

## Security and Compliance in InTrust for Databases 2.2

*An Overview*  
*December 11, 2007*

---

---

## Security and Compliance in InTrust for Databases 2.2

1	Introduction.....	3
2	About InTrust for Databases.....	3
3	Security Features in InTrust for Databases.....	4
3.1	Role Based Access Control.....	4
3.2	User Authentication and Password Policies .....	4
3.3	Required Privileges.....	4
3.4	Protection of Stored Data.....	4
3.5	Protection of Communicated Data.....	5
3.6	Network Ports .....	5
3.7	Configuration Management .....	5
3.8	Audit Log .....	5
3.9	Log File.....	6
3.10	Verification of Input .....	6
3.11	Integrity of Collected Data.....	6
3.12	Integrity of Software.....	6
3.13	Uninstalling InTrust for Databases .....	6
3.14	Maintenance.....	7
3.15	IPv6.....	7
3.16	Daylight Savings Time Extension .....	7
4	Customer Measures.....	7
5	Disclaimer.....	7
	Appendix A: InTrust for Databases and FISMA Compliance.....	8
5.1.1	NIST 800-53 Categories .....	9

# 1 Introduction

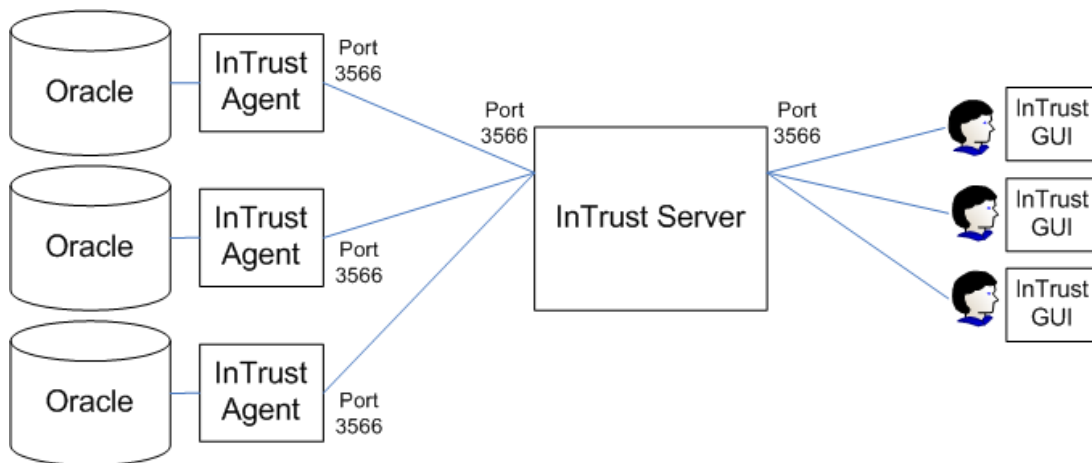
Managing the security of information systems is a matter of great priority for every organization. Indeed, the level of security provided by software vendors has become a differentiating factor for IT purchase decisions. Quest Software strives to meet standards designed to provide its customers with their desired level of security, whether it relates to privacy, authenticity and integrity of data, availability, or protection against malicious users and attacks.

This document describes the security features of Quest Software’s InTrust for Databases. The document covers access control, protection of customer’s data, secure network communication, and more. This document also includes an appendix describing how to evaluate InTrust for Databases’ security features in connection with the NIST recommended federal information security standards promulgated under the Federal Information Security Management Act (FISMA).

# 2 About InTrust for Databases

InTrust for Databases is a database audit management system that is designed to provide maximum visibility into your database activities and confidence that your data assets are secure.

The product consists of three main components: the Server, the Agents, and the GUI applications. An Agent is installed on an Oracle server and communicates its captured data to the Server. Users interact with the product through their GUI applications which connect to the Server. Figure 1 gives an overview of the InTrust for Databases components.



