Entrust® Identification Server 7.0

Entrust® Entitlements Server 7.0

Administration Guide

Document issue: 1.0

Date: June 2003

Entrust®
Securing Digital Identities & Information

Table of contents

Chapter 1

About this document

This document is the Administration Guide for Entrust Identification Server 7.0 and Entrust Entitlements Server 7.0. It provides an overview of the product and instructions about how to install and integrate Identification Server and Entitlements Server into your Entrust GetAccess installation.

This chapter of the guide tells you where you can find Entrust information and documents related to the Identification Server and Entitlements Server, explains the document's typographical conventions, and describes how to obtain technical support.

Topics in this chapter:

Related documents

This section lists and briefly describes documentation related to Entrust Identification Server 7.0 and Entrust Entitlements Server 7.0.

You can find the latest documentation on the Entrust Customer Support Web site at https://www.entrust.com/support/documentation/index.cfm.

Entrust Application Server Runtimes 7.0

Entrust Application Server Runtimes 7.0 Administration Guide

Entrust Application Server Runtimes 7.0 is a client of the Web Services interface that Entrust Identification Server provides for Entrust GetAccess.

This guide describes Entrust Application Server Runtimes 7.0. It provides information about how to install and configure the product to protect EJB resources on either BEA® WebLogic Server™ or IBM® WebSphere® Application Server.

Entrust GetAccess 7.0

- *Entrust GetAccess 7.0 Product Guide*

  This guide is an overview of Entrust GetAccess. It describes the product's features and components, and explains how they work together.

- *Entrust GetAccess 7.0 Planning and Installation Guide*

  This guide shows the system architectures that Entrust GetAccess supports and explains how to deploy them. It also provides details about how to install and run the Entrust GetAccess server components and an Entrust GetAccess Runtime Service on a front-end computer. This guide is the hub of the Entrust GetAccess documentation set. Refer to it to find all the information related to installing and configuring your chosen architecture.

- *Entrust GetAccess 7.0 System Administration Guide*

  This guide describes how to configure and administer your Entrust GetAccess system. It also provides details about the installation of components that are not installed with the Entrust GetAccess server or Runtime Service installers.

- *Entrust GetAccess 7.0 Troubleshooting Guide*

  This is the Entrust GetAccess troubleshooting guide. Refer to it if you encounter problems when you are installing or running Entrust GetAccess.

- *Entrust GetAccess 7.0 Business Administration Guide*

  This guide describes the administrative tasks necessary to protect resources with the Entrust GetAccess system. The guide helps administrators and

department managers to develop a structure of protected resources that are accessible to various groups of users with an organization.

Typographic conventions

The following typographic conventions are used throughout this guide:

Table 1:

Convention	Purpose	Example
Bold text (other than headings)	Indicates graphical user interface elements and wizards	Click **Next**.
Italicized text	Used for book or document titles	*Entrust® Identification Server 7.0 Administration Guide*
Blue text	Used for hyperlinks to other sections in the document	Refer to "Related documents" on page 2.
Underlined blue text	Used for Web links	For more information, visit our Web site at www.entrust.com.
`Courier` type	Indicates installation paths, file names, Windows registry keys, commands, and text you must type	Locate and double-click the executable file called `AppServerRuntimes_setupwin32.exe`.
Angle brackets < >	Indicates variables (text you must replace with your organization's correct values)	Navigate to `<install_path>\Tools\dvt`.
Square brackets [ ]	Indicates optional parameters	`dsa password [-ldap]`

Note and Attention text

Throughout this guide you will see paragraphs that have ruled lines above and below the text. These paragraphs provide key information with two levels of importance, as shown below.

Note: Hints, tips, and information that must be emphasized to help you get the best from your software.

Attention: Issues that, if ignored, may seriously affect performance, security, or the operation of your software.

Getting help

Entrust recognizes the importance of providing quick and easy access to our support resources. The following subsections provide details about the technical support, training, and professional services available to you.

Technical Support

Entrust offers a variety of technical support programs to help you keep Identification Server and Entitlements Server up and running. To learn more about the full range of Entrust technical support services, visit our Web site at:

http://www.entrust.com/support/

If you are registered in our support program, you can use our Web-based support services at:

https://www.entrust.com/support/contact/index.htm

The Customer Support Extranet Web site offers technical resources including online versions of Entrust product documentation, white papers and technical notes, and a comprehensive Knowledge Base.

Note: You must have an account to use the Customer Support Extranet Web site. To create an account, go to https://www.entrust.com/members/user_create.htm

---

When you contact Entrust Customer Support, please provide as much of the following information as possible:

- Your contact information
- Product name, version, and operating system information
- Your deployment scenario
- Description of the problem
- Copy of log files containing error messages
- Description of conditions under which the error occurred
- Description of troubleshooting activities you have already performed

Telephone number

For telephone assistance between 8:00 AM and 8:00 PM Eastern Standard Time (EST), Monday to Friday, call one of the numbers below:

- 1-866-267-9297 in North America
- 1-613-270-2680 outside North America

E-mail address

The e-mail address for Customer Support is:

customer.support@entrust.com

Online

To submit a question online, go to the following Web address:

https://www.entrust.com/support/supportinfo/index.htm

Professional Services

The Entrust team assists e-businesses around the world to deploy and maintain secure transactions and communications with their partners, customers, suppliers and employees. We offer a full range of professional services to deploy our e-business solutions successfully for wired and wireless networks, including planning and design, installation, system integration, deployment support, and custom software development.

Whether you choose to operate your Entrust solution in-house or subscribe to hosted services, Entrust Professional Services will design and implement the right solution for your e-business needs. For more information about Entrust Professional Services please visit our Web site at:

http://www.entrust.com

Chapter 2

About Entrust Identification Server and Entrust Entitlements Server

This chapter provides an overview of Entrust Identification Server 7.0 and Entrust Entitlements Server 7.0. It includes a brief introduction to Web services in general, and then goes on to describe the protocols used by Identification Server and Entitlements Server to expose Entrust GetAccess security as Web services.

Topics in this chapter:

Overview

Entrust Identification Server 7.0 and Entrust Entitlements Server 7.0 comprise a set of servlets that you can install and deploy on an Entrust GetAccess 7.0 Infrastructure.

Identification Server and Entitlements Server provide a public Web services interface that allows you to integrate Entrust security into your applications, giving client applications the capability to make authentication and authorization calls to Entrust GetAccess. Such applications can be Web services clients or Java™ clients.

To take advantage of the authentication and authorization services provided by Entrust GetAccess, a Web services client makes Simple Object Access Protocol (SOAP) calls containing Security Assertion Markup Language (SAML) information over HTTP to Identification Server and Entitlements Server. To gain access to the same security services without programming SOAP and SAML directly, a Java application can use the application programming interfaces (APIs) provided by the client-side software development kit (SDK), which is part of the Identification Server and Entitlements Server product.

Web services

The World Wide Web Consortium's (W3C) Web Services Architecture Working Group defines the term **Web services** as follows:

"A Web service is a software system identified by a URI, whose public interfaces and bindings are defined and described using XML. Its definition can be discovered by other software systems. These systems may then interact with the Web service in a manner prescribed by its definition, using XML based messages conveyed by internet protocols." (See the W3C Web Services Working Draft of 14 November 2002. (http://www.w3.org/TR/2002/WD-ws-arch-20021114/)

Within such a software system, Web-based applications interact with each other dynamically using open XML standards, including the Simple Object Access Protocol (SOAP).

Entrust Identification Server and Entrust Entitlements Server make it easier for you to integrate security into your Web services applications, by providing a standards-based security Web services interface to Entrust GetAccess.

Security Web services

This section briefly introduces SOAP, the Web Services Trust Language (WS-Trust), and the Security Assertion Markup Language (SAML). Identification Server and Entitlements Server make use of these three standards to secure the exchange of information with Entrust GetAccess.

Simple Object Access Protocol (SOAP)

SOAP is an XML message-based protocol for exchanging messages and invoking Web services. It enables businesses to communicate over standard transport mechanisms, such as HTTP, allowing them direct access to Web services. As well as exchanging structured messages, SOAP provides the means to make application-to-application method calls in distributed computer environments invoking an XML response.

Refer to the W3C Note (http://www.w3.org/TR/SOAP/) for the latest SOAP specifications.

Web Services Trust Language (WS-Trust)

WS-Trust is one of a set of proposed Web Services Security (WS-Security) standards that provide extensions to SOAP for building secure Web services. The WS-Trust draft specification states that "The goal of WS-Trust is to enable applications to construct trusted SOAP message exchanges."

Refer to the draft specification of December 18th. 2002 (http://www-106.ibm.com/developerworks/library/ws-trust/) for more detailed information.

Security Assertion Markup Language (SAML)

SAML is an XML vocabulary developed by the OASIS XML-Based Security Services Technical Committee. It conveys information about an entity's authentication status and authorization privileges in the form of assertions, which are structured XML elements. SAML assertions can contain nested child elements with various declarations about an entity's authentication, authorization, and security attributes.

The SAML specification defines a binding to SOAP that describes how SAML requests map to SOAP messages over HTTP. The SAML-SOAP binding is an XML-based request and response format. Using this mechanism, clients can make requests to SAML authorities, (policy decision points, and authentication and attribute authorities) to issue assertions.

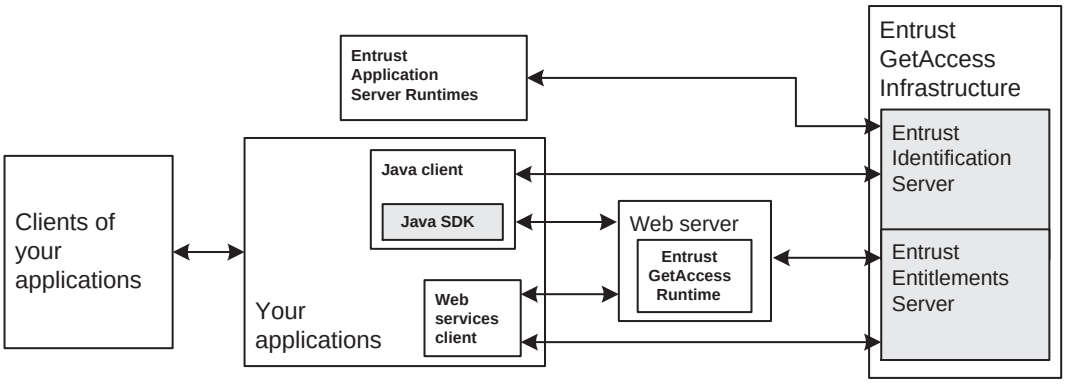
SAML operations in Entrust Identification Server and Entrust Entitlements Server conform to the SAML 1.0 specification, which is an OASIS standard. Refer to the OASIS Security Services Technical Committee Web site (http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security) for more information about SAML and for links to the SAML specification.

Entrust Identification Server and Entrust Entitlements Server

The Entrust Identification Server and the Entrust Entitlements Server are distinct from the Identification and Entitlements Services of Entrust GetAccess. They are sets of servlets that run on the Entrust GetAccess Infrastructure and communicate with core Entrust GetAccess services using the Common Object Request Broker Architecture (CORBA).

Figure 1 shows a logical view of Identification Server and Entitlements Server deployed in an Entrust GetAccess environment.

Figure 1: Identification Server and Entitlements Server deployment — logical view



Entrust Identification Server

Entrust Identification Server provides a Web services interface that allows client applications to make identification requests on behalf of their users to Entrust GetAccess. The Identification Server is a SAML authentication and attribute authority that provides Web services based on the following standards:

- WS-Trust for logging in users

  – The `loginPasswordUser` and `loginDnUser` interfaces both return an Entrust GetAccess session ID for users logging in with passwords and Distinguished Name (DN)
- SAML Authentication Query

  – The `getUserId` interface returns a user ID for an Entrust GetAccess session ID
- SAML Attribute Query

– The `getRoles` interface returns Entrust GetAccess roles for a session ID, and `getStaticRoles` returns Entrust GetAccess static roles for an Entrust GetAccess user ID

The identification request reaches the Identification Server over HTTP as a SAML or WS-Trust request in a SOAP envelope. If the request is successful, the response contains a SAML assertion comprising an authentication token (Entrust GetAccess session identifier), user identity, or user roles.

The components of Identification Server that are responsible for handling authentication requests and attribute queries and responding with authentication and attribute assertions are as follows:

- `CredentialCollector` servlet — uses WS-Trust and SOAP over HTTP, receives the authentication request, and queries the underlying Entrust GetAccess services with username and password or DN credentials to determine the user's validity
- `AuthenticationAuthority` servlet — uses the session ID of the authenticated user, issued by Entrust GetAccess, to provide a SAML authentication assertion using SOAP over HTTP
- `AttributeAuthority` servlet — returns a set of Entrust GetAccess user roles using SAML and SOAP over HTTP

Entrust Entitlements Server

Entrust Entitlements Server, as a SAML authorization authority, provides a Web services interface that accepts SAML authorization requests to determine a user's access privileges to protected resources.

When a user requests access to a protected resource, the Policy Enforcement Point (PEP) sends a SAML authorization query to the Entitlements Server's AuthorizationAuthority servlet. The Entitlements Server acts as the Policy Decision Point (PDP) using the Entrust GetAccess Entitlements Engine to make the authorization decision. When the decision about access to the resource has been made, the Entitlements Server responds to the request with an authorization assertion, which declares whether the user is entitled to gain access to the protected resource.

Note: Because the Entitlements Server uses the Entrust GetAccess Entitlements Service to make authorization decisions, it supports Entrust GetAccess policy rules.

