



Robust authentication and flexible Web Single Sign On

Logon access : a critical application requirement

From where the user stands an application's performance is directly related to criteria such as how fast it processes requests and how simple it is to access and use. Authentication, however, becomes more and more complex with the proliferation of applications on a network, each with its own ID controls and user repositories.

With all users in an organisation needing to remember multiple usernames and passwords, there are huge costs and risks for the administration and support departments - accounts must be set up in each application for each employee, users forget passwords and sometimes access accounts that are not their own, support personnel have to deal with multiple requests to reset forgotten passwords.

A simple and consistent mechanism to improve productivity and security

The innovative idea introduced by Bee Ware is to centralise and run authentication on the network perimeter, using the application gateway as a primary Authentication Control Point.

This architectural paradigm eliminates the need to assign diverse authentication schemes, some weaker than others, to heterogeneous applications running within a shared corporate environment.

Benefits

- **Assurance**
Reinforced security with a unique entry point for all applications
- **Flexibility**
Plugs in to existing application infrastructure saving on time and costs
- **User satisfaction**
Simplified authentication through Web Single Sign On
- **Simplified Administration**
Reduced account management burden and reduced risk



All members across the organisation feel the benefits :

- Heads of service can implement their own access policy, and are not forced to comply with the standard access levels imposed by applications
- Operators spend more quality time supervising a unified access point
- End-Users experience less frustration and use applications better

i-Trust, business confidence through trusted application delivery.

contact@bee-ware.net • www.bee-ware.net

About Bee Ware:

Bee Ware is the leading provider of appliance based secure web enabled delivery solutions. Built to open standards, Bee Ware's award-winning products ensure security, high performance and business continuity for the world's most demanding organisations.





Ease of use

By focusing on web applications and introducing a breakthrough level of automation with our Self-Learning mechanism, Bee Ware has designed a simple solution, requiring minimal effort from users and adding no extra workload for operators.

SIMPLE TO SET UP

i-Trust is quick and easy to set up. It can either use an existing account directory (LDAP, Radius...) or build its own internal directory by importing data. User accounts previously managed by the applications themselves are seamlessly synchronised via the Self-Learning facility included in i-Trust.

SIMPLE TO RUN

General maintenance and system monitoring are also made easier with i-Trust. The Self-Learning mechanism allows for automatic synchronisation of passwords between applications and the central base, making all fastidious administrative intervention unnecessary.

i-Trust + i-Sentry

i-Trust WSSO can work as a standalone or in module mode as a complement to i-Sentry web application firewall. The complete product offering is a global security management solution enabling resistance to attacks, detection of application vulnerabilities, granular object-oriented access policy, improved performance and reinforced, unified authentication.

Specifications

Range of 6 models of varying performance
 Secure 1U or 2U Appliance
 SSL Acceleration
 Web Management (SSL)
 SNMP and Syslog Supervision
 High Availability (optional)

Features

• Perimeter Authentication

- Login / Password Form
i-Trust internal account database
- X.509 Client Authentication
External PKI or internal LDAP / RADIUS
- LDAP Authentication
External LDAP directory
- Third party Authentication support
RSA SecurID - Elcard...
- RADIUS Authentication
External RADIUS account database
- GIP CPS Authentication
French Health Professional Card

• Application Authentication

- HTTP Basic, DIGEST, NTLM
- HTML Form
- Configurable Headers



How it works

- 1 The i-Trust agent situated on the application gateway intercepts the user's request to log on. Up to the moment of authentication the user can neither access nor view any application servers.
- 2 The i-Trust authentication server obtains user credentials (from an internal or external account database) and runs the perimeter access control process, applying the authentication model defined by the organisation (as opposed to the application-based model).
- 3 Using the retrieved credentials the i-Trust server seamlessly conducts one or several application authentications. In this way it respects the application organisation already in place.

Following this unified and secure authentication on the network perimeter via the application gateway, the end-user gains access to all his applications.

