Obtaining technical support

For support assistance by telephone call one of the numbers below:
- 1-877-754-7878 in North America
- 1-613-270-3700 outside North America

You can also email Customer Support at: support@entrust.com

Copyright © 2009 Entrust. All rights reserved.

Entrust is a trademark or a registered trademark of Entrust, Inc. in certain countries. All Entrust product names and logos are trademarks or registered trademarks of Entrust, Inc. in certain countries. All other company and product names and logos are trademarks or registered trademarks of their respective owners in certain countries.

This information is subject to change as Entrust reserves the right to, without notice, make changes to its products as progress in engineering or manufacturing methods or circumstances may warrant.

Export and/or import of cryptographic products may be restricted by various regulations in various countries. Export and/or import permits may be required.
Understanding VPN digital certificate authentication

VPN endpoints (secure gateways or clients) authenticate each other to establish a secure connection. This means that the type of authentication you use determines the level of security of your VPN. Outside of a public key infrastructure (PKI), VPNs are more susceptible to security breaches.

To establish a secure, VPN connection, use an Entrust digital certificate. There are other ways to authenticate to a VPN router, such as by using a token or user name and password; however, these do not provide the ability to encrypt and sign documents like your Entrust certificate does.

This chapter includes the following information about using digital certificates with a VPN:

- “IPSec VPN and SSL VPN (portal and tunnel)” on page 4
- “SSL VPNs and man-in-the-middle attacks” on page 5
- “VPN authentication mechanisms: digital certificates or one-time password (OTP) tokens?” on page 6
**IPSec VPN and SSL VPN (portal and tunnel)**

You can use your Entrust Digital ID with both IPSec (Internet Protocol Security) VPN as well as SSL (Secure Sockets Layer) portal and tunnel VPNs.

In business, VPNs allow employees to communicate securely with their company’s internal network so they can do their jobs from any computer. It is important to note that network security is only as strong as the method used to identify the users and devices at each end of the VPN communication.

Digital IDs used for VPN connections enable strong certificate authentication for both IPSec and SSL VPN. Strong certificate authentication ensures that authenticating to the VPN does not expose the user or company to potential data theft or authentication credential theft.

The difference between IPSec VPN and SSL VPN lies in the client-side software and connectivity requirements.

IPSec requires each end user to install client-side software on their computers, such as the Cisco VPN client. With IPSec, the end user is associated with a digital certificate that the receiving device trusts. This allows the receiving device to authenticate the end user using a digital certificate.

SSL portal VPN does not require client-side software. SSL tunnel VPN may require either a browser plug-in or traditional client. Both portal and tunnel are used with a standard Web browser. Gartner Market Size & Forecast predicted in 2006 that SSL portal VPNs will be the primary remote-access method mostly due to the convenience of not requiring client software (Gartner December 2006).
SSL VPNs and man-in-the-middle attacks

A presenter at the Black Hat Briefings USA 08 convention identified several SSL VPN security issues, identifying SSL VPN as susceptible to man-in-the-middle (MITM) attacks. A MITM attack is when an attacker intercepts communications between two parties without their knowledge. Acting as a proxy, attackers can review and manipulate the contents of the messages they are relaying between the two parties.

The SSL VPN security issues described involving MITM attacks affected installations using password authentication or a one-time password (OTP) mechanism—including those that use a token—and not those using certificates for SSL client authentication.

With OTP as the authenticator, once the attacker intercepts the session, the attacker can replay the OTP within the allotted validation period and gain access to private and sensitive information.

At the Black Hat 08 convention, the presenter intercepted the SSL VPN session by:

- obtaining a certificate from a trusted CA (trusted by the browser), which included the Fully Qualified Domain Name (FQDN) of a target SSL VPN URL
- changing the DNS record to point to the MITM proxy server IP address through a DNS attack

When certificates are used for second-factor authentication, these security concerns are alleviated. Certificate authentication requires mutual authentication and verification between the client and server, who both have a public/private key pair. Attackers cannot show the server that they have access to the private key of the certificate—which proves certificate ownership. As such, the session fails because the attacker cannot authenticate to the server.

