Technical Note

Using Entrust Authority Enrollment Server with Fortinet products

FORTINET

www.fortinet.com

Using Entrust Authority Enrollment Server with Fortinet products
Version 1
17 October 2006
01-30003-0359-20061017

Trademarks

Regulatory compliance

FCC Class A Part 15 CSA/CUS

⚠ **Caution:** If you install a battery that is not the correct type, it could explode. Dispose of used batteries according to local regulations.

Contents

Introduction

This document explains how to use Entrust Authority Server, an Entrust Public Key Infrastructure product, with the following Fortinet products:

- FortiGate Multi-Threat Security systems
- FortiClient Host Security application

FortiGate systems and the FortiClient application can use X.509 certificates to authenticate IPSec peers and SSL-VPN users. Entrust Authority Server issues digital identities to users. In combination, secure identities and strong encryption provide for secure communication between networks.

FortiGate Multi-Threat Security systems

FortiGate™ appliances improve network security, reduce network misuse and abuse, and help you use communications resources more efficiently without compromising the performance of your network.

A FortiGate unit is a dedicated, easily managed security device that delivers a full suite of capabilities including:

- Application-level services such as virus protection, intrusion protection, spam filtering, web content filtering, and IM/P2P filtering
- Network-level services such as firewall, intrusion detection, IPSec and SSL VPN, and traffic shaping
- Management services such as user authentication, logging, reporting with FortiAnalyzer, administration profiles, secure web and CLI administrative access, and SNMP

FortiClient Host Security application

FortiClient Host Security software is a secure remote access client for Windows computers. It integrates IPSec VPN, antivirus, Windows registry monitoring, firewall, and web browsing control into a single software package.

With the FortiClient software, you can:

- create VPN connections to remote networks,
- scan your computer for viruses,
- configure real-time protection against viruses and unauthorized modification of the Windows registry,
- restrict access to your system and applications by setting up firewall policies.
- restrict Internet access according the rules you specify.
- filter incoming email on your Microsoft Outlook® and Microsoft Outlook® Express to collect spam automatically.
- use the remote management function provided by the FortiManager System.

About this document

This document contains the following chapters:

- Introduction (this chapter)
- FortiGate certificate configuration
- FortiClient certificate configuration

FortiGate certificate configuration

This section describes how to configure a FortiGate unit to authenticate VPN peers using X.509 security certificates issued by Entrust Authority Enrollment Server for VPN version 7.0.

The following topics are included in this section:

Introduction

To integrate FortiGate units with the Entrust Authority Server environment, you need to:

- import the Certificate Authority server certificate to the FortiGate unit
- generate a Certificate Signing Request (CSR) on the FortiGate unit
- read the FortiGate CSR into the Entrust Enrollment Server for VPN, validate it and generate a certificate
- import the certificate into the FortiGate unit
- configure FortiGate VPNs to authenticate using the certificate

Importing the Entrust CA certificate to the FortiGate unit

In Entrust Enrollment Server for VPN, the default name for the Server Certificate is vpnconcacert.pem. The certificate is located in the Data subdirectory where the program is installed. Copy this file as securely as possible to the management computer for your FortiGate unit. Import the CA certificate to the FortiGate unit as follows.

1. Log on to the FortiGate unit web-based manager.
2. Go to **VPN > Certificates > CA Certificates**.
3. Select Import.

   The Upload CA Certificate page opens.
4. Select Browse and navigate to the vpnconcacert.pem file.
5. Select OK.

   The imported certificate is listed in the CA Certificates list. The Subject field contains several of the information fields from the certificate.

Generating the CSR

The FortiGate unit must generate a Certificate Signing Request for the Entrust Authority Enrollment Server. Do the following on the FortiGate unit web-based manager:

1. Go to **VPN > Certificates > Local Certificates**.
2. Select Generate.
3. In the Certification Name field, enter a name for the certificate.

   Do not include spaces in the name.
4. In the Subject information section, select the ID Type and provide the appropriate information.

