Contents

What is Entrust Connector.......................................................................................................................... 4
Installation...................................................................................................................................................... 5
Prerequisites .................................................................................................................................................. 5
Installation Package ...................................................................................................................................... 7
Running the Installer .................................................................................................................................. 7
Licensing ....................................................................................................................................................... 8
JCE................................................................................................................................................................. 10
Native Lib ..................................................................................................................................................... 12
Tomcat Connector ........................................................................................................................................ 13
IIS Features ................................................................................................................................................ 14
Entrust Connector Instance .......................................................................................................................... 15
  URL ............................................................................................................................................................. 16
  Logging ....................................................................................................................................................... 17
  Entrust ....................................................................................................................................................... 18
  Profiles ...................................................................................................................................................... 21
  Saving ....................................................................................................................................................... 25
Website Configuration ................................................................................................................................... 26
  Select SSL Certificate ................................................................................................................................. 28
  Create Binding .......................................................................................................................................... 34
  Finish ......................................................................................................................................................... 35
Enable IIS Client Authentication.................................................................................................................... 38
Select Client Certificate ................................................................................................................................. 39
Update IIS Client Authentication .................................................................................................................. 45
Complete Installation .................................................................................................................................. 47
Post Installation .......................................................................................................................................... 48
Configuration ................................................................................................................................................ 50
Warnings ...................................................................................................................................................... 50
Add a New Entrust Connector ........................................................................................................................ 50
Edit an Entrust Connector .............................................................................................................................. 62
Manage Client Authentication Mappings ....................................................................................................... 74
  Add Mapping ............................................................................................................................................ 76
  Edit Mapping .......................................................................................................................................... 85
Remove Mapping .............................................................................................................................................. 95
Install JCE.......................................................................................................................................................... 96
Update Tomcat Location .................................................................................................................................... 97
Update License Information ............................................................................................................................... 98
Uninstall ............................................................................................................................................................ 99
What is Entrust Connector

Entrust Connector is an implementation of the Venafi Adaptable CA API for Entrust Security Manager based Certification Authorities (CA). It is composed of two parts, a powershell script which is run by the Venafi application and a web service which performs the CA management requested by the Venafi application.

Venafi Trust Protection Platform can generate new Entrust Users in the Entrust CA by creating new Distinguished Names (DN) and requesting certificates. When creating a new Entrust User, Entrust Security Manager requires the user to have a defined Entrust user type and an Entrust certificate type.

In order to provide this in a simple way, Entrust Connector maintains profiles. A profile consists of a profile name, and a pair of Entrust user type and certificate type. When Venafi requests a new user, it supplies the profile name which the Entrust Connector web service converts into a corresponding user and certificate type to generate the Entrust user.

Multiple Entrust Connector web service instances can be run. One for each Entrust CA available. Each instance will have a configured entrust.ini, Entrust Administrator EPF, and configured profiles.

The Entrust Adaptable CA PowerShell script is available from Venafi. In order to configure an Adaptable CA template in Venafi Trust Protection Platform (TPP), two items must be created in TPP:

1. Username Credential
   The Entrust Adaptable CA PowerShell script uses this credential to authenticate with the Entrust Connector web service and perform administrative operations on the Entrust CA.

   Set the Venafi Username credential username value to the Entrust Connector webservice URL. Set the password to the configured client certificate.

2. Custom Field
   A custom field is employed to select the desired profile to be used for creating new users. The profile selected will be converted into a corresponding Entrust user type and certificate type by the web service.

   The custom field should have a meaningful name. When creating it, it must be defined as a single select list. The contents of the list will be the Entrust Connector configured profile names.

When configuring an Adaptable CA template in Venafi Trust Protection Platform, you must specify these two items. When Venafi requests an administrative action on the Entrust CA, it must include these two items in its request to the Entrust Adaptable CA PowerShell script.
Please review and accomplish all prerequisites before attempting to install Entrust Connector

Installation

Prerequisites
Entrust Connector requires:

- Windows 2012r2 or newer
- 64 bit Apache Tomcat 8.5 or newer
- 64 bit Oracle Java Runtime Environment (JRE) 1.8 or newer

Entrust Security Manager Role Requirements

An Entrust Connector instance uses an Entrust Administrator credential to implement the Venafi Adaptable CA API operations. In order to create an Entrust Connector instance, you must configure an Entrust Security Manager administrator user with the proper role requirements.

