Microsoft BizTalk Server 2006 Part-VIII

Table of Contents

Module 1: Monitoring BizTalk Server
Health and Activity Tracking
Monitoring BizTalk Server Using MOM

Module 2: Health and Activity Tracking
Checklist: Health and Activity Tracking
Best Practices for Health and Activity Tracking
Security Considerations for Health and Activity Tracking
Configuring Tracking
Using Health and Activity Tracking
Investigating Orchestration, Port, and Message Failures
Service Instance States
Viewing Message Flow
Debugging an Orchestration with HAT
Working with the Results Lists

Module 3: Configuring Tracking
What is Message Tracking?
What is Event Tracking?
How to Configure Tracking for an Orchestration
How to Configure Tracking for a Send Port
How to Configure Tracking for a Receive Port
How to Configure Tracking for a Pipeline
How to Configure Tracking for a Policy
How to Configure Tracking for a Schema

Module 4: Using Health and Activity Tracking
Sample HAT Queries
How to Open a Saved Query in Health and Activity Tracking
How to Save a Query in Health and Activity Tracking
Using the Reporting Menu in HAT
Service Metrics and Message Metrics
Viewing Archived and Live Data Using HAT
How to Change the Query Timeout Value in Health and Activity Tracking

Module 5: Using the Reporting Menu in HAT
What is the Find Message View?
How to Find Events and Messages by Message Property
What is the Query Builder View?
How to Create a Query in Health and Activity Tracking
How to View All Instance Information
How to View Completed Orchestrations or Pipelines
How to View Running Orchestrations or Pipelines
How to View Suspended Orchestrations or Pipelines
How to View Failed Orchestrations or Pipelines

Module 6: Service Metrics and Message Metrics
How to Process OLAP Cubes
How to Work with the OLAP Cube Data

Module 7: Viewing Archived and Live Data Using HAT
How to Select a Live or Archived Data Source

Module 8: Investigating Orchestration, Port, and Message Failures
Tracking Services and Messages
Viewing Tracked Information
Service Instance States
Viewing Message Flow

Module 9: Tracking Services and Messages
What is the Results List View?
Orchestration Failures in HAT
Types of Message Failures in HAT

Module 10: Viewing Tracked Information
Using the Administration Console Query Tab
How to Save a Query
How to Open a Saved Query
How to Search for All Service Instances
How to Search for Running Service Instances
How to Search for Suspended Service Instances
How to Search for Messages
How to Search for Subscriptions

Module 11: Debugging an Orchestration with HAT
Orchestration Debugger User Interface
Considerations when Using Orchestration Debugger
Working with the Orchestration Debugger View

Module 12: Orchestration Debugger User Interface
Service Pane in Orchestration Debugger
Tracked Events Pane in Orchestration Debugger
Orchestration Pane in Orchestration Debugger
Reporting Mode in Orchestration Debugger
Interactive Mode in Orchestration Debugger

Module 13: Working with the Orchestration Debugger View
Working with Breakpoints
Replaying Actions
Viewing Variables

Module 14: Working with the Results Lists
How to Access Message Flow or Orchestration Debugger View
How to Suspend Orchestrations or Ports
How to Resume Orchestrations that are Suspended by Design
How to Terminate Orchestrations that are Suspended by Fault
How to Control the Size of the Results List
How to Switch to Orchestration Debugger View from Message Flow View

Module 15: Monitoring BizTalk Server Using MOM

Checklist: Using MOM to Monitor BizTalk Server
Best Practices for Using MOM to Monitor BizTalk Server
Contents of the BizTalk Server 2006 Management Pack
How to Import the BizTalk Server Management Pack
How to Mark BizTalk Server Databases as Critical in the SQL Server Management Pack
How to Add Enterprise Single Sign-On Computers to the List of Computers Monitored by the BizTalk Server Management Pack
Operations Tasks for the BizTalk Server 2006 Management Pack
BizTalk Server Monitoring Scenarios
Tasks in the BizTalk Server 2006 Management Pack
Views in the BizTalk Server 2006 Management Pack
State Monitoring Definitions in the BizTalk Server 2006 Management Pack

Module 16: BizTalk Server Monitoring Scenarios

Resolving Suspended Message Alerts
Resolving a BAM Technical Assistance Alert
Monitoring BizTalk Messageboxes and Hosts
Monitoring Throttling Conditions

Module 17: Securing BizTalk Server

Managing BizTalk Server Security
Enterprise Single Sign-On

Module 18: Managing BizTalk Server Security

Best Practices for Security, Accounts, and Certificates
Managing BizTalk Windows Groups and User Accounts
Windows Group and User Accounts in BizTalk Server
BizTalk Server User Rights

Module 19: Managing BizTalk Windows Groups and User Accounts

Managing the BizTalk Administrators Group
Managing Hosts and Service Accounts
Creating a Host Windows Group
Managing Signing Certificates

Module 20: Windows Group and User Accounts in BizTalk Server

Local Groups
Domain Groups

Module 21: BizTalk Server User Rights

Required User Rights for Administering BizTalk Server Objects
Required User Rights for Managing Orchestrations
Required User Rights for Managing Send Ports and Send Port Groups
Required User Rights for Managing Receive Locations
Required User Rights for Managing BizTalk Hosts and Host Instances
Required User Rights for Managing a MessageBox Database
User Accounts for Database Backups
Security Considerations for Health and Activity Tracking

Module 22: Enterprise Single Sign-On
- Understanding SSO
- Installing SSO
- Using SSO
- Securing Your Deployment of SSO
- Password Synchronization
- SSO Security Recommendations

Module 23: Understanding SSO
- SSO User Groups
- SSO Components
- SSO Server
- Master Secret Server
- SSO Affiliate Applications
- SSO Mappings
- SSO Tickets
- Configuring SSO

Module 24: Installing SSO
- Upgrading from a Previous Version of SSO
- Standard Installation Options
- High-Availability Installation Options
- How to Remove SSO

Module 25: Upgrading from a Previous Version of SSO
- Using Host Initiated SSO Functionality
- Processing Servers for SSO

Module 26: Standard Installation Options
- How to Install the SSO Administration Component
- How to Install the SSO Client Utility

Module 27: High-Availability Installation Options
- How to Cluster the Master Secret Server
- How to Cluster the SQL Server
- How to Configure SSO in a Multicomputer Scenario

Module 28: Using SSO
- How to Set the SSO Server
- How to Enable SSO
- How to Change the Master Secret Server
- How to Disable SSO
- How to Update the SSO Database
- How to Display the SSO Database Information
- How to Configure the SSO Tickets
- How to Audit SSO
- How to Enable SSL for SSO
- Managing the Master Secret
- How to Specify SSO Administrators and Affiliate Administrators Accounts
- Managing Affiliate Applications
- Managing User Mappings
- Host Initiated SSO

Module 29: Managing the Master Secret
- How to Generate the Master Secret
- How to Back Up the Master Secret
- How to Restore the Master Secret
- How to Move the Master Secret

Module 30: Managing Affiliate Applications
- How to Create an Affiliate Application
- How to Delete an Affiliate Application
- How to Update the Properties of an Affiliate Application
- How to Enable an Affiliate Application
- How to Disable an Affiliate Application
- How to List Affiliate Applications
- How to List the Properties of an Affiliate Application
- How to Clear the Application Cache
- How to Set the SSO Server Using the Client Utility
- How to Display the SSO Server Using the Client Utility
- How to Set Credentials for the Affiliate Application Using the Client Utility

Module 31: Managing User Mappings
- How to List User Mappings
- How to Create User Mappings
- How to Delete User Mappings
- How to Set Credentials for a User Mapping
- How to Enable a User Mapping
- How to Disable a User Mapping

Module 32: Host Initiated SSO
- How to Configure Requirements for Host Initiated SSO
- How to Enable and Disable Host Initiated SSO
- How to Create Affiliate Applications for Host Initiated SSO
- Validating Passwords for Host Initiated SSO
- How to Manage User Mappings for Host Initiated SSO
- How to Use the Trace Utility in Host Initiated SSO

Module 33: Securing Your Deployment of SSO
- SSO Deployment Overview
- Deployment Process

Module 34: Password Synchronization
- How to Install Password Synchronization
- How to Administer Password Synchronization
- How to Configure Password Synchronization
- How to Manage Password Synchronization

Module 35: Maintaining BizTalk Server
- Backing Up and Restoring BizTalk Server
- Archiving and Purging the BizTalk Tracking Database

Module 36: Backing Up and Restoring BizTalk Server

Checklist: Back Up and Restore BizTalk Server
Best Practices for Backup and Restore
Backing Up and Restoring BizTalk Server Databases
Backing Up and Restoring BAS
Backing Up and Restoring BAM
Backing Up and Restoring the Base EDI Adapter
Resolving Data Loss
Advanced Information About Backup and Restore

Module 37: Backing Up and Restoring BizTalk Server Databases

How to Configure the Backup BizTalk Server Job
How to Configure the Destination System for Log Shipping
How to Restore Your Databases

Module 38: Backing Up and Restoring BAS

How to Back Up Your BAS Site and Database
How to Restore Your BAS Site and Database
How to Update References to the TPM Database Name and Connection String

Module 39: Backing Up and Restoring BAM

How to Back Up the BAM Analysis and Tracking Analysis Server Databases
How to Update References to the BAM Analysis Server Database Name
How to Update References to the Tracking Analysis Server Database Name
How to Update References to the BAM Star Schema Database Name
How to Update References to the BAM Archive Database Name
How to Update References to the BAM Primary Import Database Name and Connection String
How to Update References to the BAM Notification Services Databases
How to Resolve Incomplete Activity Instances

Module 40: Backing Up and Restoring the Base EDI Adapter

Best Practices for Backing Up the Documentshome Directory
How to Restore the Documentshome Directory
How to Recover Data and Resynchronize the Audit Trail
How to Generate an Engine Input File

Module 41: Resolving Data Loss

Resolving Data Loss of In-Progress Orchestrations
Identifying Lost HAT Data
Marking In-Progress Transactions as Complete in BAM

Module 42: Advanced Information About Backup and Restore

Marked Transactions, Full Backups, and Log Backups
Log Shipping
How to Schedule the Backup BizTalk Server Job
How to Back Up Custom Databases
How to Create a Linked Server
Viewing the History of Restored Backups

Module 43: Archiving and Purging the BizTalk Tracking Database

Checklist: Archiving and Purging the BizTalk Tracking Database
How to Configure the BTS_BACKUP_USERS Role for Archiving and Purging Data from the BizTalk Tracking Database
How to Configure the DTA Purge and Archive Job
How to Purge Data from the BizTalk Tracking Database
How to Manually Purge Data from the BizTalk Tracking Database
How to Enable Automatic Archive Validation
How to Copy Tracked Messages into the BizTalk Tracking Database

Monitoring BizTalk Server

Monitoring your BizTalk Server infrastructure on a regular basis and resolving any issues that you find will help to keep your BizTalk Server infrastructure accessible to your users. This section provides information about monitoring BizTalk Server.

The goal of monitoring is to minimize the amount of time that an exception goes undetected and, therefore, unresolved. Optimally, you can use monitoring to help detect a potential exception and guide you to take steps to avoid an exception.

When monitoring BizTalk Server, you are looking for any unexpected or anomalous behavior. Monitoring can be either a manual process, or an automatic process, as with using Microsoft Operations Manager (MOM).

Monitoring BizTalk Server is typically a manual process performed as follows:

- You (the BizTalk Server administrator) either find or receive a notification of an Event Viewer message posted by BizTalk Server.
- You note the instance ID of the message or orchestration instance.
- You open the Health and Activity Tracking (HAT) and perform a query to find the instance in question.
- You perform troubleshooting steps to correct the problem.

BizTalk Server monitoring falls into three main categories: availability monitoring, health monitoring, and performance monitoring.

Availability Monitoring

Availability monitoring answers the question "Is there anything preventing the system from running correctly?" These issues are almost exclusively system-level ones, such as availability of services and connections. For example, if an adapter is failing because the Enterprise Single Sign-On service is stopped, this is an availability issue. The following table shows availability-monitoring tools.

Tool	Task
Event Viewer	Look for adapter connection issues, stopped services, and so on.
BizTalk Server Administration Console	Interact with (start and stop) services and examine the overall status of the system.
Microsoft Operations Manager (MOM)	The BizTalk Server 2006 management pack contains MOM rules that automatically monitor system availability.

Health Monitoring

Health monitoring is concerned with how BizTalk Server and your solution are working at the application level. This is where your business processes live. The following table shows health-monitoring tools.

Tool	Task
Event Viewer	Detect problems that occur during the processing of messages and orchestrations.
Health and Activity Tracking (HAT)	Query for messages and debug orchestrations.
BizTalk Server Administration Console	Interact with services and check on overall status of the system.
Business Activity Monitoring (BAM)	Develop solution-specific ways to monitor the performance of a solution's stages.
Microsoft Operations Manager (MOM)	The BizTalk Server 2006 management pack contains MOM rules that automatically monitor system health.