**Figure 1.** Overview of interaction between InTrust for Databases components

## 3 Security Features in InTrust for Databases

Below follows a set of security features provided by InTrust for Databases.

### 3.1 Role Based Access Control

InTrust for Databases enforces role-based access control (RBAC). Three types of users are defined: `admin`, `operator` and `user`. An individual can only be assigned one user type.

An `admin` can operate InTrust for Databases in terms of installation, updating, configuration and user management. An `admin` accesses the product through an administration console, which differs from the user console. `admin` users cannot view data captured by InTrust for Databases.

An `operator` has authority to manage profiles and policies—including their creation, modification and deletion. An `operator` can also create instances to be monitored, which involves selecting a database to monitor and an archive in which to store the captured data. In addition, an `operator` has the same operational access as a `user`.

A `user` is able to view captured data and policies. A `user` cannot make any modifications to policies or configuration settings.

In addition to enforcing RBAC described above, InTrust for Databases provides a ticketing workflow. Tickets may be triggered based on policies. Two authoritative roles are associated with tickets: `investigator` and `approver`. An `investigator` can review tickets and propose ticket actions (e.g., closure of a ticket). An `approver` can approve or reject suggested ticket actions. Both an `operator` and a `user` can have the `investigator` and/or `approver` roles.

### 3.2 User Authentication and Password Policies

Only `admins` can perform user management, including creation of new user accounts. InTrust for Databases bases its authentication upon username and passwords. The `admin` console is used for user management. No password strength policy is enforced.

### 3.3 Required Privileges

The Server and Agent components of InTrust for Databases both require administrative privileges to install and run. This means that the user is required to be part of the Local Administrator group on Windows and have root access in Linux/Unix. On Windows the Server is installed to run as a service.

### 3.4 Protection of Stored Data

The data captured by InTrust for Databases is processed and stored on the server. Some of the data is stored in a database and some in the file system. The SQL text, stripped from any literal and constant values, is stored in a file within the InTrust for Databases directory in the file system on the server. Fields such as the table and column names are included in the SQL text. The contents of this file are not encrypted.

The full SQL statements, including the literals and constants, are stored in a file within the same InTrust for Databases directory. The confidentiality of the file's data is ensured by encrypting the contents with AES (Advanced Encryption System) with a 256-bit key. The key is generated based on a combination of system parameters, as well as key phrase. This key phrase is entered by an operator during creation of an instance (when specifying the archive used for storage). AES is on the FIPS 140-2 list of approved cryptographic algorithms. InTrust for Databases uses the OpenSSL library for its cryptographic functions.

### **3.5 Protection of Communicated Data**

There are two main channels of communication within InTrust for Databases, both of which are protected in the same way. These two channels are (1) the communication between the agent (on the monitored database server) and the InTrust for Database server, and (2) the user or admin console and the InTrust for Database server. The components authenticate each other via a Diffie Hellman exchange, during which a 256-bit AES key gets established. The Diffie Hellman 1024-bit public modulo is stored within each InTrust for Database component. New random exponents are generated for each new round of communication between components. Upon successful authentication, the components encrypt the communicated data with AES. The generated AES keys are therefore ensured to be unique and new.

### **3.6 Network Ports**

Port 3566 is reserved for Quest product communication and has been registered with IANA (Internet Assigned Number Authority), and the port is recognized as Quest Software by various network monitoring tools. A different port number can be specified during installation.

### **3.7 Configuration Management**

There is a separation of duties when it comes to managing and configuring InTrust for Databases. An `admin` is authorized to perform installation activities and user account management. An `operator` is authorized to manage policies and instances. A `user` is not authorized to perform configuration changes at any level.

Configuration management activities related to profiles and policies are recorded, versioned and logged in audit files. Each file's history can later be viewed to identify when changes took place, the version numbers for each change and the previous values or settings that were modified.

