

## Entrust<sup>®</sup> GetAccess<sup>™</sup> Secure identity and access management

### **Overview**

This white paper describes the capabilities and architecture of the Entrust<sup>®</sup> GetAccess<sup>™</sup> product portfolio, including a description of the product portfolio's primary features, services and capabilities. This technical overview also describes the Entrust<sup>®</sup> TruePass<sup>™</sup> product portfolio, which provides strong security services built upon Entrust GetAccess capabilities as part the overall Entrust<sup>®</sup> Secure Web Portal solution.

Date: May 2003

© Copyright 2003 Entrust. All rights reserved. Entrust is a registered trademark of Entrust, Inc. in the United States and certain other countries. In Canada, Entrust is a registered trademark of Entrust Limited. All Entrust product names are trademarks of Entrust, Inc. or Entrust Limited. All other company and product names are trademarks or registered trademarks of their respective owners. The material provided in this document is for information purposes only. It is not intended to be advice. ENTRUST DOES NOT WARRANT THE QUALITY, ACCURACY OR COMPLETENESS OF THE INFORMATION CONTAINED IN THIS ARTICLE. SUCH INFORMATION IS PROVIDED "AS IS" WITHOUT ANY REPRESENTATIONS, CONDITIONS, AND/OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, BY USAGE OF TRADE, OR OTHERWISE, AND ENTRUST SPECIFICALLY DISCLAIMS ANY AND ALL REPRESENTATIONS, AND/OR WARRANTIES OF MERCHANTABILITY, TITLE, NON-INFRINGEMENT, SATISFACTORY QUALITY, OR FITNESS FOR A SPECIFIC PURPOSE.

## Table of Contents

<b>I. Introduction .....</b>	<b>1</b>
<b>II. Core Functionality .....</b>	<b>2</b>
<b>III. Technical Details.....</b>	<b>4</b>
<b>Flexible Authentication and Single Sign-on (SSO).....</b>	<b>4</b>
Integration with Entrust TruePass .....	5
Multi-Domain Access (including SSO and Authorization) .....	5
<b>Authorization .....</b>	<b>6</b>
Roles-Based Access Control .....	6
Fine-grained Policy Management.....	7
<b>Best-of-Breed Security .....</b>	<b>8</b>
Inter-component security.....	8
Centralized Session Management.....	8
Intrusion Detection .....	9
Password Policy Management.....	9
Federal Information Processing Standard (FIPS) 140-2.....	10
<b>Personalization .....</b>	<b>10</b>
Dynamic Resource Menu .....	10
Customizable Look & Feel.....	10
<b>Ease of Administration and Operation .....</b>	<b>11</b>
Web-Based .....	11
n-Level Delegated Administration .....	11
Remote Management (Service Control Agent) .....	12
<b>Integration.....</b>	<b>13</b>
User API .....	13
Extensions .....	13
Localization .....	14
<b>User Self-service and Automated Provisioning.....</b>	<b>15</b>
Self-service Enrollment .....	15
Self-service Account Maintenance.....	15
Automated Provisioning .....	16
<b>IV. Entrust GetAccess Components.....</b>	<b>16</b>
<b>Runtime Service.....</b>	<b>17</b>
<b>Access Service.....</b>	<b>18</b>
<b>Identification Service.....</b>	<b>19</b>
<b>Entitlements Service.....</b>	<b>20</b>
<b>Session Management Service (SMS) .....</b>	<b>20</b>
<b>Administration Application .....</b>	<b>21</b>
<b>Logging Service .....</b>	<b>21</b>
<b>Multi-Domain Service (MDS).....</b>	<b>21</b>
<b>Service Trader .....</b>	<b>22</b>
<b>Java Application Programming Interface (API) .....</b>	<b>22</b>

---

Registry Service .....	23
Repository .....	23
<b>V. System Performance &amp; Reliability .....</b>	<b>23</b>
High Availability and Failover.....	23
Performance and Scalability.....	25
<b>VI. Complementary Entrust Products and Solutions.....</b>	<b>25</b>
Entrust TruePass .....	25
Entrust GetAccess Mobile Server .....	26
Entrust GetAccess Proxy Server .....	26
Entrust Secure Transaction Platform .....	26
Entrust Secure Identity Management .....	26
<b>VII. Summary .....</b>	<b>27</b>
<b>VIII. About Entrust.....</b>	<b>28</b>

## Table of Figures

<b>Figure 1 - Entrust GetAccess Roles-Based Access Control.....</b>	<b>7</b>
<b>Figure 2 - Entrust GetAccess Password Rules .....</b>	<b>10</b>
<b>Figure 3 - Customized Entrust GetAccess Resource Menu.....</b>	<b>11</b>
<b>Figure 4 - Entrust GetAccess Service Control Agent (SCA) .....</b>	<b>13</b>
<b>Figure 5 - Localized HTML including Entrust GetAccess login .....</b>	<b>15</b>
<b>Figure 6 - Entrust GetAccess Conceptual Architecture .....</b>	<b>16</b>
<b>Figure 7 - Entrust GetAccess Server-detailed Architecture.....</b>	<b>17</b>
<b>Figure 8 - Entrust GetAccess Multi-Domain Configuration .....</b>	<b>22</b>
<b>Figure 9 - Entrust GetAccess Failover Process .....</b>	<b>24</b>

## I. Introduction

The Entrust<sup>®</sup> GetAccess™ portfolio delivers a single entry and access point for user authentication and authorization across Web portal applications. As such, Entrust GetAccess provides organizations with security, flexibility and performance to personalize the user experience of a Web portal.

Entrust GetAccess software delivers the following key services:

- Flexible authentication, including strong authentication with Entrust<sup>®</sup> TruePass™
- Authentication interoperability via standards such as Security Assertion Markup Language (SAML)
- Single Sign-on (SSO) to Web and non-Web applications
- Authorization including fine-grained access control to online resources
- Rich policy management capabilities, allowing controlled access based on environmental considerations such as authentication method used, physical location, time of day, and day of week, as well as external data sources
- Centralized session management including support for idle and session timeouts, and real-time user revocation
- Personalization of content, enhancing user's online experience
- Integration with leading application and portal vendors
- Convenient and secure Web-based tools for business administration (user management, resource management, etc.) and operational control (start/stop services, configure system parameters, etc.)

Working with industry-leading portal management platforms, identity management products, content management tools and Web application servers, Entrust GetAccess software centralizes security management to provide a common infrastructure for managing user identities and authorization across applications and services. Moreover, Entrust GetAccess software delivers high performance for large Enterprise Web portals without sacrificing security.

As a key part of the Entrust Secure Web Portal and Secure Identity Management solutions, Entrust GetAccess can be seamlessly combined with Entrust TruePass or Waveset Lighthouse, to strongly identify users, manage user authorization, deliver verifiable, secure transactions, centrally control security management, and securely manage user identities. These capabilities provide organizations with confidence to conduct sensitive and high-value transactions through a Web portal. The Entrust Secure Web Portal solution delivers:

- Authentication of users of the portal, regardless of their location;
- Authorization, giving authorized users what they need, when they need it;
- Verification of transactions through digital signatures and customer receipts;
- End-to-end encryption from the browser, through to the backend application for storage or processing;
- Automated and transparent security management of digital IDs to help in reducing maintenance costs and overall total cost of ownership (TCO).

The Entrust Secure Identity Management solution delivers:

- Management of the complete lifecycle for identities of users that exist both inside and outside the organization
- Automated deployment of identities across a broad range of applications
- Support for organizations with heterogeneous, complex environments

- Secure delegated administration, customizable workflow, and user self-service
- Password management and automated synchronization
- Audit log of all user and administrator transactions, providing organizations that face security audits or corporate liability issues a credible record of action.

The breadth and depth of features offered by the Secure Web Portal and Secure Identity Management solutions are unrivaled by competitive solutions available today.

This paper outlines the major features of Entrust GetAccess, providing detailed descriptions of how the product delivers key authentication and authorization capabilities to Web portals. It includes descriptions of the system's capabilities and architecture, as well as how transactions are processed through the system.

## II. Core Functionality

Entrust GetAccess delivers critical authentication and authorization capabilities for Web portals with higher value, higher sensitivity information and transactions. The product identifies end-users before granting them access to sensitive online applications and services that they are authorized to use.

Entrust GetAccess provides the following security services to Web portals:

### **Single sign-on across multiple applications and Web servers**

Entrust GetAccess provides single sign-on across applications and multiple Web domains, allowing integration with an organization's Web partners and affiliates. This flexible integration is supported across both wired and wireless devices including Wireless Application Protocol (WAP), Personal Digital Assistants (PDA) and more. Single sign-on delivers an improved end-user experience and can reduce help-desk costs through fewer password resets.

### **Efficient management of flexible user authentication**

Entrust GetAccess provides a common infrastructure to administer user authentication information for multiple Web resources. This helps an organization to save time and money, and it also reduces the operational and security risks associated with updating multiple access control mechanisms to reflect change (i.e.: employees changing jobs, partnerships dissolving, customers upgrading a service). Entrust GetAccess supports many different industry-standard authentication mechanisms including X.509v3 digital certificates, tokens, lightweight directory access protocol (LDAP) directories, Microsoft Windows Domain infrastructures, Microsoft.net Passport and SAML.

### **Personalized experience for the end-user**

Entrust GetAccess makes it easier for users to navigate to pertinent, targeted information from a personalized menu by centralizing all user authorization functions based on user identity, role, and resource or application being accessed. The ability to personalize the Web experience can lead to increased user satisfaction and loyalty.

### **Fine-grained access to information based on roles and rules**

Entrust GetAccess empowers organizations to control not only who can access specific information or applications, but also how that user must identify himself/herself. This is accomplished through the software's ability to understand both how a user is identified and their requirements for accessing a particular resource. An administrator can also systematically drill-down to the level of access he/she wants to grant to each particular set of users. This ability to manage information access enables organizations to further leverage their portal investment by bringing more sensitive applications and information online.

### **Delegated user administration & management**

Through a standard Web browser, Entrust GetAccess allows the administration of services, users, roles, resources, applications, and other system properties in a flexible, delegated manner. Administrators can remotely manage system attributes, or they can delegate specific responsibilities to other administrators, as well as subsets of the user population, in order to streamline system management. Organizations can now have the flexibility to manage users from multiple locations without the need to deploy software, enabling both time and cost savings in administering a portal.

### **Centralized session management & intrusion detection**

Entrust GetAccess has built-in security mechanisms such as intrusion-detection and unique user session ID cookies. This high level of security gives organizations confidence that they can transition high-value systems to their Web portal. Entrust GetAccess provides a session management service (SMS) that is the centralized location for all Entrust GetAccess session control activity, delivering idle and session timeouts and real-time revocation capability. As the SMS serves as a 'clearing-house' for session-specific keys, Entrust GetAccess can encrypt each user's credentials with a randomly generated key that is unique to each session.