Sample messages

The `IdEntitlementsServer\docs\sampleMessages` directory contains sample XML messages demonstrating the use of WS-Trust, SOAP, and SAML to communicate with Identification Server and Entitlements Server interfaces.

Each interface has an XML request message and corresponding response message in the following subdirectories:

- `CredentialCollector`
  - `loginPasswordUser.req.xml`
  - `loginPaswwordUser.res.xml`
  - `loginDnUser.req.xml`
  - `loginDnUser.res.xml`
- `AuthenticationAuthority`
  - `getUserId.req.xml`
  - `getUserId.res.xml`
- `AttributeAuthority`
  - `getRoles.req.xml`
  - `getRoles.res.xml`
  - `getStaticRoles.req.xml`
  - `getStaticRoles.res.xml`
- `AuthorizationAuthority`
  - `isEntitled.req.xml`
  - `isEntitled.res.xml`

Except for the sample messages in the `CredentialCollector` directory, which include SOAP envelopes, the sample messages show only the contents of the SOAP body.

Identification Server and Entitlements Server interfaces

Each Identification Server and Entitlements Server interface corresponds to a method call in the SDK and each has an associated XML (SAML or WS-Trust) request and response message. Refer to the Javadoc reference documentation in the `IdEntitlements\sdk\javadoc` directory for detailed SDK method information, and to the sample request and response messages in `IdEntitlements\docs\sampleMessages.`

Table 2 lists the Identification Server and Entitlements Server methods.

Table 2: Identification Server and Entitlements Server interfaces

Interface	Description
loginPasswordUser	Logs in a user based upon userID and password and obtains an Entrust GetAccess session ID (SID)
loginDnUser	Obtains a session ID for a user corresponding to the user's Distinguished Name (DN) **Note** This method assumes that a user has been authenticated to Entrust GetAccess outside the Identification Server.
getUserId	Obtains a userID based upon the SID
getRoles	Obtains user roles based upon the SID
getStaticRoles	Obtains roles for a user based upon userID
isEntitled	Determines whether a user is entitled to gain access to a resource

The `loginPasswordUser` interface supports only Entrust GetAccess username-password authentication, which is the default authentication method for a user.

User names passed to the `loginDnUser` interface must be Entrust GetAccess users identified by a DN. Clients requiring access to protected methods should use client-authenticated SSL (optional, but recommended). To assign a DN to a user, Entrust GetAccess requires the optional Certificate Pluggable Authentication and Authorization Module (PAAM) (refer to "Installing the Entrust GetAccess Certificate PAAM" on page 55 for information).The `loginDnUser` interface does not support other authentication methods that use DNs, such as TruePass, LDAP, and custom PAAMs.

The `getStaticRoles` method uses the Entrust GetAccess user ID to obtain a list of roles for the user, but the list does not include dynamic roles that might be associated with the Entrust GetAccess session during user login.

The `getRoles` method uses the Entrust GetAccess session ID to obtain a list of user roles, including static roles and any dynamic roles associated with the session ID. If a user logs in through an Entrust GetAccess-protected Web server using the LDAP PAAM, when you use the resulting session ID with the `getRoles` method, you will obtain any dynamic roles associated with the user. Keep in mind that the `loginPassword` user interface supports only Entrust GetAccess username-password authentication, so a session ID obtained using this method will not have any associated LDAP dynamic roles. Refer to the "Optional PAAM

configurations" chapter of the *Entrust GetAccess 7.0 System Administration Guide* for more information about the LDAP PAAM and dynamic roles.

Client SDK

The Identification Server and Entitlements Server includes, as part of the installation, a Java client SDK. The SDK comprises a Java API, a set of Javadoc-generated reference documentation, and a sample client application in the following subdirectories of `IdEntitlements\sdk`:

- `javadoc` — contains the Javadoc-generated HTML reference documentation for the client SDK's API
- `lib` — contains the SDK's jar files
- `samples` — contains a sample client application and script files to run the sample

Application programming interface

The API provides the means to gain access to Entrust GetAccess by way of the Web services interface without using WS-Trust, SOAP, and SAML messages directly. It consists of four Java packages that include interfaces for the Identification Server and the Entitlements Server, and classes that implement the interfaces for Entrust GetAccess. The API calls you can make correspond to the XML request-response messages listed in "Sample messages" on page 16:

- Implemented in `com.entrust.stp.ga.GaSamlIdentificationClient`
  - `loginPasswordUser`
  - `loginDnUser`
  - `getUserId`
  - `getRoles`
  - `getStaticRoles`
- Implemented in `com.entrust.stp.ga.GaSamlEntitlementClient`
  - `isEntitled`

Refer to the Javadoc reference documentation (`javadoc\index.html`) for detailed information about the contents and capabilities of the API.

Note: The `getRoles` method and the Web services interface for SAML AttributeQuery return an expanded list of roles — they do not return macro roles.

Sample client

The sample Java client application, `IesClientTest.java`, in the `sdk\samples` subdirectory, demonstrates how to use the client SDK's API.

The subdirectory also contains a compiled class file that you can use as a command-line test client to confirm that the Identification Server and Entitlements Server are working correctly. Refer to the `sdk\samples\readme.txt` file, and to the section called "Verifying successful installation" on page 47 for information about how to use the sample client for this purpose.

Third party software

To use the client SDK, you must have version 1.3.x of the Java 2 SDK Standard Edition (J2SDK) installed on your computer. You can download the J2SDK version 1.3.x from Sun Microsystems' archive download page (http://java.sun.com/products/archive/index.html).

The client SDK uses Apache Axis 1.0 for SOAP and HTTP client support, and Apache Xerces 1.4.4 for processing XML. The `sdk\lib` directory contains the appropriate jar files.

Chapter 3

Deploying Identification Server and Entitlements Server

This chapter describes options for deploying Identification Server and Entitlements Server.

Topics in this chapter:

Overview

The servlets that comprise Identification Server and Entitlements Server are always deployed on an Entrust GetAccess Infrastructure. You can deploy Entrust GetAccess on a wide variety of system architectures — the *Entrust GetAccess 7.0 Planning and Installation Guide* discusses several of these.

This chapter describes a number of deployment options for Identification Server and Entitlements Server.

Note: The discussions refer to the Entrust Application Sever Runtimes, which you might not be using in your deployments. The Application Server Runtimes are specific examples of a Java client.

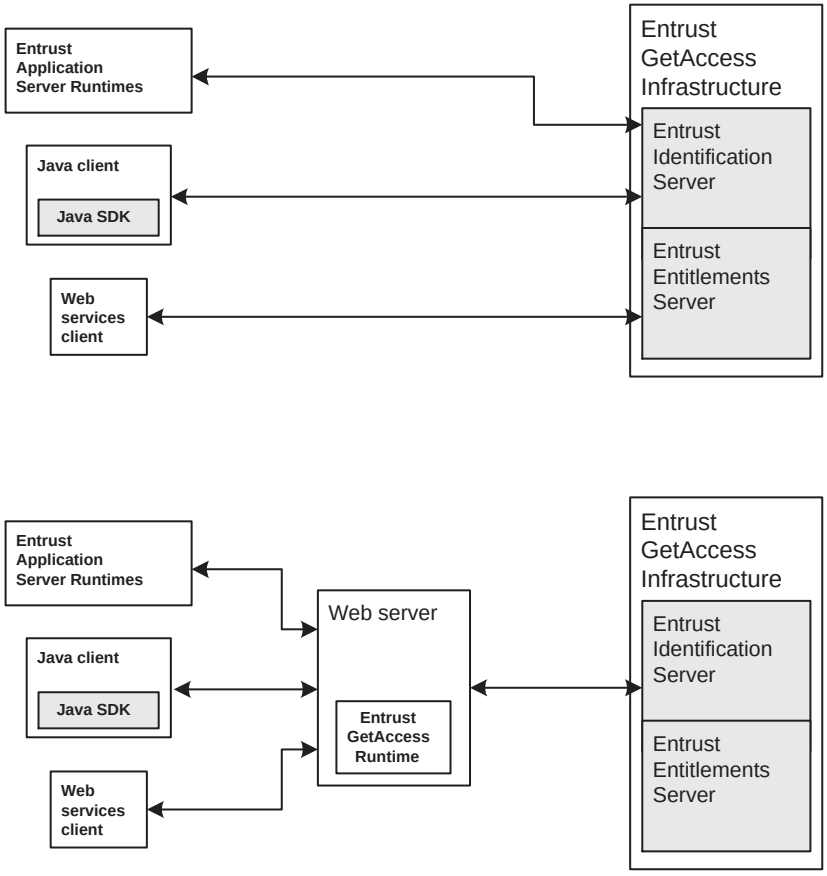
Refer to the chapter called "Configuring Identification Server and Entitlements Server communications" on page 57 for information and procedures that describe how to set up communication between Identification Server and Entitlements Server clients and Entrust GetAccess, including SSL configuration and client authorization.

Identification Server and Entitlements Server clients

Clients of Identification Server and Entitlements Server can be Web services applications that use the product's Web services interface directly, custom applications that use the Java SDK, and the Entrust Application Server Runtimes installed on Web application servers.

Figure 2 shows the communication paths between Identification Server and Entitlements Server and their clients. Communication, which consists of SAML requests and responses inside SOAP envelopes over HTTP, takes place directly with the Identification Server and Entitlements Server through the Entrust GetAccess Infrastructure port, or by way of a Web Server running an Entrust GetAccess Runtime that acts as an Access Portal.

Figure 2: Entrust Identification Server and Entitlements Server deployment — logical view



Deployment scenarios

The deployment scenarios for Identification Server and Entitlements Server described in this chapter are based upon the following four baseline deployments of Entrust GetAccess described in the *Entrust GetAccess 7.0 Planning and Installation Guide*:

- Deployment 1: single machine
- Deployment 2: distributed
- Deployment 3: distributed, centralized logins
- Deployment 6: failover

You should consider the first two deployment scenarios, single machine and distributed, as suitable only for evaluating the deployment of your applications rather than as full production environments.

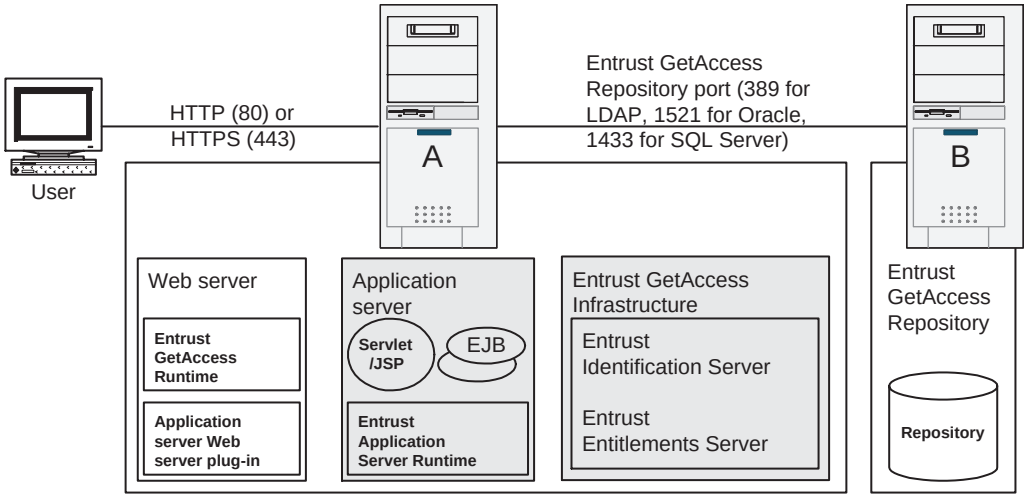
The deployment descriptions present scenarios involving Entrust Application Server Runtimes (protecting EJBs on Web application servers by way of servlets or JSPs) as clients of Identification Server and Entitlements Server. The deployment diagrams do not show Web services clients or custom Java clients using the SDK. In these cases you would not need to use front-end Web servers or Web Application servers.

A deployment worksheet accompanies each deployment description, providing high-level instructions for each configuration.

Single computer deployment

Refer to Deployment 1 in the chapter called "Deploying Entrust GetAccess" in the *Entrust GetAccess 7.0 Planning and Installation Guide* for information about this deployment architecture.

Computer A runs all of the software and components necessary for this deployment, which is intended for evaluation of the software rather than as a production environment. Computer B houses the Entrust GetAccess repository.



