

# **Entrust PKI and Check Point 2000 Install and Interoperability Guide**

**Date:** 8-May-2000  
**Version:** 1.0

The latest version of this document can be found at  
<http://www.entrust.com/resourcecenter/pdf/checkpointentrust.pdf>

Entrust is a registered trademark of Entrust Technologies Inc. in the United States and certain other countries. In Canada, Entrust is a registered trademark of Entrust Technologies Limited. All other Entrust Technologies product names and service names are trademarks of Entrust Technologies. All other company and product names are trademarks or registered trademarks of their respective owners.

The material provided in this document is for information purposes only. It is not intended to be advice. You should not act or abstain from acting based upon such information without first consulting a professional. ENTRUST TECHNOLOGIES DOES NOT WARRANT THE QUALITY, ACCURACY OR COMPLETENESS OF THE INFORMATION CONTAINED IN THIS ARTICLE. SUCH INFORMATION IS PROVIDED "AS IS" WITHOUT REPRESENTATION, WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, BY USAGE OF TRADE, OR OTHERWISE, AND ENTRUST TECHNOLOGIES SPECIFICALLY DISCLAIMS ANY AND ALL REPRESENTATIONS, AND WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A SPECIFIC PURPOSE.

# 1. Introduction

This document details the necessary steps and considerations to integrate your Entrust PKI and Check Point 2000 installations. *It is strongly recommended that you read this document before beginning to attempt any installation, upgrade, or integration.*

Entrust recommends using the latest stable release of both the Check Point and Entrust products (currently Entrust/PKI 5.0 and Check Point 2000).

*The remainder of this document assumes that you are using Check Point 2000 (Check Point VPN-1 4.1 SPI) and Entrust 5.0.*

## 2. Interoperability Overview

We strongly recommend careful planning of your installation ahead of time. This means first clearly understanding the network architecture for your VPN-1 and PKI installations before doing any actual installation and configuration.

Be sure the network is operating properly: check that routing is configured correctly at all points; the necessary interfaces can talk to each other as appropriate; etc. Verifying this before continuing will help to isolate network problems early, which will allow for the rest of the installation process to go as smoothly as possible. The Check Point documentation is an excellent resource to help you with network setup and example configurations.

We also strongly recommend installing the different software components separately and testing them independently of each other first, before attempting to integrate these components together. Again, this allows the installer to narrow down potential configuration problems as early as possible, making the interoperability process much more streamlined.

Therefore we recommend that a user first install the Entrust PKI and verify that it is working by following the steps in the Entrust documentation. Please see details and special notes below.

We then recommend installing the VPN-1 gateway, in the manner that it will be used in production, and verify that it is working within your desired network infrastructure.

Once the two products are installed, you can then integrate them, taking into account the details below.

## 3. Recommended Steps for New Install

### 3.1. Overview

We recommend a phased approach to the install, detailed below:

- Install the Entrust PKI and verify that it is functioning properly
- Install the Check Point VPN-1/SecuRemote product and verify that it is functioning properly

- Integrate the PKI and the VPN-1/SecuRemote product

As with any networking solution, an initial limited rollout for testing purposes is recommended before full deployment, in order to catch potential issues as early as possible.

## 3.2. Install PKI

This document assumes you will be installing the 5.0 version of the Entrust PKI.

Install the PKI according to the Entrust documentation, with the following considerations:

- When configuring your cryptographic information, but sure that your “Certification Authority Key Pair Algorithm” is one of the RSA options. **Do not select DSA.**
- Be sure to enable backwards compatibility for older Entrust applications (3.0 and 4.0).
- The directory, once installed, must be able to support LDAPv2. If possible, we highly recommend setting up your directory to handle both LDAPv2 and LDAPv3 (LDAPv3 is required if you ever want to use LDAP/SSL to the directory). Please refer to the documentation for your directory product to make sure you can support the necessary LDAP versions. We strongly recommend that you read Appendix A of this document, “LDAP version 2 Backwards Compatibility”.

Once you’ve installed the PKI, install the Entrust/Entelligence client on a representative client machine and verify basic functionality (enrollment, revocation, etc.).

## 3.3. Install VPN-1 and SecuRemote

Install the Check Point VPN-1/Firewall-1 in a production-like configuration (i.e. a representative network setup) as per the Check Point documentation:

- Install the VPN-1 gateway software and configure as per documentation
- Install the SecuRemote VPN client on a representative machine and configure as per documentation
- Test basic VPN functionality (using a basic IKE setup and basic shared-secret authentication) to ensure a working network and software configuration.

(The Check Point documentation manuals “Getting Started with Check Point 2000” and “Check Point Virtual Private Networks” are very useful for walking through this installation and testing process.)

## 3.4. Integrate PKI, VPN-1 and SecuRemote

Follow the documentation for integrating the gateway with the Entrust PKI as described in Chapter 3 of the “Check Point Virtual Private Network” documentation.

## Entrust Version Selection

When setting up the VPN-1 system to work with the Entrust CA (Chapter 3 of the “Check Point Virtual Private Network” documentation) be sure to specify the Entrust CA version as 4.0, not 3.0.