### **Centralized system logging for enhanced auditing**

Entrust GetAccess delivers a centralized logging service that serves as a clearing-house for the recording of system and administrator activity. Every Entrust GetAccess component delivers data to this service so that administrators can go to one location for archiving or examining the activity on the system, making it easier and more efficient to manage. The logs contain essential information such as startup, shutdown, error conditions, user activity, and system status.

### **Flexible deployment options – faster time to market**

Entrust GetAccess can be deployed in-house or as a managed service. It is a standards-based implementation that uses only standard ports for all client traffic (HTTP or HTTPS) to support standard LDAP and X.500 directories and makes it possible to support both in-house and managed service environments, allowing organizations to choose how they want to deploy and manage each specific business application. In addition, the ability to deploy Entrust GetAccess components across multiple servers and multiple physical locations, as well as in a proxy configuration, makes the product fit well in today's high volume, high value Web portals.

### **Wide variety of platform support and interoperability with 3<sup>rd</sup> party tools**

Entrust GetAccess is supported on a variety of Web infrastructure platforms (databases, directories, Web servers, operating systems, authentication technologies) and with numerous third-party tools to accommodate almost any customer environment and requirements. Entrust GetAccess also provides an out-of-box Apache proxy solution at no additional cost. As a result of its flexible architecture and adherence to open standards, Entrust GetAccess has interoperability with a broad range of 3<sup>rd</sup> party vendors and tools available in the market today. Some examples include:

- BEA WebLogic
- Lotus Domino
- Peoplesoft
- Vignette
- Epicentric
- Documentum
- IBM WebSphere
- Plumtree
- Broadvision
- SunONE/iPlanet App Server
- Oracle
- ATG Dynamo

A complete list of supported platforms can be obtained from the Entrust Web site at [www.entrust.com/getaccess/specs.htm](http://www.entrust.com/getaccess/specs.htm).

### **Scalability to address large-scale deployments**

Entrust GetAccess is scalable, easy to deploy, and easy to administer. The product supports millions of pages, dozens of applications, hundreds of Web servers, and millions of users. Services can be distributed across a number of servers to improve response times and provide high availability for customers around the globe. Entrust GetAccess has been deployed to support over a million users at several client sites and is used by hundreds more for their Intranet and Extranet applications. The Entrust GetAccess Web server Runtime (plug-in) is easy to install, configure and administer on the Web server.

### **Built for global deployments that require multiple languages**

From its broad support for users on the most popular Web browsers, to its server-side support for broad range of platforms, Entrust GetAccess is built to deliver authentication and authorization services to a truly global audience. This inherent ability to support multiple language environments and the leading platforms further leverages the portal investment, extending the portal to a truly global audience.

### **Full mobility for all users, including wireless WAP and PDA devices**

The Entrust GetAccess Mobile Server, an optional add-on to Entrust GetAccess, allows customers to extend the capabilities that the product offers to users on the move. The Entrust GetAccess Mobile Server supports leading PDAs and WAP-enabled devices including digital wireless telephones. Over the past two years, many customers worldwide have deployed the Entrust GetAccess Mobile Server into production environments, further extending their Web portal environment to multiple mobile devices, and helping to improve return on investment (ROI) from their overall portal investment.

## **III. Technical Details**

### ***Flexible Authentication and Single Sign-on (SSO)***

Entrust GetAccess provides Single Sign-on (SSO) for the Web resources and applications in a Web portal. Once a user has identified himself or herself to the Entrust GetAccess server, no further application layer authentication is needed. Entrust GetAccess will verify the user's credentials and inform the application of the identity of the user.

Entrust GetAccess gives an organization flexibility to make use of a broad set of authentication mechanisms for deployment. **Out of the box support** is provided for many types of authentication schemes including:

- Username / Password
- Entrust TruePass products (using standard X.509v3 digital certificates)
- LDAP directories
- X.509v3 digital certificates
- SAML assertions issued from a portal site
- Microsoft .net Passport
- Windows Domain Authentication
- Tokens (including RSA SecurID)

Further, due to its open and flexible architecture, Entrust GetAccess software supports the use of Java-based Pluggable Authentication and Authorization Modules (**PAAMs**) for implementing custom authentication and authorization services that meet the needs of a business or organization.

## Integration with Entrust TruePass

Entrust GetAccess is the only Web SSO and authorization product that seamlessly integrates with Entrust TruePass out-of-the-box, including the fact that the combined solution requires only a single runtime at the Web server. Entrust TruePass is a powerful, “**zero footprint**” Web product that provides strong security services including:

- Strong authentication using standards-based X.509v3 Digital Identities while keeping the user experience simple and easy
- Digital Signatures that help organizations with accountability around sensitive or valuable transactions
- Persistent encryption above and beyond secure sockets layer (SSL) protocol that helps keep data private and secured from the browser through the de-militarized zone (DMZ) and all the way into the back-end applications and databases

### Entrust TruePass Authentication

When deployed together, it is possible to use Entrust TruePass software to perform strong authentication and then seamlessly log the user into an Entrust GetAccess system. This operation makes use of the Entrust TruePass Web service, a standard component of an Entrust GetAccess system.

1. User authenticates to Entrust TruePass software. (Note: For a detailed description of Entrust TruePass authentication, as well as its other capabilities, please refer to the Entrust TruePass technical white paper, which is available at [www.entrust.com/truepass/index.htm](http://www.entrust.com/truepass/index.htm).
2. If the Entrust TruePass authentication is successful, it invokes the Entrust TruePass Web Service, an integrated part of an Entrust GetAccess system. It passes the user's DN (Distinguished Name) to the Web Service.
3. The Entrust TruePass Web Service searches the Entrust GetAccess Repository for the specified DN.
4. If the DN is not found, the Entrust GetAccess system automatically enrolls the user and gives him a set of administrator-defined default privileges. This key step reduces the amount of administrative overhead that is required.
5. The Web Service then transparently logs the user into the Entrust GetAccess system and issues the appropriate set of credentials for the user corresponding to the provided DN.
6. At this point, the user is authenticated to the Entrust GetAccess system and can access all of the resources protected by the Entrust GetAccess system for which he or she has been entitled.

In addition, Administrators can explicitly mark resources to be protected by Entrust TruePass authentication. This means that these resources can only be accessed if the user authenticates with Entrust TruePass software.

## Multi-Domain Access (including SSO and Authorization)

As organizations merge or get acquired, form partnerships with other organizations, and/or branch out into various brands, it becomes imperative to extend the same rich authentication and authorization privileges across multiple Internet domains. However, due to an inherent limitation in the way cookies are implemented, they cannot be shared across multiple domains. And, since cookies are the primary containers for delivery of credentials to the browser, this presents a substantial technical obstacle for providing cross-domain SSO and Authorization.

Unlike other vendors that provide multi-domain authentication, Entrust GetAccess software overcomes this obstacle by providing multi domain authentication, using a primary/secondary domain framework for all functions including authentication, authorization, session management, real-time revocation, and logout (i.e. single logout). Entrust GetAccess software was the first product to commercially deliver this capability and continues to lead the market in the breadth of functionality that it provides in this category.

### Security Assertion Markup Language (SAML)

In addition to the native multi-domain capability described above, Entrust GetAccess also provides cross-site interoperability by supporting the SAML standard. This standard is being widely embraced by leading security providers as a way of exchanging security data, user credentials, and authorization requests in a common and well-understood manner. The standard is particularly relevant in scenarios where multiple business entities such as partners or affiliates want to share authentication or authorization information about users who interface with both of them. In these situations, it would be optimal to only force a user

to authenticate once and then be permitted to access resources on both portals. Entrust GetAccess supports this scenario by implementing the SAML Browser/Artifact profile. This mechanism defines a standard manner in which two different sites can use standard HTTP-based messages to exchange the authentication status of a user. Implementing this profile within Entrust GetAccess yields two important capabilities to your site.

- 1) If a user authenticates to Entrust GetAccess at your site and then clicks on a link to a partner site, Entrust GetAccess can hand off a SAML authentication assertion to the other site. The partner site can then trust that your organization has authenticated the user and, since the assertion contains a reference to the user's identity, transparently authenticate the user.
- 2) Similarly, if a user has authenticated to a partner site and that site passes Entrust GetAccess a SAML assertion, Entrust GetAccess can then seamlessly authenticate and authorize the user without requiring an explicit login to take place at your site.

In either scenario, the user experience is simplified since the user only has to authenticate once in order to access applications and resources at your portal and at your partners' portals.

## Authorization

Once a user has been authenticated, it is vital to be able to determine what privileges, or access rights the user has. Authorization is used to determine the user's permissions for accessing various protected resources. In conjunction with authentication, authorization enables organizations to deliver a personalized, meaningful, and secure experience to the end-user of a portal.

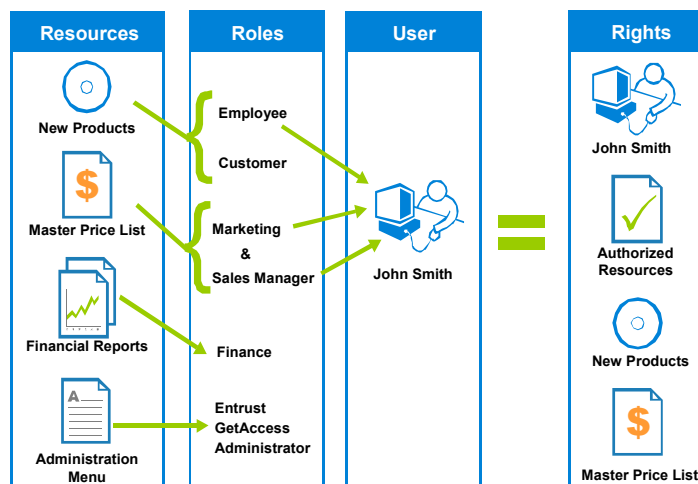
## Roles-Based Access Control

Entrust GetAccess software delivers authorization via a powerful Roles-Based Access Control (**RBAC**) model. This model uses the notion of roles as a layer of abstraction between users and the resources they need to access. Initially, an administrator can assess the resources that need to be protected and define the roles that are needed to access each of those resources. Then, as users are created, they can be assigned roles appropriate to their relationship with and within the organization (see Figure 1). Entrust GetAccess software can then dynamically calculate the resources that a user's roles allow him or her to access. This abstraction greatly reduces the effort needed for an administrator to manage large numbers of users and privileges.