Create a new Entrust role by copying the "User Reg Service (Admin Services)" role and changing the unique name to be meaningful such as "Venafi Connector Admin". The role should be for administrator users and not end users.

Edit the permissions of the role. At a minimum, the role needs the following permissions:

- Certificates
  The role should administer the categories and types of the Entrust users that Venafi will administer. Currently, only the Enterprise category of certificates is supported.
- Directory
- Bind to Directory

- Security Policy
  - View Security Policy
  - Force CRLs
    This is only required if the CA should issue new CRLs when a certificate is revoked.

- User Templates
  Make sure the role can administer the user templates of all Entrust users Venafi will administer.

- Users
  - User – General
    - View
    - Add
    - Modify Properties
    - Revoke Certificates
    - Set for key recovery
    - Cancel key recovery
    - View Activation Codes
    - Reissue Activation Codes
  - User – Advanced
    - Perform PKIX requests
    - Create user profile
    - Recover user profile

**Entrust Security Manager Policy Requirements**

The Entrust Connector role configured above requires a policy that enables Server logon. Create a new policy or use an existing policy that allows server logon.

**Creating the Entrust Connector instance Administrative User**

The certificate type used when creating the Entrust Administrative user that will be employed by the Entrust Connector instance is very important. It must contain the policy object identifier (OID) 2.16.840.1.114027.10.4. The default Admin Services User Registration certificate type already contains this policy and can be used. Alternatively, create a new certificate type and ensure it contains this policy OID.

**Important Considerations**

1. **Never create the Entrust Connector administrator epf credential using Security Manager Administration.** Security Manager Administration generates v1 profiles which cannot be used for server login. The preferred way to generate the credential is using the installation tool and providing the activation codes for the user.
2. Make sure the certificate type of the user contains the policy OID 2.16.840.1.114027.10.4. This policy OID is required to be in the certificates of the Entrust administrator user that an Entrust Connector instance will use.
3. You will configure the Entrust Connector instance to either force CRL issue after each revocation or not during the installation. If you do not require or need that CRLs be issued...
after each revocation, you do not need to enable "Force CRLs" in the Security Policy section of the Entrust role.

**Before Installing**

Make sure that the Oracle JRE is installed and Apache Tomcat are installed on the system. While a non-service tomcat installation can be used, it is better to use the Apache Tomcat service installer in order to make it easier to start and stop tomcat and have it run automatically.

The following items should be prepared prior to installing Entrust Connector:

1. Oracle Java Cryptographic Extension zip file for the installed JRE
2. 64 bit binary Apache Tomcat Connector zip file (must contain an already built isapi_redirect.dll file)
3. The entrust.ini of the Entrust CA to connect to Venafi

**Installation Package**

The zip installation package file contains the following folder structure:

- Entrustconnector
  - config
    A folder holding the installation and configuration libraries and their associated files.
  - entrust
    This is an empty folder and is intended to hold Entrust related information such as entrust.ini files and EPF credentials. Place your entrust.ini file here.
  - instances
    An initially empty folder that will be used to store all Entrust Connector instances.
  - logs
    All EntrustConnector logging will be stored here.
  - install.html
    The EntrustConnector installation guide.
  - install_configure.ps1
    The EntrustConnector installation script. Run this file from PowerShell to start the installer.
  - license.txt
    The EntrustConnector product license.

Unzip the installation package into its final location. The installer will not generate a new installation location.

**Running the Installer**

Open Windows PowerShell and navigate to the Entrust Connector installation folder. The folder will have the install_configure.ps1 script inside it. Run the script.

Note: The script requires administrator privileges to run and you will be prompted to grant administrator privileges if you run it from a regular windows account.
Licensing

Once the installer loads, the first screen is a review of the license. The license is also contained in a text file in the root folder of the installer.
If you accept the license, you will see the second license screen. This allows you to enter the license information for the product.
JCE

Entrust uses encryption key sizes that are larger than what a default JRE allows. In order to enable larger key sizes, you must install the Oracle Java Cryptographic Extension (JCE).

The installer automatically detects if the JCE is installed. If it is not installed, the installer will attempt to install it for you and you will see the below screen. If the JCE is already installed, the installer will simply go to the next installation step.