Deployment worksheet

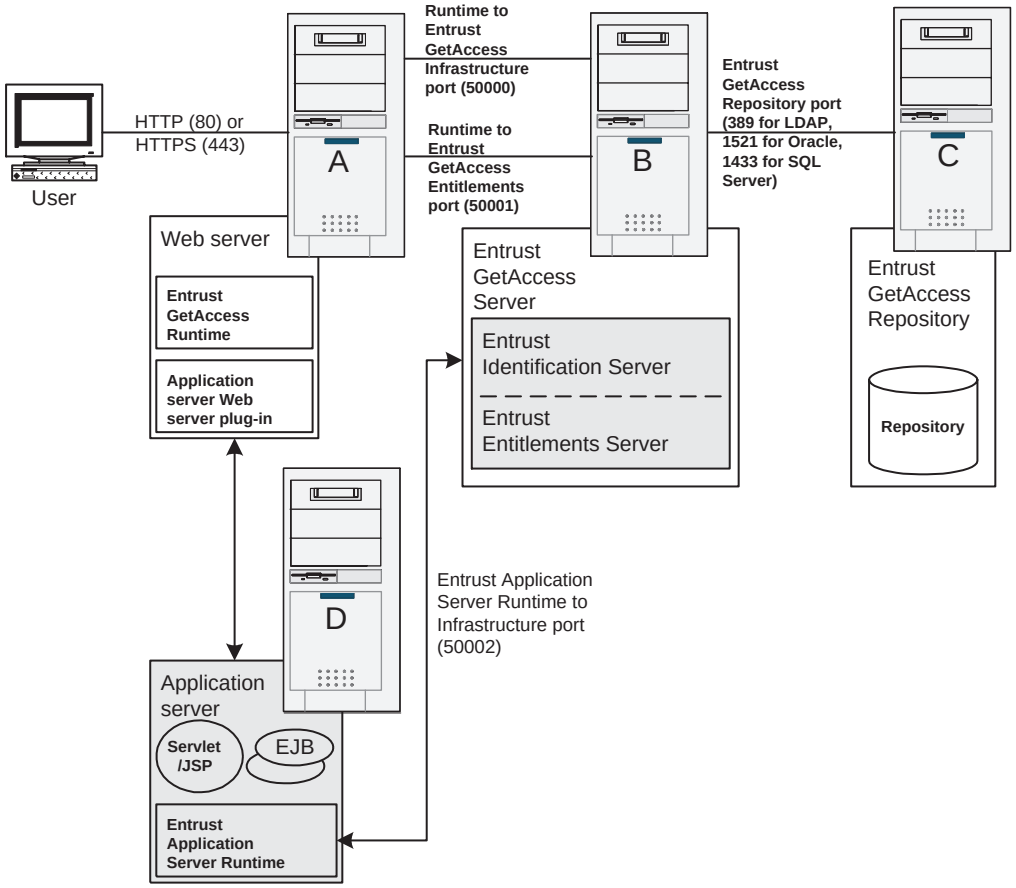
Step	Where to find information	Completed
1. Follow the instructions for Entrust GetAccess Deployment 1.	"Deploying Entrust GetAccess" chapter of the *Entrust GetAccess 7.0 Planning and Installation Guide*	
2. Install Entrust Identification Server 7.0 and Entrust Entitlements Server 7.0 on computer A.	Refer to the chapter called "Installing Identification Server and Entitlements Server" on page 39.	
3. Test the Identification Server and Entitlements Server installation. **Note** If you are installing the Application Server Runtime software, complete the remaining steps in this worksheet.	Refer to the section called "Verifying successful installation" on page 47.	
4. Install a Web application server on computer A.	Refer to your Web application server documentation.	
5. Install a Web server plug-in for your application server on Web server A.	Refer to your Web application server documentation.	
6. Create a Web application (or use the samples included with your application server) that uses one or more EJBs through a servlet or JSP. Confirm that you can gain access to the Web application through the Web server.	Refer to your Web application server documentation.	
7. Protect the servlet or JSP using Entrust GetAccess. Confirm that users with appropriate roles can gain access to your Web application.	Refer to your Entrust GetAccess documentation — *Entrust GetAccess 7.0 Business Administration Guide* and *Entrust GetAccess 7.0 System Administration Guide*.	

Step	Where to find information	Completed
8. Install the Entrust Application Server Runtimes 7.0 for your Web application server. Use port 50002 to communicate with Entrust GetAccess.	Refer to the "Installation" chapter of the *Entrust Application Server Runtimes 7.0 Administration Guide*.	
9. Protect an EJB method using Entrust GetAccess roles. Confirm that users with appropriate roles can gain access to the capabilities provided by the protected method.	Refer to the chapters called "Post installation tasks" and "Verifying installation" in the *Entrust Application Server Runtimes 7.0 Administration Guide*.	

Distributed installation deployment

Refer to Deployment 2 in the chapter called "Deploying Entrust GetAccess" in the *Entrust GetAccess 7.0 Planning and Installation Guide* for information about this deployment architecture.

In this deployment, the Entrust GetAccess components and the Identification Server and Entitlements Server are installed on different computers making this a distributed computing environment, again, for evaluation purposes rather than as a production environment.



Deployment worksheet

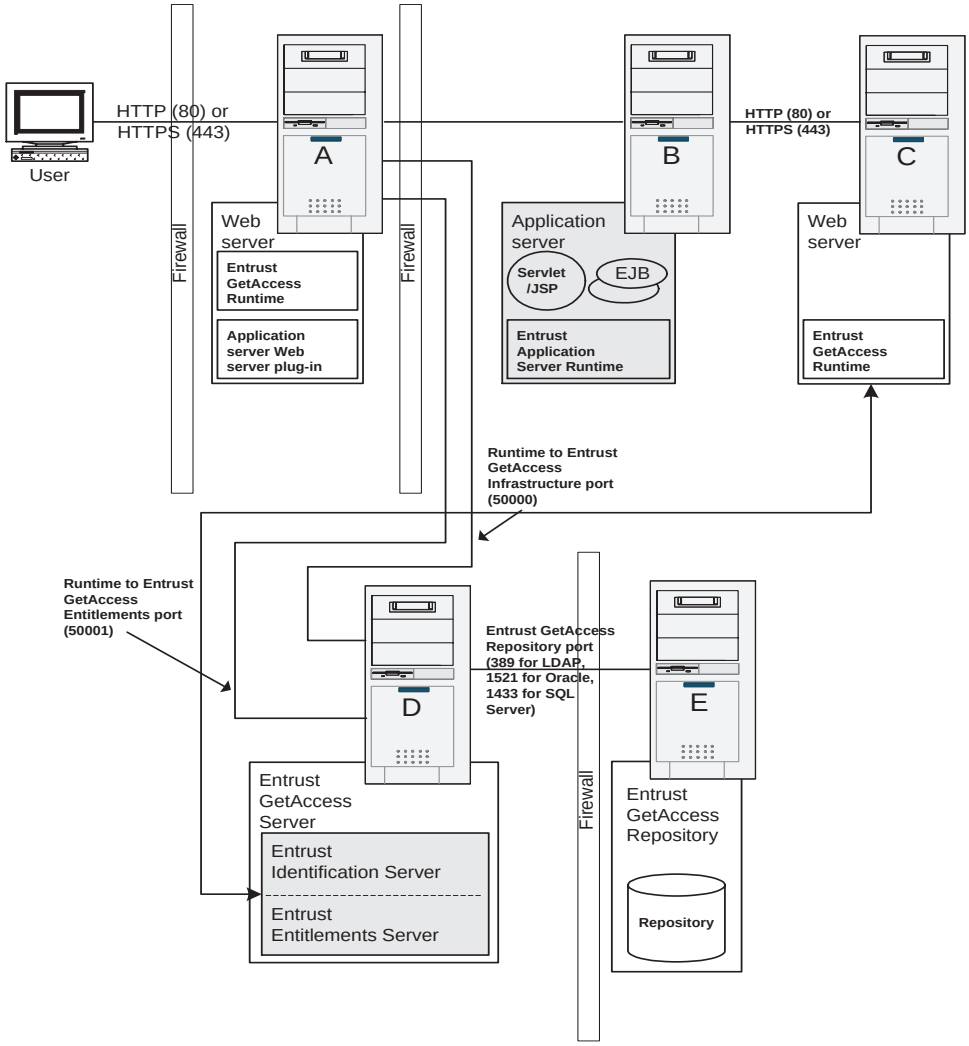
Step	Where to find information	Completed
1. Follow the instructions for Entrust GetAccess Deployment 2.	"Deploying Entrust GetAccess" chapter of the *Entrust GetAccess 7.0 Planning and Installation Guide*	
2. Install Entrust Identification Server 7.0 and Entrust Entitlements Server 7.0 on computer B.	Refer to the chapter called "Installing Identification Server and Entitlements Server" on page 39.	
3. Test the Identification Server and Entitlements Server installation. **Note** If you are installing the Application Server Runtime software, complete the remaining steps in this worksheet.	Refer to the section called "Verifying successful installation" on page 47.	
4. Install a Web application server on computer D.	Refer to your Web application server documentation.	
5. Install a Web server plug-in for your application server on Web server A.	Refer to your Web application server documentation.	
6. Create a Web application (or use the samples included with your application server) that uses one or more EJBs through a servlet or JSP. Confirm that you can gain access to the Web application through the Web server.	Refer to your Web application server documentation.	
7. Protect the servlet or JSP using Entrust GetAccess. Confirm that users with appropriate roles can gain access to your Web application.	Refer to your Entrust GetAccess documentation — *Entrust GetAccess 7.0 Business Administration Guide* and *Entrust GetAccess 7.0 System Administration Guide*.	

Step	Where to find information	Completed
8. Install the Entrust Application Server Runtimes 7.0 for your Web application server on computer D. Use port 50002 to communicate with Entrust GetAccess.	Refer to the "Installation" chapter of the *Entrust Application Server Runtimes 7.0 Administration Guide*.	
9. Protect an EJB method using Entrust GetAccess roles. Confirm that users with appropriate roles can gain access to the capabilities provided by the protected method.	Refer to the chapters called "Post installation tasks" and "Verifying installation" in the *Entrust Application Server Runtimes 7.0 Administration Guide*.	

Distributed installation with firewalls

Refer to Deployment 3 in the chapter called "Deploying Entrust GetAccess" in the *Entrust GetAccess 7.0 Planning and Installation Guide* for information about this deployment architecture.

This deployment architecture represents a suitable production environment that includes firewall protection. The Identification Server and Entitlements Server are installed on the Entrust GetAccess Infrastructure, computer D.



Deployment worksheet

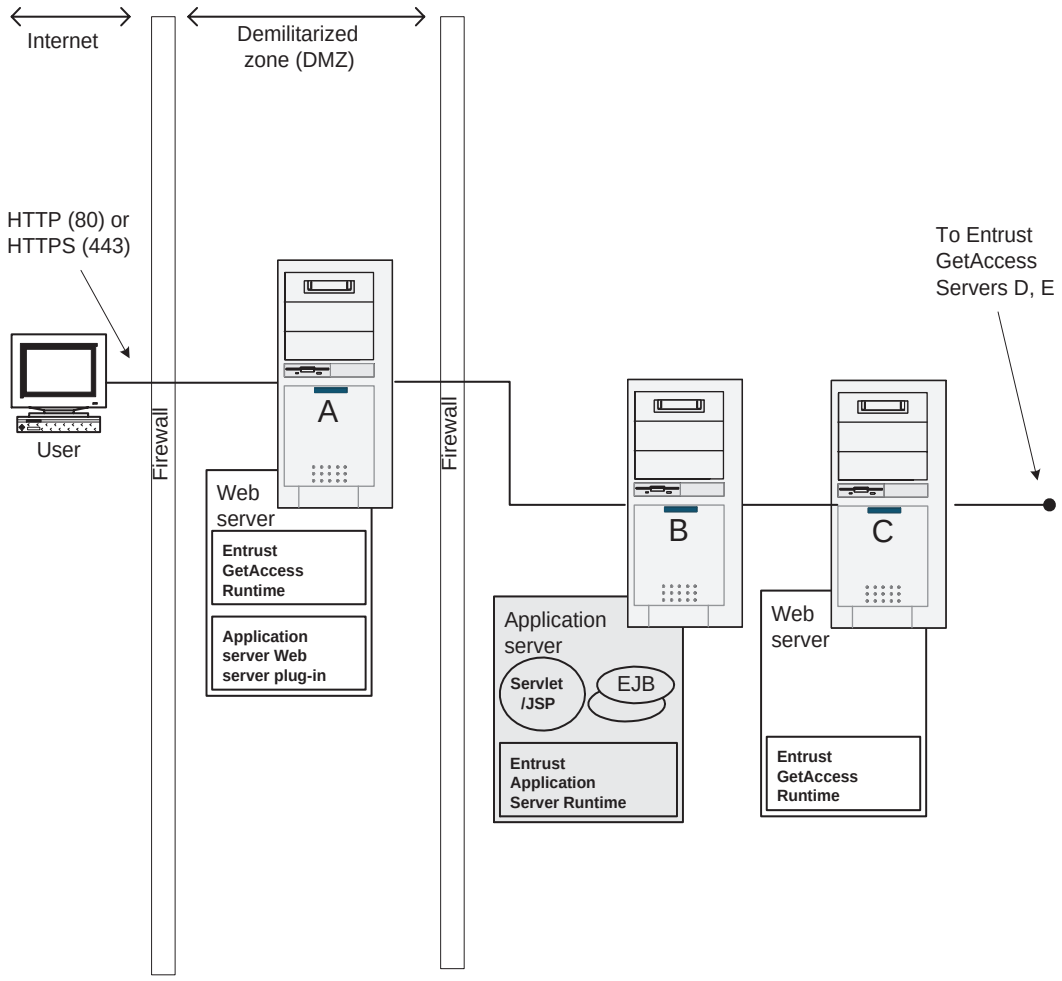
Step	Where to find information	Completed
1. Refer to the instructions for Entrust GetAccess Deployment 3. Entrust GetAccess is installed on computer D and its repository on computer E.	"Deploying Entrust GetAccess" chapter of the *Entrust GetAccess 7.0 Planning and Installation Guide*	
2. Install Entrust Identification Server 7.0 and Entrust Entitlements Server 7.0 on computer D.	Refer to the chapter called "Installing Identification Server and Entitlements Server" on page 39.	
3. Test the Identification Server and Entitlements Server installation. **Note** If you are installing the Application Server Runtime software, complete the remaining steps in this worksheet.	Refer to the section called "Verifying successful installation" on page 47.	
Install a Web server on computer A.	Refer to your Web server documentation for details.	
4. Install a Web application server on computer B.	Refer to your Web application server documentation.	
5. Install a Web server plug-in for your application server on Web server A.	Refer to your Web application server documentation.	
6. Create a Web application (or use the samples included with your application server) that uses one or more EJBs through a servlet or JSP. Confirm that you can gain access to the Web application through the Web server.	Refer to your Web application server documentation.	
7. Protect the servlet or JSP using Entrust GetAccess. Confirm that users with appropriate roles can gain access to your Web application.	Refer to your Entrust GetAccess documentation — *Entrust GetAccess 7.0 Business Administration Guide* and *Entrust GetAccess 7.0 System Administration Guide*.	