### Security Assertion Mark-up Language (SAML)

Entrust GetAccess supports multi-domain access using SAML out-of-the-box. One of the conditions of SAML itself, is that single sign-on requires users to log in to the Portal site first and then click a link to a resource on the Partner site. In other words, users who log in to Partner site first will have to log in (a second time) to the Portal site to access its secured resources. The following is a step-by-step process flow.

1. User logs into the Portal site.
2. User then requests/clicks a link to a resource on the Partner site. This link should point to the Portal SAML servlet, and include the desired Partner resource in a query string.
3. The Portal SAML servlet can then read the Partner site resource from the query string, and then redirect the user's browser to the appropriate SAML servlet on the Partner site, including the requested resource in the query string. Included with the redirection is a SAML Artifact to facilitate the single sign-on at the Partner site.
4. The Partner site then contacts the Portal site directly with a SAML authentication query with the user's Artifact.
5. If the Portal site has authentication information corresponding to the user's Artifact, it returns a SAML response containing a SAML authentication assertion back to the Partner site.
6. The Partner site then "authenticates" and logs in the user to the Partner domain.
7. And the user's browser is then redirected to the requested resource on the Partner site along with an Entrust GetAccess session cookie. The usual Entrust GetAccess resource protection checks are then made.



**Figure 1 - Entrust GetAccess Roles-Based Access Control**

## Fine-grained Policy Management

Building upon the proven security and scalability of the RBAC model, Entrust GetAccess 7.0 delivers a full-featured policy engine, which allows administrators to define and enforce extremely granular access control policies for online resources. This powerful rules-based access control enables the creation of simple rules defining particular attributes for access control policies. Examples of simple rules include mandating a particular authentication method (e.g. Entrust TruePass authentication, secure token, etc.), a physical location, or a specific window of time.

These rules can then be combined as needed to generate more sophisticated **policies**. Policies can be made up of one or more rules as required by your particular security policies. A particular rule can be used in multiple policies if desired. Finally, a policy can be applied to one or more resources in order to define the criteria that must be met prior to access being allowed to that resource. The rules based access control policies are built upon XACML standards which provides better integration of policies and rules with other applications built on the same standard.

Layering rich, site-specific policies upon the innate Entrust GetAccess RBAC model allows security administrators to define and control the precise situations in which users can gain access to resources. For instance, an administrator can deploy a low-sensitivity resource that is accessible to all users with the role of employee and have no policy defined. However, for access to highly-sensitive applications, authorization can only be granted to users with the role of Executive and only if they have signed in with strong authentication, time of access is during business hours, the source of the request is the internal company local area network (LAN), and it has not been more than 5 minutes since the user last authenticated.

Policies can be defined on many criteria including the following:

- Authentication method
- Time of day / Day of week
- Location as specified by an IP address or range(s) of IP addresses
- Data contained within HTTP header variables
- Other data about the user

Finally, an open callback mechanism is provided so that custom policies can be developed and deployed as needed. This mechanism can also be used to integrate Entrust GetAccess with other third-party policy management tools.

## **Best-of-Breed Security**

In addition to the various capabilities described above, Entrust GetAccess is generally recognized as the most secure access management product in this space. The underlying dedication to security principles that have made Entrust a global leader in information security is embodied in Entrust GetAccess through various security capabilities that have been built in the product from day one.

## **Inter-component security**

When Entrust GetAccess is initially installed, it creates a unique, self-signed certificate, which is used to encrypt inter-component communications at the security administrator's option. It is important that the credentials being used to secure this traffic are site-specific and not embedded in the product. Other products may embed credentials in the product creating a scenario where every deployment of the product is using an identical set of credentials.

The credentials created at install time are also used to support SSL connections to the Service Control Agent (SCA) operations management interface for Entrust GetAccess. In addition, when the SCA initiates a request to stop a particular service, it digitally signs the request so that the authenticity of the message can be established. The targeted service then validates the signature prior to beginning its shutdown sequence. This means that Entrust GetAccess will not entertain invalid or inappropriate shutdown requests from parties that are not trusted.

## **Centralized Session Management**

One of the critical security capabilities that Entrust GetAccess offers is centralized session management. Session management in general refers to the ability of a system to perform timeout functions. Entrust GetAccess software is capable of performing both general and idle timeouts, depending on the behavior of a user during his or her session. While system-wide defaults can be set for these settings for all users, it is also possible to change those values for specific users based on their relationship to the organization. For instance, while the idle timeout for most users may be set to 30 minutes, it can be lowered to 15 minutes for those users accessing high-value or highly sensitive applications in order to minimize the risk of compromising a high-security account. This allows a site to adhere to defined risk-management policies for timeouts with regard to end user behavior. In addition, policies can be defined on a per-resource basis, restricting access to sensitive applications and data depending on how long a user has been idle.

More importantly, Entrust GetAccess software is unique in that it delivers centralized session management. That is, all of the sessions are tracked in a single logical object within the Entrust GetAccess infrastructure. Session Management Service (SMS) gives the administrator a centralized point from which to enforce real-time revocation of user sessions and can be installed on several systems to provide redundancy, fault tolerance, and performance. Real-time revocation is a powerful security feature that allows an administrator to have total control to lock out a user quickly and effectively. In the event that a business decision is made to rescind the privileges for a particular user, Entrust GetAccess software can quickly and efficiently revoke all access from that user, across multiple sessions, and multiple domains.

Unlike competitive products, centralized session management gives Entrust GetAccess software a unique and important security advantage. All other Web SSO and authorization products rely largely upon the use of cookies as the containers for user information and security credentials following user authentication. Most vendors use the same symmetric encryption key to encrypt these cookies. This makes them vulnerable to cryptographic attack (cryptanalysis) because an attacker can collect large amounts of data (cookies harvested over the course of an hour or two) encrypted with the same key, which substantially improves the chances of breaking the encryption. Compounding this risk is the fact that once an attacker has compromised the key, they have the ability to forge credentials for the system. This security exposure can have serious consequences for the organization and ultimately to their reputation and brand.

Entrust GetAccess software helps mitigate this risk by using a small (128-bits), session cookie. More importantly, no user information is sent in this cookie back to the browser. This means that your organization can have confidence that no user information is sent out over the public Internet. By not including sensitive user-specific information in the Entrust GetAccess cookie, this helps address privacy issues that are becoming more prevalent in many countries.

## Intrusion Detection

Entrust GetAccess software provides built-in intrusion detection capabilities to help reduce the risk of account compromise in the event of an attack. Included in this capability is an alerting mechanism that notifies administrators that the system is potentially under attack. Entrust GetAccess software provides two types of intrusion detection -- per account and system-wide:

**Per Account:** Administrators can configure a parameter within the Entrust GetAccess administration tool that defines the threshold for this setting. If any account is accessed consecutively with an incorrect password in excess of that threshold, the account is locked out.

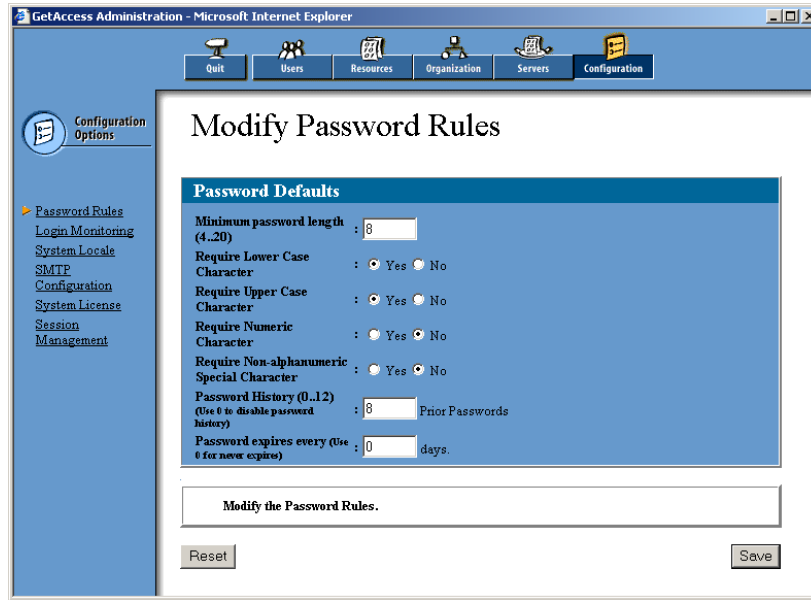
**System-Wide:** Administrators can configure two parameters (x and y) within the Entrust GetAccess administration tool where x defines a threshold of failed logins and y defines a sliding window of time, measured in minutes. If the system detects x or more failed logins within a window of y minutes, a real-time notification is sent out to a defined list of administrators.

## Password Policy Management

Many organizations mandate various types of password policies that dictate how strong user passwords have to be. While the actual details of the policies may vary from firm to firm, almost every medium to large organization needs a mechanism to manage these policies, and more importantly, enforce the passwords that users choose for themselves.

Entrust GetAccess provides a flexible way to manage multiple password policies per deployment as mandated by site-specific security policy. In addition to optionally maintaining a complete password history for every user, an administrator can create password policies made up of different rules including the following:

- Minimum length
- Required numeric characters
- Required non-alphanumeric characters
- Required upper-case characters
- Checks against a password history
- Should not contain the user's first or last name
- Should not contain a substring of the user ID



**Figure 2 - Entrust GetAccess Password Rules**

These password policies can be set up to be global or user-type specific. A global policy means that the defined policy applies to all Entrust GetAccess users. Alternately, administrators can define different policies for different types of users. For instance, the policy for contractors may be set up to be more restrictive than the one for employees. In the event that an administrator defines a policy for a certain set of users, Entrust GetAccess will override the global policy with the group specific one.

## **Federal Information Processing Standard (FIPS) 140-2**

Entrust GetAccess 7.0 is the first product in this space to use a Federal Information Processing Standard (FIPS) validated module for cryptographic operations. FIPS 140-2 is a standard set forth by the U.S. Federal Government. It mandates requirements for security of the cryptographic kernel within a product. The standard defines which algorithms may be used and how the keys used with those algorithms are to be kept secure. Although a U.S. standard, FIPS is widely held to be one of the highest levels of security and is recognized by various governments and private firms as an attestation to the level of security within a particular product.