Download the appropriate JCE from Oracle for your version of Java. Typically, there is one version per overall release of java. So, Java 8 has one JCE for all versions of Java 8.
Once you install the JCE, the right arrow button will enable and you will move to the next screen. The next screen is a message that you need to restart the installer in order for the installer to use the new JCE security policies.

This also applies to Apache Tomcat. You will need to stop and start Tomcat in order for the new JCE security policies to be loaded.
Native Lib

Entrust requires a native library be installed on the Java library path. This library allows for the use of unattended logon (UAL) files.

The installer will automatically detect if the native library is on the java library path. If it is not, it will show the following screen to help you install it.

The drop down box will contain available locations you can choose from to install the native library. Any of the choices will work fine.
The Apache Tomcat Connector is used to connect Microsoft IIS with Apache Tomcat. The Tomcat Connector passes requests for certain relative URLs to Tomcat.

The installer tries to locate Apache Tomcat. If it finds one or more installed versions, it will display a drop down box and allow you to choose the version of Apache Tomcat you are currently using. If none are found, you will be shown a field where you can browse to the installation folder of Apache Tomcat. This folder is the same as the CATALINA_HOME folder and would contain the bin, conf, and lib folders among others.

The next field is where you browse to and select the Apache Tomcat Connector zip file. This file must contain a built version of the connector which is usually called isapi_redirect.dll.

Clicking the install button will install the Tomcat Connector.
IIS must be installed along with several other features. If any of the required features are not found to be installed, the installer will display a screen allowing you to install the missing features.

- **Required Features**
  - Web Server (IIS) (Web-Server)
  - IIS Client Certificate Mapping Authentication (Web-Cert-Auth)
  - CGI (Web-CGI)
  - ISAPI Extensions (Web-ISAPI-Ext)
  - ISAPI Filters (Web-ISAPI-Filter)
  - IIS Management Console (Web-Mgmt-Console)
  - IIS Management Scripts and Tools (Web-Scripting-Tools)

Clicking the install button will install the missing Windows features.
Entrust Connector Instance

The next step is to begin the process of creating an Entrust Connector Instance. An Entrust Connector instance is a web service that Venafi will connect to through the use of an Adaptable CA PowerShell script.

One Entrust Connector instance is created during the installation. However, after installation, it is possible to add more connector instances. One for each Entrust Security Manager CAs in your environment.

The Entrust Connector installation folder contains a subfolder called "entrust". This folder is intended to hold the entrust.ini files and the epf credentials for each Entrust Connector instance. Place a copy of the entrust.ini file for the CA you wish to configure the Entrust Connector instance for in the entrust subfolder.

- Entrust Connector Instance Creation Process
URL

The first step in creating an Entrust Connector instance is setting the URL.

The context path is the name of the web application and it becomes the middle of the URL. The service name is the name of the actual web service that the Adaptable CA PowerShell script will connect to.

The overall form of the URL will be:

https://<hostname>:<port>/<context_path>/<service_name>

[Image of the Entrust Connector installation interface with fields for Context Path and Service Name]
Logging

The next step in creating an Entrust Connector instance is setting up the logging for the instance.

The log file is the name and location of the log file. The Entrust Connector instance will rotate logs. In order to rotate logs, there must be a %g in the log file name. %g will be replaced by a number as the log files are rotated through.

The log level is the level of log entries to be stored in the logs.

The number of log files is the number of log files to rotate.

The maximum log size is the maximum size a log should grow to before being rotated. This setting must be in kilobytes.
Entrust

An Entrust Connector instance uses an Administrator Credential from the CA to perform the Venafi Adaptable CA operations. The next step is to configure the administrator credential epf file.

There are four possible operations to perform depending on the situation.

The first is VERIFY. Choose this setting to verify an existing administrator Entrust EPF and a corresponding unattended logon (UAL) file for the EPF.

The second is CREATE UAL. Choose this setting if there is already an existing administrator Entrust EPF. An unattended logon (UAL) file will be generated for the EPF.

The third is CREATE USER. Choose this setting to use a new Entrust user created in Entrust Security Manager. The user must be newly added.

The fourth is RECOVER USER. Choose this setting to use an existing Entrust user in Entrust Security Manager. The user must be in the key recover state.
VERIFY

When the EPF Operation is VERIFY, the EPF and UAL files are verified. This means that the EPF can be logged into using the UAL file and the administrator credential can retrieve some data from the Entrust CA.