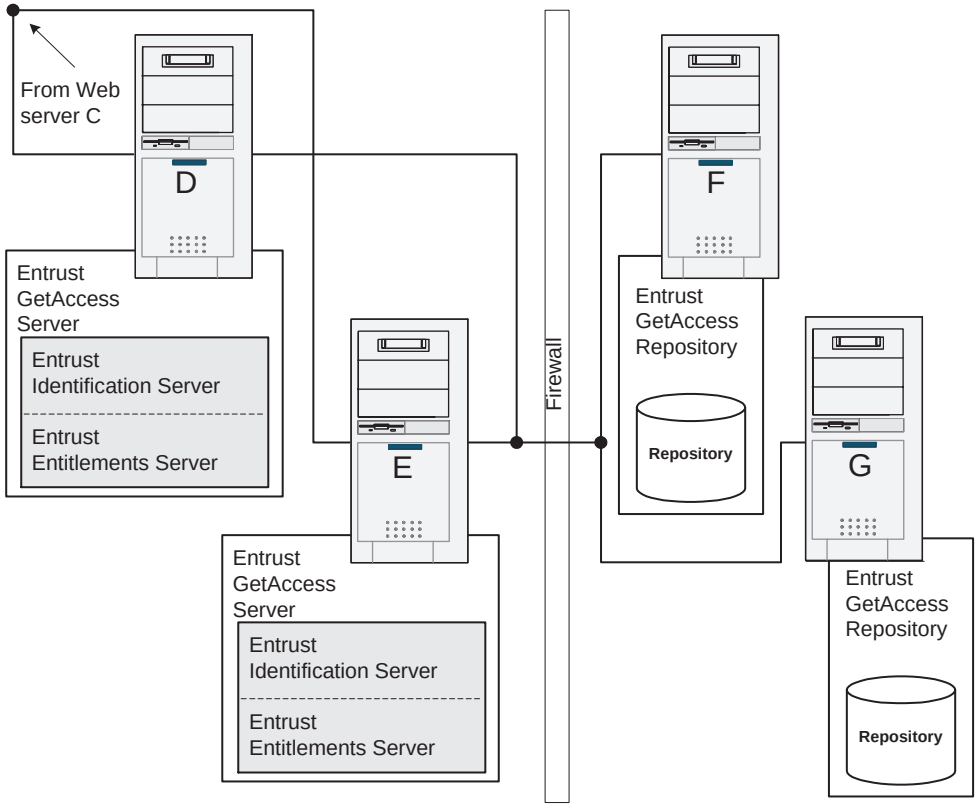
Step	Where to find information	Completed
8. Install a Web server and Entrust GetAccess Runtime on computer C. Ensure you select the Access Portal checkbox as described in the Entrust GetAccess Runtime Service installation instructions.	Refer to your Web server documentation for details. Refer to the "Installing the Runtime Service" chapter of the *Entrust GetAccess 7.0 Planning and Installation Guide.*	
9. Install the Entrust Application Server Runtimes 7.0 for your Web application server on computer B. Use port 80 or 443 to communicate with Entrust GetAccess by way of a Web server, computer C.	Refer to the "Installation" chapter of the *Entrust Application Server Runtimes 7.0 Administration Guide*.	
10. Protect an EJB method using Entrust GetAccess roles. Confirm that users with appropriate roles can gain access to the capabilities provided by the protected method.	Refer to the chapters called "Post installation tasks" and "Verifying installation" in the *Entrust Application Server Runtimes 7.0 Administration Guide*.	

Identification Server and Entitlements Server failover

Refer to Deployment 6 in the chapter called "Deploying Entrust GetAccess" in the *Entrust GetAccess 7.0 Planning and Installation Guide* for information about this deployment architecture.

This deployment architecture represents a suitable production environment that includes firewall protection. The Identification Server and Entitlements Server are installed on the two computers that are running Entrust GetAccess, computers D and E.




From Web server C
D
Entrust GetAccess Server
Entrust Identification Server
Entrust Entitlements Server
E
Entrust GetAccess Server
Entrust Identification Server
Entrust Entitlements Server
Firewall
F
Entrust GetAccess Repository
Repository
G
Entrust GetAccess Repository
Repository

Deployment worksheet

Step	Where to find information	Completed
1. Refer to the instructions for Entrust GetAccess Deployment 6. This deployment scenario is similar to Entrust GetAccess Deployment 6. Entrust GetAccess is installed on computers D and E and their repositories on computers F and G.	"Deploying Entrust GetAccess" chapter of the *Entrust GetAccess 7.0 Planning and Installation Guide*	
2. Install Entrust Identification Server 7.0 and Entrust Entitlements Server 7.0 on computers D and E. Computer D is the primary Entrust GetAccess server and fails over to computer E.	Refer to the chapter called "Installing Identification Server and Entitlements Server" on page 39.	
3. Test the Identification Server and Entitlements Server installation. **Note** If you are installing the Application Server Runtime software, complete the remaining steps in this worksheet.	Refer to the section called "Verifying successful installation" on page 47.	
4. Install a Web application server on computer B.	Refer to your Web application server documentation.	
5. Install a Web server plug-in for your application server on Web server A.	Refer to your Web application server documentation.	
6. Create Web applications (or use the samples included with your application server) that use one or more EJBs through a servlet or JSP. Confirm that you can gain access to the Web applications through Web server A.	Refer to your Web application server documentation.	
7. Protect the servlets or JSPs using Entrust GetAccess. Confirm that users with appropriate roles can gain access to your Web applications.	Refer to your Entrust GetAccess documentation — *Entrust GetAccess 7.0 Business Administration Guide* and *Entrust GetAccess 7.0 System Administration Guide*.	

Step	Where to find information	Completed
8. Install the Entrust Application Server Runtimes 7.0 for your Web application server on computer B. This computer communicates with Entrust GetAccess through the Web server and the Entrust GetAccess Runtimes on computer C.	Refer to the "Installation" chapter of the *Entrust Application Server Runtimes 7.0 Administration Guide*.	
9. Install a Web server and Entrust GetAccess Runtime on computer C. Ensure you select the Access Portal checkbox as described in the Entrust GetAccess Runtime Service installation instructions.	"Installing the Runtime Service" chapter of the *Entrust GetAccess 7.0 Planning and Installation Guide.*	
10. Protect an EJB method using Entrust GetAccess roles. Confirm that users with appropriate roles can gain access to the capabilities provided by the protected method.	Refer to the chapters called "Post installation tasks" and "Verifying installation" in the *Entrust Application Server Runtimes 7.0 Administration Guide*.	

Chapter 4

Installing Identification Server and Entitlements Server

This chapter describes how to prepare for, install, and test Entrust Identification Server 7.0 and Entrust Entitlements Server 7.0.

Topics in this chapter:

Preparation and planning

You can install and configure Entrust Identification Server 7.0 and Entrust Entitlements Server 7.0 to run on computers running Microsoft® Windows® 2000 Server, Microsoft Windows 2000 Advanced Server, or the Sun™ Solaris™ 8 and Solaris 9 (64 bit) operating systems.

Refer to the ReadMe document for specific information about the platforms and operating systems that support the Identification Server and Entitlements Server.

Dependencies

Identification Server and Entitlements Server must be installed on a computer running Entrust GetAccess 7.0. For information about Entrust GetAccess, refer to the document entitled *Entrust GetAccess 7.0 Product Guide*, and for installation instructions, to the *Entrust GetAccess 7.0 Planning and Installation Guide*.

To run the Identification Server and Entitlements Server installer application, your computer must have a Java Runtime Environment (JRE) version 1.3.1.

Obtaining the software

When your organization orders Identification Server and Entitlements Server, Entrust's Software Distribution department sends an email letter that contains instructions about how to obtain the installer software and the user ID and password you will need. Follow the instructions that explain how to use the user ID and password to gain access to the download page and download the installer executable file for your operating system to a convenient temporary location.

- For a Microsoft Windows operating system, download `IdEntitlementsServer_setupwin32.exe`
- For a Solaris operating system, download `IdEntitlementsServer_setupsolarisSparc.bin`

Installing Identification Server and Entitlements Server

Having downloaded the appropriate installer application for your operating system (refer to "Obtaining the software" on page 40), follow the steps in this section to install Identification Server and Entitlements Server.

Installing on Microsoft Windows

You can choose to install Identification Server and Entitlements Server using either a graphical user interface (GUI) or from the command line.

To install using the GUI

1 Locate and double-click the executable file called `IdEntitlementsServer_setupwin32.exe` in the temporary folder you used when downloading it.

Note: If the installer cannot find a suitable JRE, it displays an error message (refer to "Troubleshooting Identification Server and Entitlements Server" on page 75). Run the installer with the following command-line option to point to a JRE:

```
IdEntitlementsServer_setupwin32.exe -is:javahome <"Path to JRE">
```

The Welcome dialog box appears.

Click **Next**.

2 Read the license agreement for the Identification Server carefully. If you accept the terms, select the appropriate radio button and click **Next**.

The license agreement dialog box for the Entitlements Server appears.

3 Read the license agreement for the Entitlements Server carefully. If you accept the terms, select the appropriate radio button and click **Next** to continue with the installation.

The install location dialog box appears.

If you do not accept the terms of either licence agreement, select the appropriate radio button and click **Cancel** to terminate the installer application.

4 Click **Browse** to install the Identification Server and Entitlements Server in a directory other than the default directory shown in the dialog box, or click **Next** to accept the default location.

The Entrust GetAccess install location dialog box appears.

5 Click **Browse** to select the location of your Entrust GetAccess installation, or click **Next** to accept the location shown in the dialog box.

The default location of an Entrust GetAccess installation is:
`C:\Program Files\Entrust\GetAccess`

The installation details dialog box appears.

6 Read the Identification Server and Entitlements Server installation details.

Click **Next** to proceed with the installation.

7 When the installation is complete, a successful completion dialog box appears.

Click **Finish** to close the installer application.

8 Restart the Entrust GetAccess Infrastructure process.

Refer to the section entitled "Verifying successful installation" on page 47 for information about how to test for a successful installation of the product.

To run a command line installation

1 Open a command prompt window.

2 Change to the directory that contains the Identification Server and Entitlements Server executable file (the installer application), `IdEntitlementsServer_setupwin32.exe`.

This should be the temporary folder you used when downloading the installer.

3 Type `IdEntitlementsServer_setupwin32.exe -console` and press **Enter**.

The installer application opens a new command prompt window and displays information and instructions as the installation progresses.

Note: If the installer cannot find a suitable JRE, it displays an error message (refer to "Troubleshooting Identification Server and Entitlements Server" on page 75). Run the installer with the following command-line option to point to a JRE:

```
IdEntitlementsServer_setupwin32.exe -console -is:javahome
<"Path to JRE">
```

---

4 Follow the instructions in the command prompt window.

5 Restart the Entrust GetAccess Infrastructure process.

Refer to the section entitled "Verifying successful installation" on page 47 for information about how to test for a successful installation of the product.

Installing on Solaris

You can choose to install Identification Server and Entitlements Server using either a graphical user interface (GUI) or from the command line.

To install using the GUI

1. Locate the file called `IdEntitlementsServer_setupsolarisSparc.bin` in the temporary folder you used when downloading it.
2. Use the `chmod` command to change the permissions of the file to make it executable.

   ```
   chmod u+x IdEntitlementsServer_setupsolarisSparc.bin
   ```

3. Run the executable file.

Note: If the installer cannot find a suitable JRE, it displays an error message (refer to "Troubleshooting Identification Server and Entitlements Server" on page 75). Run the installer with the following command-line option to point to a JRE:

```
IdEntitlementsServer_setupsolarisSparc.bin -is:javahome
<"Path to JRE">
```

The Welcome dialog box appears.

Click **Next**.

4. Read the license agreement for the Identification Server carefully. If you accept the terms, select the appropriate radio button and click **Next**.

   The license agreement dialog box for the Entitlements Server appears.

5. Read the license agreement for the Entitlements Server carefully. If you accept the terms, select the appropriate radio button and click **Next** to continue with the installation.

   The install location dialog box appears.

   If you do not accept the terms of the either licence agreement, select the appropriate radio button and click **Cancel** to terminate the installer application.

6. Click **Browse** to install the Identification Server and Entitlements Server in a directory other than the default directory shown in the dialog box, or click **Next** to accept the default location.

   If you install Identification Server and Entitlements Server in a directory other than the default, make sure the directory name does not contain a space.

   The Entrust GetAccess install location dialog box appears.

7. Click **Browse** to select the location of your Entrust GetAccess installation, or click **Next** to accept the location shown in the dialog box.

The default location of an Entrust GetAccess installation is: `/opt/Entrust/GetAccess`

The installation details dialog box appears.

8. Read the Identification Server and Entitlements Server installation details.

   Click **Next** to proceed with the installation.

9. When the installation is complete, a successful completion dialog box appears.

   Click **Finish** to close the installer application.

10. Restart the Entrust GetAccess Infrastructure process.

    Refer to the section entitled "Verifying successful installation" on page 47 for information about how to test for a successful installation of the product.

To run a command line installation

1. Change to the directory that contains the Identification Server and Entitlements Server installer, `IdEntitlementsServer_setupsolarisSparc.bin`

   This should be the temporary folder you used when downloading the installer.

   Use the `chmod` command to change the permissions of the file to make it executable.