   You can identify the FortiGate unit by host IP, domain name, or email address. The type of identifier required depends on the Entrust Authority Server settings. Ask your Entrust administrator for this information.
5. Optionally, enter information in Optional Information section fields.

   Although this information is not required, it can make the certificate easier to find on the Entrust Authority Enrollment Server.
6. Select OK.

   The Local Certificates list includes the new CSR. The Status field shows Pending.
7. Select the Download icon for the new CSR and save the CSR to the management computer.
8. Copy this file as securely as possible to the person responsible for the Entrust Authority Enrollment Server for VPN.

Generating the certificate

With the CSR from the FortiGate unit, you can generate a security certificate on the Entrust Authority Enrollment Server for VPN.

To generate the certificate

1. Start the Entrust Enrollment Server for VPN Administration application.
2. From the main menu, select Request > Read PKCS#10 and navigate to the CSR file from the FortiGate unit.

   When the CSR has been read, the PKCS#10 Request Information window opens.
3. Enter the FortiGate serial number into the Serial Number field. Optionally, you can can enter information into other fields in the Contents section, such as Description.
4. Select Next.

   The Verify Fingerprint window opens.
5. Select Yes.
6. When the Enrollment Result page opens, select Finish.

   Do not select the Save to File button.

To export the certificate

1 In the left pane of the Entrust Authority Enrollment Server for VPN Administration application main window, right click Search Results and select Search.

The Search window opens.

2 Optionally, enter search criteria based on the information in the certificate. This is useful when there are many certificates stored on the Entrust server.

3 In the Search window, select OK.

4 In the left pane, select the new certificate under Search Results.

5 In the right pane, right-click the new certificate in the Certificates list and select Save to File.

6 Copy the saved file as securely as possible to the management computer for your FortiGate unit.

Importing the certificate to the FortiGate unit

In the web-based manager of the FortiGate unit, do the following:

1 Go to **VPN > Certificates > Local Certificates**.

2 Select Import.

3 In the Upload Local Certificate section, select Browse, navigate to the certificate file from the Entrust server, and then select OK.

The imported certificate is listed in the CA Certificates list. The Status field has changed from Pending to OK.

Using the certificate in an IPSec VPN configuration

To use the Entrust Authority Enrollment Server-issued certificate to authenticate VPN users, you need to specify the certificate in the Phase 1 part of your VPN configuration.

1 In the FortiGate unit web-based manager, go to **VPN > IPSEC**.

2 If you want to modify an existing VPN configuration, select the Edit icon for that VPN. Otherwise, select Create Phase 1 and configure the Phase 1 parameters except for Authentication Method.

3 From the Authentication Method list, select RSA Signature.

4 From the Certificate Name list, select the certificate you imported.

5 Select OK.

6 If you are configuring a new VPN, you also need to configure the Phase 2 parameters.

For more information about configuring VPNs refer to the *FortiGate Administration Guide* or the *IPSec VPN User Guide*.

Using the certificate in an SSL VPN configuration

To use the Entrust Authority Enrollment Server-issued certificate to authenticate SSL VPN users, you need to specify the certificate in the SSL VPN configuration.

1. In the FortiGate unit web-based manager, go to **VPN > SSL > Config**.
2. From the Server Certificate list, select the certificate you imported.
3. To restrict client access to only those clients who have the Entrust security certificate from the same Entrust Authority server, select Require Client Certificate.
4. Configure other SSL VPN settings as needed.
5. Select OK.

   For more information about configuring SSL VPNs refer to the *FortiGate Administration Guide* or the *SSL VPN User Guide*.

Importing a CRL to the FortiGate unit

In addition to issuing X.509 certificates, the Entrust Authority Server can also issue Certificate Revocation Lists (CRL). Using the CRL, the FortiGate unit can check that the Entrust Authority Server for VPN has not revoked the certificate.

1. Obtain the CRL file from the Entrust VPN Enrollment Server administration tool and copy it to the management computer for your FortiGate unit.
2. In the web-based manager, go to **VPN > Certificates > CRL**.
3. Select Import.
4. Select Browse, navigate to the CRL file, and then select OK.