CREATE UAL

When the EPF Operation is CREATE UAL, the password for the EPF is used to generate a UAL file and then both the EPF and UAL files are verified. This means that the EPF can be logged into using the UAL file and the administrator credential can retrieve some data from the Entrust CA.
CREATE or RECOVER USER

When the EPF Operation is CREATE USER or RECOVER USER, a new EPF and UAL will be generated. The reference number and authorization code are used to generate the EPF with the supplied password. A UAL file is generated and then both the EPF and UAL file are verified. This means that the EPF can be logged into using the UAL file and the administrator credential can retrieve some data from the Entrust CA.
Profiles

Profiles need to be configured in both an Entrust Connector instance and in Venafi. When the Venafi uses the Adaptable CA PowerShell script to create a new certificate, the profile it uses is mapped to specific Entrust User and Certificate type.

Only the profile names need to be configured in the Venafi application, but the Entrust Connector instance needs to map the profile name to specific Entrust User and Certificate types that are configured in the Entrust CA.
To add a profile, click the plus button. In the next screen, enter a unique profile name, then select the user type and certificate type. Click the Add button to add the new profile.
To edit a profile, select the profile to edit and then click the wrench button. In the next screen, edit the profile name, user, and certificate types. Click the Save button to add the new profile.
To remove a profile, select the profile to remove and then click the minus button. In the next screen, confirm the removal by clicking on the delete button.
Saving

The final step in creating a new Entrust Connector Instance is reviewing and then saving the settings.
Website Configuration

Once an Entrust Connector Instance has been created, the next step is to configure IIS to provide service for it.

Before configuring IIS, the installer must read the current IIS settings. Click the right arrow to continue.
Once the IIS settings have been read, a new website can be created or an existing website can be modified.

Create a new website if there are other websites configured on IIS or if Entrust Connector is being installed on the same IIS that is used by Venafi.

Use an existing website if there are no other websites configured or you wish to use an already created website.
Select SSL Certificate

The following screens appear in the installer when creating a new website or updating an existing website that does not have an https binding.

This process allows for selecting an existing certificate in the server's LocalMachine personal certificate store, browsing to a Pfx file, or creating a new Pfx file using the configured Entrust CA.
Selecting the certificate option allows for selecting an existing certificate in the server's LocalMachine personal certificate store.
The browsing option allows for selecting an existing Pfx file and then it installs it into the LocalMachine personal certificate store.
Creating a new SSL certificate option allows for creating a new Pfx file with a certificate generated from the configured Entrust CA.

Enter the Entrust User Distinguished Name (DN), then enter the PFX file and password in the correct fields. Click the verify DN button to check the status of the DN. The DN can refer to either a new or existing Entrust User.
If the Entrust User already exists, any configured Subject Alternative Name (SAN) entries will be shown in the table. SANs can be added, edited or removed.

**Note:** If the user is a new Entrust user, the Connector Profile selection box will be shown. This corresponds to the profiles created during the Entrust Connector Instance configuration. You must choose a profile to create the new Entrust User because the profile will specify the new Entrust User's user and certificate types.

Click the Generate Pfx button to create the Pfx file with the new certificates.
The created Pfx file must now be verified and installed so it can be used for the IIS website. Part of the verification process is making sure the certificate has the Server Authentication enhanced key usage value.
Create Binding

The following screen appears in the installer when creating a new website or updating an existing website that does not have an https binding.

The IP address can either be an asterisk or an IP address. Both the port number and hostname must also be specified.
Finish

When creating a new website, the following screen will appear to show the details of the changes to be made to IIS. Clicking on the create website button will create and configure the website.
When updating an existing website, the following screen will appear to show the details of the changes to be made to IIS. Clicking on the update website button will update and configure the website.
After creating or updating a website, the installer will ask to check the website configuration. This is accomplished by simply clicking on the link to open a web browser and attempting to view if the new Entrust Connector is active. Make sure that Apache Tomcat is running before clicking the link.
Enable IIS Client Authentication

The next step is to enable IIS Client Authentication for the website. This means the user must present a certificate in order to access the Entrust Connector instance.

IIS will take the user's presented client certificate and verify if it is valid. Then it maps it to a configured One to One mapping where a certificate is tied to a windows account. After matching the certificate to a windows account, IIS authenticates the windows account. Once all of this is successful, IIS allows the user to access the Entrust Connector instance.