   ```
   chmod u+x IdEntitlementsServer_setupsolarisSparc.bin
   ```

2. Type `IdEntitlementsServer_setupsolarisSparc.bin -console` and press **Enter**.

Note: If the installer cannot find a suitable JRE, it displays an error message (refer to "Troubleshooting Identification Server and Entitlements Server" on page 75). Run the installer with the following command-line option to point to a JRE:

```
IdEntitlementsServer_setupsolarisSparc.bin -console
-is:javahome <"Path to JRE">
```

---

3. Follow the installer application's instructions to complete the installation.
4. Restart the Entrust GetAccess Infrastructure process.

   Refer to the section entitled "Verifying successful installation" on page 47 for information about how to test for a successful installation of the product.

Chapter 5

Performing post-installation tasks

This chapter provides information about performing post-installation tasks that configure Entrust Identification Server and Entrust Entitlements Server and ensure that they are working correctly.

Topics in this chapter:

Overview

Once you have installed Identification Server and Entitlements Server, run the sample application described in "Verifying successful installation" on page 47 to ensure that your installation was successful. Perform any post-installation configuration tasks necessary to secure your resources.

Consider the following:

- Review the Identification Server and Entitlements Server configuration file settings — refer to "Editing the configuration file" on page 49
- Configure client-authenticated and server-authenticated SSL communications — refer to "Configuring SSL" on page 61
- Review the default settings for method authorization to control access to Identification Server and Entitlements Server interfaces — refer to "Configuring client authorization" on page 68

Verifying successful installation

To verify successful installation of Identification Server and Entitlements Server, run the sample application called `IesClientTest`. The sample application communicates with Entrust GetAccess from a basic Java client through the Identification Server and Entitlements Server Web services interface.

Using the `IesClientTest` command line interface, you can log in users to Entrust GetAccess and determine whether a user has access privileges to a specified resource.

Running the sample application

The sample application is in the `IdEntitlementsServer\sdk\samples` directory. The directory contains a text file (`readme.txt`) with instructions for building and running the sample. You can use the compiled class file, `IesClientTest.class`, to run the sample, or you can compile the Java source code, `IesClientTest.java`, yourself.

To run IesClientTest

1. Read the sample's documentation, `readme.txt`, and note the prerequisites for running the sample.
2. At a command line prompt, type `run.bat` or `run.sh` with the options (such as `-login` and `-getroles`) you want to test.

   The following output is the result of running the sample to login an Entrust GetAccess user (called `wasuserreg`) and to retrieve the user's roles:

```
C:\Program Files\Entrust\IdEntitlementsServer\sdk\samples>
run http://<hostname>:50002 -login wasuserreg wasasr01 -getroles

*****************************************************
*  Welcome to the Entrust Identification Server and  *
*  Entrust Entitlements Server sample client.  Run   *
*  the client with no arguments to display usage.    *
*****************************************************

C:\Program
Files\Entrust\IdEntitlementsServer\sdk\samples>"C:\Program
Files\Entrust\GetAccess\jre1.3\bin\java" -classpath
.;..\lib\entIEClient.jar;..\lib\entsaml.jar;..\lib\xerces.jar;
..\lib\axis.jar;..\lib\saaj.jar;..\lib\jaxrpc.jar;..\lib\commons-l
ogging.jar;..\lib\commons-discovery.jar
-Djava.protocol.handler.pkgs=com.sun.net.ssl.internal.www.protocol
IesClientTest http://<hostname>:50002 -login wasuserreg wasasr01
-getroles
```

```
SID: SMS_<hostname>_713ff7::ca3cb1a4fda9341d6a690782052e7b66

Roles [count=3]:
    excacc.dauthr
    excacc.spradm
    websphere.administrator
```

The sample documentation contains complete instructions and more examples.

Editing the configuration file

You can use configuration settings to customize the environment of your Identification Server and Entitlements Server installation — to set error logging levels and to determine whether users need to be authorized before they use Identification Server and Entitlements Server interfaces.

Configuration file

The `entrust-configuration.xml` file contains configuration settings for the Identification Server and Entitlements Server. Each installation of Identification Server and Entitlements Server has its own configuration file.

The default location of the configuration file is:

- On Windows — `C:\Program Files\entrust\IdEntitlementsServer\config\entrust-configuration.xml`
- On Solaris —`/opt/entrust/IdEntitlementsServer/config/entrust-configuration.xml`

The configuration file is a well-formed XML document. Make a backup of `entrust-configuration.xml` before you start, and use a text editor to edit the file. Note that you should not use non-ASCII characters in the configuration file.

To allow your configuration changes to take effect, save the file and restart the Entrust GetAccess Infrastructure process.

Configuration settings

The following sample shows the available configuration settings highlighted in bold. The settings are explained in Table 3 on page 51.

```
<entrust-configuration>
  <global>
    <iesLogging>
      <logFile>
        C:/Program Files/entrust/IdEntitlementsServer/logs/ies.log
      </logFile>

      <!-- The possible values for the log level:
        TRACE
        DEBUG
        INFO
        WARNING
        ERROR
        ALERT
        FATAL
      -->
      <logLevel>INFO</logLevel>
```

```
  </iesLogging>

  <iesGaServerListCacheUpdateInterval>300</iesGaServerListCacheUpdateInterval>
</global>

<services>
  <CredentialCollector>
    <global>
      <iesAssertionIssuer>Entrust Credential Collector</iesAssertionIssuer>

      <iesMethodAuthorization>
        <loginPasswordUser>false</loginPasswordUser>
        <loginDnUser>true</loginDnUser>
      </iesMethodAuthorization>
    </global>
  </CredentialCollector>

  <AuthenticationAuthority>
    <global>
      <iesAssertionIssuer>
        Entrust Authentication Authority
      </iesAssertionIssuer>

      <iesMethodAuthorization>
        <getUserId>false</getUserId>
      </iesMethodAuthorization>
    </global>
  </AuthenticationAuthority>

  <AttributeAuthority>
    <global>
      <iesAssertionIssuer>Entrust Attribute Authority</iesAssertionIssuer>

      <iesMethodAuthorization>
        <getRoles>false</getRoles>
        <getStaticRoles>false</getStaticRoles>
      </iesMethodAuthorization>
    </global>
  </AttributeAuthority>

  <AuthorizationAuthority>
    <global>
      <iesAssertionIssuer>Entrust Authorization Authority</iesAssertionIssuer>

      <iesMethodAuthorization>
        <isEntitled>false</isEntitled>
      </iesMethodAuthorization>
    </global>
  </AuthorizationAuthority>
```

```
  </services>
</entrust-configuration>
```

Table 3: Configuration settings

Configuration setting	Description

`<iesLogging>`
 	
`<logFile>`
`<logLevel>`
	The contents of the two child elements of `<iesLogging>` specify the location of the Identification Server and Entitlements Server log file and the logging level. Refer to the section called "Error logging" on page 80 for information about error logging.
	
	`<logFile>` — specifies the path to the error log file.The default location of the log file is:
	
	On Windows — `C:\Program Files\Entrust\IdEntitlementsServer\logs\ies.log`
	
	On Solaris — `/opt/entrust/IdEntitlementsServer/logs/ies.log`
	
	`<logLevel>` — contains the error logging level.
	
	Default setting: `INFO`.

`<iesGaServerListCacheUpdateInterval>`	The interval at which Entitlements Server checks for changes to the cached list of Entrust GetAccess servers. For example, if a Web server with an Entrust GetAccess Runtime is added to, or removed from, Entrust GetAccess, the change can take up to 300 seconds (5 minutes) to be registered by the Identification Server and Entitlements Server. The Entitlements Server uses the cached list when processing an entitlements request. Default setting: 300 seconds.

Table 3: Configuration settings

Configuration setting	Description

`<CredentialCollector>`
 	
`<iesAssertionIssuer>`
 	
`<iesMethodAuthorization>`
`<loginPasswordUser>`
`<loginDnUser>`
	The `<CredentialCollector>` element contains child elements that specify the issuer name placed in SAML assertions, and whether or not method authorization is turned on for Credential Collector methods.
	
	`<iesAssertionIssuer>` — specifies the issuer name placed in SAML assertions. To identify the issuer uniquely, set this name to `servername:port`.
	
	Default setting: `Entrust Credential Collector`
	
	`<loginPasswordUser>` — set to `true` or `false` to determine whether users of the `loginPasswordUser` interface require client authorization
	
	Default setting: `false`
	
	`<loginDnUser>` — set to `true` or `false` to determine whether users of the `loginDnUser` interface require client authorization
	
	Default setting: `true`
	
	Refer to "Configuring client authorization" on page 68 for information about client authorization.

Table 3: Configuration settings

Configuration setting	Description

`<AuthenticationAuthority>`
 	
`<iesAssertionIssuer>`
 	
`<iesMethodAuthorization>`
`<getUserId>`
	The `<AuthenticationAuthority>` element contains child elements that specify the issuer name placed in SAML assertions, and whether or not method authorization is turned on for AuthenticationAuthority methods.
	
	`<iesAssertionIssuer>` — specifies the issuer name placed in SAML assertions. To identify the issuer uniquely, set this name to `servername:port`.
	
	Default setting: `Entrust Authentication Authority`
	
	`<getUserId>` — set to `true` or `false` to determine whether users of the `getUserId` interface require client authorization
	
	Default setting: `false`
	
	Refer to "Configuring client authorization" on page 68 for information about client authorization.

Table 3: Configuration settings

Configuration setting	Description

`<AttributeAuthority>`
 	
`<iesAssertionIssuer>`
 	
`<iesMethodAuthorization>`
`<getRoles>`
`<getStaticRoles>`
	The `<AttributeAuthority>` element contains child elements that specify the issuer name placed in SAML assertions, and whether or not method authorization is turned on for Attribute Authority methods.
	
	`<iesAssertionIssuer>` — specifies the issuer name placed in SAML assertions. To identify the issuer uniquely, set this name to `servername:port`.
	
	Default setting: `Entrust Attribute Authority`
	
	`<getRoles>` — set to `true` or `false` to determine whether users of the `getRoles` interface require client authorization
	
	Default setting: `false`
	
	`<getStaticRoles>` — set to `true` or `false` to determine whether users of the `getStaticRoles` interface require client authorization
	
	Default setting: `false`
	
	Refer to "Configuring client authorization" on page 68 for information about client authorization.

`<AuthorizationAuthority>`
 	
`<iesAssertionIssuer>`
 	
`<iesMethodAuthorization>`
`<isEntitled>>`
	The `<AuthorizationAuthority>` element contains child elements that specify the issuer name placed in SAML assertions, and whether or not method authorization is turned on for Authorization Authority methods.
	
	`<iesAssertionIssuer>` — specifies the issuer name placed in SAML assertions. To identify the issuer uniquely, set this name to `servername:port`.
	
	Default setting: `Entrust Authorization Authority`
	
	`<isEntitled>` — set to `true` or `false` to determine whether users of the `isEntitled` interface require client authorization
	
	Default setting: `false`
	
	Refer to "Configuring client authorization" on page 68 for information about client authorization.

Installing the Entrust GetAccess Certificate PAAM

Follow the instructions in this section to install and configure the Entrust GetAccess Certificate PAAM if:

- Your custom applications use the `loginDnUser` interface of Entitlements Server through the SDK or through the Web services interface.
- You turn on method authorization for any of the Identification Server and Entitlements Server methods (in the `entrust-configuration.xml` file).

For information about using method authorization, refer to the section called "Configuring client authorization" on page 68.

To install and configure the Certificate PAAM

Follow the instructions for installing and configuring the Certificate PAAM in the chapter called "Configuring PAAM user identification" in the *Entrust GetAccess 7.0 System Administration Guide*.

To set the Distinguished Name for a user

Follow the instructions to select the Certificate PAAM authentication method in the section called "Modifying user authentication methods" in the "Working with users" chapter of the *Entrust GetAccess 7.0 Business Administration Guide*.

Note: You must set the DN for all users logging in using `loginDnUser`, and for all client applications that require access to protected methods in Identification Server and Entitlements Server.

Chapter 6

Configuring Identification Server and Entitlements Server communications

This chapter provides information about communicating with Entrust GetAccess, configuring Secure Sockets Layer (SSL) connections, and client authorization.

Topics in this chapter:

Configuring an Entrust GetAccess Runtime

This section describes how to configure an Entrust GetAccess Runtime to forward requests from client applications to the Identification Server and Entitlements Server. These configuration steps are necessary only if you are communicating with the Identification Server and Entitlements Server by way of a Web server.

The Entrust GetAccess Runtime must have been installed on the Web server as an Access Service (by selecting the Access Portal checkbox during installation). Refer to the *Entrust GetAccess 7.0 Planning and Installation Guide* for information about installing Entrust GetAccess Runtime software.

You can use the Entrust GetAccess Configuration Console to make the necessary additions to the Entrust GetAccess configuration file, or you can open the file, `configuration.global.xml`, in a text editor and make the changes manually. Refer to the *Entrust GetAccess 7.0 System Administration Guide* for information about working with configuration settings and for instructions for using the Configuration Console.

To edit the configuration file using the Entrust GetAccess Configuration Console

1. Start the Configuration Console
2. In the configuration tree, expand the `<services><RUNTIME><instance name=yourServerID><gaForwardedURLMappings>` node.
3. Right click **`gaForwardedURLMappings`** and from the drop-down menu, select **Add New Simple Setting**.

   The **Add New Simple Setting** dialog box appears.
4. In the left pane select **`gaForwardedURLMapping`** and click **OK**.

   The setting name dialog box opens.
5. Type the value `/ies` in the setting name dialog box and click **OK**.
6. In the configuration tree, right-click **`gaUnprotectedURLPrefixes`** and from the drop-down menu, select **Add New Simple Setting**.