Performance Monitoring

Performance monitoring answers the question, "How efficiently is the system performing its work?" This kind of monitoring focuses primarily on the load on physical resources like databases and disks. For example, if the CPU utilization is consistently at 90 to 100 percent and a backlog of messages is forming, this is a performance issue at the computer level. The following table shows performance-monitoring tools.

Tool	Task
SQL Query Analyzer	Monitor database size and content to diagnose system problems.
Microsoft Operations Manager (MOM)	The BizTalk Server 2006 management pack contains MOM measurement rules and comparison rules that automatically gather data from Microsoft Windows performance counters so that you can take appropriate corrective action to improve system performance.

In This Section

- Health and Activity Tracking
- Monitoring BizTalk Server Using MOM

Health and Activity Tracking

You can use Health and Activity Tracking (HAT) to view historical or tracked data and to troubleshoot your BizTalk Server deployment.

- HAT enables system administrators to view tracked message events, message properties and message bodies at various stages in a message's flow. This data can be used for troubleshooting or auditing purposes. The orchestration debugger tool in HAT enables the system administrator to replay the execution of a specific orchestration instance.

- Users can query for messages by specifying criteria such as message schema and message property/value pairs. Having thus located the message, users can determine the point in the message flow to which the message has progressed. Advanced users can also create custom SQL Server queries for messages.

- You can also use HAT to search for archived data in an archived or backed up Tracking database.

For information about using the keyboard shortcuts for Health and Activity Tracking, see HAT Keyboard Shortcuts .

In This Section

- Checklist: Health and Activity Tracking
- Best Practices for Health and Activity Tracking
- Security Considerations for Health and Activity Tracking
- Configuring Tracking
- Using Health and Activity Tracking
- Investigating Orchestration, Port, and Message Failures
- Service Instance States
- Viewing Message Flow
- Debugging an Orchestration with HAT
- Working with the Results Lists

Checklist: Health and Activity Tracking

Step	Reference
Review the Health and Activity Tracking (HAT) security considerations.	Security Considerations for Health and Activity Tracking
Review the HAT best practices.	Best Practices for Health and Activity Tracking
Configure tracking on artifacts in the BizTalk Server Administration Console.	Configuring Tracking

Best Practices for Health and Activity Tracking

- Review the security considerations for using Health and Activity Tracking (HAT).
- Ensure that the SQL Server Agent service is running on all MessageBox databases.

  SQL Server Agent makes message bodies available to HAT and WMI, and enables you to run jobs to clean up the MessageBox databases.
- Turn on message body tracking.

  Message body tracking is required to save messages after service instances processing is complete.

Security Considerations for Health and Activity Tracking

For security reasons, Health and Activity Tracking (HAT) does not use browsers or URLs as in previous releases of BizTalk Server. This monitoring option is now included as a part of HAT, which is installed as part of BizTalk Server when you install the administrative tools.

For backward compatibility, BizTalk Server still hosts Microsoft Internet Explorer. BizTalk Server hosts Internet Explorer inside a shell for security reasons. When you install BizTalk Server, you set up a Web site portal for HAT to use exclusively for displaying ASP pages.

Using HAT, you can access the technical details necessary to troubleshoot and optimize your BizTalk Server environment. Because HAT is a powerful tool, you should limit access to it in your production environment so that malicious or unauthorized users do not cause damage. It is recommended you follow these guidelines for securing and using HAT in your environment.

- You must be logged on as a member of the BizTalk Server Operators group to view data using Health and Activity Tracking (HAT). To access message bodies you must be logged on as a member of the BizTalk Server Administrators group.

Ensure that HAT uses the minimum credentials to perform Health and Activity Tracking tasks. For more information, see **Minimum Security User Rights**.

When you use HAT, you can access the following databases:

Database	User Group/Permissions
BizTalk Management (BizTalkMgmtDb)	BizTalk Server Administrators, BizTalk Server Operators
BizTalk MessageBox (BizTalkMsgBoxDb)	BizTalk Server Administrators, BizTalk Server Operators, or read-write permissions
BizTalk Tracking (BizTalkDTADb)	BizTalk Server Administrators, BizTalk Server Operators, or read-only permissions

- HAT generates reports about all hosts in the BizTalk Server environment based on the parameters of a query. To minimize the potential of information disclosure, only members of the BizTalk Server Administrators group can use HAT. However, if you do not want all BizTalk Server Administrators to have access to the reports HAT produces, you can limit their access to the data by adding/removing users from the HM_EVENT_WRITER and BAM_EVENT_WRITER SQL Server roles in the BizTalk Tracking (BizTalkDTADb) database.

- BizTalk uses the BAM_EVENT_WRITER and HM_EVENT_WRITER SQL Server roles to grant/deny their members permissions to read/write the tracking data in the Tracking database, but not through role membership. Do not remove these SQL Server roles. When you change a host from hosting to not hosting tracking (or vice versa), the adm_ChangeHostTrackingPrivilege stored procedure is called. This stored procedure reads the definition of the BAM_EVENT_WRITER and HM_EVENT_WRITER SQL Server roles and apply the corresponding GRANT/DENY statements to the Host Windows group. This achieves the same effect as adding the Host Windows group to these SQL roles.

- When you configure the HAT preferences to view data from an archived database, HAT connects to the databases that hold the archived data, not to the currently active BizTalk Tracking (BizTalkDTADb) database.

- You cannot debug live orchestrations across Network Address Translation (NAT) firewalls. You must have an administration computer on the Processing domain in order to debug live orchestrations.

- Depending on how you configure HAT and the pipelines, BizTalk Server may store sensitive information contained in the message context. If you use WMI or HAT to save message bodies to a file location, ensure that the location has a strong discretionary access control list (DACL) so that only BizTalk Server Administrators have read permissions to these message bodies. Apply the same DACL to any location you save the message bodies, including non-BizTalk databases where you may archive and restore them.

- You must manually grant permissions to the BizTalk Server Administrators group to access the Tracking Analysis Server (BizTalkAnalysisDb) database; by default, only OLAP administrators have permissions to it.

Configuring Tracking

You can configure various tracking options during run time for orchestrations, send ports, receive ports, and pipelines using the BizTalk Server Administration Console. You can change the tracking options for an item at any time, without interrupting the business process.

The tracking configuration settings for each receive port, send port, and orchestration allow you to track the following types of data using Health and Activity Tracking (HAT):

- Inbound and/or outbound event data. For example, message ID, start and stop times for the artifact.
- Inbound and/or outbound message properties. For example, general and promoted properties for each message that the artifact processes.
- Inbound and/or outbound message bodies and parts. For example, body and parts for each message that the artifact processes.
- Orchestrations. Execution data for orchestration shapes.

In This Section

- What is Message Tracking?
- What is Event Tracking?
- How to Configure Tracking for an Orchestration
- How to Configure Tracking for a Send Port
- How to Configure Tracking for a Receive Port
- How to Configure Tracking for a Pipeline
- How to Configure Tracking for a Policy
- How to Configure Tracking for a Schema

What is Message Tracking?

You can use Health and Activity Tracking (HAT) to track messages, including schema information, strong name, and all the promoted properties for the generated message. A message is an electronic instance of data, as typically exchanged between two running business processes or applications. A message instance is made up of a message body, message properties, and metadata.

Message Body

Tracking the message body provides a record of messages sent and received. You must have message body tracking turned on in order to save messages after service instances processing is complete. After you have set the tracking options, it can take a few minutes before you can view the messages.

You can use tracked messages to provide confirmation of receipt, to enable troubleshooting, and to allow data mining of historical transactions. HAT tracks the message bodies as the input and output of ports, pipelines, and orchestrations. You can recover these messages from HAT, or through Windows Management Instrumentation (WMI) or Operations object model (OM) application programming interfaces (APIs).

HAT does not track messages that do not successfully make it through one of the tracking points. In some cases—such as when a message is suspended because it is invalid, or if no host is expecting the message—it may be placed in the Suspended queue without being tracked. If you terminate this message there will be no record of it.

To minimize overhead, message bodies remain in the MessageBox database, and the system automatically purges the database periodically. If you need to keep any of the data, you must archive it before the system purges it.

Message Properties

Message properties, which include promoted properties, routing information, and trading partner data. Message property tracking enables you to locate a specific message from the thousands that you may have tracked, by providing a record of promoted properties for each message in the results list. You can then track a subset of the message itself, using one of these properties.

For example, if you use the Schema Editor to promote the PO Number field from a Purchase Order schema into the message shortcut, you can find the message instances that contain a particular value for that tracked field, such as PO Number = 16995.

Message property tracking creates much less overhead than message body tracking, because HAT only tracks the scheduled fields. After you set the tracking options for the message property, it can take a few minutes before you can view the properties.

Metadata

Metadata, such as the message instance identifier, the orchestration or pipeline logging the message, the point at which the orchestration or pipeline logs the message, and other relevant tracking details. For a message in the MessageBox database to route to a business process, it must contain context properties such as message type and origin. These properties become metadata. HAT uses subscription criteria to query against this metadata.

You can use HAT to track these context properties. You promote context properties by adding them to the message shortcut. HAT tracks these context properties globally—that is, HAT tracks all messages that contain a specified shortcut property. This may significantly increase the size of the Tracking database.

To track context properties, you define a property schema for the namespace used in the context to store the properties. When you deploy the property schema, it becomes available through the HAT Message Property Tracking view. From there, you can select the context properties you want to track. HAT tracks them in the same way it tracks promoted message properties.

Sensitive Data

You can secure the following data ensuring that it does not appear in HAT and therefore becomes unavailable for tracking.

- Apply the **isSensitive** attribute to any sensitive properties in a property schema, so that it is no longer visible in the Message Property tracking configuration selections.
- All out-of-box transports contain passwords marked as sensitive, so the transports cannot be tracked.
- In addition, these sensitive properties are no longer in the Management database, so if you are setting tracking options directly in the database, they are unavailable for tracking.
- If you track outbound on-the-wire message bodies, HAT removes all the transport properties from the shortcut of the tracked message body. Therefore, in addition to removing outbound transport properties from the shortcut of the tracked message body, HAT also removes properties from inbound transports.

What is Event Tracking?

Health and Activity Tracking (HAT) tracks data based on events (for example, when a service begins or ends, or when a message is sent or received). Most HAT views return a list of the events that have occurred, enabling you to see everything that happened based on the tracking filters you have set. If you track an assembly that has multiple versions, the returned results will be from the most recently deployed assembly.

You can track the start and end of orchestrations and ports, when messages are sent and received, as well as the execution of each shape in an orchestration.

The BizTalk Tracking (BizTalkDTADb) database contains a DTA_Services audit table. This table contains history of all deployed services—pipelines, transports, and orchestrations. It does not keep track of undeployments.

You can track the contents of a message as well as the promoted properties of a message. HAT defines these actions as **Message Body** tracking and **Message Property** tracking. Although envelopes appear in HAT, you cannot track message properties from them. In addition, tracking does not detect any tracking information embedded in a deployed assembly.

How to Configure Tracking for an Orchestration

This topic describes how to use the BizTalk Server Administration console to configure tracking for an orchestration.

For more information about creating and using queries, see Using the BizTalk Server Administration Console. For more information about the health and activity tracking features of BizTalk Server 2006, see Health and Activity Tracking.

Prerequisites

To perform the procedure in this topic, you must be logged on with an account that is a member of the BizTalk Server Administrators group. For more detailed information on permissions, see Permissions Required for Deploying and Managing a BizTalk Application.

To configure tracking for an orchestration

1. Click **Start**, click **Programs**, click **Microsoft BizTalk Server 2006**, and then click **BizTalk Server Administration**.

2. In the console tree, expand BizTalk Server 2006 Administration, expand the BizTalk group, expand Applications, and then expand the application containing the orchestration for which you want to configure tracking.

3. Click **Orchestrations**, right-click the orchestration for which you want to configure tracking, and then click **Properties**.

4. Click the **Tracking** tab, select the tracking options you want, as described in the following table, and then click **OK**.

Option	Description
Track Events - Orchestration start and end	Select this check box to track the orchestration instance before and after processing of the entire business process. Orchestration tracking enables you to see the instances in the reporting views of Health and Activity Tracking.
Track Events - Message send and receive	Select this check box to track message send and receive events. This check box is available only if you select the **Orchestration start and end** check box.
Track Events - Shape start and end	Select this check box when you need to debug orchestration instances in the Orchestration Debugger. When this check box is selected, the event list in the Orchestration Debugger is populated. This check box is available only if you select the **Orchestration start and end** check box.
Track Message Bodies - Messages before orchestration processing	Select this check box to save and track the actual message content prior to processing by the orchestration instance. This check box is available only if you select the **Message send and receive** check box.