## **Personalization**

### **Dynamic Resource Menu**

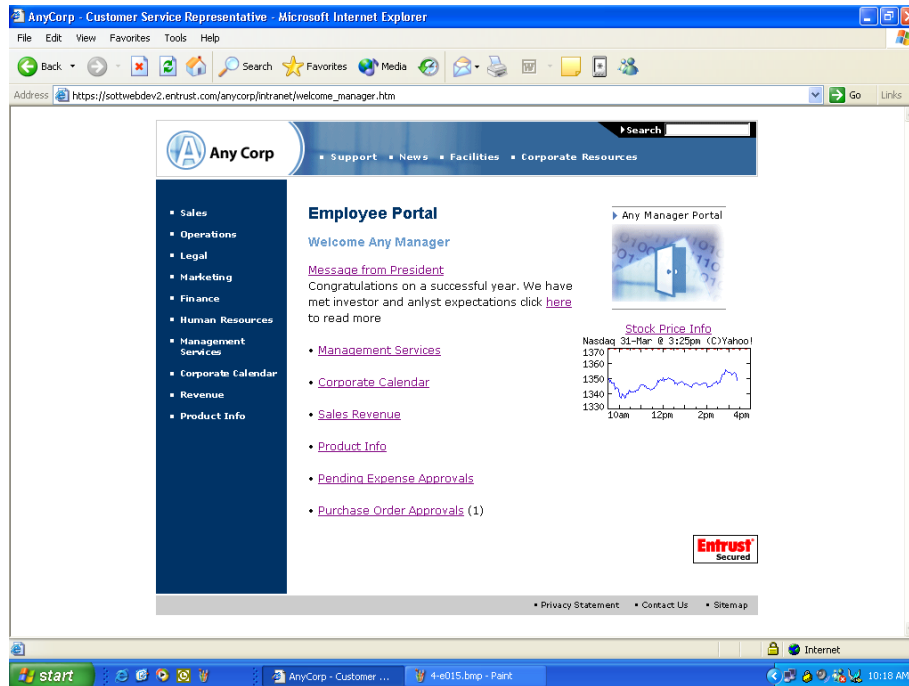
Once a user has been authenticated and authorized, Entrust GetAccess software dynamically renders a personalized HTML menu that reflects the resources and applications for which the user is granted access. This allows users to quickly navigate through their applications without having to remember or bookmark various URLs. In addition, since this menu is dynamically generated, it will continue to give the user a real-time and up-to-date view of his or her privileges each time it is accessed.

### **Customizable Look & Feel**

All the HTML pages that Entrust GetAccess software generates are completely template driven, making it very straightforward to change the look-and-feel of the implementation to match the rest of the site. Updating the pages that a user will see is as easy as making the appropriate modifications to the

provided templates. This makes it quick and easy to integrate Entrust GetAccess software into an existing or new Web site.

Figure 3 illustrates the degree to which the standard menu can be customized.



**Figure 3 - Customized Entrust GetAccess Resource Menu**

## ***Ease of Administration and Operation***

### **Web-Based**

Administering users in a timely and cost-effective manner is a very important aspect of managing and deploying a site to large user-based populations. The Entrust GetAccess server ships with a comprehensive browser-based administration tool. This tool can be used to manage users, roles, resources, and other objects and parameters within the Entrust GetAccess server. Since this tool only requires a browser, there is no installation required on the administrators' machines.

### **n-Level Delegated Administration**

Being able to scale a site to hundreds of thousands and even millions of users requires a sophisticated administration model that can help divide the administration effort so that it can be delegated to various people. One of the unique differentiators for Entrust GetAccess software is the manner in which it delivers this type of delegated administration capability.

Entrust GetAccess software enables the delegation of n-levels of administrative activity through a unique approach that allows the master-user to combine who a delegated administrator can see with what actions they can take on that population.

With the flexibility that this delegation model provides, it is possible to give many different levels of administrative privileges to different delegated administrators. This means that Entrust GetAccess software can be deployed in a manner that will fit almost any business scenario.

Entrust GetAccess software delivers this capability in the core product, and not as an add-on or extra. Unlike competing products, the administration tool is designed to provide this flexible delegation against any type of supported repository including Relational Databases or LDAP directories. In addition, Entrust GetAccess permits security administrators to define these security domains in an arbitrary fashion independent of any existing hierarchies defined in a directory structure. Competing products are bound to the directory structure and therefore cannot impose a different security hierarchy independent of the directory structure.

## Remote Management (Service Control Agent)

Ease of management and remote monitoring/maintenance are crucial requirements for any infrastructure component, but particularly so for the security layer of a 24 X 7 customer-facing Web portal. Entrust GetAccess software has provided these capabilities for a number of years with the Service Control Agent (SCA) component. Like the Entrust GetAccess administration tool, the SCA is also completely browser-based and is provided with the core Entrust GetAccess offering at no extra cost. It is a fully functional GUI for adding and removing services, monitoring them to know that they are operational, and for starting and stopping them remotely as needed.

Since the SCA is browser-based, administrators don't need to have any specialized software deployed on their desktop, making deployments much simpler to manage. This also allows the system to be remotely managed via an organization's private network or VPN. If security policies so allow, it also makes it possible for the SCA to be exposed to the public network, making it possible to administer the Entrust GetAccess infrastructure from a browser connected to the Internet from anywhere in the world.

### n-Level Delegation Example

A financial services firm that has thousands of brokers across the world can be set up with administrators who only have access to particular branches (e.g. New York, San Francisco, Tokyo, London). When an administrator for London uses the Entrust GetAccess administration tool to request a list of all users, he or she will only see the users in the London branch. He or she will have no visibility to the users at the various other branches. The London branch administration can then be extended down to n-levels whereby the London administrator can delegate administrators to only see/manage their specific group of users at each level, but the London administrator would still be able to see/manage the entire London branch.

Similarly, these multiple administrators can be set up within the London branch to have varying levels of administrative authorization. For example, Andrew can see only users in London – Finance and create, modify, and delete them and all their associated privileges. Brian can see only London – Human Resources users, but only has the ability to reset their passwords. He doesn't have the ability to see their other attributes or ascertain what privileges they do or do not have. Charlene is an application owner responsible for managing access to a trading application and can see only London – Trading users, but cannot do anything to their passwords or other privileges. She can only assign or remove the entitlement that will give users access to that application.

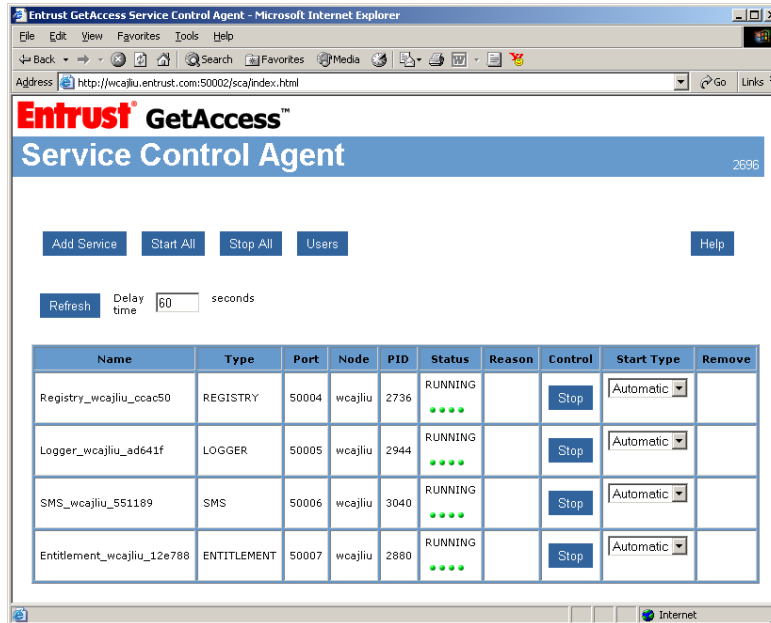


Figure 4 - Entrust GetAccess Service Control Agent (SCA)

## Integration

Due to the varying business requirements of every organization, any commercial software product needs to provide flexible and robust interfaces for customization and integration. Entrust GetAccess provides flexibility by delivering two types of integration mechanisms to allow a strong fit into diverse business environments. The first mechanism is a rich set of APIs for managing how data gets in and out of Entrust GetAccess. The other is a set of “exits”, called Events, which allow programmatic customization of system behavior.

## User API

In order to support the integration of Entrust GetAccess software into customer environments, the product comes with a rich API that allows user management functions to be accessed programmatically. Implemented in Java, this API can be used to interface with other user management systems including ERP / HR systems and third-party administration tools. It can also be used to develop ‘meta-tools’ allowing organizations to manage several infrastructure components, including the Entrust GetAccess server, from a single interface. Similarly, the API can also be used to accept real-time or batch updates from external systems.

## Extensions

While the capabilities that Entrust GetAccess software provides are broad and rich, there will always be scenarios where business requirements mandate modification to some aspect of the behavior of the system. In order to provide the flexibility that these deployments demand, the Entrust GetAccess system has a wide variety of interfaces, called **Events**, that occur at defined points. Examples of events include successful login, failed login, password reset, etc. Developers or Systems Integrators can then create customized behavior by attaching **Extensions** to the appropriate events. Extensions are compiled java code that extend core Entrust GetAccess functionality and allow a deployment to meet its functionality requirements.

While a complete list of the more than 20 events can be obtained from the Entrust GetAccess Programmer’s Guide, a subset is listed below, along with some examples of how customers have extended these particular events:

- **onSuccessLogin:** User successfully authenticates himself or herself to the Entrust GetAccess system
  - *Usage:* Display trade notices for the day; Issue additional credentials based on real-time entitlements checks such as giving extra privileges if a bank balance is greater than a pre-determined value.
- **onFailLogin:** User fails to log in successfully
  - *Usage:* Log username into a “follow-up” file for user experience team.
- **onFirstLogin:** The very first time the user is authenticating to the Entrust GetAccess system
  - *Usage:* Display legal notices and disclaimers about the user’s online access; Get acknowledgement of notices and disclaimers.
- **onLogout:** User logs out of the Entrust GetAccess system
  - *Usage:* Send notification to external systems that user has logged out.
- **onSuccessSelfReg:** User successfully self-enrolls into the Entrust GetAccess system
  - *Usage:* Display customized “Welcome” page informing user of the benefits of their online access.
- **onChangePassword:** User changes his own password
  - *Usage:* Enforce site-specific password rules including dictionary checks.
- **onClickNewUser:** Administrator begins to create a new Entrust GetAccess user
  - *Usage:* Randomly generate and pre-populate a password into the user’s record.
- **onBeforeSaveNewUser:** Administrator is about to complete new user creation
  - *Usage:* Validate entered data against external systems for authenticity and validity.
- **onSuccessSaveNewUser:** Administrator successfully creates a new user
  - *Usage:* Propagate user account information to external systems.

The power and flexibility that this unique event/extension model provides allows Entrust GetAccess software to seamlessly meet the most challenging requirements and scenarios faced today.

