

IFS APPLICATIONS™ 7 SECURITY

**WHITE
PAPER**

IFS APPLICATIONS™ 7 SECURITY

This document is an excerpt from the architecture and technology white paper describing security in IFS Applications 7. It is written for an audience familiar with software, Internet, and business application architecture concepts.

Security

Business applications contain vast amounts of information that is critical to your business, and much that is sensitive or secret. Protecting this information from unauthorized access, tampering, destruction and other malicious behavior remains imperative.

A decade or two ago, IT security was much about controlling system access and backing up data to prevent information loss in the event of system failure or physical destruction such as fire. With the growth of local area networks, wide area networks and later the Internet, focus shifted toward network security. Organizations have since run a tight race against intruders to install firewalls, encryption, virus scanners, and other technologies to protect corporate networks and resources from penetration and sabotage.

As networks are becoming more secure, intruders turn their attention to the applications that run on them. Recent years have seen waves of e-mail viruses and numerous penetrations of well-known web sites. It should be expected that sooner or later similar attention will be paid to business applications. Authorities are also turning up the regulatory pressure on fraud prevention and accountability. Legislation such as the Sarbanes-Oxley Act (SOX) puts a spotlight on the ability of business applications to support segregation of duties, logging, and non-repudiation.

IFS Applications is built on the principle of “secure by design and secure by default” to prevent application vulnerabilities. Security is enforced at the architecture and framework levels, minimizing the risk of vulnerabilities being introduced through the oversight of individual developers. In addition the Foundation1 platform provides a rich set of security services and tools leveraged by IFS Applications and IFS’ customers to implement appropriate security practices.

When it comes to network security, IFS firmly believes in the use of widespread and proven security solutions over home-made “security by obscurity” technology. IFS also believes that security concepts and the underlying application architecture must be easy to understand and consistently implemented to enable organizations to properly configure the right security. In IFS Applications security is built in—not an afterthought.

Secure by design and secure by default

To preempt security vulnerabilities, IFS Applications is “secure by design and secure by default”.

Any designs that might affect the security properties of IFS Applications are reviewed by security experts. Questionable designs are rejected in favor of designs whose security implications are easily understood and allow a strong security regime to be implemented. IFS Applications is also designed to prevent exploitation of vulnerabilities that are known to potentially exist in business applications. For example, IFS Applications has built-in protection against SQL injection, session theft, cross-site scripting, and other common vulnerabilities presented by the Open Web Application Security Project (OWASP) and others. Secure by design also means minimizing the damage should a system be penetrated. With this in mind all sensitive data in configuration files are encrypted, so if a web server is compromised, an attacker will not find plain-text passwords or similar that would help further the attack.

Because not all organizations have the same security requirements, there is sometimes a tradeoff between the highest security, ease of use, and cost. Many aspects of IFS Applications can be configured with different implications for security and convenience. For such configurations, the more secure option is always default. This means that initially IFS Applications runs in a “clamped down” mode, and it is up to each organization to enable the additional features or configurations.

Authorization and segregation of duties

IFS Applications uses a role-based authorization system, which allows clear segregation of duties, including administrative duties, between users. Depending on the duties to be performed, a user is assigned one or more permission sets. Each permission set details exactly what information and functionality may be viewed, updated, or used. Permission sets can also include other permission sets, making it possible to create rights structures of arbitrary depth.

Strong security while maintaining ease of use is achieved through server-enforced permissions with an adaptive user interface. As permissions are set, IFS Applications also grants and revokes the physical software objects, such as database views, that correspond to the permissions. This assures that permissions are enforced even if users access the database directly using 3rd party tools. The user interfaces adapt to reflect what permissions the user has, hiding screens, fields, menu items, etc. that are not available to the user. This helps users focus on the duties they are supposed to perform without getting distracted by things they cannot perform.