The username is a windows logon username and the password is the password for the specified user. Verify the username and password by clicking on the verify button.

Note: The password entered here can be updated after installation by running the configuration tool.

https://econnector4.test.org/EntrustConnector/AdaptableCA
Select Client Certificate

A client SSL certificate must be assigned to the client authentication mapping. The client certificate can be selected from the LocalMachine personal certificate store, browsed for in an existing Pfx file, or created by using the configured Entrust CA.
Selecting the certificate option allows for selecting an existing certificate in the server's LocalMachine personal certificate store.
The browsing option allows for selecting an existing Pfx file and then it reads and verifies the certificate in the file.
Creating a new SSL certificate option allows for creating a new Pfx file with a certificate generated from the configured Entrust CA.

Enter the Entrust User Distinguished Name (DN), then enter the PFX file and password in the correct fields. Click the verify DN button to check the status of the DN. The DN can refer to either a new or existing Entrust User.
If the Entrust User already exists, any configured Subject Alternative Name (SAN) entries will be shown in the table. SANs can be added, edited or removed.

**Note:** If the user is a new Entrust user, the Connector Profile selection box will be shown. This corresponds to the profiles created during the Entrust Connector Instance configuration. You must choose a profile to create the new Entrust User because the profile will specify the new Entrust User's user and certificate types.

Click the Generate Pfx button to create the Pfx file with the new certificates.
After creating a new certificate and storing it in a Pfx file, the certificate must be read and verified. The verification will check if the certificate contains the Client Authentication enhanced key usage value in addition to verifying the certificate's revocation status.
Update IIS Client Authentication

The next step is to update IIS and add the new Client Authentication mapping. Verify the summary of changes and then click on the update website button.
After updating the client authentication settings, you must verify that the website requires and accepts the certificate. Make sure the web browser can use the client certificate and then click on the link provided to verify the connection to the Entrust Connector instance. You should be asked to present a client certificate to visit the connector web service.
Complete Installation

The final screen shows the next steps to perform. A new username credential must be created in the Venafi application that contains the information in the final screen. Venafi will use this username credential to connect to the Entrust Connector instance by using the Entrust Adaptable CA powershell script.

The client certificate that was selected must be made installed on the Venafi server in the LocalMachine personal certificate store. The Entrust Adaptable CA powershell script will use the certificate to connect to the Entrust Connector instance.

Click the finish button to complete installation.
Post Installation

**Configure Venafi to use Entrust Connector**

Each Entrust Connector instance requires a Venafi custom field and a user name credential.

**Creating the Venafi Custom Field**

The Entrust Adaptable CA PowerShell script requires a custom field be created in the Venafi Aperture application. This custom field will contain the profiles configured during the installation. **Create a custom field for each Entrust Connector instance.** One Entrust Connector instance is created during installation. Additional Entrust Connector instances may be added later.

Refer to the Venafi documentation for creating a custom field in the Venafi Aperture Application. The field must be a list type and be single select only. The values of the list custom field must match the profile names that are configured in the Entrust Connector instance.
Creating the Venafi User Name Credential

Refer to the Venafi Trust Protection Platform for instructions on creating a user name credential. The user name value of the credential must be the URL of the Entrust Connector instance web service.

The password value of the credential must be the thumbprint of the client authentication certificate. The client authentication certificate must be installed in the LocalMachine certificate store on the Venafi Trust Protection Platform server in order that it may be used by the Entrust Adaptable CA PowerShell script.

Creating the Venafi Adaptable CA Template

Refer to the Venafi Trust Protection Platform for instructions on creating an Adaptable CA Template. There are three settings which must be set:

1. Choose the Entrust Adaptable CA PowerShell script
2. Choose the User name credential (described above) and verify
3. Add the custom field (described above) and save

Entrust Connector Post Installation Configuration

Open PowerShell and run the install_configure.ps1 script again to perform post installation configuration of Entrust Connector.

Post installation configuration of the Entrust Connector includes:

- Adding another Entrust Connector Instance
- Editing an Entrust Connector Instance
- Removing an Entrust Connector Instance
- Changing an administrator EPF password
• Updating the Client Authentication Settings
  • Updating the certificates
  • Changing the windows user or password

Configuration

Entrust Connector is an implementation of the Venafi Adaptable CA API. It is composed of two parts, a powershell script and an Entrust Connector web service.