## Localization

Entrust GetAccess software is an internationalized product, which allows it to be localized into any language. The entire set of HTML pages that an end-user can see is rendered using canned templates that are provided and pre-populated with a standard product. These templates are language / locale specific and can be localized by duplicating the template directory and making the necessary changes to the templates in the new directory.

In addition, each user’s Entrust GetAccess profile stores that user’s locale preferences. This allows a site to be deployed in several languages. Once a user is authenticated to Entrust GetAccess server, it uses this information to select the templates for displaying information to that user. This enables the user to see logout, resource menu, timeout messages, and other Entrust GetAccess pages in the language of his or her choosing. Entrust also delivers language-specific user administration for key languages, including French and Japanese. Entrust customers around the world have localized the Entrust GetAccess user-facing interface into various languages including French, Japanese, Swedish, and Spanish.

The following figure shows a customized home page of an Entrust GetAccess customer including the Entrust GetAccess Login interface at the lower left corner of the window.

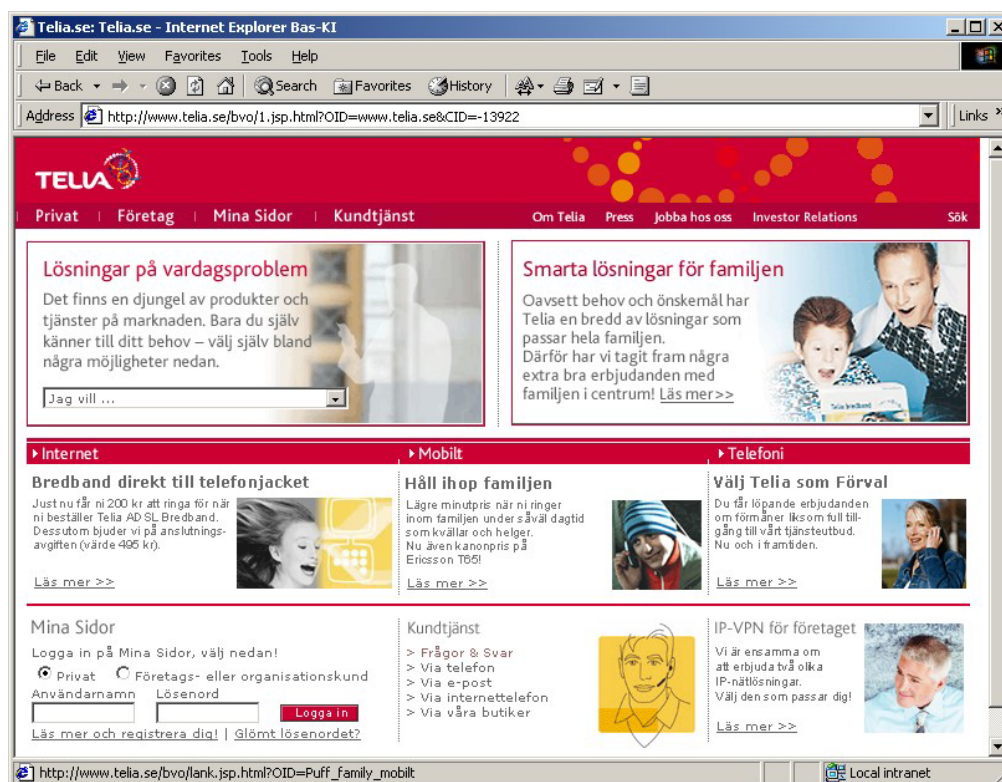


Figure 5 - Localized HTML including Entrust GetAccess login

## User Self-service and Automated Provisioning

Entrust GetAccess software can help an organization reduce the Total Cost of Ownership (TCO) of the overall portal by providing powerful provisioning and account management features for user self-service.

## Self-service Enrollment

Self-service allows users to enroll themselves, without any administrative intervention, into the Entrust GetAccess server and dynamically receive privileges based on their relationship with the organization. Entrust GetAccess software helps drive significant cost-savings helping to reduce or even eliminate administrator involvement in the enrollment and user management process.

Entrust GetAccess software is capable of leveraging an existing user management repository such as an LDAP directory or a Windows Domain infrastructure. A user that exists in the external directory can self-enroll and obtain an Entrust GetAccess account by presenting authentication credentials for that external directory. Entrust GetAccess software can validate these credentials against that directory and automatically create a corresponding Entrust GetAccess account for that user if the authentication attempt is successful. This behavior can also be modified per the events/extensions described earlier in this paper to model business processes.

## Self-service Account Maintenance

Entrust GetAccess software also provides user self-service capabilities for maintaining accounts. Authenticated users can manage their own accounts by selecting preferences, managing their passwords, and performing other tasks that would otherwise require expensive calls to the corporate

support Help Desk. These processes can also be customized so that additional capabilities and privileges are provided to the user population.

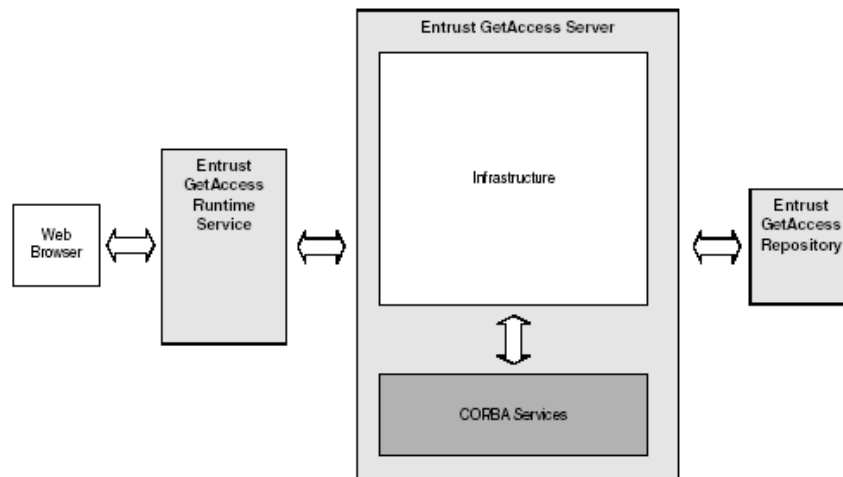
## Automated Provisioning

Entrust GetAccess software can also help reduce costs by leveraging existing business processes for managing user privileges. If users and their corresponding roles and privileges are being administered in an external directory, Entrust GetAccess software can dynamically pick up this information each time the user logs in. It can then authorize the user based on the new data in the external directory. This can translate directly into cost savings as administrators can continue to use the same tools and mechanisms for user management. This addresses data redundancy and the need to re-train the administration staff on using new tools.

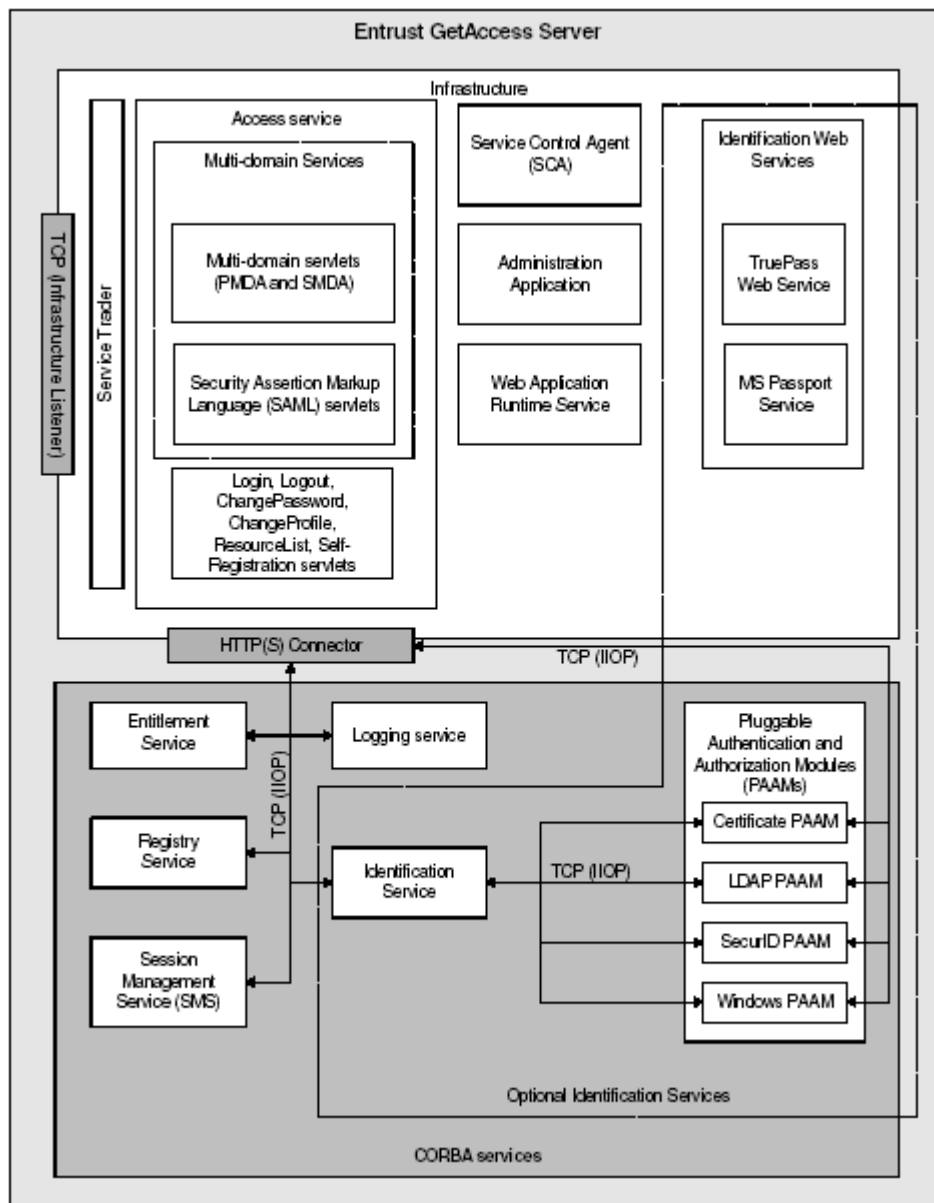
## IV. Entrust GetAccess Components

Entrust GetAccess software has been designed from the ground up to be very modular and flexible and plug seamlessly into a broad range of network architectures. The entire system can be collapsed onto a single machine for proof-of-concept or other small deployments. It can just as easily be distributed across various machines hosted in a traditional three-tier Internet architecture (DMZ, Trusted Network, High Security Zone). The appropriate components can be striped across various hardware systems to deliver high-end availability and performance. Finally, it can also be deployed in geographically distributed data centers to support high levels of fault-tolerance and disaster recovery.