   The **Add New Simple Setting** dialog box appears.
7. In the left pane select **`gaPrefix`** and click **OK**.

   The setting name dialog box opens.
8. Type the value `/ies` in the setting name dialog box and click **OK**.
9. From the **File** menu, select **Save** to write your changes to the `configuration.global.xml` file.
10. Restart your Web server.

If you are using the Sun ONE Web server, stop and start the Web server.

If you are using Microsoft Internet Information Services (IIS), perform the following steps:

- Run the command, `net stop iisadmin /y` to stop the server.

  Wait for approximately 20 seconds before restarting the server to allow the IIS service to terminate properly after the `net stop` command completes.
- Run the command, `net start w3svc` to restart the server.

11 Update the server configuration in the Entrust GetAccess Administration Console.

Refer to the *Entrust GetAccess 7.0 Business Administration Guide* for details.

To edit the configuration file manually

1 Locate and open `configuration.global.xml` in a text editor.

The default location of this file is:

`C:\Program Files\Entrust\GetAccess\config\configuration.global.xml`, on a Windows operating system or

`/opt/Entrust/GetAccess/config/configuration.global.xml`, on a Solaris operating system.

2 Add the <gaForwardedURLMapping> and <gaPrefix> elements and their contents to your runtime as shown in bold text in the following XML fragment.

```
<ent-configuration>
  <global>
    ...
    <gaAccessServiceLocations>
      <gaAccessService>
        hostname.entrust.com:hostname.entrust.com:50000
      </gaAccessService>
    </gaAccessServiceLocations>
  </global>
  <services>
    ...
    <RUNTIME>
      <global>
        ...
      </global>
      <instance name="main-https-jsmith.entrust.com">
        ...
      </instance>
      <instance name="wottdmortime80uyiivf">
        <gaRuntimeInstanceType>VirtualServer</gaRuntimeInstanceType>
        <gaAccessServiceConnector>true</gaAccessServiceConnector>

        <gaForwardedURLMappings>
```

```
          <gaForwardedURLMapping>/GetAccess/servlet</gaForwardedURLMapping>
          <gaForwardedURLMapping>/auth/login#/auth/Login</gaForwardedURLMapping>
          <gaForwardedURLMapping>/auth/Login</gaForwardedURLMapping>
          <gaForwardedURLMapping>/GetAccess/images</gaForwardedURLMapping>
          ...
          <gaForwardedURLMapping>/ies</gaForwardedURLMapping>
        </gaForwardedURLMappings>

        <gaUnprotectedURLPrefixes>
          <gaPrefix>/GetAccess/servlet/Login</gaPrefix>
          <gaPrefix>/auth/login</gaPrefix>
          <gaPrefix>/auth/Login</gaPrefix>
          <gaPrefix>/GetAccess/images</gaPrefix>
          ...
          <gaPrefix>/ies</gaPrefix>
        </gaUnprotectedURLPrefixes>
      </instance>
    </RUNTIME>
    ...
  </services>
</ent-configuration>
```

3. Restart your Web server.

   If you are using the Sun ONE Web server, stop and start the Web server.

   If you are using Microsoft Internet Information Services (IIS), perform the following steps:

   - Run the command, `net stop iisadmin /y` to stop the server.

     Wait for approximately 20 seconds before restarting the server to allow the IIS service to terminate properly after the `net stop` command completes.
   - Run the command, `net start w3svc` to restart the server.

4. Update the server configuration in the Entrust GetAccess Administration Console.

   Refer to the *Entrust GetAccess 7.0 Business Administration Guide* for details.

Configuring SSL

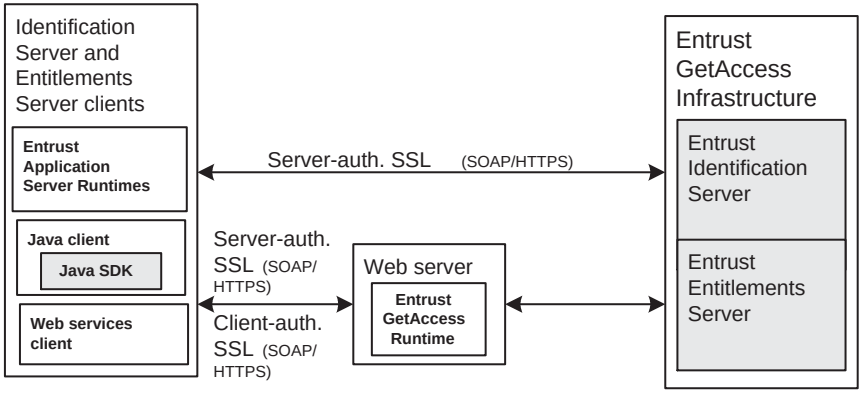
This section describes how to set up server-authenticated SSL and client-authenticated SSL communication with Identification Server and Entitlements Server.

Server-authenticated SSL

There are two server-authenticated SSL configurations that you can configure between Identification Server and Entitlements Server and their clients corresponding to the following two communications paths:

- Direct HTTPS communications between Identification Server and Entitlements Server clients and the Entrust GetAccess Infrastructure (by default, port 50002)
- HTTPS communications between Identification Server and Entitlements Server clients and a Web server running an Entrust GetAccess Runtime serving Entrust GetAccess Infrastructure URLs

Figure 3: Entrust Identification Server and Entrust Entitlements Server SSL configurations



Server-authenticated SSL between clients and Entrust GetAccess Infrastructure

The first of these SSL configurations requires that you turn on SSL on the Entrust GetAccess Infrastructure by enabling the <gaServicesSSL> configuration setting (refer to the "Enhancing security" chapter of the *Entrust GetAccess 7.0 System Administration Guide* for more information). Once you have enabled Entrust GetAccess services SSL, the URLs to which Identification Server and Entitlements Server clients make requests must change from HTTP to HTTPS. For example,

```
https://hostname.entrust.com:50002/ies/CredentialCollector
```

Server-authenticated SSL between clients and a Web server

This configuration is independent of the Entrust GetAccess <gaServicesSSL> setting and sets up server-authenticated SSL communication between Identification Server and Entitlements Server clients and a Web server. Server-authenticated SSL must be enabled between the client and the Web server for client-authenticated SSL to work. The Web server must be running an Entrust GetAccess Runtime, not for security reasons, but to forward requests to the Identification Server and Entitlements Server on the Entrust GetAccess Infrastructure (refer to "Configuring an Entrust GetAccess Runtime" on page 58).

You do not have to use the same Web server that hosts other Entrust GetAccess Infrastructure applications, allowing you to control SSL independently for the Identification Server and Entitlements Server. Once you have enabled SSL, the URLs your clients request become HTTPS. For example,

```
https://hostname.entrust.com/ies/...
```

Client-authenticated SSL

You can use client-authenticated SSL to authenticate clients requesting access to Identification Server and Entitlements Server URLs. Such requests must be made to a front-end Web server running an Entrust GetAccess Runtime (to forward requests to the Identification Server and Entitlements Server on the Entrust GetAccess Infrastructure).

You cannot use client-authenticated SSL on direct communication paths between Identification Server and Entitlements Server clients and the Entrust GetAccess Infrastructure.

The Web server uses its built-in client-authenticated SSL capabilities and you must configure it to request a client certificate either for all URLs or for specific URLs, and to trust the Certification Authority (CA) that issues the client certificate.

Configuring clients to use SSL

This subsection contains high-level procedures that describe how to configure your custom Java client applications to use SSL. Figure 3 on page 61 shows the possible configurations. The client SDK uses Sun's Java Secure Sockets Extension (JSSE) to support SSL, and Java key store for client key and certificate storage.

Where appropriate, the procedures mention Entrust and third-party tools and applications. The following references point to relevant documentation:

- For information about using the Sun ONE Web Server, refer to its online documentation at http://docs.sun.com/source/816-5691-10/index.html. (You can find information about SSL in Chapter 5, "Securing your Web server".)
- For information about using Microsoft IIS, refer to the IIS help documentation, http://localhost/iisHelp.
- For information about using the Java Key and Certificate Management Tool, keytool, refer to http://java.sun.com/j2se/1.3/docs/tooldocs/win32/keytool.html or http://java.sun.com/j2se/1.3/docs/tooldocs/solaris/keytool.html

To prepare the Java client SDK to use SSL

1 Download and unpack Sun Microsystems' JSSE distribution.

Version 1.0.3_01 of the JSSE is available at http://java.sun.com/products/jsse/index-103.html.

Note: The Java client SDK requires JRE version 1.3.x

2 Follow the JSSE installation instructions in `INSTALL.txt`.

Consider the most straightforward option of setting up the JSSE as an installed extension by copying the jar files from the distribution's `lib` directory to your `<JAVA_HOME>\lib\ext` directory, and adding the SunJSSE Provider to your Java security properties file (static registration).

To set up server-authenticated SSL between the Java client SDK and a Web server

1 Import the CA certificate into a client key store using Java keytool.

For example:

```
>keytool -import -alias <keystore alias> -file <CA cert file name>
-keystore <keystore name> -storepass <keystorepassword>

Owner: OU=Entrust PKI Demonstration Certificates, O=Entrust, C=US
Issuer: OU=Entrust PKI Demonstration Certificates, O=Entrust, C=US
Serial number: 3b992f45
Valid from: Fri Sep 07 16:04:13 EDT 2001 until: Tue Sep 07
16:34:13 EDT 2021
Certificate fingerprints:
         MD5:  7D:29:12:AE:43:68:0D:17:03:3A:05:53:1A:5A:6F:03
         SHA1:
13:38:0A:7A:0E:65:56:07:D2:33:1B:37:82:36:B5:48:68:F3:0F:EC
Trust this certificate? [no]:  yes
```

```
Certificate was added to keystore
```

The CA certificate you import must belong to the CA that issued the Web server certificate.

If you are using an Entrust PKI, you can use an administration tool, such as Entrust Authority™ Security Manager Administration Feature (formerly Entrust/RA) or Entrust/WebConnector™, to obtain the CA certificate in a binary format.

2 Set the following system properties in the client environment.

```
-Djava.protocol.handler.pkgs=com.sun.net.ssl.internal.www.protocol
-Djavax.net.ssl.trustStore=c:/your_location/your_keystore.jks
```

Your client application can now use the HTTPS protocol (`https:// ...`) to communicate with Identification Server and Entitlements Server.

To set up client-authenticated SSL between the Java client SDK and a Web server

1 Complete the procedure called "To set up server-authenticated SSL between the Java client SDK and a Web server" on page 63.

2 Add or install the CA certificate as a trusted CA at your Web server.

The CA certificate must belong to the CA that will issue the client certificate.

Note: If you are using an Entrust PKI, add a user before moving to the next step. This will give you the reference number to use in the client name.

---

3 Create a key pair at the client using Java keytool.

If you are using an Entrust PKI, use the reference number you obtained when you added the user as the common name.

For example:

```
>keytool -genkey -keyalg RSA -keysize 1024 -keystore <keystore
name> -storepass <keystore password>

What is your first and last name?
  [Unknown]:  34271903
What is the name of your organizational unit?
  [Unknown]:
What is the name of your organization?
  [Unknown]:
What is the name of your City or Locality?
  [Unknown]:
What is the name of your State or Province?
  [Unknown]:
What is the two-letter country code for this unit?
```

```
  [Unknown]:
Is <CN=34271903, OU=Unknown, O=Unknown, L=Unknown, ST=Unknown,
C=Unknown> correct?
  [no]:  yes

Enter key password for <mykey>
        (RETURN if same as keystore password):
```

4 Generate a certificate request using Java keytool.

```
>keytool -certreq -keystore <keystore name> -storepass <keystore
password>

-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBrTCCARYCAQAwbTEQMA4GA1UEBhMHVW5rbm93bjEQMA4GA1UECBMHVW5rbm93bj
EQMA4GA1UEBxMHVW5rbm93bjEQMA4GA1UEChMHVW5rbm93bjEQMA4GA1UECxMHVW5r
bm93bjERMA8GA1UEAxMIMzQyNzE5MDMwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAo
GBALIOqFm6jxZxtXkoh3phzLlhtmCjF99aKryMLSq2uEXO8tGp8vhJpAOEFgyXf502
fSZEtAgSqb0Ngj3nikJdZmV6A7rQrlxfRp68ChHdmv+ApESxJNQ6BMrFFLrF2YNQ6q
MxGg8NAuyeAal5oe+gir4sibLCMB16xvcpr9JsjCRtAgMBAAGgADANBgkqhkiG9w0B
AQQFAAOBgQAhKdHqAtmfUe6cozi8T/Extxp04gUATL6w/sf/lcevMNU//uJaA3SRYH
XJ+zJUd+4zE26+5uXEnQzoEZQBUJj5vMJiaL4SDHYN7sTjan7VJ8SRyNKl8q10Ilw5
AhF7EPLzT3U9cMIsZm84KQteNbWO/hLn5XVKiocAv34vlPQwCg==
-----END NEW CERTIFICATE REQUEST-----
```

5 Submit the certificate request to a CA.

6 Import the CA certificate into the client's local keystore if it is not already present.

For example:

```
>keytool -import -file <CA cert file name>  –alias <keystore
alias> -keystore <keystore name> -storepass <keystore password>

Owner: O=Entrust, C=CA
Issuer: O=Entrust, C=CA
Serial number: 3da5b175
Valid from: Thu Oct 10 12:27:25 EDT 2002 until: Mon Oct 10
12:57:25 EDT 2022
Certificate fingerprints:
         MD5:  96:05:E7:DB:DB:7B:C6:0F:34:20:21:10:AE:EA:D0:C0
         SHA1:
DB:F5:98:C7:59:0B:5A:5A:BA:3F:AF:D8:12:E4:AB:76:8D:7C:E9:4F
Trust this certificate? [no]:  yes
Certificate was added to keystore
```

7 Import the new client certificate into the client's local key store.

For example:

```
>keytool -import -file <client cert file name> -keystore <keystore
name> -storepass <keystore password>
```

```
Certificate reply was installed in keystore
```

8 Set the following system properties in the client environment.

```
-Djavax.net.ssl.keyStore=your_keystore.jks
-Djavax.net.ssl.keyStorePassword=your_password
```

Note: The global system property `javax.net.ssl.keyStore` specifies the keystore. This ensures that all applications running in the JVM use the same keystore. If there is more than one client certificate in the keystore, the JSSE implementation selects an appropriate certificate to use when the session is established. There is no way to override this selection in the Java SDK, so Entrust recommends that you use a keystore with only one client certificate.

