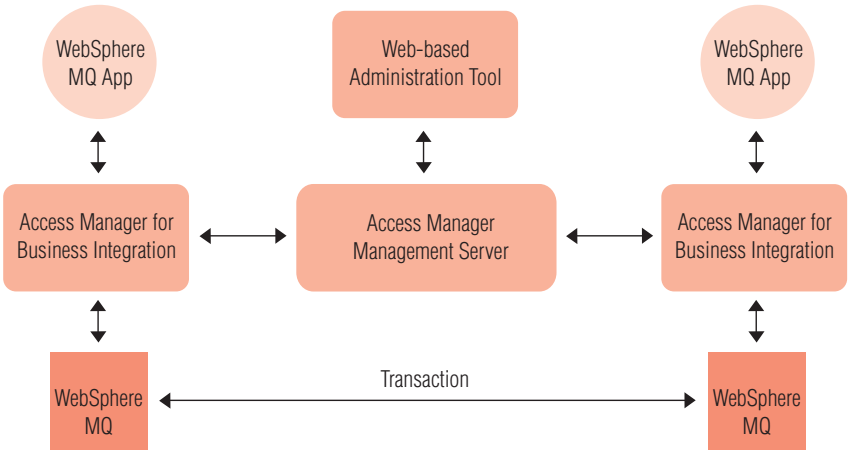
Tivoli software

IBM Tivoli Access Manager for Business Integration

Highlights

- ***Helps minimize security risks with authorization, data integrity and data confidentiality services for WebSphere® MQ® applications***
- ***Helps protect data as it sits in a queue and as it flows across the network***
- ***Manages security of WebSphere MQ resources across heterogeneous systems***
- ***Implements security without writing complex security code***
- ***Defines and enforces centralized policies, including authorization and data protection***
- ***Shares a common infrastructure with IBM® Tivoli® Access Manager for e-business and IBM Tivoli Access Manager for Operating Systems***



IBM 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, and the authorized requests get passed to MQ. Messages are signed or signed and encrypted based on policy you set.

Communicate securely across platforms

IBM Tivoli Access Manager for Business Integration is a centralized security management solution for IBM WebSphere MQ. It helps WebSphere MQ-based applications communicate securely across a variety of platforms. This scalable, high-performance solution provides access control to govern which applications can put messages to, or get messages from, specific queues. Using public key technology it helps protect messages, maintaining both message integrity and confidentiality. These services are supplied transparently to WebSphere MQ-based applications; many existing applications are already compatible and do not have to be changed.

IBM Tivoli Access Manager for Business Integration also supports central administration of the authorization and data protection policies it enforces, providing a consolidated view and update of information.

Verify application authorization to access WebSphere MQ services

With IBM Tivoli Access Manager for Business Integration, you have control over which applications or, on Microsoft® Windows® platforms, which users of those applications can send and receive 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, IBM 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, the interceptor determines—based on a policy you define—whether the data in the transaction should be digitally signed, or signed and encrypted, before placing the message in the requested queue. IBM Tivoli Access Manager for Business Integration also supports applications written to the Java™ Messaging Service application program interface (API), in bindings mode, that run on distributed servers.

Verify message origination and integrity with public key-based credentials

IBM Tivoli Access Manager for Business Integration can leverage public/private key-based credentials for user and application authentication. It also uses these credentials to digitally sign message data, allowing later verification that the message has not been tampered with while in a queue or in transmission to a destination server. Messages are signed with the keys associated with the sender.

IBM Tivoli Access Manager for Business Integration supports credentials issued by popular certificate authorities, including Entrust, Baltimore, Netscape and IBM. 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 encrypting your sensitive WebSphere MQ messages, IBM Tivoli Access Manager for Business Integration helps prevent unauthorized users from accessing data as it moves from sender to receiver or while a message is in a queue. It uses the PKCS #7 standard to encapsulate your message data so that the message can be unwrapped by a process that has access to the private key of the application, or by the user to whom the message is being 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, IBM Tivoli Access Manager for Business Integration checks three security policies.