### **3.8 Audit Log**

InTrust for Databases keeps multiple types of audit logs. All changes to profiles and policies (by operators) are versioned and stored in these logs. Each audit log entry contains the information fields "When," "Version Number," and "New Policy." The "When" shows when the modification occurred. The "Version Number" associates each log entry with its own number. The "New Policy" field describes the new version of the

modified policy, including the new parameter values. The policies audit log also contains the “Who” field, which identifies the username of the operator who modified the policy. Both the profile and policy audit logs are viewable via the user console by both operators and users.

### **3.9 Log File**

A separate log is used to record actions performed by `admins`, such as installation management, and starting and stopping the server component. These log records are stored in log files within the InTrust for Databases directory in the file system on the server and are protected via file-level access control.

### **3.10 Verification of Input**

InTrust for Databases verifies user input by validating its data type and length. For example, no text characters will be accepted in a field that accepts only numeric characters. Passwords are masked with asterisks during input.

### **3.11 Integrity of Collected Data**

A similar approach to the one described above is used to ensure the integrity of collected data. All data collection files are populated with timestamps at one-second intervals. These timestamps are received from the remote collector (agent) and provide evidence of when the collection occurred. Each data collection file also contains an HMAC in the file header that represents an integrity checksum for the file’s contents. All files are encrypted with AES 256 (as described in the “System and Communications Protection” section) in order to protect confidentiality and prevent tampering. Upon decryption, the HMAC checksum is verified for accuracy to provide proof of integrity.

### **3.12 Integrity of Software**

InTrust for Databases protects the integrity of both its software and the data it collects during operation in the following way. All software files contain HMAC checksums (keyed-hashed messages authentication code) in their file headers. These HMAC digests are based on the MD5 hash algorithm. The HMAC digests are, in turn, signed with the InTrust for Databases self-signed RSA (private) key. The RSA verification key (public portion) is contained within the InTrust for Databases code and is used to validate RSA signatures when a software file is loaded by the packet manager. Upon validation, the HMAC digests are verified for accuracy. Should this verification step fail, the package manager will display an alert message.

### **3.13 Uninstalling InTrust for Databases**

The options for uninstalling both the InTrust for Databases Agent and Server are the same. The customer can choose between a complete or partial uninstall. During a partial uninstall, only the InTrust for Databases components are removed, while the Quest Software framework on which the components are built upon remain. The partial uninstall option should be used if the customer plans on re-installing the product in the future.

### **3.14 Maintenance**

InTrust for Databases releases patches that you can use to update your instance of the product. Patches are distributed as packages of files. Each file within a package, as well as the package itself, contain an HMAC checksum (keyed-hashed message authentication code), which in turn is digitally signed with an InTrust for Databases self-signed RSA key. The public (verification) RSA key is contained within InTrust for Databases and permits verification of the authenticity and integrity of the package and files therein, preventing rogue code from being loaded. All files within a package are identified by the version number of the patch.

### **3.15 IPv6**

The current release is not IPv6 compliant.

### **3.16 Daylight Savings Time Extension**

InTrust for Databases is not affected by the changes introduced by the Daylight Savings Time (DST) Extension (U.S. Energy Policy Act of 2005). It relies upon the Operating System for time management and does not implement any special logic around DST settings.

## **4 Customer Measures**

The security features of InTrust for Databases are only one part of a secure environment. The customer's operational and policy decisions will have a great influence upon the overall level of security achieved. In particular, the customer is responsible for the physical security of the InTrust for Databases and the security of the network from which the InTrust for Databases is accessible. Administrators should also change default passwords and replace them by strong passwords.

## **5 Disclaimer**

While efforts have been made by Quest to ensure that the information provided in this document is accurate, Quest makes no representation about the content and suitability of this information for any purpose. This information may be modified by Quest at any time. Nothing contained herein shall be construed as a warranty, express or implied, regarding the operation of Quest's products.

