



Deploying and administering certificates

When you purchase certificates, there are three costs to consider: the cost of the certificates themselves, the cost to deploy them to your users, and the cost to administer them once deployed. On all three counts, Entrust is a winner: we offer competitive certificate pricing, several deployment options to minimize rollout time and maximize security, and a full-featured administration service that lets administrators easily keep the system in check. Let's take a closer look at these features.

Competitive certificate pricing

If you only need to supply certificates to a handful of users, then purchasing a few personal certificates for them for a flat fee off a Web site may be perfectly acceptable—mind you, you won't get any deployment or administration capabilities.

Now let's say you need to deploy to a larger user base where deployment and administration costs become a concern. This is where Entrust excels: we provide you with a full-featured, enterprise-class administration service GUI from which to deploy, manage, and report on certificates—and we do so at a price that is very competitive.

Multiple deployment options to minimize roll-out time and maximize security

Deploying certificates using a low-cost approach often involves compromising on security. But if security is important to you, paying a little extra for an approach that meets your security standards might sound reasonable. Entrust understands the need to balance security and cost. That's why we provide a number of options for certificate enrollment. You can decide which one best matches your security and budgetary requirements. The enrollment methods are described on the following pages.

Full-featured administration service

Once deployed, you need to be able to manage your certificates. There are two fundamental management functions: the ability to revoke certificates immediately and the ability to track their status.

Instant certificate revocation

Say an employee leaves your company, or one of your partnerships dissolves. Do you really want these people to be able to access whatever assets are protected with those certificates? Of course not, and that's why *you need to be able to revoke their certificates instantaneously*. Other certificate services may only provide a delayed revocation, requiring that you email them requesting a revocation. This email could take days or weeks to process, and in the meantime, your assets remain available to untrusted people. Entrust, by contrast, recognizes the importance of instant revocation, and makes it available through its administration service, as part of its standard service offering.

Certificate status tracking

When are your server certificates slated for expiry? How many users have signed up for certificates? Who has recently been revoked? These are just some of the questions you can investigate when you have proper reporting functionality at your disposal. Entrust makes this functionality available through its administration service, as part of its standard offering.

Enrollment options

Option 1: Single user enrollment

How it works:

1. An administrator at your organization creates a one-time passcode for a single person using the administration service
2. The administrator gives the passcode to the user
3. The user enters the passcode on a Web site
4. Certificates are downloaded to the user's computer

Benefits:

- No custom development—administration service + Web site are provided with the standard service
- Good for scenarios where you only need to enroll a single user, such as a new employee or partner

Option 2: Username & password

How it works:

1. An administrator at your organization bulk loads usernames and passwords using the administration service
2. An email is sent to each user with a link to a Web site + username
3. The user clicks the link, and enters the appropriate username/password on the Web site
4. Certificates are downloaded to the user's computer

Benefits:

- No custom development—bulk loading + Web site are provided with the standard service
- Flexible bulk loading—username/password combinations can be dumped from an existing system, or created from scratch

Option 3: Email with embedded passcode

How it works:

1. An administrator at your organization bulk loads your users' email addresses using the administration service
2. The administration service generates an email containing a link + embedded, one-time passcode for each user
3. The email is sent to each user securely
4. The user clicks the link in the email and is taken to a Web site where the passcode is checked
5. Certificates are downloaded to the user's computer

Benefits:

- No user input required—the user simply needs to click a link to download their certificates
- No custom development—bulk loading + Web interfaces + passcode functionality are all provided with the standard service

Option 4: Self-registration + approvals

How it works:

1. Each user self-registers on a Web page, selecting a password
2. An administrator at your company approves the registration using the administration service
3. The administration service sends an email to the user
4. The user clicks the link in the email, which takes them to a Web page where they enter their password and download their certificate

Benefits:

- No custom development—administration service + Web site are provided with the standard service
- No need to create a bulk loading file
- Approvals ensure security
- Easy for users—they can access to the registration page without having to supply a username/password

Option 5: Existing certificates + self-registration

How it works:

1. Your users already have certificates issued by another certificate service
2. Each user goes to a Web site which uses the existing certificate to authenticate them (i.e. client SSL authentication) and then grants them access to a registration page
3. The user supplies personal information
4. A new certificate from Entrust is downloaded to their computer to take over from the older certificate

Benefits:

- No need to create a bulk loading file
- Leverages your existing investment in certificates to provide a more secure authentication approach
- Easy for users—they can authenticate to the registration Web page without having to supply a username/password

Note: There is an additional charge for this option

Option 6: Existing username/password + self-registration

How it works:

1. You have an existing, in-house authentication system (Windows login for example)
2. Each user logs in to a registration Web page using a username/password from the existing authentication system
3. The user submits personal information
4. Certificates are downloaded to the user's computer

Benefits:

- No need to create a bulk loading file
- Leverages your existing investment in another authentication system
- Easy and familiar for users—they supply a username/password that they already know

Note: There is an additional charge for this option

Option 7: Custom registration page

How it works:

1. A Web developer at your organization creates a Web-based registration application
2. The user logs in to this registration page using any authentication mechanism of your choosing
3. The user submits their personal information which is sent to the administration service
4. The administration service redirects the user to a Web page (supplied by Entrust) where they click a button to download their certificates

Benefits:

- No need to create a bulk loading file
- Leverages your existing investment in another authentication system for up-to-date passwords
- Easy and familiar for users—they supply a username/password that they already know
- Custom development can be completed by your organization without the help of Entrust and with no additional fees

Option 8: Auto-creation and auto-updates

How it works:

1. A thin client is installed on users' computers or unmanned machines
2. An administrator creates a one-time passcode for each user or machine using the administration service
3. The user enters the passcode into the thin client and certificates are downloaded to their computers

Note: When the client is installed on an unmanned machine, the client detects that certificates are missing and communicates with the administration service to automatically generate and download certificates

Benefits:

- Certificates are automatically updated—no need to go back to a Web site to pick up new certificates
- Complete automation available—perfect for unmanned machines
- No custom development
- Many client installation options, from near complete automation, to clicking 'Next' through an installer
- Client also simplifies deployment of Microsoft Encryption File System (EFS), adds file encryption, and includes a built-in OCSP client

Note: There is an additional charge for this option

About Entrust

Entrust [NASDAQ: ENTU] secures digital identities and information for consumers, enterprises and governments in more than 1,650 organizations spanning 60 countries. Leveraging a layered security approach to address growing risks, Entrust solutions help secure the most common digital identity and information protection pain points in an organization. These include SSL, authentication, fraud detection, shared data protection and e-mail security. For information, call 888-690-2424, email entrust@entrust.com or visit www.entrust.com.

Entrust[®] Securing Digital Identities & Information

Entrust is a registered trademark of Entrust, Inc. in the United States and certain other countries. In Canada, Entrust is a registered trademark of Entrust Limited. All other Entrust product names and service names are trademarks or registered trademarks of Entrust, Inc. or Entrust Limited in certain countries. All other company names, product names and logos are trademarks or registered trademarks of their respective owners. © Copyright 2009 Entrust. All rights reserved.