## Selecting the Correct “entrust.ini” File

A number of steps in the documentation refer to copying the “entrust.ini” file from the Entrust CA to the gateway and, potentially, to the client machines where SecuRemote is installed. You will find the correct entrust.ini file in the directory where you installed the Entrust/Authority component (i.e. the default WinNT path to the appropriate entrust.ini file is C:\Program Files\Entrust\Entrust Authority\entrust.ini).

*Note:* the correct entrust.ini file will not contain a FIPS mode line (i.e. FIPS\_MODE=1). If, for whatever reason, the entrust.ini file you are using for VPN-1 or SecuRemote contains the line FIPS\_MODE=1, the file should be edited to read FIPS\_MODE=0.

## Preparing to Enroll VPN Users into your CA

As is common industry practice, we recommend that both the Entrust CA and your directory sit in behind the corporate firewall.

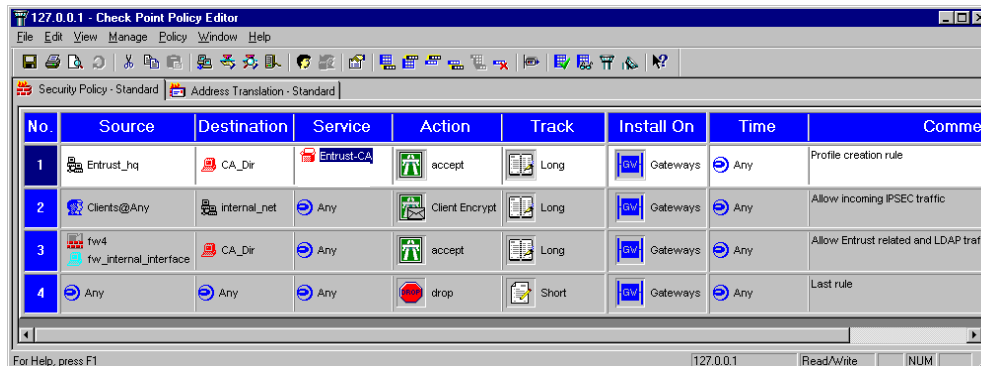
In order for your remote VPN users to enroll in the Entrust CA, however, they must be able to talk through the firewall to the CA.

Therefore, a basic VPN configuration requires the following setup:

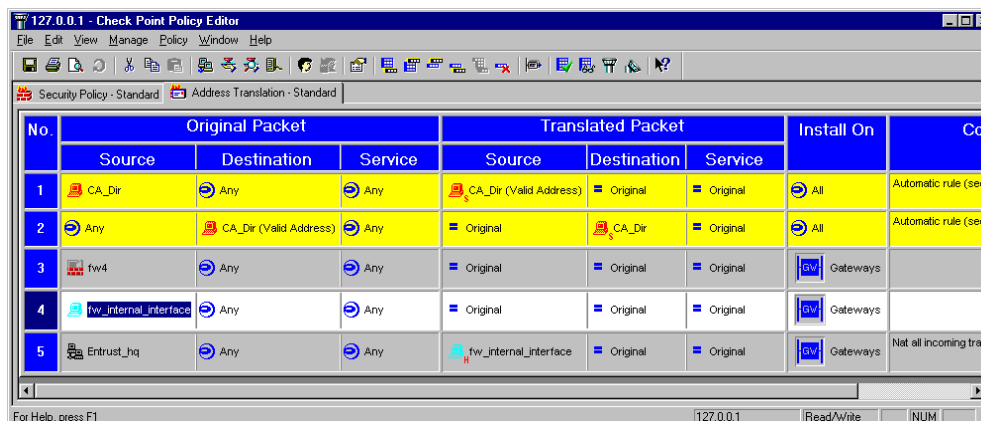
- Rules that cause traffic over the CA ports to be forwarded through the firewall to the CA servers (using Network Address translation on the internal connection);
- Rules that allow authenticated users to create secure VPN connections through the firewall; and
- Any other rules required by your setup to allow or deny certain types of traffic.

*Note:* Entrust/PKI 5.0’s support of PKIX-CMP requires that the client be able to connect to the CA server over port 829. It is necessary, therefore, to open this port up to client traffic, just as 709/710 is open for CA traffic. To do this, edit the “Entrust-CA” service (as highlighted below), and add TCP port 829.

The following screen shot shows a sample set of rules for a basic setup. Remember, these rules are only examples and will vary in your custom environment:



The next screenshot details the necessary NAT (network address translation rules) that this setup requires in order to allow CA and directory traffic to be properly passed between the firewall and the directory and CA servers. (Please be sure to refer to Check Point documentation for full understanding of NAT implications, such as routing and anti-spoofing considerations).



## Enrolling VPN Users

Once the necessary rules and configurations are made on the firewall, users will be ready to enroll. The following steps describe a common method of enrollment.

*Note 1:* if you are installing the Entrust 5.0 desktop software (Entelligence, etc.), we recommend installing this first before installing SecuRemote.