Track Message Bodies - Messages after orchestration processing	Select this check box to save and track the actual message content after processing by the orchestration instance. This check box is available only if you select the **Message send and receive** check box.
Track Message Properties - Incoming messages	Select this check box to track message receive events. You must select this option to track incoming message bodies.
Track Message Properties - Outgoing messages	Select this check box to track message send events. You must select this option to track outgoing message bodies.

How to Configure Tracking for a Send Port

This topic describes how to use the BizTalk Server Administration console to configure tracking for a send port. You can select options to view message bodies and promoted properties in the reporting views of Microsoft Health and Activity Tracking (HAT). This helps you monitor the health of your BizTalk implementation and identify any bottlenecks. The tracking settings that you configure apply to all of the instances of the send port.

For background information on tracking, see Configuring Tracking. For complete information about configuring and using HAT, see Health and Activity Tracking.

Prerequisites

To perform the procedure in this topic, you must be logged on with an account that is a member of the BizTalk Server Administrators group. For more detailed information on permissions, see Permissions Required for Deploying and Managing a BizTalk Application.

To configure tracking for a send port

1. Click **Start**, click **Programs**, click **Microsoft BizTalk Server 2006**, and then click **BizTalk Server Administration**.

2. In the console tree, expand the BizTalk group and the BizTalk application for which you want to configure tracking for a send port.

3. Click **Send Ports**, right-click the send port, click **Properties**, and then click **Tracking**.

4. Configure the tracking options you want, as described in the following table, and then click **OK**.

Use this	To do this
Track Message Bodies - Request message before port processing	Select this check box to enable you to save and track message content before the message is received.
Track Message Bodies -	Select this check box to enable you to save and track

Request message after port processing	message content after the message is received.
Track Message Bodies - Response message before port processing	Select this check box to enable you to save and track message content before the message is sent. This check box is available only for solicit-response send ports.
Track Message Bodies - Response message after port processing	Select this check box to enable you to save and track message content after the message is sent. This check box is available only for solicit-response send ports.
Track Message Properties - Request message before port processing	Select this check box to track the promoted properties of an inbound message.
Track Message Properties - Request message before port processing	Select this check box if you want to track the promoted properties of an outbound message.
Track Message Properties - Response message before port processing	Select this check box to save and track message properties before the message is sent. This check box is available only for solicit-response send ports.
Track Message Properties - Response message after port processing	Select this check box to save and track properties after the message is sent. This check box is available only for solicit-response send ports.

How to Configure Tracking for a Receive Port

This topic describes how to use the BizTalk Server Administration console to configure tracking for a send port. You can select options to view message bodies and promoted properties in the reporting views of Microsoft Health and Activity Tracking (HAT). This helps you monitor the health of your BizTalk implementation and identify any bottlenecks. The tracking settings that you configure apply to all of the instances of the send port.

For background information on tracking, see Configuring Tracking. For complete information about configuring and using HAT, see Health and Activity Tracking.

The tracking settings that you configure apply to all of the instances of the receive port.

Prerequisites

To perform the procedure in this topic, you must be logged on with an account that is a member of the BizTalk Server Administrators group. For more detailed information on permissions, see Permissions Required for Deploying and Managing a BizTalk Application.

To configure tracking for a receive port

1. Click **Start**, click **Programs**, click **Microsoft BizTalk Server 2006**, and then click **BizTalk Server Administration**.

2. In the console tree, expand the BizTalk group and the BizTalk application for which you want to configure tracking for a receive port.

3. Click **Receive Ports**, right-click the receive port and click **Tracking**.

4. Configure the tracking options you want, as described in the following table, and then click **OK**.

Use this	To do this
Track Message Bodies - Request message before port processing	Select this check box to save and track message content before the message is received.
Track Message Bodies - Request message after port processing	Select this check box to save and track message content after the message is received.
Track Message Bodies - Response message before port processing	Select this check box to save and track message content before the message is sent. This check box is available only for request-response receive ports.
Track Message Bodies - Response message after port processing	Select this check box to save and track message content after the message is sent. This check box is available only for request-response receive ports.
Track Message Properties - Request message before port processing	Select this check box to track the promoted properties of an inbound message.
Track Message Properties - Request message before port processing	Select this check box if you want to track the promoted properties of an outbound message.
Track Message Properties - Response message before port processing	Select this check box to save and track message properties before the message is sent. This check box is available only for request-response receive ports.
Track Message Properties - Response message after port processing	Select this check box to save and track properties after the message is sent. This check box is available only for request-response receive ports.

How to Configure Tracking for a Pipeline

This topic describes how to use the BizTalk Server Administration to configure tracking for a pipeline. You might want to configure tracking for troubleshooting and auditing purposes.

You can view message properties, port events, and message events in the Find Message and Results views of Health and Activity Tracking (HAT). You can also track message events and port events for messages in the Message Flow view of HAT. For more information about HAT, see Health and Activity Tracking.

You can configure tracking for one of the default pipelines included with BizTalk Server 2006 or a custom pipeline that has been deployed into a BizTalk application. The tracking settings that you configure apply to all of the instances of the pipeline.

Prerequisites

To perform the procedure in this topic, you must be logged on with an account that is a member of the BizTalk Server Administrators group. For more detailed information on permissions, see Permissions Required for Deploying and Managing a BizTalk Application.

To configure tracking for a pipeline

1. Click **Start**, click **Programs**, click **Microsoft BizTalk Server 2006**, and then click **BizTalk Server Administration**.

2. In the console tree, expand BizTalk Server 2006 Administration and expand the BizTalk group containing the pipeline for which to configure tracking.

3. Do one of the following:

   - To configure tracking for one of the default BizTalk pipelines, expand <All Artifacts>.

   - To configure tracking for a custom pipeline that has been deployed into a BizTalk application, expand the application containing the pipeline.

4. Click the **Pipelines** folder, right-click the pipeline, and then click **Tracking**.

5. Configure tracking options you want, as described in the following table, and then click **OK**.

Use this	To do this
Port start and end events	Select this check box to track only when an instance starts and ends. Details include item name, assembly, and other metadata.
Message send and receive events	Select this check box to track message send and receive events. This check box is available only if **Port start and end events** is selected.
Messages before pipeline processing	Select this check box to save and track the message bodies received by the pipeline, which holds metadata such as URLs and promoted properties. If this is a receive pipeline, the message body is the raw message as submitted to the pipeline by the transport component. Depending on the application, the message might be encrypted, signed, or encoded. This check box is available only if **Message send and receive events** is

	selected.
Messages after pipeline processing	Select this check box to save and track the message bodies sent by the pipeline, which holds metadata such as URLs and promoted properties. If this is a receive pipeline, the message body is the processed message to be submitted to the MessageBox database, which may be XML depending on your application. This check box is available only if **Message send and receive events** is selected.

How to Configure Tracking for a Policy

This topic describes how to use the BizTalk Server Administration console to configure tracking for a policy. You can select options to view instance data, results of conditions, actions, and agenda updates in the query views of the administration console Group Hub page.

For more information about creating and using queries, see Using the BizTalk Server Administration Console. For more information about the health and activity tracking features of BizTalk Server 2006, see Health and Activity Tracking.

Prerequisites

To perform the procedure in this topic, you must be logged on with an account that is a member of the BizTalk Server Administrators group. For more detailed information on permissions, see Permissions Required for Deploying and Managing a BizTalk Application.

To configure tracking for a policy

1. Click **Start**, click **Programs**, click **Microsoft BizTalk Server 2006**, and then click **BizTalk Server Administration**.

2. In the console tree, expand the BizTalk group and the BizTalk application for which you want to configure tracking for a policy.

3. Click **Policies**, right-click the policy, click **Properties**, and then click **Tracking**.

4. Select the tracking options you want, as described in the following table, and then click **OK**.

Use this	To do this
Fast activity	Select this check box to track the instance data on which the policy operates.
Condition evaluation	Select this check box to track the true/false results of conditions in the selected policy.
Rule firings	Select this check box to track the actions started as a result of the policy.
Agenda updates	Select this check box to track updates to the agenda. The agenda contains

	a list of actions that are "true" and need to fire.

How to Configure Tracking for a Schema

This topic describes how to use the BizTalk Server Administration console to configure tracking for a schema. To configure tracking, you specify the properties of the messages that you want to view in the query views of the administration console Group Hub page.

For more information about creating and using queries, see Using the BizTalk Server Administration Console. For more information about the health and activity tracking features of BizTalk Server 2006, see Health and Activity Tracking. For background information about tracking message properties, see **Message Properties**.

Prerequisites

To perform the procedure in this topic, you must be logged on with an account that is a member of the BizTalk Server Administrators group. To you want to view tracking options only, you can be logged on as a member of the BizTalk Server Operators group. For more detailed information on permissions, see Permissions Required for Deploying and Managing a BizTalk Application.

To configure tracking for a schema

1. Click **Start**, click **Programs**, click **Microsoft BizTalk Server 2006**, and then click **BizTalk Server Administration**.

2. In the console tree, expand BizTalk Server 2006 Administration, expand the BizTalk group containing the schema for which you want to configure tracking, and then expand the application containing the schema.

3. Click **Schemas**, right-click the schema, and then click **Properties**.

4. In the left pane, click **Tracking**.

5. Do one of the following to specify which properties to use for tracking messages, and then click **OK**:

   - Select the **Always track all properties** check box use all message properties regardless of the schema version. This check box is available only for document schemas.

   - Select the **Select all message properties** check box to use all the listed properties.

   - Under **Properties list**, select the check box of each property that you want to use.

Using Health and Activity Tracking

This section provides task-specific information about using Health and Activity Tracking (HAT). It is recommended that you gain an understanding the features before using HAT:

- HAT displays the processing steps taken by messages. For more information about processing steps by messages, see Viewing Message Flow.
- HAT can retrieve messages by using either data or system information. For more information about retrieving messages, see How to Find Events and Messages by Message Property.
- HAT can display both archived and real-time data. For more information about archived and real-time data, see Viewing Archived and Live Data Using HAT.
- HAT limits data access to those people with appropriate permissions. For more information about data access, see **Access Control and Data Security**.
- HAT enables you to modify which data you want to track without affecting the rest of the BizTalk environment—no redeployment is necessary. For more information about modifying data, see Configuring Tracking.
- HAT enables you to do real-time debugging of your orchestrations. For more information real-time debugging, see Working with the Orchestration Debugger View.

In This Section

- Sample HAT Queries
- How to Open a Saved Query in Health and Activity Tracking
- How to Save a Query in Health and Activity Tracking
- Using the Reporting Menu in HAT
- Service Metrics and Message Metrics
- Viewing Archived and Live Data Using HAT
- How to Change the Query Timeout Value in Health and Activity Tracking

Sample HAT Queries

You can access the following Health and Activity Tracking query samples in a drop-down list from the **Queries** menu. The table below describes these queries.

Query name	Description
Message count in past week	Shows number of messages sent and received in past week.
Message counts	Shows of number of messages sent and received in the last 1, 2, 7 and 14 days in a table.
Messages received in past day	Displays all inbound messages for the last 24 hours.
Messages sent in past day	Displays all outbound messages for the last 24 hours
Most recent 100 service instances	Displays instances sorted by service start time.
Most recent 100 services terminated with errors	Displays instances sorted by service start time.
Recent service instances	Displays the most recently received messages not sent by another service instance and returns all service instances started after that time. For example, a message is submitted that starts 3 service instances. The query returns those 3 instances and no previously run instances.
Services running longer than 24 hours	Lists services that have been running for over 24 hours.

How to Open a Saved Query in Health and Activity Tracking

You can open an existing message or service instances query in Health and Activity Tracking (HAT).

Prerequisites

You must be logged on as a member of the Administrators group to perform this procedure.

To open a saved query in Health and Activity Tracking

1. Click **Start**, click **Programs**, click **Microsoft BizTalk Server 2006**, and then click **Health and Activity Tracking**.
2. On the **File** menu, click **Open**.
3. Click the query you want, and then click **Open**.

4. A security warning displays the first time you open a query. Optionally check **Don't show this message again**. Click **Yes** to continue.

How to Save a Query in Health and Activity Tracking

You can save a message or service instances query in Health and Activity Tracking (HAT).

Prerequisites

You must be logged on as a member of the Administrators group to perform this procedure.

To save a query in Health and Activity Tracking

1. Click **Start**, click **Programs**, click **Microsoft BizTalk Server 2006**, and then click **Health and Activity Tracking**.

2. On the **File** menu, click **Save Query As**.

3. In the **Save Query As** dialog box, in the **Path** box, provide the path to the destination directory where you want to save the query, or click **Browse** to select the destination directory. Be sure to include an appropriate file name for the query.

4. Type an optional description, and then click **OK**.

Using the Reporting Menu in HAT

The **Reporting** menu enables you to track archived data, to build a query and to create a report. Use a query in one of the Reporting views to examine an orchestration. The Reporting views give you access to the archived data. Reporting uses historical data that you may have been tracking for a long time. Use Reporting to see trends such as how many failures a month there are. You can troubleshoot by tracking the steps of a process or message. For example, if an order routed incorrectly, you can follow the message through to see where the request came in, where it went, and why.

