

Microsoft® SQL Server™ 2005

Security-Enhanced Database Platform

Overview of SQL Server 2005

Today, database professionals need more tools to fight security threats as database systems are being widely used for critical applications. Because databases are increasingly exposed via web servers, administrators must properly secure them from both internal and external threats. Securing a database involves establishing a strong policy as well as adequate access controls.

In response to these needs, Microsoft has implemented strong security features into the **Microsoft® SQL Server™ 2005**, which provides a security-enabled platform for enterprise-class relational database and analysis solutions. SQL Server 2005 provides cutting edge security technology and addresses several security issues, including automatic secured updates and encryption of sensitive data.

In addition to these enhanced security features, SQL Server 2005 running on Microsoft Windows Server® works well with other Microsoft platforms and products. Microsoft has also invested deeply in standards-based interoperability with other platforms and products.

Security Features of SQL Server 2005

SQL Server 2005 provides enhanced security features that allow you to meet the following security challenges:

Security Challenge	Security Feature
Keeping your installation updated	Automated software updates
Managing services exposure	Reduced surface area
Guidance for secure deployment	Knowledge resources for secure deployment
Weak passwords	Password policy enforcement
Lack of audit information	Capture and audit DDL activities
Data confidentiality	Built-in encryption and Key Management
Metadata protection	Catalog security
Agent services security	Roles-based agent services management
Insecure application code	Secure development and code execution
Schema level permission	User – schema separation
Granular permission to execute statements in a module.	Execution context

SQL Server and Trustworthy Computing

Security, Privacy, Reliability and Business Practices are the driving forces of the Microsoft Trustworthy Computing initiative. Security is a key feature of SQL Server 2005, which provides confidentiality, integrity, and availability of mission-critical data.

As part of our focus on technology investments, Microsoft takes a "defense-in-depth" approach to protect and align three core elements: fundamentals, threat and vulnerability mitigation, and identity and access control.

Microsoft commits significant resources toward enhancing privacy protection, from the software itself to the services and products we offer customers to help them manage the privacy of their information.

Microsoft addresses reliability by providing dependable software and support. We also provide value by being a reliable business partner, maintaining an open dialogue with customers and industry partners, and actively seeking feedback about improving software and services.

Microsoft follows the concept of citizenship. We conduct business in the communities as a responsible global corporate citizen. High standards of transparency and integrity have helped to build continually-increasing trust of communities for Microsoft.

Security Features at a Glance

Automated Software Updates

Windows Update is built to ensure timely download and application of patches that significantly reduce specific security vulnerabilities. Windows Update automatically detects any edition of SQL Server 2005 installed on a particular machine and—based on the update analysis—can automatically install particular patches, greatly reducing the threat caused by known software vulnerabilities.

Reduced Surface Area

In any database, maximum security is achieved by limiting surface area exposure. The Surface Area Configuration tool of SQL Server 2005 allows administrators to manage services and connections—including analysis services, remote connections, full-text search service, SQL Server browser service, anonymous connection, linked objects, user-defined functions, CLR integration, SQL Mail, and native XML Web services—with an easy-to-use, graphical user interface. By limiting exposure of these services, security vulnerabilities can be greatly reduced.

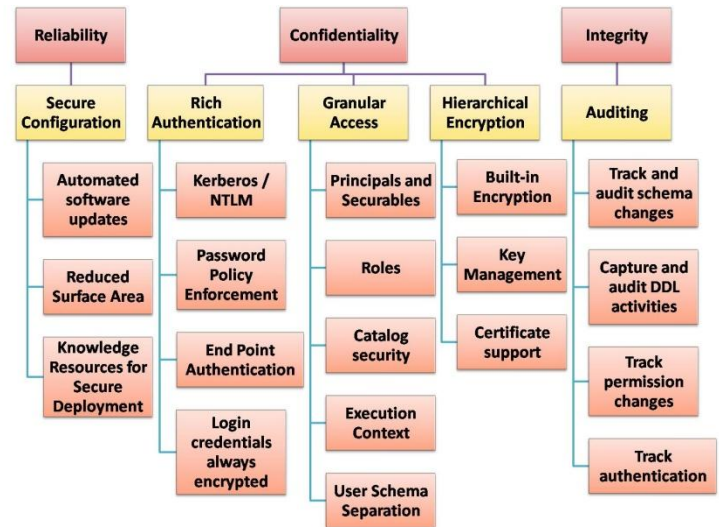
Knowledge Resources for Secure Deployment

A set of new deployment tools and documentation helps ensure that SQL Server 2005 can be securely deployed into an existing SQL Server topology or a new installation. These tools provide a step-by-step approach by giving detailed information, analyzing the existing topology, checking for prerequisites, recommending a configuration setting, and validating each step. Microsoft also publishes security bulletins and patches as appropriate for SQL Server 2005.

