



IBM Tivoli Access Manager for Business Integration

Highlights

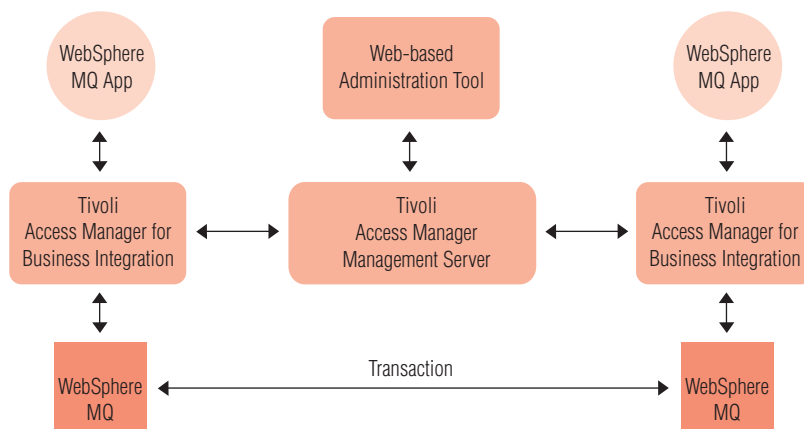
- **Enhances the native security services of IBM® WebSphere® MQ to provide application-level data protection for WebSphere MQ-based applications**
- **Provides message-level audit function, and generates audit records that can demonstrate specific compliance with the defined security policy**
- **Offers centralized administration of both access control and data protection policies across mainframe and distributed servers**
- **Implements comprehensive security without writing complex security code or modifying or recompiling existing applications**
- **Runs independently of the IBM Tivoli Enterprise™ Management Framework**

Securing WebSphere MQ-based applications

Although WebSphere MQ provides a set of security services out of the box, those services don't always cover all of a customer's security requirements, especially if the data being processed requires application-level data integrity and confidentiality. The IBM Tivoli® Access Manager for Business Integration security management solution can address these needs and provide you with the services to protect your most sensitive message data within your company and between your company and customers or business partners.

Application-level security without application change

Tivoli Access Manager for Business Integration is a value-added security management solution that greatly enhances the WebSphere MQ native security environment across a variety of platforms. It upgrades WebSphere MQ's data protection to provide application-level data protection for existing WebSphere MQ-based applications, without the need to modify or even recompile them. This is critical for customers using WebSphere MQ to process personally identifiable information or other types of sensitive data, such as financial transactions.



Tivoli Access Manager for Business Integration controls access to WebSphere MQ resources and provides message protection by intercepting application requests to WebSphere MQ. It then enforces the security policies you specify, allowing only authorized requests to get passed on to WebSphere MQ for processing. Messages are signed, or signed and encrypted, based on the policy you set.

Verify application authorization to access WebSphere MQ services

With Tivoli Access Manager for Business Integration you can remotely manage which applications can put and get messages from specific queues or queue managers.

When an application makes a call to the WebSphere MQ interface to put a message in the queue, Tivoli Access Manager for Business Integration intercepts and analyzes the call to verify whether the sending application is authorized to access the requested queue. If the call is authorized, it determines—based on a policy you define—whether the data in the transaction should be digitally signed, signed and encrypted, or passed on unchanged before placing the message in the requested queue. Administration of these security policies is done remotely, using a Web-based tool that replaces the need for administrators to visit each physical system.

Tivoli Access Manager for Business Integration is designed to support applications that are written to the WebSphere MQ native programming application program interface (API), the Java™ Messaging Service API (bindings mode only on distributed servers) and the Application Messaging

Interface API as defined by the Open Application Group.

Verify message origination and integrity using public key-based credentials

Tivoli Access Manager for Business Integration uses public key-based credentials for application authorization. It uses the matching private key to digitally sign message data, allowing later verification that the message has not been tampered with while being processed by WebSphere MQ (both while in a queue and while in transmission to a destination server). Tivoli Access Manager for Business Integration supports public key credentials issued by popular certificate authorities including VeriSign, Entrust, Baltimore and Netscape. Credentials generated by other certificate authorities that follow the X.509, Version 3 standard may also be compatible.

Protect the confidentiality of valuable data

By signing and encrypting your sensitive messages before they even get to WebSphere MQ for processing, Tivoli Access Manager for Business Integration allows you to demonstrate whether or not the integrity and confidentiality of these messages has been compromised while they were under the control of WebSphere MQ.

Message encapsulation is performed using the industry-proven PKCS #7 standard. Your message data can be unwrapped only by a process that has access to the application's private key to which the message was specifically directed. You can choose the encryption strength (RC2, DES or Triple DES) that best meets your security needs.