Right-click the record in the results view and select the Orchestration Debugger. Use the debugger to step through the orchestration.

If you want to print the resulting report, you must first export it to an Excel spreadsheet and then print it from there. Export to Excel is an option on the shortcut menus.

In This Section

- What is the Find Message View?
- What is the Query Builder View?

What is the Find Message View?

You can use the Service Instances view in Health and Activity Tracking (HAT) to see what state suspended orchestrations or pipelines are in. The Service Instances view shows you metadata about the orchestration or pipeline.

When you need to troubleshoot transport-level problems, use the Message view to see undelivered messages. The Message view shows you metadata for each message as well as for the associated service instance.

When you see a suspended service or message in the BizTalk Server Administration Console, you can investigate it further by right-clicking the suspended service or message and then clicking **Service Details**, **Message Flow**, or **Orchestration Debugger**.

In many cases, you cannot resume a suspended message—for example, if it is corrupt. However, you can choose to save a message to disk before removing it from the Suspended queue.

If a message does get suspended, an error is sent to the transport component, which might trigger a fix. If this does not happen, you can retrieve that message body, modify it, and resubmit it through another port.

Use the **Resume** option to resend a failed outbound message.

Depending on the cause of the suspension, you might be able to resume suspended services. For example, if an orchestration hits a **Suspend** shape, or if a transport was unable to deliver a message, you can resume the instance by using the shortcut menu **Resume** command.

If you cannot resume the services, and you finish investigating the cause, you can terminate the instance. This removes the service from the message box. Terminating also removes any messages associated with this instance, if no other instance references them.

Service instances and message properties filter options

The Service Instances and Messages views both provide the same filtering capability. Selecting a filter or filters restricts the size of the Results list. If the Results list is too large, the query will time out and no longer access the MessageBox database.

The following table describes the filters you can set.

Filter	Description
Host	Filters records for service instances that are enlisted in the selected **Host** or **All**.
Class	Filters records for service instances that match the service class, which can be **Orchestration** or **Messaging** or **All**.
Name	Filters records for the specified service name or **All**.

Status	Filters records where the service instance has a specified status of **Suspended** or **Active** or **All**.
Select Query Limit	Filters by a range of dates, to a specified number of matches.

In This Section

- How to Find Events and Messages by Message Property

How to Find Events and Messages by Message Property

You can use the Find Message view in Health and Activity Tracking (HAT) to locate a specific message. The Find Message view lists both standard document and property schemas. After you select the message schema you want to investigate, you can optionally apply additional filters to look for messages based on routing properties, based on the message properties, or both. You can also specify no filters, and track all messages containing the properties in the selected schema. However, you should restrict the amount of data you retrieve if possible. HAT also includes a list of default queries on the **Queries** menu that you can use without having to build them yourself.

When you run a query, a results list displays all the details and promoted properties for messages that match your query. The results list contains many columns; you can use the Field list to hide some of the columns. For an explanation of the fields, see What is the Results List View?. For more information about sizing the results list, see How to Control the Size of the Results List.

Prerequisites

You must be logged on as a member of the Administrators group to perform this procedure.

To find events and messages by message property

1. Click **Start**, click **Programs**, click **Microsoft BizTalk Server 2006**, and then click **Health and Activity Tracking**.

2. On the **Reporting** menu, click **Find Message**.

3. In **Find Message View**, click **Schema**, and then select the either the orders or valuation schema for the inbound message as appropriate.

4. If additional filtering is desired, select one or more of the routing properties filters or message properties filters as desired.

   Routing properties filter

   The routing properties filter enables you to query for messages based on how they are being routed through BizTalk Server. You can search on the following parameters:

Parameter	Action
Port	Looks for messages processed by a specific port, whether they are being sent or received. The default value is all ports.
Party	Looks for messages based on sending or receiving party. The default value is **All parties**. Use the **Empty** option to search for messages from unidentified parties.
From time/To time	Narrows your search by specifying a time range for tracking sent or received messages.

Message properties filter

The Message properties filter allows you to query for messages based promoted properties. You can specify up to five promoted property conditions to filter the results. There is an implicit **AND** clause between multiple conditions, so the data returned matches all the conditions. Promoted properties from the schema populate list fields.

Use this	To do this
First **Message Property** drop-down list	Select the property you want to search on.
First **Operator** drop-down list	Select the operator you want to search on.
First **Value** field	Enter the required value.

You must select a property, select an operator, and then enter the value on which to search. When the operator appears as IS NULL, or IS NOT NULL, you cannot write a value, and the text box is dimmed.

To specify a bounding range, you can query the same property in multiple fields. For example, you can perform the following query:

DISCOUNT < 100

DISCOUNT > 20

5. Click **Run Query**.

The results list displays the results of your query at the bottom of the screen. For more information about the views and actions available, see What is the Results List View?.

What is the Query Builder View?

Use the Query Builder view from the **Reporting** menu in Health and Activity Tracking (HAT) to track both live and archived data, and to create queries against any of the standard metadata associated with tracked events. You should use the Query Builder view when you

need to locate a tracked event that is not covered by the Find Message view, such as service instances.

The SQL Views pane of this view contains a tree of the fields that you can use to build your query:

- Service metrics: Fields associated with service instances.
- Message metrics: Fields associated with messages.

You can expand this tree to view all of the fields.

You can create your own query against the SQL Server and Analysis Server databases in the SQL Query pane. Use standard T-SQL syntax combined with dragging the specific data items from the SQL Views pane. For example, you might type **Select * from** in the SQL Query pane and then drag the ServiceMetrics folder from the SQL Views pane into the query in the right pane.

The more information you provide, the narrower the search becomes, and the faster it executes. For example, if you want to trace a particular schedule that failed or was terminated, you will get faster and more specific results if you enter the timeframe and the name of the assembly.

The query results appear in the Results list on the bottom of the same screen as the query. You can save any queries that you create for later use.

For more information about the views and actions available from the Results list, see What is the Results List View?.

In This Section

- How to Create a Query in Health and Activity Tracking
- How to View All Instance Information
- How to View Completed Orchestrations or Pipelines
- How to View Running Orchestrations or Pipelines
- How to View Suspended Orchestrations or Pipelines
- How to View Failed Orchestrations or Pipelines

How to Create a Query in Health and Activity Tracking

The Query Builder view in Health and Activity Tracking (HAT) is available for both live and archived data through the **Reporting** menu. When you complete the following steps to create a query, your query might look similar to this:

Prerequisites

You must be logged on as a member of the Administrators group to perform this procedure.

To create and execute a query in Health and Activity Tracking

1. Click **Start**, click **Programs**, click **Microsoft BizTalk Server 2006**, and then click **Health and Activity Tracking**.
2. On the **Reporting** menu, click **Query Builder**.
3. In the **SQL Query** pane, type **Select * from**.
4. In the **SQL Views** pane, drag either **ServiceMetrics** or **MessageMetrics** to the **SQL Query** pane.
5. To add more fields to your query:
   a. Type **where** beside the query.
   b. On the left pane expand the metric you are querying, and drag the field you want to query to the right pane.
   c. Type an operand (predicate?) (<>=) .
   d. Type a value.
6. Click **Run Query** to execute the query.

   The results list appears at the bottom of the Query Builder view. You can now examine any of the instances displayed in the Results list.

To view detailed result information

- Right-click a cell in the Results list and select **Orchestration Debugger** or **Message Flow** from the shortcut menu

How to View All Instance Information

To view all the information

1. Click **Start**, click **Programs**, click **Microsoft BizTalk Server 2006**, and then click **Health and Activity Tracking**.
2. On the **Reporting** menu, click **Query Builder**.
3. In the **SQL Query** pane, type **Select * from** [dbo].[dtav_ServiceFacts]
4. To filter for time to reduce the number of events you see, type **where** [ServiceInstance/StartTime] **> '10/11/2002 10:15'**

5. Click **Run Query** to execute the query.

The results list appears at the bottom of the Query Builder view. You can now examine any of the instances displayed in the Results list.

How to View Completed Orchestrations or Pipelines

To view completed orchestrations or pipelines

1. Click **Start**, click **Programs**, click **Microsoft BizTalk Server 2006**, and then click **Health and Activity Tracking**.
2. On the **Reporting** menu, click **Query Builder**.
3. In the **SQL Query** pane, type **Select * from** [dbo].[dtav_ServiceFacts] **where** [ServiceInstance/State] **= 'Completed'**
4. Click **Run Query** to execute the query.

The results list appears at the bottom of the Query Builder view. You can now examine any of the instances displayed in the Results list.

How to View Running Orchestrations or Pipelines

To view running orchestrations or pipelines

1. Click **Start**, click **Programs**, click **Microsoft BizTalk Server 2006**, and then click **Health and Activity Tracking**.
2. On the **Reporting** menu, click **Query Builder**.
3. In the **SQL Query** pane, type **Select * from** [dbo].[dtav_ServiceFacts] **where** [ServiceInstance/State] **= 'Running'**
4. Click **Run Query** to execute the query.

The results list appears at the bottom of the Query Builder view. You can now examine any of the instances displayed in the Results list.

How to View Suspended Orchestrations or Pipelines

To view suspended orchestrations or pipelines

1. Click **Start**, click **Programs**, click **Microsoft BizTalk Server 2006**, and then click **Health and Activity Tracking**.
2. On the **Reporting** menu, click **Query Builder**.
3. In the **SQL Query** pane, type **Select * from** [dbo].[dtav_ServiceFacts] **where** [ServiceInstance/State] **= 'Suspended'**

4. Click **Run Query** to execute the query.

   The results list appears at the bottom of the Query Builder view. You can now examine any of the instances displayed in the Results list.

How to View Failed Orchestrations or Pipelines

To view failed orchestrations or pipelines

1. Click **Start**, click **Programs**, click **Microsoft BizTalk Server 2006**, and then click **Health and Activity Tracking**.

2. On the **Reporting** menu, click **Query Builder**.

3. In the **SQL Query** pane, type **Select * from** [dbo].[dtav_ServiceFacts] **where** [ServiceInstance/ExitCode] **<> 0**

4. Click **Run Query** to execute the query.

   The results list appears at the bottom of the Query Builder view. You can now examine any of the instances displayed in the Results list.

What is the Results List View?

All Health and Activity (HAT) tracking presents the results of your queries in a results list that appears in a pane at the bottom of the current view. The results list is an Office Web Component PivotTable report and operates very much like a PivotTable report in Excel. You can access a shortcut menu for each results list. The menu shows all of the actions you can perform on the selected record within the currently active views. For example, if the record contains a Service Instance ID, then service-related actions appear. If there is a Message ID, then Message-related actions appear.

You cannot directly access the results list. This view is always invoked from the Message Metrics or Service Metrics views, the Query Builder, or the Find Message view. The results list appears at the bottom of the screen, below the view that originated the query.

The following table shows a complete list of the items that appear on the results list.

Service or Message Field	Description
Service/Name	Name of the message or service instance.
Type	Type of service (for example, messaging (reported as Pipeline), orchestration, transport adapter.
Instance/State	Shows the current state of the instance.
Exit Code	Error code (if any) reported by the service instance when it finished.

Error Info	Detailed error information reported by the service instance that has finished.
Start Time	Time the operation started.
End Time	Time the operation ended.
Duration	How long the operation took.
Host	Name of the BizTalk Server Host running the service instance.
Assembly Name	Name of the .net assembly that implements the service instance.
Assembly Version	Version number of the related assembly.
Deployment Time	Time that service instance assembly deployed into BizTalk.
Activity ID	Identifies unique service instance activity (for example, messages sent/receive by the pipeline/orchestration have the same ID).
Instance ID	Globally Unique Identifier (GUID) that identifies a run of a service instance.
Version GUID	GUID that identifies a given version of a deployed service type. Different versions of the same service type will have same service GUID but different Version IDs.
Service GUID	A service independent GUID that identifies a service (for example, orchestration).

Because you may not need all the information contained in this complete list, you can select only those columns you wish to view, or you can replace columns that you removed. For more information.

You can sort the results list, by right-clicking the header of the column you want to sort, and clicking **Sort Ascending** or **Sort Descending** from the shortcut menu.

Shortcut Menus

A shortcut menu appears when you right-click a service or message instance in a Results list in the HAT tool. The shortcut menu accessed from service or message metrics Results list offers these action options:

- Message Flow
- Orchestration Debugger
- Save All Tracked Messages

- Sort Ascending
- Sort Descending
- Export to Excel
- Field List
- Copy

The following table shows the options available in the shortcut menu for **All Messages** when you right-click a **Message instance** in the Results list.

Option	Action
Service Details	Opens the Service Details view, which shows the details of the selected service instance.
Message Flow	Opens the Message Flow view for the selected service instance that enables you to trace messages from the point of arrival through messaging and orchestrations to their completion.
Orchestration Debugger	Opens the Orchestration Debugger for the selected orchestration instance, which enables you to follow the execution of individual shapes within an orchestration.
Save All Tracked Messages	Saves all the tracked message instances related to a specific service instance. You select the save location for these messages.