## Appendix A: InTrust for Databases and FISMA Compliance

The Federal Information Security Management Act<sup>1</sup> (FISMA) was passed by the U.S. Congress and signed by the U.S. President, and is part of the Electronic Government Act of 2002. It requires “each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information system that support the operations an assets of the agency, including those provided or managed by another agency, contractor, or other source.”

A major component of FISMA implementation is the publication by the National Institute of Standards and Technology (NIST), entitled “*Recommended Security Controls for Federal Information Systems*”, listed as NIST Special Publication 800-53<sup>2</sup>. This document lists 17 general security categories against which an information security control program should be evaluated, so as to measure its level of compliance with an agency’s obligations under FISMA. Quest Software wishes to provide its customers with enough information regarding security aspects of InTrust for Databases to enable them to perform their own evaluation of how InTrust for Databases fits in with their desired FISMA compliance levels. In this appendix we list the 17 categories listed in 800-53 and describe how InTrust for Databases addresses those that apply.<sup>3</sup>

We should emphasize that the secure deployment of InTrust for Databases forms only one part of an information security program. A statement in this appendix that a particular security category is “applicable” to InTrust for Databases means only that InTrust for Databases contains security features that are or may be relevant to some or all aspects of the security category in question. It does not necessarily mean that InTrust for Databases fully meets all of the requirements described in that security category, or that the use of InTrust for Databases by itself will guarantee compliance with any particular information security standards or control programs. Indeed, the selection, specification, and implementation of security controls in accordance with a customer-specific security program is ultimately dependent upon the manner in which the customer deploys, operates, and maintains all of its network and physical infrastructure, including InTrust for Databases.

### 5.1.1 NIST 800-53 Categories

<b>Category:</b>	Access Control (AC)
<b>Applicable:</b>	Yes
<b>Description:</b>	InTrust for Databases enforces role-based access control (RBAC). Three types of users are defined: admin, operator and user. An individual can only be assigned one user type.  In addition to enforcing RBAC described above, InTrust for Databases provides a ticketing workflow. Tickets may be triggered based on policies.
<b>Further Details:</b>	Section(s) 3.1
<b>Category:</b>	Awareness and Training (AT)
<b>Applicable:</b>	Yes
<b>Description:</b>	Quest Software offers Professional Services to support implementation of InTrust for Databases. This offering includes training on how to best use the product to fit unique needs. It also includes assistance with you adjusting configuration settings, setting up profiles and policies, viewing audit and log history, and examining collected data.
<b>Further Details:</b>	N/A
<b>Category:</b>	Audit and Accountability (AU)
<b>Applicable:</b>	Yes
<b>Description:</b>	InTrust for Databases keeps multiple types of audit logs. All changes to profiles and policies (by operators) are versioned and stored in these logs. A separate log is used to record actions performed by admins, such as installation management, and starting and stopping the server component.
<b>Further Details:</b>	Section(s) 3.8, 3.9
<b>Category:</b>	Certification, Accreditation and Assessments (CA)
<b>Applicable:</b>	No
<b>Description:</b>	This category is not relevant to InTrust for Databases, since it is your responsibility to install the product as well as develop and review your own security assessment, accreditation and certification policies.
<b>Further Details:</b>	N/A
<b>Category:</b>	Configuration Management (CM)