*Note 2:* both SecuRemote and Entrust/SingleSignOn allow for single domain login for NT domains. Currently, we do not recommend having both applications configured to allow for single domain login, as conflicts may arise.

To enroll a user, we recommend the following steps (this procedure assumes you have read and are comfortable with the documentation on the SecuRemote client described in “Check Point Virtual Private Network”):

- If a site is already defined, disable it (you will re-enable it later)
- Under “Certificates” choose “Create Profile”

- Follow the steps in creating your profile. You will be asked for reference numbers and authorization codes. Your Entrust CA administrator can make these available to you.
- After your profile is created, either re-enable the site, or create a new site as instructed by your network administrator.
- At this point, you must exit SecuRemote completely (“File” | “Kill”) and restart the client.

The user is now enrolled. At this point the Entrust administrator has enabled the user on the CA, and the VPN-1 administrator has entered the user’s DN into the firewall ruleset as per the Check Point documentation.

Attempt to connect to a machine behind the gateway from this external client. SecuRemote will intercept this and attempt to authenticate the user. When prompted, select certificate authentication; select your profile; then type in the password to your profile. Your first authentication may take a few moments.

SecuRemote should respond that you have been authenticated, and your network connection should proceed.

## Client Distribution Suggestions

To ease larger distribution of client software, we recommend following the directions in Chapter 9 of the “Check Point Virtual Private Network” documentation.

# 4. Recommended Steps for Upgrading

As above, we recommend a phased approach to upgrading. Upgrade first the PKI, then the Check Point 2000 components.

## 4.1. Upgrading the PKI from 4.0 to 5.0

Upgrade the PKI according to the Entrust documentation, with the following considerations:

- If reconfiguring your cryptographic information, but sure that your “Certification Authority Key Pair Algorithm” is one of the RSA options. **Do not select DSA.**
- Be sure to enable backwards compatibility for older Entrust applications (3.0 and 4.0).
- The directory, once installed, must be able to support LDAPv2. If you also have applications that require LDAPv3, your directory must be configured to handle both protocols. Please refer to the documentation for your directory product to make sure you can support the necessary LDAP versions.
- The directory, once installed/upgraded, must be able to support LDAPv2. If possible, we highly recommend setting up your directory to handle both LDAPv2 and LDAPv3. Please refer to the documentation for your directory product to make sure you can support the necessary LDAP versions. We strongly recommend that

you read Appendix A of this document, “LDAP version 2 Backwards Compatibility”.

Once you’ve upgraded the PKI, install/upgrade the Entrust/Entelligence client on a representative client machine and verify basic functionality (enrollment, revocation, etc.).

## 4.2. Upgrade VPN-1 and SecuRemote

Upgrade the Check Point VPN-1/Firewall-1 as per the Check Point documentation.

Pay close attention the Check Point release notes, and make sure you have a current version of the Check Point release notes.

# Appendix A: LDAP version 2 Backwards Compatibility

*Note:* this section is from the Entrust/PKI 5.0 release notes. Please see the latest version of this document for any changes or corrections.

If LDAP version 2 and LDAP version 3 will be used to access the same Directory, it is important to determine if backwards compatibility is properly supported by the Directory. An example of such a configuration would be if Entrust/PKI 4.x or earlier versions will be used together with Entrust/PKI 5.0 where the PKI is running in LDAP version 3 mode (earlier Entrust products only support LDAP version 2). The following is a list of features which may cause compatibility problems:

### Proper support for the “;binary” attribute option

LDAP version 3 uses the ;binary option to access userCertificate, caCertificate, authorityRevocationList, certificateRevocationList, crossCertificatePair and attributeCertificate. LDAP version 2 does not include the use of attribute options however some Directory products require the use of “;binary” in order to access attributes in LDAP version 2. The Directory should not require the use of “;binary” in LDAP version 2 however if its use is mandatory, a configuration may allow compatibility. Contact Entrust Support for more information.

### RFC2253 DN formatting

RFC2253 defines how DNs that are generated by LDAP version 3 applications must be formatted. The allowed format is a subset of the available formats previously defined in RFC1779. For example, RFC1779 allows the quoted format as well as the escaped format as shown below:

```
cn="John Smith + E12", o=Your Company Inc., c=US (allowed by
RFC1779 / LDAP version 2)
```

```
cn=John Smith \+ E12,o=Your Company,c=US (mandated by RFC2253 /
LDAP version 3)
```

Release 4.x and earlier versions of Entrust/PKI and client applications don't support the escaped format which uses the slash “\” character to escape special characters. This problem is only manifested if the following special characters are used in attribute values:

, = + < > # ; \

## **Character set encoding**

If support for both LDAPv3 and LDAPv2 is detected, the 5.0 Directory Verification Tool (DVT) will test the character set used by your Directory in LDAPv2 to determine if you may encounter problems. If the DVT reports an error for the Language Encoding Test and you intend to use non-ASCII characters in DNs or other string attributes contact Entrust Support for more information on how to configure your Directory for Latin-1.