The following table shows the options in the shortcut menu for the Results list itself.

Option	Action
Sort Ascending	Sorts the Results list by the selected column in ascending order.
Sort Descending	Sorts the Results list by the selected column in descending order.
Export to Excel	Exports results to an Excel spreadsheet.*
Field List	Opens the PivotTable Field List window and enables you to add and remove columns from the Results list.
Copy	Copies the selected cell.

* If you want to print the resulting report, you must first export it to an Excel spreadsheet and then print it from there.

All the above options are interactive Office 2000 Web Components (OWC) functions.

When you sort the Results list by time, the instances sort up to milliseconds, even if no milliseconds appear on the list.

From the Results list, you can go to the Orchestration Debugger view or Message Flow view.

Orchestration Failures in HAT

Orchestrations vary in complexity; for example, an orchestration may call a .NET object or construct messages via transform and assignment shape. As a result, it is impossible to list out every possible failure, due to the variety of its content as well as level of customization. However, all failures encountered in orchestrations appear as exceptions.

If an orchestration does not include any **CatchException** shape for an exception, the exception causes the orchestration to be Suspended, but not resumable. This means that Health and Activity Tracking (HAT) or a WMI script cannot recover the instance. However, you can save all messages associated with the Suspended (not Resumable) instance using HAT (or WMI script) for diagnostic and manual retry.

To diagnose the problem, use the Orchestration Debugger in HAT to see the last shape executed before the instance is suspended. You can also view exception details using the Orchestration Debugger.

Types of Message Failures in HAT

This topic lists different points where a message failure may occur. You cannot use Health and Activity Tracking (HAT) to recover from any of these failures.

Failures in the disassembly phase

Processing might also fail during the disassembly phase; that is, failure in one of the pipeline components. For example, decryption failed due to absence of decryption cert on the processing server, or parsing failure due to problem either in the schema or in the message.

Failures in routing

After a message disassembles successfully, the next potential failure point is routing; for example, users enable a corresponding receive location of an orchestration and forget to enlist the orchestration. In this case, the message picked up from the receive location fails routing and the MessageBox database generates a Routing Failure report.

Routing Failure reports are listed in the BizTalk Server Administration Console as non-resumable suspended messages. Each Routing Failure report contains a message property snap shot taken when the routing failure occurred. You can use the information in each report to determine why routing failed for its associated message. If the associated message is resumable, you can correct the routing problem and resume the message so that processing continues. When you search for service instances in HAT, Routing Failure

reports are listed in the results list with a blank service name and service type. When you terminate a suspended instance, the Routing Failure report associated with the suspended instance is automatically deleted by the Operations_OperateOnInstances_OnMaster_BizTalkMsgBoxDb job that runs every minute by default.

Failures during the transformation phase

- **Received Messages**. When a message is received from Receive Location, the message might optionally be transformed to a different format via an Inbound Map specified on Send Port; then the transformed message is disassembled (for exampled decrypted and parsed) and published to the MessageBox for routing to an orchestration or a Send Port. In this case, processing may fail during transformation phase due to incorrect Inbound Map, or problems in the schema or in the message received.

- **Sent Messages**. When a message is to be sent to a Send Location, an Outbound Map configured on Send Port might optionally transform the message. Then the transformed message is assembled and handed to the adapter for final transmission to the Send Location. In this case, processing may fail during transformation phase due to incorrect Outbound Map or problem in schema or source message.

Failures in the message assembly phase

Processing can also fail during message assembly phase – in other words, failing in pipeline component. After a message successfully assembles, the next potential failure point becomes transmission to Send Location; for example, the Send Location (which belongs to the partner) might be down or not exist.

Viewing Tracked Information

When you run a query, the tracked information appears in the results list at the bottom of the Health and Activity Tracking (HAT) window. For more information about the views and actions available, see What is the Results List View?.

Viewing message details

You have several options in HAT to view the message details:

- You can right-click any message referenced by a service instance and select Message details.

- If the message is already processed but it was tracked—because you had tracking turned on in HAT—you can save it to your hard disk and examine it.

- You can attach to the orchestration instance and use the Orchestration Debugger.

Viewing service details

When a suspended service appears in the event log, you can track the service by using one of the Operations views. You can investigate a service by using the **Service Details**, **Message Flow**, or **Orchestration Debugger** options from the **Context** menu.

Viewing orchestration details

Use the Orchestration Debugger to view the path a message instance has taken through an orchestration. As you step through, a rendered image of the orchestration shows the progress of the message, and allows you to place breakpoints in the orchestration for debugging purposes.

Viewing suspended instances

You can access the service instances and referenced messages through the Operations views.

If a failure occurs in the pipeline, the instance is suspended and the message body is not tracked, because HAT tracks only successfully sent and retrieved message. The MessageBox stores messages associated with suspended pipelines. You can retrieve the messages using the Operations views. To view suspended instances, select the **Suspended** filter for the instance.

Using the Administration Console Query Tab

You can use the Query tab in the BizTalk Server Administration Console to search for and locate specific running and suspended service instances, messages, or subscriptions. Queries performed using the Administration Console locate live items, which are stored in the MessageBox database. A new query tab appears each time you run a new query.

To locate archived messages or service instances, you use Health and Activity Tracking (HAT). For more information, see Health and Activity Tracking.

In This Section

- How to Save a Query
- How to Open a Saved Query
- How to Search for All Service Instances
- How to Search for Running Service Instances
- How to Search for Suspended Service Instances
- How to Search for Messages
- How to Search for Subscriptions

How to Save a Query

To save a query

1. Click **Start**, click **Programs**, click **Microsoft BizTalk Server 2006**, and then click **BizTalk Server Administration**.
2. In the console tree, expand **BizTalk Server 2006 Administration**, and then click the BizTalk group.
3. In the details pane, click the **New Query** tab.
4. Create a query as desired, and then click **Save As**.
5. In the **Save As** dialog box, browse to or create the folder where you want to save the query.
6. In **File name**, type a name for the query, and then click **Save**.

How to Open a Saved Query

To open a saved query from disk

1. Browse to the folder where the saved query is stored.
2. Double-click the saved query, which opens the BizTalk Server Administration Console and executes the query.

To open a saved query from the Administration Console

1. Click **Start**, click **Programs**, click **Microsoft BizTalk Server 2006**, and then click **BizTalk Server Administration**.
2. In the console tree, expand **BizTalk Server 2006 Administration**, and then click the BizTalk group.
3. In the details pane, click the **New Query** tab, and then click **Open Query**.
4. In the **Open** dialog box, browse to the saved query that you want to open, select that query, and then click **OK**.

How to Search for All Service Instances

To search for all service instances

1. Click **Start**, click **Programs**, click **Microsoft BizTalk Server 2006**, and then click **BizTalk Server Administration**.
2. In the console tree, expand **BizTalk Server 2006 Administration**, and then click the BizTalk group.

3. In the details pane, click the **New Query** tab.

4. In the **Query Expression** group, in the **Value** column, select **All Service Instances** from the drop-down list box.

5. In the **Field Name** column, in the empty drop-down list box next to the asterisk (*****), select one or more of the following:

Item	Description
Application Name	The BizTalk Server application.
Creation Time	Find all service instances created before or after the specified date.
Group Results By	You can group results by application, host name, service class, service instance status, or service name.
Host Name	The name of the BizTalk Host.
Instance Status	You can search for all running instances, all suspended instances, active instances, dehydrated instances, ready to run instances, scheduled instances, suspended but not resumable instances, or suspended and resumable instances.
Maximum Matches	The number of matches to display.
Service Class	You can search for isolated adapters; messaging; messaging, MSMQT, and isolated adapters; MSMQT; Orchestration; or Routing Failure Report.
Service Instance ID	You can group or filter service instances by service instance ID.
Service Name	You can group or filter service instances by service name.
Service Type ID	You can group or filter service instances by service type ID.

6.Complete the **Value** column as appropriate for the selection you made in the **Field Name** column.

Continue adding additional lines to the query as appropriate, by completing the **Field Name**, **Operator**, and **Values** columns, and then click **Run Query**.

How to Search for Running Service Instances

To search for running service instances

1. Click **Start**, click **Programs**, click **Microsoft BizTalk Server 2006**, and then click **BizTalk Server Administration**.

2. In the console tree, expand **BizTalk Server 2006 Administration**, and then click the BizTalk group.

3. In the details pane, click the **New Query** tab.

4. In the **Query Expression** group, in the **Value** column, select **Subscriptions** from the drop-down list box.

5. In the **Field Name** column, in the empty drop-down list box next to the asterisk (*****), select one or more of the following:

Item	Description
Maximum Matches	The number of matches to display.
Service Instance ID	You can group or filter running services instances by service instance ID.
Service Name	You can group or filter running service instances by service name.
Subscription Type	You can group or filter running service instances by Activation Subscription or Instance Subscription.

6. Complete the **Value** column as appropriate for the selection you made in the **Field Name** column.

7. Continue adding additional lines to the query as appropriate, by completing the **Field Name**, **Operator**, and **Values** columns, and then click **Run Query**.

How to Search for Suspended Service Instances

To search for suspended service instances

1. Click **Start**, click **Programs**, click **Microsoft BizTalk Server 2006**, and then click **BizTalk Server Administration**.

2. In the console tree, expand **BizTalk Server 2006 Administration**, and then click the BizTalk group.

3. In the details pane, click the **New Query** tab.

4. In the **Query Expression** group, in the **Value** column, select **Suspended Service Instances** from the drop-down list box.

5. In the **Field Name** column, in the empty drop-down list box next to the asterisk (*****), select one or more of the following:

Item	Description
Application Name	The name of the BizTalk Server application.
Creation Time	Find suspended service instances created before or after the specified date.
Error Adapter	You can group or filter suspended service instances by adapter type: EDI, File, FTP, HTTP, MQSeries, MSMQ, POP3, SMTP, SOAP, SQL, or Windows SharePoint Services.
Error Code	You can group or filter suspended service instances by error code to show all that service instances have been suspended with that error code.
Error Description	You can group or filter suspended service instances with the specified error description.
Group Results By	You can group or filter results by adapter, application, error code, error description, host name, service class, service instance status, service name, or URI.
Host Name	Group or filter suspended service instances by host name.
Instance Status	You can search for suspended but not resumable instances, or suspended and resumable instances.
Maximum Matches	The number of matches to display.
Service Class	You can search for isolated adapters; messaging; messaging, MSMQT, and isolated adapters; MSMQT; Orchestration; or Routing Failure Report.
Service Name	You can group or filter suspended service instances by service name.
Service Type ID	You can group or filter suspended service instances by service type ID.
Suspension Time	You can group or filter suspended service instances suspended before or after the specified date.
URI	You can group or filter suspended service instances by URI.

6. Complete the **Value** column as appropriate for the selection you made in the **Field Name** column.

7. Continue adding additional lines to the query as appropriate, by completing the **Field Name**, **Operator**, and **Values** columns, and then click **Run Query**.

How to Search for Messages

To search for messages

1. Click **Start**, click **Programs**, click **Microsoft BizTalk Server 2006**, and then click **BizTalk Server Administration**.

2. In the console tree, expand **BizTalk Server 2006 Administration**, and then click the BizTalk group.

3. In the details pane, click the **New Query** tab.

4. In the **Query Expression** group, in the **Value** column, select **Messages** from the drop-down list box.

5. In the **Field Name** column, in the empty drop-down list box next to the asterisk (*****), select one or more of the following:

Item	Description
Creation Time	Find messages created before or after the specified date.
Error Adapter	You can group or filter messages by adapter type: EDI, file, FTP, HTTP, MQSeries, MSMQ, POP3, SMTP, SOAP, SQL, or Windows SharePoint Services.
Error Code	You can group or filter messages by error code.
Error Description	You can group or filter messages by error description.
Host Name	You can group or filter messages by host name.
Instance Status	You can search for all of the following types of instances: all running instances, all suspended instances, active instances, dehydrated instances, ready-to-run instances, scheduled instances, suspended but not resumable instances, or suspended and resumable instances.
Maximum Matches	The number of matches to display.
Message ID	You can group or filter messages by message ID.
Message Status	You can search for messages with consumed, in process, suspended, suspended but not resumable, suspended and resumable, undelivered, undelivered but scheduled, and undelivered but waiting for retry status.
Message Type	You can group or filter messages by message type.
Service Class	You can search for isolated adapters; messaging; messaging, MSMQT, and

	isolated adapters; MSMQT; Orchestration; or Routing Failure Report.
Service Instance ID	You can group or filter messages by service instance ID.
Service Name	You can group or filter messages by service name.
Service Type ID	You can group or filter messages by service type ID.
URI	You can group or filter messages by URI.

6. Complete the **Value** column as appropriate for the selection you made in the **Field Name** column.

7. Continue adding additional lines to the query as appropriate, by completing the **Field Name**, **Operator**, and **Values** columns, and then click **Run Query**.