First, IBM Tivoli Access Manager for Business Integration verifies whether the receiver is authorized to retrieve the message from the queue; if not, access is denied.

Next, it confirms whether the message conforms to the data protection policy

for the queue. Messages that fail either of these checks are viewed as rogue messages and are not passed back to the requesting application for processing.

Finally, it views the header appended to a transaction and verifies that the ID of the message originator is authorized to put to that queue.

Control access to nonsupported platforms

Digital signing and encryption of messages require IBM Tivoli Access Manager for Business Integration to run on both sides of a transaction. If IBM Tivoli Access Manager for Business Integration does not currently provide platform support to a particular destination server, you can still enforce access control over whether an application running on a distributed server can put a message to a queue on the iSeries™ server. If data protection is required in this environment, you can install IBM Tivoli Access Manager for Business Integration on a gateway server before the message gets to the iSeries server.

An example of this is where a remote network of distributed servers runs transactions across a public network to the iSeries server. The solution: install IBM Tivoli Access Manager for Business Integration on each of the remote servers and on a distributed server at the IS center running as a gateway to the iSeries server. The data is then protected across the public network and up to the gateway.

Integration with other Tivoli products

When using IBM Tivoli Access Manager for Business Integration, it is not necessary to license or deploy the Tivoli framework. IBM Tivoli Access Manager for Business Integration shares several components with IBM Tivoli Access Manager for e-business and IBM Tivoli Access Manager for Operating Systems. These include the management server, the IBM Tivoli Web Portal Manager and an IBM LDAP Directory. If you have already deployed Version 3.7.1 or 3.8 of these IBM Tivoli shared components, you may need to deploy only the component from IBM Tivoli Access Manager for Business Integration that runs directly on a WebSphere MQ server.

Mainframe servers running IBM Tivoli Access Manager for Business Integration, Version 3.7.1 require Version 3.7.1 of the management server. A customer that has already deployed a Version 3.8 or later management server will need to also deploy a Version 3.7.1 of it to provide authorization services to the mainframe. Common administration of security policies for Web objects and WebSphere MQ objects can be done with a single instance of IBM Tivoli Policy Director Web Portal Manager administration tool.

Implement better WebSphere MQ security

IBM Tivoli Access Manager for Business Integration can provide data protection for IBM WebSphere MQ without requiring application changes. It allows you to centrally define which specific WebSphere MQ resources an application can access and then enforces that policy. IBM Tivoli Access Manager for Business Integration also enables you to centrally define if and

IBM Tivoli Access Manager for Business Integration

Supported platforms
Sun™ Solaris™ 7, 8
IBM AIX® 4.3.3
Microsoft Windows NT® 4.0, Service Pack 6 or later
Microsoft Windows 2000, Service Pack 1 or later
OS/390®, Version 2, Release 10
z/OS™, Version 1, any release
Components on distributed servers
IBM Tivoli Policy Director for MQSeries Interceptor, Version 3.8
IBM Tivoli Web Portal Manager 3.8
IBM Tivoli Policy Director 3.8 Management Server
IBM LDAP Directory
Components on mainframe servers
Tivoli Policy Director for MQSeries Interceptor, Version 3.7.1
Prerequisite of IBM Policy Director Authorization Services for z/OS

how the messages associated with those resources are protected. Protected messages can be made safe from being read or modified when they are sitting in a queue, as well as when they are in transit. IBM Tivoli Access Manager for Business Integration is also compatible with MQSeries® Integrator, Version 2.01 and MQ Workflow, Version 3.3 when running on distributed servers.

To learn more

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

Tivoli software from IBM

An integral part of the comprehensive IBM e-business infrastructure solution, Tivoli technology management software helps traditional enterprises, emerging e-businesses and Internet businesses worldwide maximize their existing and future technology investments. Backed by world-class IBM services, support and research, Tivoli software provides a seamlessly integrated and flexible e-business infrastructure management solution that uses robust security to connect employees, business partners and customers.

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

Printed in the United States of America
04-02

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

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

e business software

G325-1692-02