This section of the document examines some of the primary components of the Entrust GetAccess system, their function, and how they communicate with each other. The following diagrams show the basic Entrust GetAccess system architecture and the internal architecture for the Entrust GetAccess server.



**Figure 6 - Entrust GetAccess Conceptual Architecture**



**Figure 7 - Entrust GetAccess Server-detailed Architecture**

## Runtime Service

Runtime Service is a plug-in or a filter for Web servers that protect your Web resources. Specifically, it:

- intercepts incoming requests for resources—protected or not—and redirects the requests to the Entitlements Service for further processing
- receives commands back from the Entitlements Service to allow or deny access to a requested resource
- routes login requests to the Access Service

The Runtime Service is configured to forward all requests, even those for unprotected resources, to the Entitlements Service to be checked. For improved performance, you can have unprotected resources returned immediately to the user, instead of having them forwarded to the Entitlements Service.

## **Access Service**

The Access Service is a collection of servlets that provide the front end of the various user-facing functionality areas within an Entrust GetAccess system. The Access Service is an Infrastructure service. Its main responsibilities are to:

- create and return login pages to users
- verify user login information, such as user names and passwords
- create logout, resource menu, account management, and self-registration pages

### **Creates a login page and returns it to the user**

The Access Service receives a request from the Runtime Service to create a login page. The Access Service checks which authentication methods you are using on your Web site. Authentication methods may include: Entrust GetAccess username and password, Certificate PAAM, LDAP PAAM, SecurID PAAM, Windows PAAM, Entrust TruePass Web service or Microsoft Passport Web service.

For example, the Web server may determine that you are supporting certificate authentication (enabled by the “Certificate PAAM”) and LDAP authentication (enabled by the “LDAP PAAM”). The Access Service creates a login page that includes these authentication methods as options in a drop-down list and returns the page to the Runtime Service, which returns it to the user. If only a single identification method is used in your system, the Access Service creates a login page with no drop-down menu.

### **Enables username and password authentication**

The Access Service authenticates users with the default Entrust GetAccess username and password identification method. Once the user identifies himself/herself, the information is sent to the Access Service, which maps the information to the Entrust GetAccess user entry in the Entrust GetAccess Repository. Once the user is valid, the Access Service calls the Session Management Service to create the session. The session is labeled with a session ID and is returned to the Access Service. The Access Service places the session ID into a cookie and returns the cookie to the user. The cookie is the user’s proof of authentication for the remainder of the session.

**Note:** For security reasons, the user’s password—both in the Access Service’s cache and in the Entrust GetAccess Repository—is stored in hashed format using the SHA-1 hashing algorithm, not in clear text. When users submit their passwords, the Access Service makes a hash of the submitted password and compares it to the hash in the Repository and determines whether there is a match. The keys used to create a hash of the user’s password are unique for each user.

### **Creates a logout page and returns it to the user**

When a user selects the logout link from an Entrust GetAccess page, the Access Service calls the SMS to remove that particular session. For added security, the Access Service overwrites the user’s Entrust GetAccess cookie.

### **Creates a resource menu page and returns it to the user**

When users log in directly to Entrust GetAccess, the Access Service creates a personalized resource menu page. The page includes a list of the resources that users are allowed to access based on their roles. The Access Service then returns this page to users.

**Creates account management and self-registration pages**

The Access Service provides the appropriate Web interface to support user account management and self-registration requests for enrollment, password management, and profile management.

The Access Service is a client of the Identification Service, SMS, and Registry Service. It is accessed via HTTP or HTTPS by the end-user's browser.

**Identification Service**

The Identification Service plays several important roles in the Entrust GetAccess operating environment. It is responsible for accepting authentication requests during enrollment or login, and forwarding them on to the appropriate PAAM or Web service for validation. If the authentication is successful, the Identification Service then communicates with the Entrust GetAccess SMS in order to have a new session generated for that user. It is also responsible for encrypting the credentials for that user based on the random key generated for that user at login time.

The authentication modules include both PAAMs and Web Services, which contain all the specific functionality for a particular type of authentication. This abstraction allows the rest of the Entrust GetAccess infrastructure to be deployed without needing specific knowledge of the internals of any particular PAAM or Web service.

**Pluggable Authentication and Authorization Module (PAAMs)**

A PAAM is a CORBA service that is an interface to third-party authentication software (either Entrust or another vendor). It identifies and assigns roles to users using that third-party software instead of using internal Entrust GetAccess functions. Capable of providing both authentication and authorization capabilities, PAAMs have been developed by customers, third-party vendors, and Entrust Professional Services for various authentication mechanisms and technologies. PAAMs receive calls from the Identification Service to identify a user. They function as clients to their respective server-side component. For example, the LDAP PAAM is a client for the LDAP-compliant Directory and the SecurID PAAM is a client for the RSA ACE/Server<sup>®</sup>. Entrust GetAccess supports LDAP PAAM, Certificate PAAM, SecurID PAAM, and Windows PAAM.

For added flexibility, all PAAMs support the self-registration feature, except the Certificate PAAM. You can use the self-registration feature to migrate existing user entries to the Entrust GetAccess Repository automatically. Furthermore, if you don't want to use the Administration Application to assign a user type and roles to a user, you can use the PAAM to have Entrust GetAccess assign users a user type and roles automatically when they self-register or log in.

It is the logic in the Identification Service that drives the flexibility of the PAAM framework. It abstracts all authentication and authorization logic away from the rest of the Entrust GetAccess architecture. The Identification Service is called by the Access Service and serves as a client of the various PAAMs and the Registry Service.

**Web Services**

A Web service is a program that runs within an Application server that communicates with other requesting components using the Simple Object Access Protocol (SOAP). You can invoke a Web service across a network using Extensible Markup Language (XML). Components request only the part of the Web service program that they need at the time. The object code is returned in a SOAP envelope. The object is then loaded and executed on the client.

Web services provide the following advantages:

- The SOAP protocol provides standardized parsing (encoding and decoding) of object code for a Web service and its clients. Programmers do not have to write their own code and programs written by different companies can communicate with the Web service.
- In the Entrust GetAccess system, SOAP envelopes are sent within HTTP requests. You do not have to open additional ports in your firewall for clients to communicate with the Web service.
- Web services are language, platform and location independent.

The Identification Web services function as clients to their respective server-side components. For example, the Entrust TruePass Web service interfaces with the Entrust TruePass Authentication servlets. Entrust GetAccess offers authentication via Entrust TruePass and Microsoft Passport Web services.

## ***Entitlements Service***

The Entitlements Service is a CORBA service that determines the resources that users are allowed to access.

### **Loads resources**

When the Entitlements Service starts, it sends a request to the Entrust GetAccess Repository asking for a list of locations of all the Entrust GetAccess-protected resources and corresponding roles. It then loads the list into memory.

### **Authorizes the user**

To authorize the user, the Entitlements Service performs the following tasks:

- Checks the Entrust GetAccess cookie
- Compares the roles of the user to those of the requested resource.
- Checks policies
- Checks whether it's an Entrust TruePass-protected resource
- Informs the Runtime Service to allow or disallow access to the resource.

## ***Session Management Service (SMS)***

In order to deliver a high level of security, Entrust GetAccess software provides its session management capabilities from a centralized service. The Entrust GetAccess SMS is a CORBA service that creates, validates and removes user sessions. It is responsible for session creation (when users are authenticated) and session tracking (as users access various protected resources on the site).

### **Creates a Session object and corresponding cookie**

When a new session request from the Access Service reaches the SMS, it creates a Session object for the user who had just logged in and had been identified. The Session object includes an expiration time, session ID, and other information. The SMS adds the Session object to its session table and sends a copy to the other SMSs in your system. The SMS sends the session ID from the session object to the Access Service. The Access Service then places the session ID in an Entrust GetAccess cookie and returns it to the user. As noted previously, this cookie is only 128-bits in length and contains no user-sensitive data for privacy and security concerns.

### **Validates users who have been identified already**

If users who have identified themselves already request an Entrust GetAccess-protected resource, the Entitlements Service sends a request to the SMS asking it to validate the users. SMS looks for a Session object in its cache with a session ID that matches the one in the user's Entrust GetAccess cookie. If a matching session ID is found, it is proof that the user has already been identified successfully. The SMS then checks if the session has expired. If not, the SMS updates the session with a new expiration time and indicates to the Entitlement service that the user is still valid.

## Logs users out of Entrust GetAccess

When a user logs out of Entrust GetAccess (by selecting a *Logout* link on a Web page), the Access Service forwards a request to the SMS to remove the user's session object and the user's Entrust GetAccess cookie. Even if you set the Entrust GetAccess cookie as persistent, it is destroyed when the user clicks *Logout*.

## Administration Application

The Administration Application is a browser-based GUI for the Entrust GetAccess Registry Service. It uses a servlet that resides in the Infrastructure and is a resource that is protected by the Web Application Runtime Service. You use the Administration Application to add, remove and modify users, roles, resources, policies, and other objects and parameters within Entrust GetAccess. In the administration application, you can setup and designate as many administrators or delegated administrators with the same level of privileges (or reduced, delegated privileges) to the Administration Application.

## Logging Service

Entrust GetAccess provides a centralized Logging Service to make the entire system easier to manage, troubleshoot, and audit. Entrust GetAccess provides flexible logging capabilities by allowing an administrator to define, at a component level, the desired degree of details to capture in the log file. Ranging from "Info", providing information on normal activity, to "Debug", which captures information down to the code level, this powerful feature allows deployment administrators and infrastructure managers to finely control the amount and types of information being gathered to help to manage risk and optimize resources. Entrust GetAccess logs activity by user, administrator and system events.