The security-enhanced development environment enabled by SQL Server 2005 allows developers easy sign on, verification, and code management. Common Language Runtime (CLR) assemblies that run in the database and all managed code uses Code Access Security (CAS).

Password Policy Enforcement

Strong password policies lead to more secure passwords and fewer opportunities for security breaches of database servers. Under strong password policies, SQL Server 2005 supports password complexity and password expiration. These policies require minimum password length, proper character combinations, and regularly-changing passwords. When SQL Server 2005 is running on Microsoft Windows Server 2003, Windows® secure password policies can also be applied to SQL Server password policies, providing enhanced security.



Roles

Granting role-based access to SQL Server Agents gives database administrators more flexibility in managing the Agent services. Execution of the SQL Server Integration Services (SSIS) package as a job step is more secure with Multiple Proxy Accounts in SQL 2005. By default, in SQL Server 2005, only system administrators can create the following tasks in a job:

- Active Scripting
- SQL Server Integration Services Package
- Analysis Command
- Analysis Query
- All replication subsystems

Catalog Security

SQL Server 2005 provides a more secure environment for metadata accessibility than SQL Server 2000. Catalog views of SQL Server 2005 now include both INFORMATION_SCHEMA and compatibility views. Additionally, catalog views are more secure as users are able to only view objects they are permitted to see.

Execution Context

SQL Server 2005 introduces the ability to mark modules with an execution context, such that the statements within the module can execute as a particular user as opposed to the calling user. This way, while the calling user still needs permissions to execute the

module, the permissions for statements within the module are checked against the execution context that the module was marked with. This behavior can be used to overcome some of the shortcomings of ownership chaining because it applies to all statements within the module. An alternative to marking execution context on modules is the signing feature. By adding a signature to a module, permissions can be associated to the signature for the duration of the execution of the procedure.

User Schema Separation

User schema separation simplifies managing large databases by providing flexibility in assigning permissions. In SQL Server 2005, by granting permissions on a schema, administrators can grant permissions to every object currently contained in the schema and any objects added to the schema in the future. They do not need to update permissions for every user when a new object is added.

Built-in Encryption

SQL Server 2005 provides data encryption directly in the database and is available across all SKUs.

Key Management

To enhance security, SQL Server 2005 maintains certificate stores, provides key management for symmetric and asymmetric keys, and uses algorithms like 2-key TripleDES, AES, DES, RC2, and RSA. The key management of a SQL Server 2005 instance is based on a hierarchy of keys rooted in the Service Master Key (SMK), which is encrypted using both the machine key and service key.

An asymmetric key consists of a private key and public key pair. Information is encrypted using the public key and can only be decrypted using the private key. A symmetric key is a single key that can be used for both encryption and decryption.

Capture and Audit DDL Activities

The powerful features of Data Manipulation Language (DML) triggers have been extended to Data Definition Language (DDL) statements. At the server or database level, certain occurrences of events can fire DDL triggers. As DDL responds to the server- and database-level events, these events can be logged, which is important for auditing activities and enhancing security.

Conclusion

As one of the first products to complete the Security Development Lifecycle, SQL Server 2005 offers security enhancements that provide reduced surface area exposure, more secure code execution, and better management of authentication and access. The revamped security infrastructure within SQL Server 2005 offers a significantly more secure database platform with a guiding principle of least privilege, which limits users to only the information they need to complete their tasks.

Additionally, the availability of data encryption secures confidential, mission-critical data in case of physical compromise or otherwise unauthorized access to the database system.

Additional Resources

For more information about Microsoft SQL Server 2005, see the following:

- SQL Server Homepage
<http://www.microsoft.com/sql>
- Product Overview Whitepaper
<http://www.microsoft.com/sql/2005/productinfo/overview.msp>
- Developer Center
<http://msdn.microsoft.com/sql/>
- Attend a free webcast or chat
<http://www.microsoft.com/sql/community/webcasts.asp>