The Adaptable CA powershell script is available from Venafi and is run by the Venafi application. In performing operations, the script connects to an Entrust Connector instance to create, recover, retrieve, or revoke certificates.

An Entrust Connector instance requires an Entrust administrator user to perform the certificate management operations.

Warnings

The configuration tool looks for some configuration issues while loading and it will prompt you to fix them.

It checks for the following issues:

1. **Java Cryptographic Extension not installed**
   This can occur when Java has been updated.
2. **Entrust Connector native library was not found**
3. **Apache Tomcat folder does not exist**
   This can occur when Apache Tomcat has been updated.

Add a New Entrust Connector

Select "New Connector" from the File menu. In the first screen enter the new instance context path and service name. These values form the URL of the new Entrust Connector web service.
**Entrust Connector Instance Logging**

The next step in creating an Entrust Connector instance is setting up the logging for the instance.

The log file is the name and location of the log file. The Entrust Connector instance will rotate logs. In order to rotate logs, there must be a `%g` in the log file name. `%g` will be replaced by a number as the log files are rotated through.

The log level is the level of log entries to be stored in the logs.

The number of log files is the number of log files to rotate.

The maximum log size is the maximum size a log should grow to before being rotated. This setting must be in kilobytes.
**Entrust Connector Instance Administrator Credential**

An Entrust Connector instance uses an Administrator Credential from the CA to perform the Venafi Adaptable CA operations. The next step is to configure the administrator credential epf file.

There are four possible operations to perform depending on the situation.

The first is **VERIFY**. Choose this setting if there is already an existing administrator Entrust EPF and a corresponding unattended logon (UAL) file for the EPF.

The second is **CREATE UAL**. Choose this setting if there is already an existing administrator Entrust EPF. An unattended logon (UAL) file will be generated for the EPF.

The third is **CREATE USER**. Choose this setting to use a new Entrust user created in Entrust Security Manager. The user must be newly added.
The fourth is RECOVER USER. Choose this setting to use an existing Entrust user in Entrust Security Manager. The user must be in the key recover state.

VERIFY
When the EPF Operation is VERIFY, the EPF and UAL files are verified. This means that the EPF can be logged into using the UAL file and the administrator credential can retrieve some data from the Entrust CA.
CREATE UAL

When the EPF Operation is CREATE UAL, the password for the EPF is used to generate a UAL file and then both the EPF and UAL files are verified. This means that the EPF can be logged into using the UAL file and the administrator credential can retrieve some data from the Entrust CA.
CREATE or RECOVER USER

When the EPF Operation is CREATE USER or RECOVER USER, a new EPF and UAL will be generated. The reference number and authorization code are used to generate the EPF with the supplied password. A UAL file is generated and then both the EPF and UAL file are verified. This means that the EPF can be logged into using the UAL file and the administrator credential can retrieve some data from the Entrust CA.
**Entrust Connector Instance Profiles**

Profiles need to be configured in both an Entrust Connector instance and in Venafi. When the Venafi uses the Adaptable CA PowerShell script to create a new certificate, the profile it uses is mapped to specific Entrust User and Certificate type.

Only the profile names need to be configured in the Venafi application, but the Entrust Connector instance needs to map the profile name to specific Entrust User and Certificate types that are configured in the Entrust CA.
To add a profile, click the plus button. In the next screen, enter a unique profile name, then select the user type and certificate type. Click the Add button to add the new profile.
To edit a profile, select the profile to edit and then click the wrench button. In the next screen, edit the profile name, user, and certificate types. Click the Save button to add the new profile.
To remove a profile, select the profile to remove and then click the minus button. In the next screen, confirm the removal by clicking on the delete button.
Saving the Entrust Connector Instance Settings

The final step in creating a new Entrust Connector Instance is reviewing and then saving the settings.
**New Instance Created**

Use the information on the final screen to create the Venafi Custom field and user name credential. The username part of the credential is the web service URL, and the password part of the credential is the thumbprint of the client authentication certificate (see editing client authentication mappings to locate the configured certificate thumbprint).

Use the profile names as the values in a new Venafi custom field. Set the custom field type to be a single select list and then enter the profile names as the list values.
Edit an Entrust Connector

Select "Edit Connector" from the File menu. At the top of the resulting screen is a selection box that allows for choosing which Entrust Connector instance to edit.

