in return (secure HTTP supports public key certificates).

Basic authentication

When X.509 certificates are not used for authentication purposes, the FortiGate unit uses a self-signed security certificate to authenticate itself to HTTP clients whenever they initiate a secure HTTP connection using SSL. When the certificate is offered, two security messages are displayed in the client browser.

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.



Note: If you install a CA-issued server certificate on the FortiGate unit, you can choose to have the FortiGate unit identify itself (as required by the SSL protocol whenever an HTTPS connection is initiated) 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 user groups through security certificates” on page 15](#).

After successful log in:

- FortiGate administrators may view FortiGate settings and configure the FortiGate unit. Data is encrypted using SSL and transmitted through the secure HTTP link.
- Members of SSL VPN user groups are presented with an SSL VPN portal, through which they may access server applications and network file services on the private network behind the FortiGate unit. Data is encrypted and transmitted through the secure HTTP link.

Strong authentication

The FortiGate unit supports strong (two-factor) authentication through X.509 security certificates (version 1 or 3). Strong authentication can be configured for SSL VPN user groups only.

When configured to implement strong authentication, the FortiGate unit prompts the client to authenticate itself using the X.509 certificate before accepting the user name and password supplied by the user (as described in [“Basic authentication” on page 9](#)). The certificate supplied by the client computer must match the root CA certificate installed on the FortiGate unit in order for a connection to be granted.

To enable strong authentication:

- Optionally install a signed server certificate for the FortiGate unit on the FortiGate unit and install the corresponding root certificate and Certificate Revocation List (CRL) from the issuing CA on the client computer(s).



Note: You do not have to install a CA-issued server certificate on the FortiGate unit to authenticate SSL VPN users. The FortiGate unit is shipped with a self-signed certificate that can be used instead of a CA-issued certificate. Using a CA-issued certificate will suppress the two security messages that are displayed to SSL VPN users when they log in. For more information, see [“Authenticating SSL VPN user groups through security certificates” on page 15](#).

- For members of the SSL VPN user group, install the same signed group certificate on each client computer and install the corresponding root certificate and CRL from the issuing CA on the FortiGate unit.

For more information, see [“Managing X.509 certificates” on page 11](#) and [“Configuring strong authentication” on page 15](#).

Authenticating VPN peers and clients with security certificates

End-users may access the private network behind the FortiGate unit through an SSL or IPSec VPN tunnel. When security certificates are used, the VPN server and its VPN peer or client exchange security certificates automatically before the tunnel is established.

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 match the root CA certificate installed on the FortiGate unit in order for a VPN tunnel to be established.

To enable the FortiGate unit to authenticate VPN peers or clients:

- Install a signed server certificate for the FortiGate unit on the FortiGate unit and install the corresponding root certificate (and CRL) from the issuing CA on the remote peer or client.
- For a remote peer, install a signed server certificate on the remote peer and install the corresponding root certificate (and CRL) from the issuing CA on the FortiGate unit.
- For remote clients, install the same group certificate on each client computer and install the corresponding root certificate (and CRL) from the issuing CA on the FortiGate unit.



Note: FortiGate IPSec VPNs do not support CRL lookups.

For more information, see [“Managing X.509 certificates” on page 11](#) and [“Configuring authentication for VPN peers and clients” on page 16](#).

Managing X.509 certificates

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.

Obtaining a signed server certificate for the FortiGate unit

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.

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 and send the signed certificate to you to install on the FortiGate unit.

To generate the certificate request

- 1 Go to **VPN > Certificates > Local Certificates**.
- 2 Select **Generate**.

- 3 In the Certification 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.

Locality (City) Name of the city or town where the FortiGate unit is installed.

State/Province Name of the state or province where the FortiGate unit is installed.

Country Select the country where the FortiGate unit is installed.

e-mail Contact email address.

6 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.

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

12 Submit the request to your CA as follows:

- Using the web browser on the management computer, browse to the CA web site.
- Follow the CA instructions to place a base-64 encoded PKCS#10 certificate request and upload your certificate request.
- Follow the CA instructions to download their root certificate and CRL, and then install the root certificate and CRL on each remote client (refer to the browser documentation).

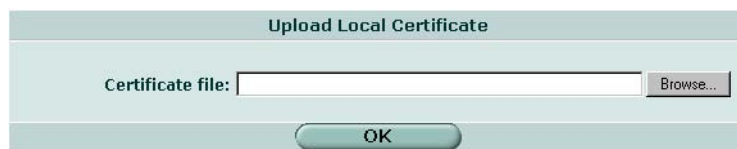
13 When you receive the signed server certificate from the CA, install the certificate on the FortiGate unit. See [“To install the signed server certificate”](#) below.

To install the signed server certificate

1 When you receive the signed server certificate from the CA, save the certificate on the management computer.

2 On the FortiGate unit, go to **VPN > Certificates > Local Certificates**.

- 3 Select Import.



- 4 Under Upload Local Certificate, select Browse, browse to 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.

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.



Note: FortiGate IPSec VPNs do not support CRL lookups.