The client application and Web server should now be able to communicate securely using client-authenticated SSL.

To set up server-authenticated SSL between the Java client SDK and the Entrust GetAccess Infrastructure

1 Turn on (or confirm that it is turned on) the `gaServicesSSL` configuration setting in the Entrust GetAccess Infrastructure (refer to the "Enhancing security" chapter of the *Entrust GetAccess 7.0 System Administration Guide* for more information).

Locate and run the script file called `ConfigureSSL` in the `bin` directory of your Entrust GetAccess installation.

The default location of the script file is `C:\Program Files\Entrust\GetAccess\bin\ConfigSSL.bat` on Windows operating systems, and `/opt/Entrust/GetAccess/bin/ConfigSSL.sh` on Solaris operating systems.

```
*************************************************************
                          Entrust Inc.
                      Entrust GetAccess
*************************************************************

Runtime SSL is off. Services SSL is off.
a) Enable Runtime SSL
b) Enable Services SSL
x) Exit
Enter Selection:  b

Runtime SSL is off. Services SSL is on.
a) Enable Runtime SSL
b) Disable Services SSL
```

```
x) Exit
Enter Selection:
```

2 Import the Entrust GetAccess self-signed certificate, `gaCA.der`, located in the `config` directory of your Entrust GetAccess installation into the client's trust store.

The default location of the self-signed certificate is `C:\Program Files\Entrust\GetAccess\config\gaCA.der` on Windows operating systems, and `/opt/Entrust/GetAccess/config/gaCA.der` on Solaris operating systems.

All direct communications with Identification Server and Entitlements Server on the Entrust GetAccess Infrastructure (including those originating with Entrust Application Server Runtimes and client applications using the SDK) can now use the HTTPS protocol. For example `https://hostname.entrust.com:50002/ies/CredentialCollector`.

Configuring client authorization

Client communications with Identification Server and Entitlements Server use the Identification Server and Entitlements Server interfaces. You can control access to these interfaces, or methods, by defining them as protected resources in Entrust GetAccess. Users will then have to be authorized before they can use the protected methods — this is client, or method, authorization.

Note: Client authorization is optional, but desirable, and in the case of the `loginDnUser` method, strongly recommended. Without client authorization, anyone using the `loginDnUser` method can retrieve an Entrust GetAccess session ID if they know a user's name.

Configuring method authorization

You can configure client authorization individually for the methods listed in Table 2 on page 17 by enabling method authorization in the configuration file, `entrust-configuration.xml`. Refer to the section called "Editing the configuration file" on page 49 for information about how to edit configuration settings that enable method authorization. The configuration setting that controls whether client authorization is required for the `loginDnUser` method is set to `true` by default — the default setting for each of the other methods is `false`.

To turn on method authorization

1. Install the Entrust GetAccess Certificate PAAM.

   Refer to the section called "Installing the Entrust GetAccess Certificate PAAM" on page 55.

2. Perform the steps (or similar steps for non-Java clients — Web services, for example) described in the procedure called "To set up client-authenticated SSL between the Java client SDK and a Web server" on page 64.

   Refer to the *Entrust Application Server Runtimes 7.0 Administration Guide* for information about configuring SSL communications between the Application Server Runtimes and the Identification Server and Entitlements Server.

3. Turn on method authorization in the configuration file.

   Refer to the section called "Editing the configuration file" on page 49 for information about how to edit configuration settings that enable method authorization.

4. For each method you protect:

- Define it as a resource in Entrust GetAccess using the values in the following table:

Field	Value	Example
Resource ID	Arbitrary	loginDnUser
Resource Name	Arbitrary	IES login by DN
Description	Arbitrary	Method that takes a DN and returns a session ID
Web Server	Specify the Web server where client-authenticated SSL is enabled	`hostname.entrust.com`

Relative URL	`/ies/method`
	where `method` is one of:
	`loginPasswordUser`
	`loginDnUser`
	`getUserId`
	`getRoles`
	`getStaticRoles`
	`isEntitled`
		`/ies/loginDnUser`

- Define appropriate roles to represent Identification Server and Entitlements Server clients. For example:

  Role ID — IESClient

  Role Name — IES client
- Assign these roles to the protected method and to the users representing Identification Server and Entitlements Server clients who will require access to them

The *Entrust GetAccess 7.0 Business Administration Guide* contains procedures for defining resources and assigning them to roles and users.

5 Issue a client certificate to each user allowed access to a protected Identification Server and Entitlements Server method, and assign the DN from the client certificate to the corresponding Entrust GetAccess user.

Once you have completed this procedure and turned on method authorization, only those users who are associated with the appropriate roles, and who use client-authenticated SSL can gain access to protected methods.

Chapter 7

Uninstalling Identification Server and Entitlements Server

This chapter describes how to remove Identification Server and Entitlements Server from your computer.

Topics in this chapter:

Uninstalling on Windows

The following procedure describes the steps you should take to remove Identification Server and Entitlements Server from your computer.

To uninstall on Windows

1. From the **Start** menu, click **Settings** > **Control Panel** and open **Add or Remove Programs**.
2. In the left pane, click **Add or Remove Programs** and select **Entrust Identification Server 7.0 and Entrust Entitlements Server 7.0**.
3. Click **Change/Remove** and follow the instructions in each dialog box.
4. Click **Finish** when the last dialog box displays a message saying that the uninstaller application has successfully uninstalled Entrust Identification Server and Entrust Entitlements Server.
5. Stop your Entrust GetAccess Infrastructure process.
6. Delete the following directories
   - The `ies` directory under the Entrust GetAccess installation, `<GA_root>\infrastructure\instance1\webapps\ies`

     where `<GA_root>` is the Entrust GetAccess installation directory, usually `C:\Program Files\Entrust\GetAccess.`
   - `The IdEntitlementsServer` directory, usually `C:\Program Files\Entrust\IdEntitlementsServer`
7. Restart your Entrust GetAccess Infrastructure process.

Note: You can invoke the uninstaller application from the command line with the following command:

```
<path to uninstaller executable file>\uninstaller.exe -console
```

Uninstalling on Solaris

The following procedure describes the steps you should take to remove Identification Server and Entitlements Server from your computer.

To uninstall on Solaris

1. Change to the directory that contains the Identification Server and Entitlements Server uninstaller executable file.

   The default location of the uninstaller is `/opt/entrust/IdEntitlementsServer/_uninst/uninstaller.bin`
2. Run the application.
3. Follow the instructions in each dialog box.
4. Click **Finish** when the last dialog box displays a message saying that the uninstaller application has successfully uninstalled Entrust Identification Server and Entrust Entitlements Server.
5. Stop your Entrust GetAccess Infrastructure process.
6. Delete the following directories
   - The `ies` directory under the Entrust GetAccess installation, `<GA_root>/infrastructure/instance1/webapps/ies`

     where `<GA_root>` is the Entrust GetAccess installation directory, usually `/opt/Entrust/GetAccess.`
   - The `IdEntitlementsServer` directory, usually `/opt/entrust/IdEntitlementsServer`
7. Restart your Entrust GetAccess Infrastructure process.

Note: You can invoke the uninstaller application from the command line with the following command:
`<path to uninstaller executable file>/uninstaller.bin -console`

Chapter 8

Troubleshooting Identification Server and Entitlements Server

This chapter provides information and tips about troubleshooting problems you might encounter installing and using Entrust Identification Server and Entrust Entitlements Server.

Topics in this chapter:

Overview

This chapter provides information to help you solve problems you might encounter when you install and run Identification Server and Entitlements Server. The chapter includes sections with installation-related and SSL-related troubleshooting advice, a section that describes the Identification Server and Entitlements Server log files (where you should look for error messages), and a section with tables listing error messages, their causes, and possible solutions.

The Identification Server and Entitlements Server run on an Entrust GetAccess Infrastructure. The *Entrust GetAccess 7.0 Troubleshooting Guide* is an additional sources of problem solving information.

If you are unable to solve your problem after reading this chapter, refer to the section called "Getting help" on page 6 for information about how to obtain technical support.

Troubleshooting installation problems

This section contains information about problems related to the installation of Identification Server and Entitlements Server.

Removing remnants of a previous installation

The Entrust Identification Server and Entrust Entitlements Server installer application will not allow you to install more than one instance of the Identification Server and Entitlements Server on the same computer. If the installer displays the message "A previous install of this product has been found on this system. Please select Next to exit the installer and uninstall the previous installation.", when you try to install the software, refer to the chapter called "Performing post-installation tasks" on page 45 for the steps you should take to remove the product.

If the installer continues to display the error message after you have taken these steps, there might be remnants of a previous failed installation or uninstallation on your computer. Follow the steps set out in this section to remove these remnants and to prepare your computer for a fresh installation of the Identification Server and Entitlements Server software.

To recover from a failed installation on Windows

1. In the `%WINDIR%` directory, the default Windows directory (usually, `C:\WINDOWS` or `C:\WINNT`), locate the file called `vpd.properties`.
2. Open the `vpd.properties` file in a text editor, search for, and delete all lines containing the string, `IdEntitlementsServer`
3. Locate and delete the Identification and Entitlements Server installation folder, usually `C:\Program Files\Entrust\IdEntitlementsServer`
4. Refer to the section called "Installing Identification Server and Entitlements Server" on page 41 and follow the instructions to reinstall the Identification Server and Entitlements Server software.

To recover from a failed installation on UNIX — root user

1. Locate the `/var/sadm/pkg` directory.
2. Delete the subdirectory called `ENTUIES7`.
3. Locate and delete the Application Server Runtimes installation directory, usually `/opt/entrust/IdEntitlementsServer`.

4 Refer to the section entitled "Installing Identification Server and Entitlements Server" on page 41 and follow the instructions to reinstall the Identification Server and Entitlements Server software.

To recover from a failed installation on UNIX — non-root user

1 In the user's `$HOME` directory, locate the file called `vpd.properties`.

2 Open the `vpd.properties` file in a text editor, search for, and delete all lines containing the string, `IdEntitlementsServer`.

3 Locate and delete the Application Server Runtimes installation directory, usually `/opt/entrust/IdEntitlementsServer`.

4 Refer to the section entitled "Installing Identification Server and Entitlements Server" on page 41 and follow the instructions to reinstall the Identification Server and Entitlements Server software.

Redirecting temporary installation files

The installer application writes files to a temporary directory. If the temporary directory is full, or if the system's `temp` directory is not defined, you might receive an error message telling you to use the `-is:tempdir` command. In this case run the installer application as follows:

- On Windows

  ```
  IdEntitlementsServer_setupwin32.exe -is:tempdir <"Path to
  temporary directory">
  ```

- On Solaris

  ```
  IdEntitlementsServer_setupsolarisSparc.bin -is:tempdir
  <"Path to temporary directory">
  ```

Troubleshooting SSL communications

This section provides information about possible causes for exceptions you might encounter when configuring SSL communications with Identification Server and Entitlements Server.

Exception messages

The Java exceptions listed in the following table are possible indications of steps you might have missed in setting up SSL communications as described in "Configuring SSL" on page 61.

Table 4: Java exceptions associated with SSL configuration problems

Exception	Description
`java.net.MalformedURLException: unknown protocol: https`	**Cause**: You might not have set `java.protocol handler.pkgs` correctly. **Solution**: Refer to Step 2 of the procedure called "To set up server-authenticated SSL between the Java client SDK and a Web server" on page 63.
`javax.net.ssl.SSLException: untrusted server cert chain`	**Cause**: The client does not trust the CA that issued the server certificate. **Solution**: Make sure you imported the correct CA certificate in Step 1 of the procedure called "To set up server-authenticated SSL between the Java client SDK and a Web server" on page 63 and that you are pointing to the correct trust store in Step 2.
`javax.net.SocketException: SSL implementation not available`	**Cause**: This exception might occur if your keystore or keystore password are set incorrectly. **Solution**: Refer to Step 8 of the procedure called "To set up client-authenticated SSL between the Java client SDK and a Web server" on page 64.

Note: To obtain useful and detailed SSL debugging information, set the system property `java.net.debug` to `ssl:trustmanager`. Refer to the JSSE installation instructions for more information.

Error logging

If you encounter problems with Identification Server and Entitlements Server, check the error log file. Identification and Entitlements Server logs errors in a log file called `ies.log` in the `IdEntitlementsServer\logs` directory.

The `ies.log` file is the current error log, created daily, but you can read older log entries in dated log files. Log files written earlier than the current date have the following name format:

```
ies.log.YYYY-MM-DD
```

You can read the log files with a text editor.

Customizing the log file entries

You can customize the error level that the Identification Server and Entitlements Server write to the log file to meet your requirements for the depth of error logging information you need. The following table lists the error logging levels in order of increasing severity.