If there are more than one Entrust Connector instances, then a remove button is available to remove the selected instance.
Clicking the remove button provides a prompt to confirm the removal of the selected Entrust Connector instance.
Updating the Entrust Connector Instance Entrust Settings

On the initial edit instance pane, in the lower section, the Entrust Connector instance entrust.ini and EPF locations are shown. In addition, there is an EPF Operation selection box with four possible values.

- **Verify**
  Select this option to simply verify the credential and corresponding Unattended Logon (UAL) file.

- **Change Password**
  Select this option to change the EPF file password. A new UAL file will be generated and then verified.

- **Rebind UAL**
  Select this option to generate a new UAL file.

- **Create/Recover**
  Select this option to generate a new EPF by supplying Entrust activation codes. Once the EPF has been generated, a new UAL file will be created and then verified.
Changing the EPF password allows you to enter the current password, and then the desired new password.
Rebinding the UAL file requires the current EPF password. The UAL file is verified after creation.
When creating or Recovering the EPF file, make sure to check the new user check box if the Entrust user is new. If recovering an existing Entrust user, do not check the new user check box.

Enter the desired EPF password and the Entrust User's current activation codes (reference number and authorization code).
Entrust Connector Instance Profiles

Profiles need to be configured in both an Entrust Connector instance and in Venafi. When the Venafi uses the Adaptable CA PowerShell script to create a new certificate, the profile it uses is mapped to specific Entrust User and Certificate type.

Only the profile names need to be configured in the Venafi application, but the Entrust Connector instance needs to map the profile name to specific Entrust User and Certificate types that are configured in the Entrust CA.

Note: You must also make changes to the corresponding Venafi custom field. The profile names must be the same in both lists.
To add a profile, click the plus button. In the next screen, enter a unique profile name, then select the user type and certificate type. Click the Add button to add the new profile.
To edit a profile, select the profile to edit and then click the wrench button. In the next screen, edit the profile name, user, and certificate types. Click the Save button to add the new profile.
To remove a profile, select the profile to remove and then click the minus button. In the next screen, confirm the removal by clicking on the delete button.
**Editing the Logging Settings**

The last section allows for updating the Entrust Connector instance logging settings.
Saving the Entrust Connector Instance Settings

The final step in editing an Entrust Connector Instance is to review and save the settings.

Note: You must restart Apache Tomcat to ensure the new settings are read.
Manage Client Authentication Mappings

About Client Authentication Mapping

Entrust Connector requires client authenticated SSL to secure the web service. What this means is that the client must present a certificate to be allowed to use the web service.

In this case, the client is the Entrust Adaptable CA PowerShell script. It will present a certificate to the web service in order to be able to use the service. The client certificate must be installed in the LocalMachine certificate store of the Venafi TPP server in order for the Entrust Adaptable CA PowerShell script to access it.

The Entrust Adaptable CA PowerShell script accesses the web service using the information in the Venafi Username Credential that is supplied by Venafi TPP. The Username of the Venafi Username Credential is the URL of the Entrust Connector instance web service. The password of the Venafi Username Credential is the thumbprint of the client certificate to present to the web service.
IIS configured client authenticated SSL by linking a client certificate with a Windows account. When the certificate is presented, IIS will authenticate the windows user associated with the client certificate. **Note:** the Windows account does not need and should not have any privileges. It is only used for verifying the client certificate.

**Managing Client Authentication Mappings**

In the File menu, select the Edit Cauth Mapping. In the screen, there are options to add, edit, and remove a mapping. Common client authentication management operations are:

- **Add Mapping**
  - If more than one Venafi TPP will be connecting to an Entrust Connector instance, then a new client certificate mapping can be made for each Venafi TPP.
  - **Note:** The same Windows user can be used for multiple mappings as long as the client certificates are unique. The client certificate is first validated followed by authenticating the Windows user.

- **Edit Mapping**
  - Change Windows User Password
  - Update the Client certificate

- **Remove Mapping**
  - If a particular mapping is no longer needed, then it can be removed.
Add Mapping

There are three steps to creating a new client authentication mapping:

1. Choose the client certificate to map.
2. Enter the Windows User information to map the certificate to
3. Review and add the mapping

Choosing the Client Authentication Certificate

The first step in creating a new client authentication mapping is to choose the client certificate that will be mapped to a Windows user account.