How to Search for Subscriptions

To search for subscriptions

1. Click **Start**, click **Programs**, click **Microsoft BizTalk Server 2006**, and then click **BizTalk Server Administration**.

2. In the console tree, expand **BizTalk Server 2006 Administration**, and then click the BizTalk group.

3. In the details pane, click the **New Query** tab.

4. In the **Query Expression** group, in the **Value** column, select **Subscriptions** from the drop-down list box.

5. In the **Field Name** column, in the empty drop-down list box next to the asterisk (*****), select one or more of the following:

Item	Description
Maximum Matches	The number of matches to display.
Service Instance ID	You can group or filter subscriptions by service instance ID.
Service Name	You can group or filter subscriptions by service name.
Subscription Type	You can group or filter subscriptions by Activation Subscription or Instance Subscription.

6. Complete the **Value** column as appropriate for the selection you made in the **Field Name** column.

7. Continue adding additional lines to the query as appropriate, by completing the **Field Name**, **Operator**, and **Values** columns, and then click **Run Query**.

Service Instance States

As a message is processed, the following actions take place:

- In the receive location, the receive adapter—or transport component—receives the message from an external application and submits it to BizTalk for processing.
- The receive pipeline decrypts, decodes, and disassembles the message.
- The message engine sends the message and its shortcut properties—such as message type and origin—to the MessageBox database.
- When a matching subscription is filled, the message is processed according to a set of schemas and maps, and sometimes business rules or policies that reside on the host server.
- After it is processed, the resulting message is persisted (written) to the MessageBox database. The shortcut properties have been modified to indicate where to send the message, for example, which send port to use.
- The shortcut properties of the message are evaluated against the filter expressions defined for the send port, and the MessageBox database delivers the message to the appropriate send port.
- A subscription to a send pipeline and/or send port must be met for the message to be sent. The message is encrypted and transmitted.

Each process in this cycle generates its own set of events.

As service instances (receive ports, orchestrations, send ports) process messages moving through BizTalk Server, these service instances can be in one of several states. This section discusses what those states are, and shows examples of states at different times in their lifecycle.

The following table shows the various possible states of a service instance, with an explanation for each state.

State	Explanation
In breakpoint	An active orchestration hits a breakpoint, typically one set by a BizTalk Server solutions developer. This state is valid only for orchestrations.
Ready to run	A service instance that has been activated but has not yet started running, typically due to temporary unavailability of resources, such

	as a heavy processing load on the server.
Active	Running service instance.
Dehydrated	Instance state persists in the MessageBox database and no Windows service is running that instance.
Suspended (resumable)	Instance suspended, you can resume it.
Suspended (not-resumable)	Instance suspended, but you cannot resume it. You can save the Messages referenced by the instance, and then you can terminate the instance.
Pending suspend/Pending terminate	A status, not an independent state. You can combine it with other states. A control message to suspend or terminate was sent to a service instance, but has not yet been picked up by the instance. Only one pending operation allowed at a time. When an instance with a pending operation becomes dehydrated, you can terminate the instance.

The following table shows the states before and after an operation.

Starting state	**New state after operation is applied**					
	In breakpoint	**Active**	**Dehydrated**	**Suspended**	**Terminated**	**Pending terminate**
In breakpoint	Attach from debugger	Continue from debugger	Stop Windows Service			Terminate
Ready to run				Suspend	Terminate	
Active			Stop Windows Service			Terminate
Dehydrated			Stop Windows Service	Suspend	Terminate	
Suspended (resumable)	Resume in breakpoint from debugger	Resume			Terminate	
Suspended (not-					Terminate	

resumable)						
Pending suspend	Attach can be attempted but should eventually fail		Stop Windows Service	Request processed	Terminate will only work when instance is dehydrated	
Pending terminate	Attach can be attempted but should eventually fail		Stop Windows Service, instance dehydrates		Request processed, or instance dehydrated	

The following table shows the change of state when the system performs an operation on an instance.

Starting state	**Operation**					
	Terminate	**Suspend**	**Resume**	**Resume in breakpoint**	**Continue**	**Attach**
In breakpoint	Terminated	Suspended			Active	In breakpoint
Ready To run	Terminated	Suspended				
Active	Terminated	Suspended				
Dehydrated	Terminated	Suspended				
Suspended (resumable)	Terminated		Active	In breakpoint		
Suspended (not-resumable)	Terminated					
Pending suspend	Terminated; will only work when instance is dehydrated					Race condition
Pending terminate	Terminated; will only work, when instance is dehydrated					Race condition

Viewing Message Flow

A message flow is the set of contiguous processing steps taken by a message. You access the Health and Activity Tracking (HAT) Message Flow view through the shortcut menu that appears when you right-click a service or message instance. You can switch back and forth between the Message Flow view and the Orchestration Debugger.

The Message Flow view shows you details about a particular orchestration or pipeline instance after the orchestration or pipeline has completed processing the message. You can see which messages the system sent and received, and technical details of each message, such as the URL, port, and party used. The Message Flow view enables you to drill down into the orchestrations and/or pipelines that sent and received the message to see what happened. You can trace the entire path of an activation message through all of the pipelines and orchestrations and associated messages.

The top of the Message Flow window displays the Service Instance information, such as start and end time, error codes, and version. The bottom of the window displays the Message Activity for the Service Instance, detailing which messages were received or sent. You can view more details for each message instance by selecting the Expand or Collapse buttons. The message instances show all the details by default.

Next to the In/Out column, target namespace and root element identify the schema. Then you can find the details about the message. Underneath the schema information, appears a link with an item name, for example, EquityLoanReceivePipeline. Clicking the link provides you with the information for that item, thus enabling you to follow the message through it.

To return to the service that you started with, click the corresponding source or destination item in the other item.

The following table shows the technical information displayed for each service.

Name	Contents
Instance ID	The Globally Unique Identifier (GUID) associated with the instance.
Host	Name of the Host executing the orchestration or pipeline.
State	Current state of the instance. Possible states are Running, Completed, Manually Suspended, Error, Terminated, In Debug Mode, and Breaking.
Start Time	Time the orchestration/pipeline started.
End Time	Time the orchestration/pipeline completed.
Duration	How long, in milliseconds, the item took to run.
Exit Code	Technical Exit code.
Error Info	Text message about error.

Name	Name of the orchestration or pipeline.
Type	Type of the item—orchestration or pipeline.
Version ID	Unique version of the item.
Deployment Time	When the orchestration/pipeline deployed.

Below the Item detail table shows the message activity for the service instances sent or received by the particular orchestration or pipeline. Each row of the table represents one message and you can expand a message instance to show details about the message, such as ID, size, and name of port.

The following table shows the information that is displayed for each message instance.

Name	**Contents**
In/Out	A Message Received or a Message Sent icon indicates the states of messages.
Message Instance	Target namespace and top-level element; Unparsed Interchange if unknown.
Message Status	Possible statuses: OK, In Transmission, Transmission Failure, Transmission Failure (to be retried), and Transmission Failure (to be resubmitted in backup transport).
Timestamp	Time this particular message was involved in the current action (send/receive).

After you expand the message instance, the following information is displayed.

Name	**Contents**
Message Instance ID	GUID of the message.
Size	Size of the message. No value is displayed if the message has no size.
Parts	Number of parts in the message not including shortcut.
Adapter	Adapter used to transmit the message. Some possible adapters are File, HTTP, SOAP, BizTalk Message Queuing, and SOAP.
URL	Source or destination URL.

Port	Name of the port the message was sent or received.
Party Name	Name of the party sending/receiving the message. This field displays only if the information is known.
Decryption Certificate	Thumbprint of the certificate used for decrypting the message. This field only displays if a message includes a decryption certificate.
Signature	Signature in the message. This field only displays if the message was signed.
Status Icon	The current status of the message which can include Received, Sent, or in Work Queue).
Source/Target Item URL	The item (Orchestration or Pipeline) identified as the source/destination for the message. When clicked, the system redirects the user to a view for that item instance.

When you view an orchestration instance, you can switch to the Orchestration Debugger view by clicking **Switch to Orchestration Debugger**.

Debugging an Orchestration with HAT

The Orchestration Debugger enables you to track the activity of a single orchestration instance on a shape-by-shape basis. It displays a rendered view of the orchestration created in the Orchestration Designer.

You access the Orchestration Debugger through a shortcut menu by right-clicking any service or message instance associated with an orchestration type. You can switch back and forth between the Orchestration Debugger and the Message Flow view.

The Orchestration Debugger provides the following functionality:

- Displays a rendered view of the orchestration in which you can replay each processing step for that particular orchestration.
- Enables you to set breakpoints before any orchestration shape and continue execution.
- Enables you to look at specific variables and message data.
- Automatically enables all of the tracking options for a particular orchestration instance when that instance opens in the Orchestration Debugger.
- It gives you the ability to continue, resume in debug, and terminate the particular orchestration instance.

The two modes for using the Orchestration Debugger are:

- Reporting Mode in Orchestration Debugger
- Interactive Mode in Orchestration Debugger

The capabilities differ depending on the state of the service. You can perform interactive debugging by invoking any service instance currently in the In Breakpoint state, from any view. For information about debugging an orchestration, see How to Switch to Orchestration Debugger View from Message Flow View.

In This Section

- Orchestration Debugger User Interface
- Considerations when Using Orchestration Debugger

Orchestration Debugger User Interface

In interactive (debug) mode, the Orchestration Debugger view contains three areas: Service pane, Tracked Events pane, and the Orchestration pane. In addition, in interactive mode, the Variable list and Variable properties display across the bottom of the view.

In This Section

- Service Pane in Orchestration Debugger
- Tracked Events Pane in Orchestration Debugger
- Orchestration Pane in Orchestration Debugger
- Reporting Mode in Orchestration Debugger
- Interactive Mode in Orchestration Debugger

Service Pane in Orchestration Debugger

The top pane of the Orchestration Debugger window displays the following information.

Tag	Detail
Name	Indicates the current view (Orchestration Debugger), and allows you to navigate to the Message Flow view.
Instance Details	Displays the service name and the GUID that uniquely identifies the current orchestration instance.
Modes	Debug mode (Replay/Live), Orchestration state (Started, Suspended, Completed, etc.), Attached (Yes or No), and Breakpoint mode (On Class or On Instance).
Service	Drop-down list of actions that you can perform based on the state of the

Options	debugger and the instance.

Below this information, the Orchestration Debugger has two panes—the Tracked Events pane on the left, and the Orchestration pane on the right.

Tracked Events Pane in Orchestration Debugger

The Tracked Events pane lists the status of every action performed in the orchestration, such as whether it started or completed. As you select each of the rows in this pane, the corresponding shape in the Orchestration pane appears highlighted in green when the shape starts and blue when the shape finishes.

The Tracked Events pane shows the following columns.

Option	Action
Action Status (left column)	Status of the particular action. An arrow indicates the action has started and a termination shape indicates it has completed.
Action Name	Name of the action in the orchestration.
Action Type	Type of shape that represents the action. An arrow indicates that the action has started and a termination shape indicates it has completed.
Time	Time the action was performed.
Date	Date the action was performed.

Orchestration Pane in Orchestration Debugger

The Orchestration pane in Health and Activity Tracking (HAT) is the area where the orchestration instance renders with all of its shapes. The following table shows the Context menu actions for the Orchestration pane.

Option	Action
Set Breakpoint on Class	Right-click a shape for the **Set Breakpoint on Class** option. A red dot appears on the shape indicating the breakpoint has been set.
Set Breakpoint on Instance	Right-click a shape for the **Set Breakpoint on Instance** option. A red dot appears on the shape indicating the breakpoint has been set.
Remove Breakpoint on Class	Right-click a shape for the **Remove Breakpoint** option. The red dot disappears from the shape indicating the breakpoint has been removed.
Remove Breakpoint on Instance	Right-click a shape for the **Set Breakpoint on Instance** option. The red dot disappears from the shape indicating the breakpoint has been removed.

Variable List and Variable Properties panes

These panes only appear for interactive debugging when attached to the Orchestration runtime using the **Attach** service option. These panes appear at the bottom of the screen.

The Variable List displays the Name, Value, and Type of the variable. The Value indicates if the variable is Null or, if not, then what kind of object it contains. Type is the **Assembly.Namespace.Name** of the object.

The Variable Properties pane displays properties for the variable that vary according to the type of object. For example, for ports this includes Address, Name, Scope, Type, and Value. Messages show the shortcut; for each part in the message, there is Name, Size, Properties, Type, and Value. Collections such as Context and Properties display in a pop-up. A partial display of the Value appears as a ToolTip.

The user advances through the schedule from breakpoint to breakpoint and examines the state of these variables.

The following table shows the Context menu actions for the Variable List.

Option	Action
Save Message	Right-click a Message that is non-null in the Variable List pane for the **Save Message** option. A message appears prompting you to select a directory to which to save it.