   The CRL list is added to the list of CRLs.

FortiClient certificate configuration

This section describes how to configure a FortiClient Host Security VPN client to authenticate VPN peers using X.509 security certificates issued by Entrust Authority Enrollment Server for VPN version 7.0.

The following topics are included in this section:

Introduction

To integrate FortiClient VPN users with the Entrust Authority Server environment, you need to:

- import the Certificate Authority server certificate to the FortiClient application
- generate a Certificate Signing Request (CSR)
- read the FortiClient CSR into the Entrust Enrollment Server for VPN, validate it and generate a certificate
- import the certificate into the FortiClient application
- configure FortiClient VPNs to authenticate using the certificate

There are two ways to accomplish this: you can use SCEP to retrieve the CA and client certificate directly or you can manually import the certificates.

Importing the Entrust CA certificate to the FortiClient application

If you do not use Online SCEP, you need to manually import the Entrust Enrollment Server CA certificate so that you can create a Certificate Signing Request to the Entrust Enrollment Server.

In Entrust Enrollment Server for VPN, the default name for the Server CA Certificate is vpnconcacert.pem. The certificate is located in the Data subdirectory where the program is installed.

There are two ways to import the CA certificate to the FortiClient application:

- import the CA certificate directly to the FortiClient application using HTTPS (if the Entrust Enrollment Server supports it)

- import the CA certificate file to the computer on which the FortiClient application is installed and then import the CA certificate to the FortiClient application

To import the CA certificate using HTTPS

1. In the FortiClient Console, go to **VPN > CA Certificates**.
2. Select Retrieve, enter the URL for the Entrust Enrollment Server, and then select OK.

To import the CA certificate manually

1. Copy the CA certificate file as securely as possible to the computer where FortiClient is installed.
2. In the FortiClient Console, go to **VPN > CA Certificates**.
3. Select Import. Navigate to the CA certificate file and then select Open.

   The Upload CA Certificate page opens.
4. Select Browse and navigate to the vpnconcacert.pem file.
5. Select OK.

   The imported certificate is listed in the CA Certificates list.

   If you also want to add the certificate to the Windows secure Certificate Store, double-click the certificate file, select Install Certificate and follow the Certificate Import Wizard to completion.

Generating the CSR and obtaining the certificate

The FortiClient application must generate a Certificate Signing Request for the Entrust Enrollment Server. You can do either of the following:

- Use Online SCEP to submit the CSR and receive the both the CA certificate and your client certificate.
- Export the CSR file, transfer it to the Entrust Enrollment Server and then import the signed certificate file. You must have already imported the CA certificate. See “Importing the Entrust CA certificate to the FortiClient application”, preceding.

To generate the CSR

1. In the FortiClient Console, go to **VPN > My Certificates**.
2. Select Generate.
3. In the Certificate Name field, enter the name you will use for the certificate in the FortiClient application.
4. In the Subject Information section, select the ID Type for the subject: domain name, email address or IP address.
5. Enter the information for the ID type that you selected.

Domain name	If you selected domain name, enter the fully qualified domain name of the FortiClient computer being certified.

Email address If you selected email address, enter the email address of the owner of the FortiClient computer being certified.

IP address If you selected IP address, enter the IP address of the FortiClient computer being certified.

6. Optionally select Advanced and enter the advanced setting information.

Email Enter a contact email address for the FortiClient computer user.

Department Enter a name that identifies the department or unit within the organization requesting the certificate for the FortiClient computer (such as Manufacturing or MF).

Company Enter the legal name of the organization requesting the certificate for the FortiClient computer.

City Enter the name of the city or town where the FortiClient Computer is located.

State/Province Enter the name of the state or province where the FortiClient computer is located.

Country Enter the name of the country where the FortiClient computer is located.

7. Follow either the “To obtain the CA certificate and local certificate using online SCEP” or “To submit the CSR as a file” procedures below.