## Multi-Domain Service (MDS)

The Multi-domain services provided by Entrust GetAccess allows the transfer of the user's authentication information across multiple Internet domains so that users only have to log in once to access resources in multiple domains. As mentioned earlier, Entrust GetAccess supports two methods to enable multi-domain functionality: multi-domain servlets and SAML. Using multi-domain servlets, users can log in and log out once to and from all domains. Using the multi-domain servlets, you can manage

### Multi-domain Servlets

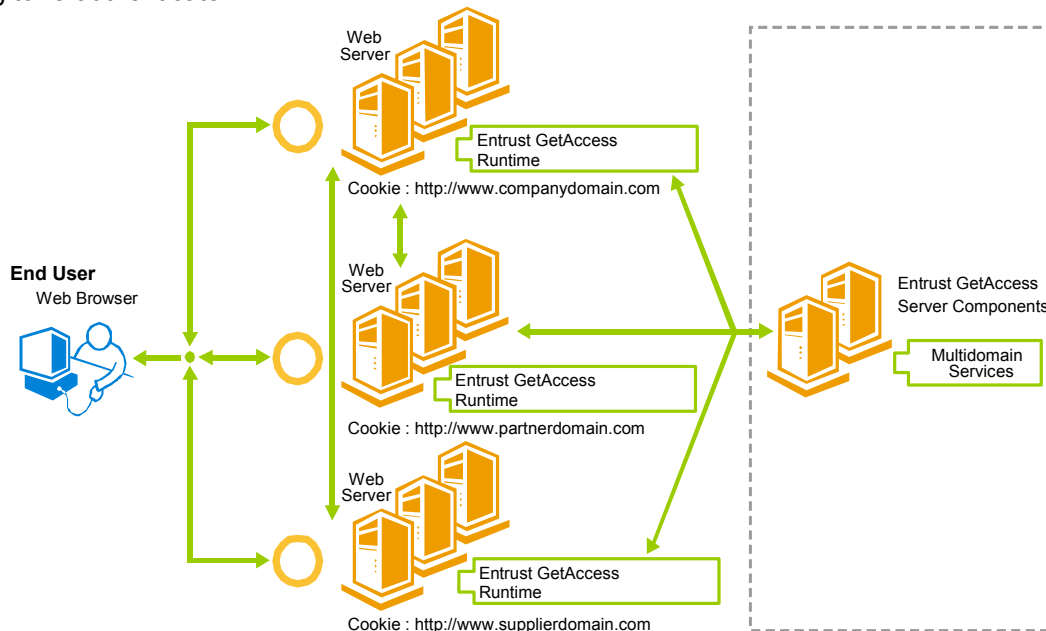
This scenario describes how credentials from the Primary Domain are secured and handed off to a Secondary Domain. The scenario assumes that the user has already authenticated to the Primary Domain and is attempting to access a resource on the Secondary Domain. For the purposes of this example, the Primary Domain is referred to as Domain A, and the Secondary Domain is referred to as Domain B.

1. User requests access to a protected resource in Domain B.
2. The Resource Protection Service intercepts the request through the Entrust GetAccess Runtime. Since it cannot find Entrust GetAccess cookies in the HTTP header, the service redirects the user to the SMDA (front-ended by a URL in Domain B).
3. The SMDA redirects the request on to the PMDA (front-ended by a URL in Domain A). This step is required to enable the PMDA to track the source of the request and re-route it back correctly later.
4. The PMDA, a resource protected by the Runtime in Domain A, picks up the Entrust GetAccess cookie from the HTTP header and captures the user's Session ID from the cookie.

**Note:** Since the PMDA is a protected resource in Domain A, and this example assumes that the user is authenticated to Domain A, the PMDA has access to the user's cookies. In the event that the user had not yet authenticated to Domain A, he would have been directed to the Access Service for login. The rest of this scenario would then behave as described.

5. The PMDA redirects the browser back to the SMDA with the user's Session ID embedded in the URL. It is able to do this because it tracked the source of the request by examining the "Referring URL" tag in the HTTP header. This is why Step 3 is necessary.
6. The SMDA extracts the Session ID from the URL, and issues it back to the user's browser in the form of an Entrust GetAccess cookie for the secondary domain. This means that the user's session continues to be centrally tracked, and that he or she has the same set of privileges across Domain A and Domain B.
7. The SMDA redirects the user to the resource he or she was originally attempting to access in Step 1.
8. The Resource Protection Service once again intercepts the request. This time, it finds the cookies that weren't present in Step 2. From this point on, it behaves like a primary domain Runtime by decrypting the cookie, validating the session, and checking that the user's privilege level is sufficient. If all checks pass successfully, the user is permitted to access the requested resource.

user sessions and deliver personalized content across domains. Once a user is authenticated to the primary domain, he or she can access secured resources on all primary and secondary domains without needing to re-authenticate.



**Figure 8 - Entrust GetAccess Multi-Domain Configuration**

## Service Trader

The Service Trader is one of the most critical pieces in the Entrust GetAccess architecture. It is an Infrastructure Web service responsible for providing a central registration service for all other Entrust GetAccess components and letting other services know the availability and location of these components.

### Stores a list of service references

When a CORBA service is started, it registers itself with the Service Trader by sending it a service reference that indicates the CORBA service instance's unique name and location. After the initial registration, CORBA services periodically re-register themselves with the Service Trader. The Service Trader also keeps a list of service references for the other Infrastructure services. When a service, for example the Entrust GetAccess Entitlement Service, is started and begins to initialize, it connects to each Service Trader and informs the Trader that it is now ready to accept connections. Then, when the Trader gets a request from a client that depends on this service (e.g. the Runtime), the Trader informs the requestor of the name and location of all available Entitlement Services. This allows clients to discover and bind to the services on which they rely.

Once a service is registered with the Trader, the Trader periodically polls the service to determine that it is still available. The frequency of the poll is an administrator configurable setting that can be tuned to increase uptime while still managing network traffic load. If a particular service becomes unavailable, the Trader will stop providing it's information to clients requesting that type of service.

## Java Application Programming Interface (API)

The Entrust GetAccess software development kit (SDK) includes a public Java API. The API gives application developers access to the Entrust GetAccess Repository and to the software user

management functions, allowing them to customize an Entrust GetAccess environment. For example, the API allows you to alter the resource menu application.

## ***Registry Service***

Entrust GetAccess software uses the Registry Service to abstract the specifics of the repository implementation away from the rest of the system architecture. The Registry Service is a repository-specific service that provides a universal and common interface to the repository from all other Entrust GetAccess components. The Registry Service allows the remaining components of the system to leverage the same code base by hiding the specifics of the repository implementation. This leads to a more robust and stable system.

The common interface that is exposed by the Registry Service is the **Entrust GetAccess API**. The complete Entrust GetAccess API is comprised of other private APIs that deliver resource and server management functions. By making this common interface available, Entrust GetAccess software allows other components, such as the Administration Application, to deliver the same behavior and functionality regardless of the Repository type. More importantly, it allows customer applications to be shielded from the particulars of a repository implementation.

## ***Repository***

While Entrust GetAccess software is capable of leveraging external directories and databases for authentication and authorization information, it maintains its own Repository for the purposes of storing data about secured resources and other system information. This repository also maintains Entrust GetAccess-specific data on end-users, including user role information, timeout values, failed and successful login attempts, etc. Entrust GetAccess software natively supports both databases and directories for use as the repository. A complete list of supported repository platforms can be obtained from the Entrust Web site at [www.entrust.com/getaccess/specs.htm](http://www.entrust.com/getaccess/specs.htm).

# **V. System Performance & Reliability**

Designed and built on top of standards-based components and almost entirely in pure Java, Entrust GetAccess software delivers a robust, stable, and scalable environment. This section highlights some of the salient points that need to be considered when evaluating Web portal security solutions.

## ***High Availability and Failover***

**Availability** refers to the percentage of time that a system is available to a user. When increasing the level of availability, your goal should be to attain the level of “high availability” (HA) or “fault tolerant” availability. HA systems must be maintainable so that administrators can service a failed component in the system without shutting down the entire operation.

Entrust GetAccess software is designed to avoid a “single point of failure” within the system. A customer can deploy multiple instances of each component to reduce system downtime. When deployed in an HA configuration, Entrust GetAccess software automatically detects the presence of redundant components and transparently fails over to them as needed. This failover requires no administrative intervention and is transparent to the end-user.

After adding and configuring extra Entrust GetAccess components in your system, you can configure failover. You can configure failover and balance the load between users and multiple Runtime Services.

To do so, you must place a load-balancer in front of your Runtime Services. More importantly, you can configure failover for Infrastructure and CORBA services, whereby there is a definitive order of failover from the Runtime Service to Entrust GetAccess server, and from one Entrust GetAccess server to another. You may also configure failover if you have multiple instances of a particular CORBA service residing on the same machine. You can specify the order in which client machines should connect to each instance of the CORBA service.

Failover is achieved by grouping machines and service instances into nodes and clusters. A node usually refers to a machine, but can also be assigned to any of the following:

- an instance of a CORBA service
- a group of CORBA service instances
- a group of machines

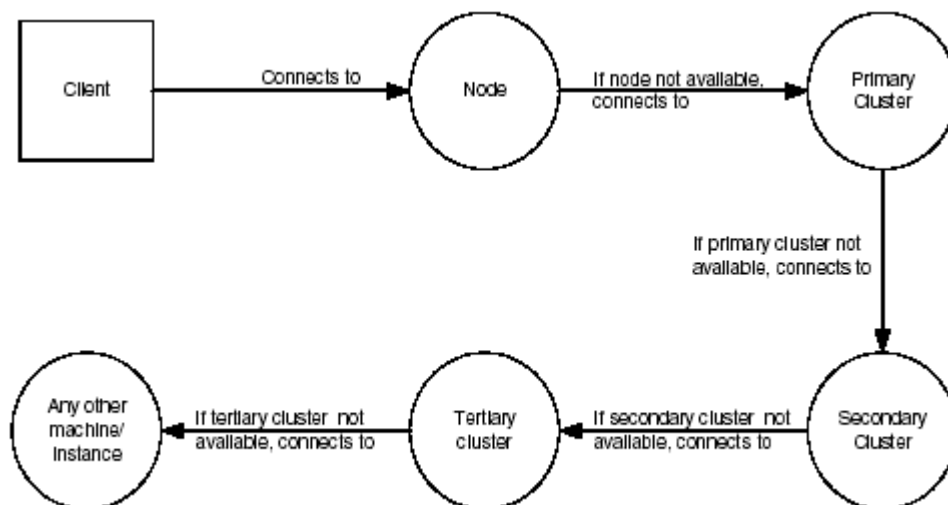
A cluster is a group of nodes. If a node refers to a machine, then a cluster is a group of machines. Clusters, like nodes, are defined in the Entrust GetAccess centralized configuration file.

When you group machines or instances into nodes and clusters, failover can then occur. A client machine attempts to connect to machines or instances in its own node. If no working machines or instances are found in its own node, it connects to:

- machines or instances in its own cluster. If no working machines or instances can be found in its own cluster, then it will connect to
- machines or instances in a secondary cluster. If no working machines or instances can be found in the secondary cluster, then it will connect to
- machines or instances in a tertiary cluster. If no working machines or instances can be found in the tertiary cluster, then it will connect to
- any other available machines or instances.

There is no limit to the number of secondary or tertiary clusters you can configure. If you have multiple tertiary clusters, connections to them are made in no particular order.

The failover process is illustrated below.