Service Options drop-down list

The Service Options drop-down list shows you the valid actions based on the state of the instance and the debugger. The following table shows the available actions in the Service Options drop-down list.

Option	Action
Continue Service	Continues an orchestration instance that stopped at a breakpoint if you attached the service.
Resume in Debug mode	Resumes a suspended orchestration instance in debug mode. This enables you to go into interactive mode, attach to the instance, and debug it interactively. Available from the Operations views and the Orchestration Debugger. It only applies to orchestrations.
Terminate Service	Terminates an orchestration instance.
Attach	Attaches the service to the orchestration instance and retrieves the current state and variables
Remove all Breakpoints on Class	Removes all the breakpoints in the orchestration class. Only available when not attached.
Remove all Breakpoints	Removes all the breakpoints in the orchestration instance. Only available when attached.
Save All Messages	Saves all the messages associated with the orchestration instance as long as you have selected to track all inbound/outbound messages.
Show Action in Breakpoint	Highlights the shape as yellow for the last action executed before breaking.
View Calling Orchestration	Returns the view to the orchestration instance that made the call. That is, it takes you back to the parent orchestration. Only available on a called orchestration instance.

Reporting Mode in Orchestration Debugger

Reporting mode uses tracked events to show what has happened. It uses data tracked using the **Orchestration Events** option flag. This flag must be set prior to the execution of the orchestration instance. You set this flag in the **Orchestrations** option of the **Configuration** menu.

The **Orchestration Events** option tracks the execution of each shape in the orchestration as it happens. In reporting mode, you can replay the steps or set breakpoints on the class of orchestration so that you can then debug new instances using interactive mode.

After you have executed the business process you are interested in, you can use one of the Reporting view queries for the orchestration you wish to examine.

Interactive Mode in Orchestration Debugger

In interactive—debug—mode, the Orchestration Debugger view in Health and Activity Tracking (HAT) contains three areas: Service pane, Tracked Events pane, and the Orchestration pane. In addition, in interactive mode, the Variable list and Variable properties display across the bottom of the view.

Considerations when Using Orchestration Debugger

Tracking atomic scopes

An orchestration can contain atomic scopes to include calls to the Rule Engine. When you attach to an instance in the orchestration debugger, any atomic scopes in the orchestration instance will cause gaps to appear in the tracked events list. This happens for two reasons:

- Becauseevents for the shapes inside atomic transactions do not get persisted until the scope commits
- The debugger reloads events onto the end of the list, so any gaps remain unfilled during the live session.

You can eliminate the gaps if you refresh the view.

Tracking a modified orchestration

If you track an orchestration modified without changing the version number, you must restart all the host instances to which the orchestration is enlisted. This insures that any shape change in the newly deployed version displays correctly, as you step through the Orchestration Debugger.

Tracking simple types

The Orchestration Debugger only supports simple types. For example, if you track a multipart message that contains a .NET object you can view the properties of all message parts, with the exception of the .NET object properties.

When an orchestration appears in the In Breakpoint state and the Orchestration Debugger starts, you can perform the following actions:

- Use the **Attach** service option.
- Review the steps that have already completed.
- View the state of variables and messages.
- Set additional breakpoints.
- Select the **Continue Service** option.
- Repeat any steps as required.

Working with the Orchestration Debugger View

You can access the Orchestration Debugger view by right-clicking a cell in a Results list and selecting Orchestration Debugger.

The Orchestration Debugger presents the technical processing activity of a single instance. The view displays a rendered image of the orchestration.

From the Orchestration Debugger view, you can go to the Message Flow view.

In This Section

- Working with Breakpoints
- Replaying Actions
- Viewing Variables

Working with Breakpoints

You can set breakpoints by attaching to a suspended orchestration, or by setting a breakpoint on a class.

To attach to a suspended orchestration

1. Refresh the view to check that the instance now appears in a Suspended state.
2. Click **Resume in Debug**.

The orchestration resumes in an In Breakpoint state. You can now debug interactively.

To switch to the Message Flow view

- Right-click a cell in the Results list and select **Message Flow** from the shortcut menu.

To select a Service option

- To the right of the top pane in Orchestration Debugger, there is a **Service Options** drop-down list. Select the option you require, as described in the following table, and click **OK**.

Select this	To do this
Suspend Service	Suspend orchestration instances.
Resume Service	Resume orchestration instances.
Resume in Debug	Resume orchestration instances in debug mode.

Mode	
Terminate Service	Terminate orchestration instances.
Save All Messages	Save all message instances related to a specific orchestration instance.

Replaying Actions

The Orchestration Debugger enables you to replay the actions of an orchestration step by step. When you open an orchestration, the cursor is placed at the first action, for example, Initialization. Use the Up and Down arrows to step forward and backward through the orchestration. Follow the progress as the rendered orchestration focus moves from shape to shape.

Viewing Variables

You can view variables in two modes:

- When you are tracking archived data - offline
- When you are doing interactive debugging on live data

When working with archived data, the statuses of some variables that you can see are:

- Variables not yet in scope
- Currently active
- Values you can click for more details
- Values that have passed out of scope; you can no longer access any details

Working with the Results Lists

When you run a query it generates a Results list containing the search results, such as relevant messages, pipelines, and assemblies. The Results lists are displayed in the form of a PivotTable field list.

In This Section

- How to Access Message Flow or Orchestration Debugger View
- How to Suspend Orchestrations or Ports
- How to Resume Orchestrations that are Suspended by Design
- How to Terminate Orchestrations that are Suspended by Fault

- How to Control the Size of the Results List
- How to Switch to Orchestration Debugger View from Message Flow View

How to Access Message Flow or Orchestration Debugger View

To access Message Flow or Orchestration Debugger

1. Click **Start**, click **Programs**, click **Microsoft BizTalk Server 2006**, and then click **Health and Activity Tracking**.
2. In a Results list, right-click the cell you want to the see the instance activity for, and then click **Message Flow** or **Orchestration Debugger**.

How to Suspend Orchestrations or Ports

You can only suspend all instances from a Results list generated from the Service or Message metrics views, not from the Query Builder. To suspend more than one orchestration and/or pipeline instance but not all of them, you must suspend each instance individually. You cannot suspend an orchestration or pipeline instance if you are accessing archived data.

Prerequisites

You must be logged on as a member of the BizTalk Server Administrators group to perform this procedure.

To suspend orchestration or pipeline instances

1. Click **Start**, click **Programs**, click **Microsoft BizTalk Server 2006**, and then click **Health and Activity Tracking**.
2. Run a query on **Messages** or **Services**.
3. On the **Results** list, select the active orchestration or pipeline you want to suspend.
4. Right-click the selected instance.
5. On the shortcut menu, click **Suspend**.

To suspend all instances

1. On the **Service Options** list, click **Suspend All**.
2. Click **OK**.

How to Resume Orchestrations that are Suspended by Design

If you have suspended an orchestration by design, you can resume the orchestration from the Results list shortcut menu.

Prerequisites

You must be logged on as a member of the BizTalk Server Administrators group to perform this procedure.

To resume orchestration or pipeline instances

1. Click **Start**, click **Programs**, click **Microsoft BizTalk Server 2006**, and then click **Health and Activity Tracking**.
2. On the **Results** list, select the instance you want to resume.
3. Right-click the selected instance, and then click **Resume**.

To resume all instances

1. Click **Start**, click **Programs**, click **Microsoft BizTalk Server 2006**, and then click **Health and Activity Tracking**.
2. On the **Service Options** list, click **Resume All**.
3. Click **OK**.

To resume orchestration or pipeline instances in debug mode

1. Click **Start**, click **Programs**, click **Microsoft BizTalk Server 2006**, and then click **Health and Activity Tracking**.
2. On the **Results** list, select the instance you want to resume.
3. Right-click the selected instance.
4. On the shortcut menu, click **Resume in Debug Mode**.

How to Terminate Orchestrations that are Suspended by Fault

You can terminate any suspended by fault orchestrations or pipelines from the Results list shortcut menu.

Prerequisites

You must be logged on as a member of the BizTalk Server Administrators group to perform this procedure.

To terminate orchestration or pipeline instances

1. Click **Start**, click **Programs**, click **Microsoft BizTalk Server 2006**, and then click **Health and Activity Tracking**.

2. On the **Results** list, select the orchestration or pipeline instance you want to terminate.

3. Right-click the selected instance.

4. On the shortcut menu, click **Terminate**.

To save all message instances related to an orchestration or pipeline

1. Click **Start**, click **Programs**, click **Microsoft BizTalk Server 2006**, and then click **Health and Activity Tracking**.

2. On the Results list, right-click the appropriate orchestration or pipeline instance.

3. Select **Save All Message Instances** from the shortcut menu.

   The Save As dialog box appears.

4. Browse to the folder and type a name for the file.

5. Click **OK**.

How to Control the Size of the Results List

Results lists, or PivotTable field lists, contain many columns of information so that you need to scroll in order to view them. One way you can reduce the size is to use the **Field List** to add or remove columns, displaying only the information that you need.

The **Field List** shows all the fields available in the Service and Message Metrics views or Results list. The fields already displayed in the Service and Message Metrics views or Results list are bolded, while the fields that can be added are in regular font.

You can add or remove information by dragging items from the Field list to the PivotTable field list or Results list.

Prerequisites

You must be logged on as a member of the BizTalk Server Administrators group to perform this procedure.

To add or remove columns in a results list

1. Click **Start**, click **Programs**, click **Microsoft BizTalk Server 2006**, and then click **Health and Activity Tracking**.

2. Right-click any cell in the Results list, and then click **Field List**.

The **Field List** report opens.

3. Drag items between the Results list and Field List report.

You can control the number of results that HAT returns by using the tracking filters that HAT provides when you are creating or running a query.

How to Switch to Orchestration Debugger View from Message Flow View

Use the following procedure to switch to Orchestration Debugger view.

Prerequisites

You must be logged on as a member of the BizTalk Server Administrators group to perform this procedure.

To switch to the Orchestration Debugger view

1. Click **Start**, click **Programs**, click **Microsoft BizTalk Server 2006**, and then click **Health and Activity Tracking**.

2. Right-click a cell in the Results list and select **Orchestration Debugger** from the shortcut menu.

Monitoring BizTalk Server Using MOM

The Microsoft BizTalk Server 2006 Management Pack for Microsoft Operations Manager 2005, Service Pack 1 (SP1) provides both proactive and reactive monitoring of BizTalk Server. This management pack is provided as a Web download for users of BizTalk Server 2006. The BizTalk Server management pack provides for comprehensive monitoring of important BizTalk events and performance counters to provide a centralized management and monitoring experience for a BizTalk installation.

The BizTalk Server 2006 management pack is a level 2 management pack that includes the following features:

- Event and Performance-based alerts for all major BizTalk Server 2006 components. All alerting rules contain product knowledge.

- Streamlined Alerts: Redundant alerts are minimized. Alert suppression typically based on end points, especially for suspended messages in BizTalk Server.

- Rich views specific to the BizTalk Server 2006 management pack.

- State Monitoring View for BizTalk provides green/yellow/red state for important health aspects of BizTalk Server and indicates overall health.

- BizTalk Server MOM Tasks to execute common operational tasks.

- Additional MOM Tasks enable you to transition directly from a MOM alert to BizTalk Server Administration Console or to Health and Activity Tracking.
- Comprehensive monitoring for the health of BizTalk Server MessageBoxes and hosts.
- The management pack for Enterprise Single Sign-On updated with new alerts for BizTalk Server 2006

In This Section

- Checklist: Using MOM to Monitor BizTalk Server
- Best Practices for Using MOM to Monitor BizTalk Server
- Contents of the BizTalk Server 2006 Management Pack
- How to Import the BizTalk Server Management Pack
- How to Mark BizTalk Server Databases as Critical in the SQL Server Management Pack
- How to Add Enterprise Single Sign-On Computers to the List of Computers Monitored by the BizTalk Server Management Pack
- Operations Tasks for the BizTalk Server 2006 Management Pack
- BizTalk Server Monitoring Scenarios
- Tasks in the BizTalk Server 2006 Management Pack
- Views in the BizTalk Server 2006 Management Pack
- State Monitoring Definitions in the BizTalk Server 2006 Management Pack

Checklist: Using MOM to Monitor BizTalk Server

Step	Reference
Ensure that you have appropriate permissions to install and configure software on your BizTalk Servers.	**Minimum Security User Rights**
Install the MOM agent on each BizTalk Server you want to monitor and point it to the Consolidator/Agent Manager.	Chapter 8 - MOM Agent Management
Download and import the following management packs: • BizTalk Server 2006 (**required**)	Management Pack and Product Connector Catalog

• Enterprise Single Sign-On (**required**) • Windows Base OS (Server) (**optional**) • SQL Server 2000, 2005 (**optional**) • Windows Internet Information Services (IIS) 2000, 2003 (**optional**) • Windows Message Queuing Service (MSMQ) 2000 (**optional**) • Windows .NET Framework 1.0, 1.1 (**optional**)	
Read the best practices for using MOM to monitor BizTalk Server.	Best Practices for Using MOM to Monitor BizTalk Server
Enable or disable the BizTalk Server management pack rules as appropriate.	Best Practices for Using MOM to Monitor BizTalk Server
Add any Enterprise Single Sign-On computers to the list of computers to be monitored by the BizTalk Server 2006 management pack.	How to Add Enterprise Single Sign-On Computers to the List of Computers Monitored by the BizTalk Server Management Pack

Best Practices for Using MOM to Monitor BizTalk Server

- **Review and prioritize alerts on a daily basis.**

  Reviewing and prioritizing alerts on a daily basis helps to ensure that issues are resolved in a timely manner.