A built-in history log function is available to track any modification or removal of data done by users. The log stores information about who made the change, when and where, and records old and new values. Together with security checkpoints that force users to re-authenticate themselves when “electronically signing” certain transactions, the history log is a powerful tool for enforcing accountability and non-repudiation.

Grant Permission Set to User		APPROVE_EQUIPMENT_AQUISITION	APPROVE_EQUIPMENT_LOSS	CONDUCT_EQUIPMENT_INVENTORY	MAINTAIN_EQUIPMENT	REPORT_EQUIPMENT_LOSS
Permission Sets						
Users						
+ Department Managers		<input checked="" type="checkbox"/>				
- Jacques Villeneuve			<			
Magne Salesman			<			
- Engineers						
Scott Epping			<	<		
Scott McGraw			<			
Terje Oftedal			<			
- Alain Leveaux				<	<	
Anders Blom				<	<	
Gavin DeGrave				<	<	
Harald Svensrud				<	<	
Ingrid Argenius				<	<	
- Mechanics						
Jakob Heinemann				<	<	
Perry Como				<	<	
Per Öquist				<	<	

Open and flexible network security

The most important aspect of network security is the use of well-known technologies that have been proven in real-life applications over long periods of time. IFS Applications is built using established technologies with known security properties, including Oracle database, J2EE application servers, Apache and IIS web servers, Active Directory, LDAP, JAAS, Http, SSL, and PKI. Because IFS Applications relies on standards, it can be used with network level security solutions such as firewalls, proxies, and hardware security modules (HSM). De-militarized zone (DMZ), hardened perimeter defense, and other firewall strategies can all be used.

IFS WHITE PAPER
IFS APPLICATIONS 7 SECURITY

IFS Web Client and all integrations leverage JAAS for user authentication, which means that IFS Applications can leverage login modules provided with the application server used (IBM WebSphere, Oracle Application Server, or JBoss), as well as compatible 3rd party modules. In addition IFS also provides an optional login module for the Oracle database, allowing Oracle database user accounts to be used also for authentication of web users.

Security between servers, for example from IFS Connect or IFS Mobile Server to the application server, uses the same unified security model as normal users—each server needs to log on as with a user account present in the chosen directory (Active Directory, LDAP, Oracle). This provides effective protection against forged servers.

This is an excerpt from the IFS Applications 7 Architecture and Technology White Paper

About IFS

IFS, the global enterprise applications company, provides solutions that enable organizations to respond quickly to market changes, allowing resources to be used in a more agile way to achieve better business performance and competitive advantage.

IFS was founded in 1983 and now has 2,600 employees worldwide. IFS has pioneered component-based enterprise resources planning (ERP) software with IFS Applications™, now in its seventh generation. IFS' component architecture provides solutions that are easier to implement, run, and upgrade. IFS Applications is available in 54 countries, in 20 languages.

IFS Applications provides extended ERP functionality, including supply chain management (SCM); enterprise asset management (EAM); maintenance, repair, and overhaul (MRO); product lifecycle management (PLM); customer relationship management (CRM); and corporate performance management (CPM) capabilities.

IFS has over 500,000 users across seven key vertical sectors: aerospace & defense, automotive, high-tech, industrial manufacturing, process industries, construction & facilities management, and utilities & telecom. IFS also provides a cross-industry solution for Retail & Wholesale Distribution.

More details can be found at www.ifsworld.com. For further information e-mail info@IFSWORLD.com

www.IFSWORLD.com

This support offer has been made in order to respond to the requirements of IFS' customers. Since the customers' requirements may be different in some markets, variations of this offer may exist.

IFS and all IFS product names are trademarks of IFS. The names of actual companies and products mentioned herein may be the trademarks of their respective owners. The example companies, organizations, products, domain names, email addresses, logos, people and events depicted herein are fictitious.

No association with any real company, organization, product, domain name, email address, logo, person or event is intended or should be inferred.

This document may contain statements of possible future functionality for IFS' software products and technology.

Such statements of future functionality are for information purposes only and should not be interpreted as any commitment or representation.