Since SSL VPN does not require client-side software, it is viewed as a more convenient and less costly solution than IPSec VPN. To ensure that client credentials remain protected even in this recent MITM attack scenario, you can use Entrust certificates for client authentication.
VPN authentication mechanisms: digital certificates or one-time password (OTP) tokens?

To ensure users can securely gain network access through a virtual private network (VPN), the VPN must incorporate an authentication mechanism that secures the end points of the VPN. A user name and password alone is not secure and increases the risk that an attacker can gain access to the network. As such, a second factor authentication mechanism is necessary.

Both digital certificates and one-time password (OTP) tokens are often used for second factor authentication (often with user name and password as the first factor authenticator). However, digital certificates offer greater cost savings, security, and ease of use when compared to the OTP token.

See the table below for more information.

Table 1: Comparing OTP tokens to digital certificates as a VPN authentication mechanism

<table>
<thead>
<tr>
<th>Item/feature</th>
<th>OTP token</th>
<th>Digital certificate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>Tokens can cost up to $50 per user. It also represents a large overhead for those users who only require remote access a few times. ($$)</td>
<td>Certificates can cost as low as $5 per user.</td>
</tr>
<tr>
<td>mechanism cost</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td>OTPs do not address the sophisticated attacks of today, which are based on perpetrating fraud through impersonation. OTPs are vulnerable to man-in-the-middle attacks.</td>
<td>Digital certificates provide the strongest level of authentication and enable trust. For enhanced security, Entrust supports smart cards for storage of cryptographic keys and certificates.</td>
</tr>
<tr>
<td>Compatibility</td>
<td>Tokens are proprietary and require compatibility with the VPN device.</td>
<td>The X.509 standards allow for easy interaction between components. The majority of VPNs are CAPI compliant, making the connection seamless and transparent.</td>
</tr>
<tr>
<td>Flexibility</td>
<td>Limited to authentication.</td>
<td>Certificates are not restricted to VPN access, but can be used to authenticate to a wide variety of devices and applications, to digitally sign, and to encrypt. They also provide non-repudiation.</td>
</tr>
</tbody>
</table>
### Table 1: Comparing OTP tokens to digital certificates as a VPN authentication mechanism

<table>
<thead>
<tr>
<th>Item/feature</th>
<th>OTP token</th>
<th>Digital certificate</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Administration</strong></td>
<td>Must issue and physically provide users with tokens. Also must provide support for forgotten passwords and lost tokens. ($$$)</td>
<td>With Entrust Managed Services PKI, you can issue and manage certificates through a Web-based application anywhere, anytime.</td>
</tr>
<tr>
<td><strong>Management</strong></td>
<td>Must replace lost tokens ($$$).</td>
<td>With Entrust Managed Services PKI, administrators and users can centrally manage certificates from a Web-based application. Administrators can create accounts (individual and in bulk), approve pending requests, edit accounts, reset accounts, deactivate and reactivate accounts, and search accounts, requests, and audits. Users can register, create, and recover a certificate as well as perform account management tasks. This includes resetting their account, revoking their account, putting their account on hold, removing a hold, changing their registration password, and viewing their activation codes for creating their certificate.</td>
</tr>
<tr>
<td><strong>Convenience</strong></td>
<td>Users have to carry their token with them and enter the numeric sequence displayed by their token. Tokens are also small and easy to lose.</td>
<td>With Entrust Managed Services PKI, certificates are stored in CAPI and added to the trusted certificate store, which makes it easy to use with VPN and other applications. You can also export keys out of CAPI to move credentials from computer to computer.</td>
</tr>
</tbody>
</table>
### Table 1: Comparing OTP tokens to digital certificates as a VPN authentication mechanism