To install a CA root certificate

- 1 After you download the root certificate of the CA, save the certificate on the management computer.
- 2 On the FortiGate unit, go to **VPN > Certificates > CA Certificates**.
- 3 Select Import.



- 4 Browse to 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 **VPN > Certificates > CRL**.
- 3 Select Import.



- 4 Browse to 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.

Configuring strong authentication

To verify a user's identity, strong authentication combines something the user knows (a user name and password) with something the user has (a client-side certificate). Strong authentication can be configured for SSL VPN user groups using X.509 (version 1 or 3) digital certificates.

Authenticating SSL VPN user groups through security certificates

You can use strong authentication to verify the identities of SSL VPN user group members. To enable strong authentication for an SSL VPN user group:

- 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.
- 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 14](#)).
- Follow the procedure below to configure strong authentication for the group of users having a copy of the group certificate.

The procedure assumes that accounts for individual users and user groups containing those users have been created. It also assumes that a firewall encryption policy has been created to permit access by that user group. For information about how to create user accounts and user groups, see the “User” chapter of the *FortiGate Administration Guide*. For information about how to create a firewall encryption policy for SSL VPN users, see the “SSL VPN administration tasks” chapter of the *FortiGate SSL VPN User Guide*.



Note: The SSL protocol requires that the FortiGate unit identify itself whenever a web browser accesses the web portal login page through an HTTPS link. If you would like to configure the FortiGate unit to identify itself using a CA-issued server certificate instead of the factory-installed self-signed certificate, select the name of the signed server certificate from the Server Certificate list on the SSL-VPN Settings page when you enable strong authentication for SSL VPN users. The server certificate must be installed before you can select it from the list. To obtain and install a server certificate, see [“Obtaining a signed server certificate for the FortiGate unit” on page 11](#).

To enable strong authentication for an SSL VPN user group

- 1 Go to **VPN > SSL > Config**.
- 2 Select **Require Client Certificate**, and then select **Apply**.
- 3 Go to **Firewall > Policy**.
- 4 Select the **Edit** icon in the row that corresponds to the firewall policy for traffic generated by holders of the group certificate.
- 5 Select **SSL Client Certificate Restrictive**.
- 6 Select **OK**.

Configuring authentication for VPN peers and clients

After the required server or group certificates and CA root certificates have been installed on the VPN peers and clients, the peers and clients identify themselves using those certificates when prompted by the FortiGate unit. The FortiGate unit provides its public key to the remote peer or client so that the remote peer or client can send encrypted messages to the FortiGate unit. Conversely, the remote peer or client provides its public key to the FortiGate unit, which uses the key to encrypt messages destined for the remote peer or client.

Refer to one of the following user guides to configure additional authentication options for VPN peers or clients:

- For SSL VPNs, see “Preliminary configuration tasks” in the *FortiGate SSL VPN User Guide*.
- For IPsec VPNs, see “Authenticating remote peers and clients” in the *FortiGate IPsec VPN User Guide*.

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 **VPN > 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** 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 key export <cert_name> <exp_filename>
<tftp_ip> <password>
```

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.
 - <password> is a password that will need to be entered later to import the PKCS12 file.
- 3 Move the output file from the TFTP server location to the management computer for future reference.

To import a previously exported server certificate and private key

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

- 2 Under Upload PKCS12 Certificate, select Browse.
- 3 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 Under Upload Certificate, select the Browse button beside the Certificate file field.
- 3 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.

- 5 Browse to the location on the management computer where the key file has been saved, select the file, and then select Open.
- 6 If required, in the Password field, type the associated password, and then select OK.
- 7 Select Return.

Index

A

- authentication
 - for SSL VPN users 10
 - for VPN peers and clients 11
 - overview 9
 - two-factor (strong) 10
 - without X.509 certificates 9

C

- certificate management 5
- certificate request 12
 - generating 12
- certificate revocation list
 - importing 14
- certificates
 - for strong authentication 10
 - for VPN peers and clients 11
 - importing CRL 14
 - installing root CA 14
 - installing signed server 13
 - obtaining signed server 11
- comments
 - on documentation, sending 8
- customer service 8

D

- documentation
 - commenting on 8
 - Fortinet 7

F

- firewall policy and strong authentication 16
- FortiGate documentation
 - commenting on 8
- Fortinet customer service 8
- Fortinet documentation 7
- Fortinet Knowledge Center 8

I

- introduction
 - Fortinet documentation 7

L

- Local certificates
 - generating request 12
 - installing signed 13
- logging in, security messages 9

P

- PKCS12 file format 5

R

- Require Client Certificate option 16
- revocation list, importing 14
- root certificate, installing 14

S

- self-signed certificate, installing 9
- server certificate
 - CA-issued 15
 - installing signed 13
 - obtaining 11
- Server Certificate list 15
- SSL Client Certificate Restrictive option 16
- SSL VPN users
 - enabling strong authentication 10
- strong authentication 10, 15
 - for SSL VPN users 15

T

- technical support 8

V

- VPN peers/clients
 - enabling certificate exchange 11

X

- X.509 security certificates 10
 - managing 11
 - overview 5

FORTINET™

www.fortinet.com

FORTINET™

www.fortinet.com