To obtain the CA certificate and local certificate using online SCEP

1. In the Enrollment Method section, select Online SCEP.
2. Select an issuer CA from the list provided or enter the URL of the CA server.

   If the FortiClient computer uses a proxy server, you must configure the proxy server settings before you can use online SCEP. See “Configuring proxy server settings” in the General chapter of the *FortiClient Host Security User Guide*.
3. In the Challenge Phrase field, enter the challenge phrase if the Entrust Enrollment Server requires it.
4. Select OK.

   The FortiClient software:

   - submits the local certificate request,
   - retrieves and imports the signed local certificate,
   - retrieves and imports the CA certificate.

   The signed local certificate is displayed on the Local Certificates list. The type field shows Certificate. The CA certificate is displayed on the CA Certificates list. The expiration dates of the certificates are listed in the Valid To column of each list.

   You can now use the certificate for authentication in VPNs. To continue configuring you FortiClient application, go to “Using the certificate in a VPN configuration” on page 15.

To submit the CSR as a file

1. In the Enrollment Method section, select File based.
2. Select OK.

   The My Certificates list includes the new CSR. The Type column shows Request.
3. Select the new CSR and then select Export.

4 Navigate to the folder where you want to save the CSR, enter a name for the file, and then select Save.

5 Copy the CSR file as securely as possible to the Entrust Authority Enrollment Server for VPN.

Generating the certificate on the Entrust Authority Enrollment Server

If you generated a CSR file, you need to manually create the client certificate on the Entrust Authority Enrollment Server for VPN.

To generate the certificate

1 Start the Entrust Enrollment Server for VPN Administration application.

2 From the main menu, select **Request > Read PKCS#10** and navigate to the CSR file from the FortiClient application.

When the CSR has been read, the PKCS#10 Request Information window opens.

3 Enter the user name in the Description field to clearly identify the certificate.

4 Select Next.

The Verify Fingerprint window opens.

5 Select Yes.

6 When the Enrollment Result page opens, select Finish.

To export the certificate

1 In the left pane of the Entrust Enrollment Server for VPN Administration application main window, right click Search Results and select Search.

2 In the Search dialog, select OK.

3 In the left pane, select the new certificate under Search Results.

4 In the right pane, right-click the new certificate in the Certificates list and select Save to File.

5 Copy the saved file as securely as possible to the computer on which the FortiClient application is installed.

Importing the certificate to the FortiClient application

You need to import the certificate into the FortiClient application.

1 In the FortiClient Console, go to **VPN > My Certificates**.

2 Select Import.

3 Navigate to the certificate file from the Entrust server, and then select Open.

The imported certificate is listed in the My Certificates list. The Status field has changed from Request to Certificate.

Using the certificate in a VPN configuration

To use the Entrust Authority Enrollment Server-issued certificate to authenticate VPN users, you need to specify the certificate in your VPN configuration. You can use certificates only in manually configured VPNs.

1. In the FortiClient Console, go to **VPN > Connections**.
2. If you want to modify an existing VPN configuration, select it in the list and then select **Advanced > Edit**. Otherwise, select **Advanced > Add** and configure the parameters as needed except for Authentication Method.
3. From the Authentication Method list, select RSA Signature.
4. From the Certificate Name list, select the certificate you imported.
5. Select OK.

For more information about configuring FortiClient VPNs, refer to the *FortiClient Host Security User Guide*.

Importing a CRL to the FortiClient application

In addition to issuing X.509 certificates, the Entrust Authority Server can also issue Certificate Revocation Lists (CRL). Using the CRL, the FortiClient application can check that the Entrust Authority Server for VPN has not revoked the certificate.

1. Obtain the CRL file from the Entrust VPN Enrollment Server administration tool and copy it to the computer on which the FortiClient application is installed.
2. In the web-based manager, go to **VPN > CRL**.
3. Select Import.
4. Navigate to the CRL file, and then select OK.

The CRL list is added to the list of CRLs.

FORTINET™

www.fortinet.com

FORTINET™

www.fortinet.com