Logging level	Description
TRACE	Messages useful for tracing events — `Updating the server-list cache`, for example.
DEBUG	Messages generated by events in the application's code — successful connection information for example. Intended for use by developers.
INFO	Informative messages — `CredentialCollector initialized successfully`, for example.
WARNING	Warnings of recoverable errors.
ERROR	Error messages that are not fatal, — Java exceptions, for example.
ALERT	Messages for the administrator — too many login attempts, for example.
FATAL	Fatal error that have occurred — unrecoverable exceptions, for example.

Note: If you set error logging to a particular level, all logging levels with a severity greater than the level you set are written to the log. For example, the default logging level is INFO, but errors with log levels WARNING, ERROR, ALERT, and FATAL are logged as well.

Set the logging levels by editing the Identification Server and Entitlements Server configuration file, `IdEntitlementsServer\config\entrust-configuration.xml`. Refer to the section called "Editing the configuration file" on page 49 for information about editing the configuration file.

Log file format

The log file contains a header section, followed by a section that contains the log file entries.

Log file header

The top of the log file contains a header that indicates environment parameters such as the operating system and version. The log file header has the following format:

```
Entrust Identification Server and Entrust Entitlements Server
Version: <product version>
Logger version: <logger version>

Operating system: <name and version>
System architecture: <architecture information>
JRE Vendor: <name of JRE vendor>
JRE Version: <JRE version>
JVM Vendor: <name of JVM vendor>
JVM Version: <JVM version>
Classpath in use: <classpath>
User: <username>
```

Log file entries

Log file entries have the following format:

```
[date/time][level][component][classname] message
```

where:

- `date/time` is the local host time in ISO 8601 format: `YYYY-MM-DD HH:MM:SS` (`+HHMM` or `-HHMM` indicates that the local time being used is `HH` hours and `MM` minutes ahead of, or behind, Coordinated Universal Time (UTC), respectively).
- `level` is the logging level for that entry, as specified in the configuration file.

- `component` is the name of the Identification Server and Entitlements Server component that originated the log entry
- `classname` is always blank
- `message` is the log entry description

The following is an example of a typical log file entry:

```
[2003-05-08 10:04:18-0700][INFO ][CredentialCollector][]
CredentialCollector initialized successfully.
```

Error messages

This section describes error messages, their cause, and possible solutions. Identification Server and Entitlements Server displays error messages either in message boxes during the installation and uninstallation processes, or writes them to a log file. Refer to the section called "Error logging" on page 80 for information about the error log file.

Installer error messages

The installer application displays the error messages listed in the following table if it encounters problems during the installation of Identification Server and Entitlements Server.

Table 5: Installer error messages

Error message	Description
A suitable JVM could not be found. Please run the program again using the option -is:javahome <JAVA HOME DIR>	**Cause**: The installer application requires a JRE version between 1.3.0 and 1.4.1. It searches the Windows registry or the `/usr/java` directory on UNIX for the default JRE. If it cannot find a suitable JRE, it displays this error message. **Solution**: Run the installer with the command-line option `-is:javahome` to point to a suitable JRE other than the default.
A previous install of this product has been found on this system. You must uninstall the previous installation before running this installer. Click Next to exit the installer	**Cause**: The installer application does not allow multiple installations of the Application Server Runtimes. **Solution**: Uninstall the previously installed version and reinstall the Application Server Runtime software.
Entrust GetAccess 7.0 is not installed in your system. You must install Entrust GetAccess 7.0 before installing Entrust Identification Server 7.0 and Entrust Entitlements Server 7.0. Select "Next" to exit the installer.	**Cause**: The installer cannot detect an Entrust GetAccess 7.0 installation on your computer. **Solution**: Install Entrust GetAccess 7.0 and run the installer application again. Refer to the section called "Related documents" on page 2 for pointers to the relevant Entrust GetAccess documentation.

Table 5: Installer error messages

Error message	Description
Please type or select a valid GetAccess installation directory.	**Cause**: The installer cannot find the specified Entrust GetAccess installation directory. **Solution**: Type a valid Entrust GetAccess installation directory for the installation to continue.
The GetAccess Infrastructure already contains an exploded Identification Server and Entitlements Server Web application. Be sure to delete the exploded directory before restarting the GetAccess Infrastructure.	**Cause**: The installer has detected a previous installation of the Entrust Identification Server and Entrust Entitlements Server. **Solution**: The Identification Server and Entitlements Server Web archive file, `ies.war`, is copied to the `IdEntitlementsServer\webaps` directory after you restart the Entrust GetAccess Infrastructure. Delete the `ies.war` file and click **OK** on the warning dialog box to continue installing the product.

Identification Server and Entitlements Server error messages

The following table lists error messages that are written to the log file, `ies.log`. Refer to "Error logging" on page 80 for information about error logging.

Table 6: Identification Server and Entitlements Server error messages

Error message	Description
Fatal configuration error detected — {0}	**Cause**: This error occurs when the Identification Server and Entitlements Server encounters an incorrect configuration parameter. **Solution**: Refer to {0} and to the log file for more information about the error.
Servlet failed to start up.	**Cause**: This error occurs when any of the servlets comprising Identification Server and Entitlements Server encounters a problem during startup. **Solution**: Refer to the log file for more information about the error.
Duplicate server name found in GetAccess: {0}. The resources on the duplicate server will not be recognized.	**Cause**: This error occurs when more than one server with the same name are defined in Entrust GetAccess. **Solution**: Identification Server and Entitlements Server do not support duplicate server names (even if their server IDs are different). Ensure you use unique names for the servers you define in Entrust GetAccess.

SDK error messages

The tables in this subsection list the errors that appear in the `ies.log` file when exceptions are thrown by the classes in the client SDK, or by classes that implement the interfaces in the SDK.

Refer to "Error logging" on page 80 for information about error logging.

ServerException error messages

The error messages in the following table can appear when a `ServerException` is thrown. The SAML error messages listed in Table 12 can also appear when `ServerExceptions` are thrown.

Table 7: ServerException error messages

Error message	Description
Invalid user id - {0}	**Cause**: An invalid user ID has been passed to the Identification Server and Entitlements Server client. **Solution**: Ensure that the user ID you are passing is correct and not null or empty.
Invalid password - {0}	**Cause**: An invalid password has been passed to the Identification Server and Entitlements Server client. **Solution**: Ensure that the password you are passing is correct and not null or empty.
Invalid DN - {0}	**Cause**: An invalid DN has been passed to the Identification Server and Entitlements Server client. **Solution**: Ensure that the DN you are passing is correct and not null or empty.
Invalid authentication token - {0}	**Cause**: An invalid authentication token has been passed to the Identification Server and Entitlements Server client. **Solution**: Ensure that the authentication token you are passing is correct and not null or empty.
Invalid resource - {0}	**Cause**: An invalid resource has been passed to the Identification Server and Entitlements Server client. **Solution**: Ensure that the resource you are passing is correct and not null or empty.

Table 7: ServerException error messages

Error message	Description
A client certificate was not sent with the request. Request not authorized to perform the operation: {0}	**Cause**: This error occurs when the request requires the Identification Server and Entitlements Server to perform an operation involving client authorization and a client certificate has not been sent with the request. **Solution**: The operation {0} has been configured to use client authorization. Refer to the section called "Configuring client authorization" on page 68 for more information.
The DN found in the certificate sent with the request does not have the authorization to perform the operation {0}. DN: {1}	**Cause:** This error occurs when the request requires the Identification Server and Entitlements Server to perform an operation involving client authorization and the DN in the client certificate does not have the requisite privileges. **Solution**: Ensure the client certificate you use when connecting to the SAML authority is the correct certificate. Also ensure that the user identified by the DN in the client certificate is properly authorized to access method {0} in Entrust GetAccess. Refer to Step 5 in the procedure called"To turn on method authorization" on page 68.

AuthenticationException error messages

The error messages in the following table can appear when an `AuthenticationException` is thrown.

Table 8: AuthenticationException error messages

Error message	Description
Authentication failed for user {0} - {1}	**Cause**: This error occurs when authentication for user {0} has failed. **Solution**: The reason for the failed authentication is specified in {1}. Values represented by {1} are: `System error`[1] — Entrust GetAccess is not configured correctly. Refer to the Entrust GetAccess log files for more information. `Password based login is not enabled` — the Entrust GetAccess Infrastructure does not allow password-based login. `Incorrect password` — An incorrect password was provided during the login operation. `Password locked` — Entrust GetAccess has locked out the password. `Password inactive` — The password belongs to a user whose Entrust GetAccess account has been revoked. `Password expired` — The password provided during the login operation has expired. `User id has expired` — The user ID provided during the login operation has expired. `User has been locked out` — Entrust GetAccess has locked out the user. `User account has been locked` — Entrust GetAccess has locked out the user.
Authentication error for user {0}	**Cause**: This error occurs when authentication for user {0} has failed. **Solution**: Ensure that you use the correct user name and password during the login operation.

1. If the system error is a `GeneralDaoError` that occurs when multiple client applications are accessing Identification Server and Entitlements Server simultaneously, a possible solution is to increase the value of the `<gaMaxSize>` setting in the Entrust GetAccess configuration file and/or to adjust the Repository tuning parameters. Refer to the *Entrust GetAccess 7.0 System Administration Guide* for information about working with Entrust GetAccess configuration settings.

InvalidTokenException error messages

The error messages in the following table can appear when an `InvalidTokenException` is thrown.

Table 9: InvalidTokenException error messages

Error message	Description
Invalid authentication token	**Cause**: An invalid authentication token has been passed to the Identification Server and Entitlements Server. **Solution**: Ensure that you use the value returned by the server during the login operation.

UnknownUserException error messages

The error messages in the following table can appear when an `UnknownUserException` is thrown.

Table 10: UnknownUserException error messages

Error message	Description
Unknown user - {0}	**Cause**: An unknown user ID has been passed to the Identification Server and Entitlements Server. **Solution**: Ensure that the user ID you are passing is valid.

EntitlementResult error messages

The error messages in the following table can appear when an instance of the `EntitlementResult` class is created to contain the result of calling the `isEntitled` method of `EntitlementInterface` (refer to the Javadoc reference for more detailed information.)

Table 11: EntitlementResult error messages

Error message	Description
Unknown Web Server specified in resource url {0}	**Cause**: An unknown server name was passed in the entitlement request and the requested resource cannot be identified. **Solution**: Ensure that you use a valid server name defined in Entrust GetAccess.
Invalid authentication token	**Cause**: An invalid authentication token has been passed to the Identification Server and Entitlements Server. **Solution**: Ensure that you use the value returned by the server during the login operation.

SAML error messages

The following table lists error messages caused by problems encountered during SAML message exchanges. These error messages also appear as `ServerException` messages thrown by the `GaSamlIdentificationClient` and `GaSamlEntitlementClient` classes in the SDK.

Table 12: SAML error messages

Error message	Description
Invalid SAML response received from server	**Cause**: The Java SDK has received an invalid SAML response from the Identification Server and Entitlements Server. **Solution**: This error might have been caused by a network transmission error. If the error persists, contact support. Refer to "Getting help" on page 6 for contact information.
Invalid SAML request	**Cause**: The SAML request sent to the Identification Server and Entitlements Server is not valid. **Solution**: If you are sending your own SAML requests, refer to the sample messages in the `IdEntitlementsServer\docs\sampleMessages` directory and make sure you are sending a supported SAML request format. If this error occurred when you were using the Java SDK or the Entrust Application Server Runtime software, it might have been caused by a network transmission error. If the error persists, contact support. Refer to "Getting help" on page 6 for contact information.
No valid security tokens found in the request	**Cause**: The Identification Server received a request that does not contain a supported security token. **Solution**: If you are sending your own SOAP requests directly to the Identification Server, refer to the sample messages in the `IdEntitlementsServer\docs\sampleMessages` directory and make sure you are sending a supported WS-Trust message. If this error occurred when you were using the Java SDK or the Entrust Application Server Runtime software, it might have been caused by a network transmission error. If the error persists, contact support. Refer to "Getting help" on page 6 for contact information.

Table 12: SAML error messages

Error message	Description
A valid SAML Attribute Query was not found in the request	**Cause**: The SAML request does not contain a valid SAML Attribute Query. **Solution**: If you are sending your own SAML/SOAP requests directly to the Identification Server and Entitlements Server, refer to the sample messages in the `IdEntitlementsServer\docs\sampleMessages` directory and make sure you are sending the SAML Attribute Query in a supported format. If this error occurred when you were using the Java SDK or the Entrust Application Server Runtime software, it might have been caused by a network transmission error. If the error persists, contact support. Refer to "Getting help" on page 6 for contact information.
A valid SAML Authentication Query was not found in the request	**Cause**: The SAML request does not contain a valid SAML Authentication Query. **Solution**: If you are sending your own SAML/SOAP requests directly to the Identification Server and Entitlements Server, refer to the sample messages in the `IdEntitlementsServer\docs\sampleMessages` directory and make sure you are sending the SAML Authentication Query in a supported format. If this error occurred when you were using the Java SDK or the Entrust Application Server Runtime software, it might have been caused by a network transmission error. If the error persists, contact support. Refer to "Getting help" on page 6 for contact information.
A valid SAML Authorization Query was not found in the request	**Cause**: The SAML request does not contain a valid SAML Authorization Query. **Solution**: If you are sending your own SAML/SOAP requests directly to the Identification Server and Entitlements Server, refer to the sample messages in the `IdEntitlementsServer\docs\sampleMessages` directory and make sure you are sending the SAML Authorization Query in a supported format. If this error occurred when you were using the Java SDK or the Entrust Application Server Runtime software, it might have been caused by a network transmission error. If the error persists, contact support. Refer to "Getting help" on page 6 for contact information.