<table>
<thead>
<tr>
<th>Item/feature</th>
<th>OTP token</th>
<th>Digital certificate</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>External access to VPN for business partners</strong></td>
<td>Must supply OTP tokens to all business partners if you want to provide access to your VPN.</td>
<td>You can establish a VPN between business partners by cross-certifying CAs. Alternatively, you can issue a certificate from your CA to your business partners. With Entrust Managed Services PKI, you can issue certificates in minutes and business partners can obtain their certificates through the Web-based application anywhere, anytime.</td>
</tr>
<tr>
<td><strong>Scalability</strong></td>
<td>Must purchase additional tokens. Also, an increased number of tokens increases the administration requirements, as there is a greater risk of forgotten passwords and lost tokens. ($$)</td>
<td>Administrators can create new accounts in minutes. Users can receive their certificate anywhere, anytime, using Entrust Managed Services PKI Web-based interface.</td>
</tr>
</tbody>
</table>
Setting up certificate authentication for VPN

To use your Entrust certificate for VPN authentication, you need to import your certificate into your VPN client.

This guide assumes you already have an Entrust certificate. For instructions on obtaining a certificate from Entrust Managed Services PKI, see one of the following guides available from the Resources tab of www.entrust.com/managed_services based on your role. If you are an:

- administrator, see the Entrust Managed Services PKI Administrator Guide
- end-user, see one of the following based on your organization's deployment:
  - Getting an Entrust certificate using Entrust Authority Administration Services
  - Getting an Entrust certificate using Entrust Entelligence Security Provider

This chapter includes the following topics:

- “Importing your Entrust certificate into your VPN client” on page 9
- “Configuring your router to trust certificates issued to VPN clients” on page 11
- “Associating users with tunnel groups based on certificate matching” on page 12

Importing your Entrust certificate into your VPN client

When you activate your digital ID, its certificate is placed in the Windows security store. This lets you use the certificate for VPN authentication.

To import your Entrust certificate into your VPN client

1. Open your VPN client.
2 Import the certificate from the certificate store into the VPN client. 
Using the Cisco VPN client as an example, import a certificate as follows:

a Click **Certificates** > **Import**.

The **Import Certificate** dialog box appears.

b Select **Import from Microsoft Certificate store**.

c Select your certificate from the **Import Certificate** drop-down list.

d Enter a password if required.

e Click **Import**.
A new dialog box appears.

3 For each connection entry, select the type of authentication to use. Using the Cisco VPN client, select Certificate Authentication and click Save.

4 Once you configure your connection, start a VPN session. The VPN router on the server you connect to checks the certificate used by your VPN client. If the certificate is signed by a CA that the router trusts, the connection succeeds.

Configuring your router to trust certificates issued to VPN clients

You need to configure your VPN router or gateway on the server end of the VPN connection to trust the Entrust certificates imported into the VPN client. Do this before users begin enrolling for certificates. The exact configuration details vary with the router. See your vendor’s documentation.

Keep in mind that you must configure the router to only accept certificates that:

- were issued by the Entrust CA, which is accomplished just by loading the CA certificate and removing all others
- have the correct subject Distinguished Name (DN)

Each customer of Entrust Managed Services PKI has a dedicated subtree in the Directory of a shared CA. This means, the subject DN uniquely identifies your certificates within the Directory; for example: cn=User1, ou=MyCompany, c=CA. No other user of the shared PKI will have certificates with ou=MyCompany. So,
configure the router to accept only those certificates with your organization name in the DN.

**Associating users with tunnel groups based on certificate matching**

VPN tunnel groups allow you to determine VPN user access rights based on group membership. This allows you to give your marketing department, for example, access to one area of your network while preventing another department access to that same area.

To configure VPN tunnel groups based on certificates, you need to establish specific connection policies for each tunnel group and then set group policies for each group. The policy must define a “certificate matching policy”, which groups users based on certain fields in the certificate’s distinguished name (DN), for example, the organizational unit (\textit{ou}).

For example, to associate a tunnel group using certificate matching in Cisco ASA, you must use the \texttt{tunnel-group-map} command in combination with a certificate map.

---

**Note:** With Entrust Managed Services PKI, organizations under the standard certificate service offering must use the certificate matching policy to ensure only users from their \textit{ou} (or any other field in the DN) can access their network using VPN.

---

For more information on configuring tunnel groups for certificate matching, see your VPN vendor’s documentation.