Scan messages for origination and adherence to security policies

When an application makes a call to WebSphere MQ to get a message, Tivoli Access Manager for Business Integration performs four separate security checks. It verifies whether the application requesting the message is authorized for get access on the queue specified. If it is not authorized, the get attempt fails with the standard WebSphere MQ return code of access denied. If the application is authorized, it then verifies whether the message conforms to the data protection policy that has been set for the queue. If the message format doesn't match the stated policy, the message is viewed as a rogue message and is moved to an error queue to prevent it from being passed back to the requesting application. At this point if the message data was secured, the digital signature

on the message will be validated. If this check fails, it means that the message was modified after it was generated. Message processing will stop, and the message will be placed in an error queue. If the message was also encrypted it will now be converted back to clear text. Tivoli Access Manager for Business Integration will view the public key ID of the application that originated the message—contained in a header appended to the transaction—to verify that the originator was authorized to put messages into that queue. If all these checks are successful, it will pass the clear text message to the requesting application.

Integration with other Tivoli Access Manager products

Tivoli Access Manager for Business Integration shares a common set of services with other Tivoli Access Manager products. These products include IBM Tivoli Access Manager for e-business (provides single sign-on and authorization services for Web resources) and IBM Tivoli Access Manager for Operating Systems (provides access control for UNIX® and Linux® resources). All three products use and ship the same set of shared services including a central security

policy manager, a central credential directory and a Web-based administration tool. A single instance of these shared services can support the installation of all three products, allowing you to consolidate the administration and management of security policy across WebSphere MQ queues, Web resources and UNIX and Linux resources. When you use Tivoli Access Manager for Business Integration it is not necessary to license or deploy the Tivoli Enterprise Management Framework.

Integrated identity management

Tivoli Access Manager for Business Integration is an integrated component of the IBM identity management solution that can help you get users, systems and applications online and productive fast, reduce costs and maximize return on investment. IBM identity management provides identity lifecycle management (user self-care, enrollment and provisioning), identity control (access and privacy control, single sign-on and auditing), identity federation (sharing user authentication and attribute information between trusted Web services applications) and identity foundation (directory and workflow) to effectively manage internal users as well as an increasing number of customers and partners through the Internet.

Integrated security event management

Audit information from Tivoli Access Manager for Business Integration can be sent to IBM Tivoli Risk Manager, which can store this information in the Tivoli Enterprise™ Data Warehouse. Tivoli Risk Manager can correlate and evaluate this data with other enterprise events, and then automate responses. New reporting capabilities can be used to leverage the information in the data warehouse.

Implement better WebSphere MQ security

A security management solution for WebSphere MQ should recognize and address an enterprise's messaging security requirements. It should provide a single point of administration for security policy, application-level message integrity and confidentiality, high performance and scalability. Tivoli Access Manager for Business Integration was developed specifically to address these issues. The first enterprise security management solution for WebSphere MQ, it provides centralized administration of queue data protection as well as put and get access control policies. It is a highly scalable, comprehensive solution that can transparently secure existing WebSphere MQ applications without modification and can also generate detailed auditing records showing

Tivoli Access Manager for Business Integration

Supported platforms

Sun™ Solaris™ 7, 8

IBM AIX® 4.3.3, 5.1

Microsoft® Windows NT® 4.0, Service Pack 6 or later

Microsoft Windows® 2000, Service Pack 1 or later

IBM OS/390®, Version 2, Release 10

IBM z/OS™, Version 1, any release

Components on distributed servers

Tivoli Access Manager for Business Integration, Version 4.1

IBM Tivoli Web Portal Manager 4.1

IBM Tivoli Access Manager 4.1 Management Server

IBM Directory Server

Components on mainframe servers

Tivoli Access Manager for Business Integration, Version 3.7.1

Prerequisite of IBM Policy Director Authorization Services for z/OS

which transactions were expressly authorized and properly protected, as well as attempts to violate your stated security policies.

Tivoli Access Manager for Business Integration supports WebSphere MQ Integrator, Version 2.1, allowing you to secure messages to and from a WebSphere MQ Integrator hub. It also supports MQSeries® Workflow, Version 3.3.2, allowing you to securely exchange workflow documents from system to system as they are being processed.

To learn more

For information on Tivoli Access Manager for Business Integration and integrated solutions from IBM, contact your IBM sales representative or visit tivoli.com/security



© Copyright IBM Corporation 2002

IBM Corporation
Software Group
Route 100
Somers, NY 10589
U.S.A.

10-02
All Rights Reserved

IBM, the e-business logo, the IBM logo, AIX, MQSeries, OS/390, Tivoli, Tivoli Enterprise, WebSphere, WebSphere MQ and z/OS are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries or both.

Microsoft, Windows and Windows NT are registered trademarks of Microsoft Corporation in the United States, other countries or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java, all Java-based trademarks, Sun and Solaris are trademarks of Sun Microsystems, Inc. in the United States, other countries or both.

Linux is a registered trademark of Linus Torvalds.

Other company, product and service names may be the trademarks or service marks of others.

The Tivoli home page on the Internet can be found at ibm.com/tivoli

The IBM home page on the Internet can be found at ibm.com