<b>Applicable:</b>	Yes
<b>Description:</b>	There is a clear separation of duties when it comes to managing and configuring InTrust for Databases, enforced via role based access control. Configuration management activities related to profiles and policies are recorded, versioned and logged in audit files.
<b>Further Details:</b>	Section(s) 3.1, 3.8, 3.9
<b>Category:</b>	Contingency Planning (CP)
<b>Applicable:</b>	Yes
<b>Description:</b>	InTrust for Databases can generate archives containing discrete ranges of audit data. This data supports effective and efficient recovery if there is any disruption to the IT systems such as a power-outage, or equipment damage caused by natural disasters or terrorist attacks. These archives ensure that appropriate sets of audit data are available as specified in your contingency plans.
<b>Further Details:</b>	N/A
<b>Category:</b>	Identification and Authentication (IA)
<b>Applicable:</b>	Yes
<b>Description:</b>	Only <code>admins</code> can perform user management, including creation of new user accounts. InTrust for Databases bases its authentication upon username and passwords. The admin console is used for user management. No password strength policy is enforced.
<b>Further Details:</b>	Section(s) 3.2
<b>Category:</b>	Incident Response (IR)
<b>Applicable:</b>	No
<b>Description:</b>	This category is not relevant to InTrust for Databases, since it is your responsibility to install the product as well as develop and review your own incident response policies and procedures.
<b>Further Details:</b>	N/A
<b>Category:</b>	Maintenance (MA)
<b>Applicable:</b>	Yes
<b>Description:</b>	InTrust for Databases releases patches that you can use to update your instance of the product. Patches are distributed as packages of files which contain HMAC checksums to provide proof of integrity and authenticity.
<b>Further Details:</b>	Section(s) 3.14
<b>Category:</b>	Media Protection (MP)
<b>Applicable:</b>	No

**Description:** This category is not relevant to InTrust for Databases, since it is your responsibility to install the product as well as develop and review your own media protection policy.

**Further Details:** N/A

**Category:** Physical and Environmental Protection (PE)

**Applicable:** No

**Description:** This category is not relevant to InTrust for Databases, since it is your responsibility to install the product as well as develop and review your own physical and environmental policy.

**Further Details:** N/A

**Category:** Planning (PL)

**Applicable:** No

**Description:** This category is not relevant to InTrust for Databases, since it is your responsibility to install the product as well as develop and review your own security planning policy.

**Further Details:** N/A

**Category:** Personnel Security (PS)

**Applicable:** No

**Description:** This category is not relevant to InTrust for Databases, since it is your responsibility to install the product as well as enforce your own personnel security policies, including personnel screening and termination.

**Further Details:** N/A

**Category:** Risk Assessment (RA)

**Applicable:** No

**Description:** This category is not relevant to InTrust for Databases, since it is your responsibility to install the product as well as develop and review your own risk assessment policy.

**Further Details:** N/A

**Category:** System and Services Acquisition (SA)

**Applicable:** No

**Description:** This category is not relevant to InTrust for Databases, since it is your responsibility to install the product as well as develop and review your own system and services acquisition policy.

**Further Details:** N/A

**Category:** System and Communications Protection (SC)  
**Applicable:** Yes  
**Description:** The data captured by InTrust for Databases is processed and stored in multiple locations. The AES encryption algorithm is used to protect the contents of flat files which contain full SQL statements.

There are two main channels of communication within InTrust for Databases, both of which are protected in the same way. Components authenticate each other via a Diffie Hellman exchange, abased upon a 1024-bit modulo, which also establishes a 256-bit AES key. Upon successful authentication, the components encrypt the communicated data with AES.

InTrust for Databases uses the OpenSSL cryptographic library for its cryptographic functions.

**Further Details:** Section(s) 3.4, 3.5

**Category:** System and Information Integrity (SI)  
**Applicable:** Yes  
**Description:** InTrust for Databases verifies user input by validating its data type and length. The integrity of both its software and the data it collects during operation is ensured through the use of keyed-hashed message authentication codes.

**Further Details:** Section(s) 3.11, 3.12

---

<sup>1</sup> <http://csrc.nist.gov/sec-cert/>

<sup>2</sup> <http://csrc.nist.gov/publications/nistpubs/800-53/SP800-53.pdf>

<sup>3</sup> Note that under 800-53, these seventeen listed categories define general security control “families” (e.g., “AC”), and that each family in turn contains several subcategories (e.g., “AC-1”, “AC-2”, “AC-3”, etc.) that further detail related aspects of information security and assurance. Consult Appendix F of 800-53 for further information.