There are three options:
Selecting a certificate will search for and show certificates from the LocalMachine personal store that have the client authentication enhanced key usage setting.
Browsing for a Pfx file allows for choosing an existing client certificate. The certificate will be read from the Pfx file and verified.
Creating a new certificate will generate a new certificate from an Entrust CA using a configured Entrust Connector instance. The first step is to choose which Entrust Connector instance to use.
Next, enter the Distinguished Name (DN) of the certificate to generate. The DN can refer to an existing Entrust user or a new Entrust user can be created.

After entering the DN and the Pfx file and password to save the certificate to, click the Verify DN button. This will verify the DN in the Entrust CA. If it refers to an existing user, the user's Subject Alternative Name entries are read. If it is a new user, then the parent DN is verified to make sure it exists.
The next step in generating a new certificate is adding, editing, or removing subject alternative name entries. Once the Subject Alternative Name entries are correct, click the Generate Pfx to create the Pfx.
The final step is reading the Pfx to verify the certificate. Part of the verification is checking if the certificate contains the client authentication enhanced key usage.
Entering the Windows User Information

Enter in the Windows user and password into the fields. Clicking on the verify button authenticates the username and password to ensure they are valid.

**Note:** The windows user does not require any privileges and is only used by IIS to authenticate the username and password.

**Note:** The same windows user may be used for multiple client authentication mappings as long as the client certificates are unique.
Adding the New Mapping

Review the new client authentication mapping details and then add the new mapping, or cancel and return to the edit client authentication main screen.
Edit Mapping

There are two items to edit in a client authentication mapping:

1. The Windows user account information
2. The client certificate
Updating the Windows User Information

Click on the Update Windows Account check box to update the Windows account information. Common management tasks are to update the Windows account password.

Edit the Windows user and password information as needed. Clicking on the verify button authenticates the username and password to ensure they are valid.

Note: The windows user does not require any privileges and is only used by IIS to authenticate the username and password.

Note: The same windows user may be used for multiple client authentication mappings as long as the client certificates are unique.
Choosing the Client Authentication Certificate

Click on the Change Certificate check box to update the client certificate. Common management tasks include updating the certificate when it is nearing expiration.

There are three options:
Selecting a certificate will search for and show certificates from the LocalMachine personal store that have the client authentication enhanced key usage setting.
Browsing for a Pfx file allows for choosing an existing client certificate. The certificate will be read from the Pfx file and verified.
Creating a new certificate will generate a new certificate from an Entrust CA using a configured Entrust Connector instance. The first step is to choose which Entrust Connector instance to use.
Next, enter the Distinguished Name (DN) of the certificate to generate. The DN can refer to an existing Entrust user or a new Entrust user can be created.

After entering the DN and the Pfx file and password to save the certificate to, click the Verify DN button. This will verify the DN in the Entrust CA. If it refers to an existing user, the user's Subject Alternative Name entries are read. If it is a new user, then the parent DN is verified to make sure it exists.
The next step in generating a new certificate is adding, editing, or removing subject alternative name entries. Once the Subject Alternative Name entries are correct, click the Generate Pfx to create the Pfx.
The final step is reading the Pfx to verify the certificate. Part of the verification is checking if the certificate contains the client authentication enhanced key usage.
Updating the Mapping

Clicking the Update Mapping button on the Edit Mapping screen updates the IIS client authentication mapping with the new values.
Remove Mapping

Review the client authentication mapping details and then either remove the mapping or cancel.
Install JCE

The Entrust Connector instances as well as the configuration tool use encryption key sizes and or algorithms that are larger or more advanced than what is supported in the default Oracle Java installation. The Java Cryptographic Extension (JCE) can be downloaded from Oracle and installed to overcome the cryptographic limitations.

Select "Install JCE" from the File menu and then browse to the JCE zip file. Click the install button to install the JCE.
Update Tomcat Location

If Apache Tomcat is updated and has a new CATALINA_HOME folder, then it must also be updated in the configuration tool. Simply select the new Tomcat home folder from the selection box, or browse to the Tomcat home folder if the tool was unable to locate Apache Tomcat installations.

Select "Update Tomcat" from the File menu.
Update License Information

Select "Update License" from the File menu and then enter the license information obtained from Cygnacom Solutions.
Uninstall

Select "Uninstall" from the File menu.
After confirmation, the product is uninstalled and then the final screen is shown:
Uninstallation Complete