**Figure 9 - Entrust GetAccess Failover Process**

Entrust GetAccess offers added flexibility to configure the time that a machine (which has failed over to a cluster other than its own) waits before attempting to reconnect to the service in its own node or cluster,

as well as the time the Runtime Service waits before attempting to reconnect to any services if no services are available in any node or cluster.

## ***Performance and Scalability***

When considering the behavior of systems under peak load, there are two critical axes against which to measure the suitability of a given solution, performance and scalability.

**Performance** refers to how fast your system can respond to user requests. A system with good performance must have sufficient hardware (such as the CPU, hard disk, RAM) and must be scalable. Entrust GetAccess software has been proven to perform at the high levels the market demands (multi-million active user deployments). Indeed, it meets and exceeds the requirements of many million-user B2C portals currently deployed on the Internet.

**Scalability** refers to the ability of a system to use all available hardware effectively so that performance is optimized. A scalable system allows:

- Fluctuating waves of client requests to be handled without a major difference in performance. In high-volume real-world deployments, Entrust GetAccess software has demonstrated that it can handle spikes of activity gracefully. Inbound requests, if they exceed hardware limitations, are queued and handled as resources become available. No administrator intervention is needed.
- Administrators to add hardware or software to handle more client requests to the site. In independent benchmarks, Entrust GetAccess software has consistently been shown to be “linear” in scale. That is, the system is purely hardware bound, and performance can be improved in a measurable and predictable manner by adding additional hardware resources.

## **VI. Complementary Entrust Products and Solutions**

Entrust GetAccess serves as the foundation for deploying several other Entrust offerings, which can add increasing value to a Secure Web Portal deployment.

### ***Entrust Certificate Services:***

Entrust Certificate Services offers Web and WAP server certificates that provide the first step of Internet security and helps to enable e-commerce on the Internet. SSL Web server certificates identify a Web site and enable encrypted communications through SSL (Secure Socket Layer) for online transactions. SSL certificates protect businesses against site spoofing, data corruption and provide customers with information about the Website that they are communicating with. For more information on Entrust Certificate Services visit [http://www.entrust.com/certificate\\_services/index.html](http://www.entrust.com/certificate_services/index.html)

### ***Entrust TruePass***

Entrust TruePass can be easily integrated with Entrust GetAccess to provide strong authentication, digital signatures and end-to-end encryption. Entrust TruePass is a “zero footprint” client application that is easy to administer and manage. For more information on Entrust TruePass visit [www.entrust.com/products/truypass.html](http://www.entrust.com/products/truypass.html).

## ***Entrust GetAccess Mobile Server***

Entrust GetAccess software was the first product to provide mobile access capabilities with the delivery of the Entrust GetAccess Mobile Server in December 2000. The Mobile Server plugs into an Entrust GetAccess environment and allows users to access the same applications and services that they can with a browser, but by using wireless devices such as PDAs and cell phones. For more information on Entrust GetAccess Mobile Server visit [www.entrust.com/getaccess/mobile/index.htm](http://www.entrust.com/getaccess/mobile/index.htm).

The Mobile Server continues to be offered by Entrust today and has been deployed into production environments by many customers in North America, Europe, and Asia.

## ***Entrust GetAccess Proxy Server***

The Entrust GetAccess software provides support for Apache proxy capabilities out-of-the-box. However, for added value, Entrust also offers the Entrust GetAccess Proxy Server. The Entrust GetAccess Proxy Server provides the same capabilities as the Apache proxy, in addition to:

- A full featured proxy server itself not requiring other 3<sup>rd</sup> party proxy servers
- Delivers full GUI-based operational control for administration and management
- Provides trace-level security and performance logging
- Built-in load balancing of proxied applications
- Added security capabilities, such as turning proxying on/off for a particular server with one button, detecting which proxied servers are no longer responding, configuring customizable “Unavailable” pages, and checking for “bad” HTTPs

For more information on Entrust GetAccess Proxy Server visit [www.entrust.com/getaccess/proxy/index.htm](http://www.entrust.com/getaccess/proxy/index.htm).

## ***Entrust Secure Transaction Platform***

The Entrust Secure Transaction Platform (STP) provides security services, as Web services, for applications. These services are based on XML and **SAML standards**, and are thus interoperable into Web services environments. This product includes the following modules:

- Identification Server – SAML authentication and attribute assertions; it is a plug-in to Entrust GetAccess (allows you to programmatically authenticate subjects and determine subject attributes)
- Entitlements Server – SAML authorization assertions; plug-in to Entrust GetAccess (allows you to programmatically permit/deny access to resources)
- Verification Server – time stamping and digital signatures
- Privacy Server – encryption capabilities

Additionally, Entrust Secure Transaction Platform will provide application server runtimes. These are plug-ins for BEA WebLogic and IBM WebSphere application servers to protect **Enterprise Java Beans (EJB) and method levels** using Entrust GetAccess capabilities. For more information on Entrust STP visit [www.entrust.com/stp/index.htm](http://www.entrust.com/stp/index.htm).

## ***Entrust Secure Identity Management***

The Entrust Secure Identity Management Solution can increase security, improve productivity and lower the cost of your operations by enabling you to:

- have complete visibility into user access privileges across multiple applications
- enforce policy consistently and automatically across applications, platforms and user communities
- streamline user provisioning and enable user self-service
- improve quality and speed of service to users
- increase reliability and accuracy of identity information in all applications
- deploy quickly with minimal impact on your current environment

Using Entrust GetAccess as part of the Secure Identity Management Solution enables one identity and security profile across the entire infrastructure, identity management, provisioning, workflow, auditing and reporting capabilities. For more information on Entrust Identity Management visit [www.entrust.com/identity\\_management/index.htm](http://www.entrust.com/identity_management/index.htm)

## VII. Summary

The Entrust GetAccess™ portfolio delivers a single entry and access point for user authentication and authorization across Web portal applications. Supporting a broad range of authentication methods, and user devices available today, Entrust GetAccess makes it possible for organizations to personalize services, and secure identities, content and data for the diverse needs of a varied user community.

Entrust GetAccess is unique in delivering enterprise-scale performance without sacrificing security. Moreover, as the foundation of the [Entrust Secure Web Portal](#) solution, it can be combined with Entrust TruePass software to provide organizations with the confidence to conduct sensitive and high-value transactions through a portal.

Entrust GetAccess software delivers the following key services:

- One identity and security profile across the entire infrastructure, identity management, provisioning, workflow, auditing and reporting capabilities.
- Flexible authentication, including enhanced identification with the Entrust® TruePass™ product portfolio
- Single Sign-on (SSO) to Web and non-Web applications
- Authorization including fine-grained access control to online resources
- Centralized session management including support for idle and session timeouts, and real-time user revocation
- Easy Administration and Deployment with N-level delegation administration, rules-based access
- Open and interoperable based on industry standards
- Personalization of content, enhancing user's online experience
- Integration with leading application and portal vendors

For more information on Entrust GetAccess products:

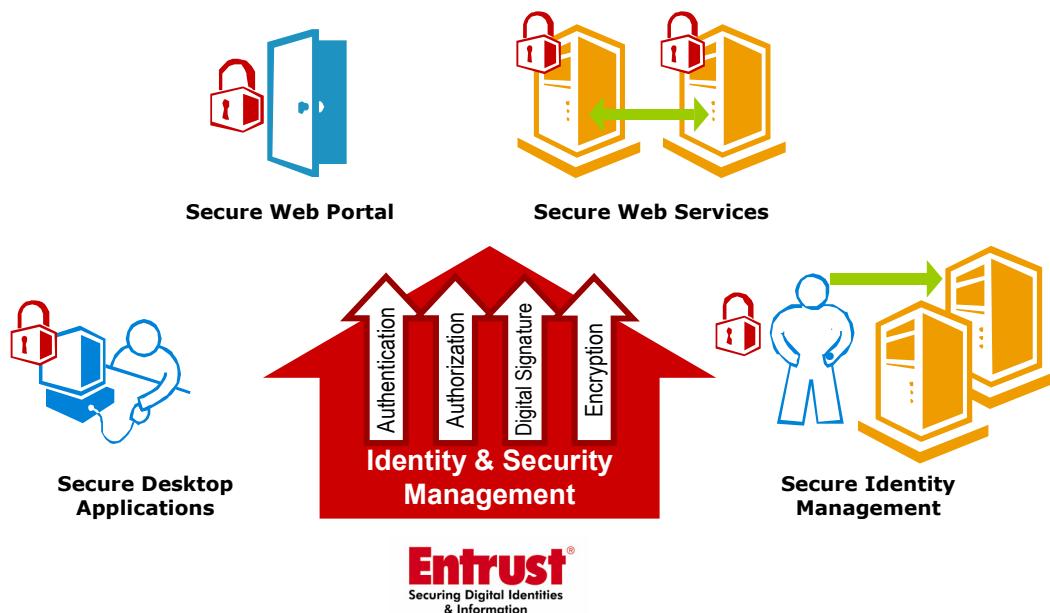
[www.entrust.com/getaccess/index.htm](http://www.entrust.com/getaccess/index.htm)

**North America: 1-888-690-2424**

**Europe: +44 (0) 118 902 2098**

## VIII. About Entrust

**Overview:** Entrust, Inc. [Nasdaq: ENTU] is a world leader in securing digital identities and information, enabling businesses and governments to transform the way they conduct online transactions and manage relationships with customers, partners and employees. Entrust's solutions promote a proactive approach to security that provides accountability and privacy to online transactions and information. The company's portfolio of solutions provides security for the broad range of technologies organizations are using today, and planning to use tomorrow including: desktop applications (e-mail, e-forms, files/folders, VPNs and Wireless LANs), Web portals, Web services and Identity Management. Over 1,200 enterprises and government agencies in more than 40 countries use Entrust's security solutions, and most recently, both the U.S. Government and the Canadian Government purchased Entrust solutions to secure their network environments. For more information, please visit [www.entrust.com](http://www.entrust.com) or call 1-888-690-2424.



**Awards & Innovation:** Entrust is recognized as a leading innovator in the field of Internet security, with over 90 patents and pending patent applications; its employees are authors, visionaries, and drivers on more than 30 industry standards boards and forums. In addition, Entrust was the first security mover to recognize the value of combining authorization technology with Public-Key Infrastructure (PKI) and to extend this value with XML, wireless devices and other innovations. These actions have led to an industry-leading 40 percent share<sup>1</sup> of the PKI software market. Entrust currently has over 500 employees worldwide. The global corporate headquarters of Entrust, Inc. is located in Addison, Texas, with U.S. offices in Virginia, New York and California. Research and development facilities are located in Santa Clara, California and Ottawa, Canada.

<sup>1</sup>Gartner Dataquest, October 2002