- **Enable and disable rules as necessary.**

  By default, some of the rules in the BizTalk Server 2006 management pack are disabled. These disabled rules are of the following types: rules needing customization, rules that serve as templates, and rules for monitoring additional BizTalk Server events.

- **Customize rules as necessary for your environment.**

  You should customize some of the rules in the BizTalk Server 2006 management pack to suit your BizTalk Server deployment. Some rules require thresholds that are best defined based on your specific BizTalk Server deployment.

- **Create additional rules as necessary, based on the rules included in the BizTalk Server 2006 management pack.**

  Rules are provided for use as templates for artifacts that you create, such as BizTalk

Server Hosts. You should use these template rules as a reference when creating artifact-specific rules such as:

- Host Specific Rules, for example, Host Queue Monitoring, and Host Throttling Monitoring
- MessageBox Specific Rules
- Rules for additional third party components, for example, MQSeries adapter

Contents of the BizTalk Server 2006 Management Pack

The Microsoft BizTalk Server 2006 management pack enables you to monitor BizTalk Server events, collect BizTalk Server-specific performance counters in one central location, and raise alerts that require operator intervention. The BizTalk Server 2006 management pack contains rules that cover the following categories:

- **Availability Monitoring**

  Availability monitoring rules monitor the availability of service from computers running BizTalk Server. Availability monitoring rules are rules that cause a service to become unavailable and have names prefixed with "Service Unavailable."

- **Health Monitoring**

  Health monitoring rules monitor for different types of errors in BizTalk Server that require operator intervention. There are four types of health monitoring rules, which have names prefixed with "Error," "Critical Error," "Warning," and "Information:"

  - Error: Errors are events which usually represent individual message processing problems. In isolation they represent one-off problems which can be rectified either at the sender end or the receiver end of a message transmission.
  - Critical Error: Critical errors represent events which indicate a significant problem has occurred. This can affect a wide functionality of BizTalk.
  - Warning: Warnings are typically problems which are intermittent in nature and may occur intermittently. Sometimes these problems are of a transient nature and may not recur. They do not represent major problems in operation and may de-prioritize compared to other alerts.
  - Information: Information alerts include information about BizTalk Server. These messages are neither errors nor warnings.

- **Utilization/Performance Tracking**

  Utilization/performance tracking rules enable you to monitor the operationally relevant performance counters for BizTalk Server. These are divided into measurement rules and comparison rules.

Availability Monitoring

The BizTalk Server 2006 Core rule group contains the following rules to address availability monitoring, that is, monitoring related to whether BizTalk Server is currently operable and able to process work. All of the rules are configured to suppress duplicate alerts for identical event content, which means a repeat count will be incremented for a single alert rather than seeing multiple alert instances in the Microsoft Operations Manager 2005 Operator Console. This helps to avoid a flood of alerts that an administrator must deal with; too much information can be as problematic as too little. None of the rules contain automated responses, such as email/pager notifications, though you can easily add these as needed.

Rule Name	Enabled	Description
Service Unavailable: A receive location is shutting down.	Yes	
Service Unavailable: All receive locations are being temporarily disabled because either the MessageBox or Configuration database is not available.	Yes	
Service Unavailable: BAM Portal cannot connect to Primary Import Database - Login failed	Yes	
Service Unavailable: BizTalk HTTP receive adapter failed to initialize itself	Yes	
Service Unavailable: Error connecting to the BAM Primary Import Database - Db not found	Yes	
Service Unavailable: Failed to connect to BizTalk Management Database	Yes	
Service Unavailable: Failed to initialize UPM profile context	Yes	
Service Unavailable: The Messaging engine could not contact the SSO server.	Yes	
Service Unavailable: The Messaging Engine encountered an error initializing a receive adapter.	Yes	
Service Unavailable: The Messaging Engine failed to initialize a transport adapter.	Yes	

Health Monitoring

The BizTalk Server 2006 Core rule group contains the following rules to address health monitoring, that is, monitoring related to various non-fatal failure modes. Typically, the situation may be isolated to individual interchanges or may possibly resolve itself. The BizTalk Server service is still, in some capacity, able to process work. The primary intent of these rules is to provide operations staff with information relating to messages that are stuck in the system and that require manual intervention of some sort, and to give them the information required to rectify the root problem.

All of these rules are configured to suppress duplicate alerts for identical event content, which means a repeat count will be incremented for a single alert rather than seeing multiple alert instances in the Microsoft Operations Manager 2005 Operator Console. None of the rules contain automated responses, but you can easily add such responses if necessary.

Rule Name	Enabled	Description
Consolidate Inbound Message Rejected on Authentication Failure	Yes	
Critical Error: A BizTalk host instance has stopped and is not processing information.	Yes	
Critical Error: A BizTalk subservice has failed while executing a service request	Yes	
Critical Error: A stored procedure call failed.	Yes	
Critical Error: Monitor BizTalk NT Service Availability	Yes	
Critical Error: The Messaging Engine failed to register an adapter.	Yes	
Critical Error: The Messaging Engine failed to retrieve the configuration from the database.	Yes	
Critical Error: The MSMQT subservice failed to start because Windows MSMQ service is running on the computer.	Yes	
Error connecting to the BAM Primary Import Database – DB server not found	Yes	
Error: A message going to a one-way send port is being suspended. The send port configuration corresponding to the message was not found.	Yes	
Error: A receive location is invalid or incorrectly configured.	Yes	
Error: A response message is suspended.	Yes	
Error: An adapter raised an error during message processing.	Yes	
Error: An attempt to connect to a BizTalk database failed.	Yes	
Error: An outbound message is being suspended by the adapter.	Yes	
Error: BAM Portal Encountered Internal Server Error	Yes	
Error: BAM Portal Encountered Internal Server Exception - Web Services may have received badly-formatted requests	Yes	
Error: BAM Technical Assistance Required	Yes	

Error: Connection to a SMTP host failed	Yes	
Error: Error connecting to the BAM Primary Import Database - Referenced DB not found	Yes	
Error: Failed to archive the processed message.	Yes	
Error: Failed to delete processed message	Yes	
Error: Failed to un-mark the file	Yes	
Error: FILE-Receive-Message Suspended	Yes	
Error: FTP-Receive-Message Suspended	Yes	
Error: HTTP-Receive-Message Suspended	Yes	
Error: Messaging Engine has suspended a message. Failed to correlate a response message to an existing request message.	Yes	
Error: MQSeries-Receive-Message Suspended	Yes	
Error: MSMQ-Receive-Message Suspended	Yes	
Error: Orchestration instance suspended due to errors, needs manual intervention	Yes	
Error: POP3 adapter could not authenticate to the server using supplied credentials	Yes	
Error: POP3 adapter could not establish connection with the POP3 server	Yes	
Error: POP3-Receive-Message Suspended	Yes	
Error: SMTP send adapter could not authenticate with the SMTP server	Yes	
Error: SOAP-Receive-Message Suspended	Yes	
Error: SQL-Receive-Message Suspended	Yes	
Error: The FILE send adapter cannot open file for writing.	Yes	
Error: The host instance failed to connect to the BizTalk Configuration database.	Yes	
Error: The HTTP send adapter cannot connect to the remote server.	Yes	
Error: The Messaging Engine is dropping the message due to an	Yes	

authentication failure.		
Error: The processed file is either read-only or a system file.	Yes	
Error: There was a failure executing a receive pipeline at a http receive location.	Yes	
Error: There was a failure executing a receive pipeline.	No	
Generic Error: All error events from BizTalk Server 2006	No	
Generic Information: All information events from BizTalk Server 2006	No	
Generic Warning: All warning events from BizTalk Server 2006	No	
Information: A BizTalk Server Host Instance Windows Service Has Stopped	No	
The Messaging Engine has suspended one or more inbound message(s).	No	
The Messaging Engine has suspended one or more outbound message(s).	No	
There was a failure executing a send pipeline.	No	
There was an error executing a pipeline component.	No	
Warning: Cube DTS has not been run	Yes	
Warning: FILE receive adapter cannot reach a receive location due to network problems	Yes	
Warning: TDDS failed to batch execution of streams	Yes	
Warning: The Messaging Engine encountered an error publishing a batch of messages.	Yes	

Utilization/Performance Tracking

There are two types of performance rules within MOM: measurement rules and comparison Rules. Measurement rules gather data from Microsoft Windows performance counters, or other data sources, with a specified sampling rate and store the data for historical analysis. Comparison rules allow actions to be taken and alerts to be raised when a given performance value varies by a specified threshold from expected values, which can include averages of past samples. Some of the comparison rules require customization based on your particular environment.

The table below shows the performance rules for the BizTalk Server 2006 Core rule group.

Measurement Rule Name	Enabled	Description
BizTalk Messaging Active Receive Locations	Yes	
BizTalk Messaging Inbound Latency	Yes	
BizTalk Messaging Outbound Latency	Yes	
BizTalk Messaging Outbound Latency	Yes	
BizTalk Messaging Request-Response Latency	Yes	
BizTalk Messaging Request-Response Timeouts	Yes	
BizTalk: WSS Adapter % Web Service Call Failures	No	
BizTalk: WSS Adapter Total Receive Commit Failures	Yes	
BizTalk: WSS Adapter Total Receive Message Failures	Yes	
BizTalk: WSS Adapter Total Received Messages	Yes	
BizTalk: WSS Adapter Total Send Message Failures	Yes	
BizTalk: WSS Adapter Total Sent Messages	Yes	
BizTalk: WSS Adapter Total Web Service Call Failures	Yes	
BizTalk: WSS Adapter Total Web Service Calls/sec	Yes	
BizTalk:TDDS Total Events	Yes	
BizTalk:TDDS Total Records	Yes	
BizTalk:TDDS-Total Failed Events	Yes	
CPU Usage BizTalk Machines	Yes	
CPU Usage BizTalk Server Process	Yes	
CPU Usage BizTalk Server Processes	Yes	
CPU Usage BizTalk Servers	Yes	
Documents processed	Yes	
Documents processed/sec	Yes	
Documents received	Yes	

Documents received/sec	Yes	
Documents suspended	Yes	
Documents suspended/sec	Yes	
FILE receive Adapter Bytes	Yes	
FILE Receive Adapter Bytes/Sec	Yes	
FILE Receive Adapter Messages Received / Sec	Yes	
FILE Receive Adapter-Messages received	Yes	
FILE Send Adapter Bytes	Yes	
FILE Send Adapter Bytes/Sec	Yes	
FILE Send Adapter Messages Sent / Sec	Yes	
FILE Send Adapter-Messages Sent	Yes	
FTP Receive Adapter Bytes Received	Yes	
FTP Receive Adapter Bytes Received/sec	Yes	
FTP Receive Adapter Messages Received	Yes	
FTP Receive Adapter Messages Received/Sec	Yes	
FTP Send Adapter Bytes	Yes	
FTP Send Adapter Bytes/Sec	Yes	
FTP Send Adapter Messages Sent	Yes	
FTP Send Adapter Messages/Second	Yes	
Host - Instance State Message References - BizTalkServerInProcessHost	Yes	
Host Queue Size - All BizTalk Hosts	Yes	
Host Suspended Queue Size - All BizTalk Hosts	Yes	
HostQ - Instances - BizTalkServerInProcessHost	Yes	
HTTP Receive Adapter Messages Received / Sec	Yes	
HTTP Receive Adapter Response Messages Sent / Sec	Yes	

HTTP Receive Adapter-Messages received	Yes	
HTTP Receive Adapter-Response Messages sent	Yes	
HTTP Send Adapter Messages Received	Yes	
HTTP Send Adapter Messages Received/Sec	Yes	
HTTP Send Adapter Messages Sent/Sec	Yes	
HTTP Send Adapter-Messages Sent	Yes	
ID Process	Yes	
Logical Disk %Free Space BizTalk Servers	Yes	
MessageBox databases connection failures	Yes	
MessageBox Dead Processes Cleanup	Yes	
MessageBox Instances Size	Yes	
MessageBox Msg Cleanup	Yes	
MessageBox Parts Cleanup	Yes	
MessageBox Spool Size	Yes	
MessageBox Tracked Message Copy	Yes	
MessageBox Tracking Data Size	Yes	
MessageBox Tracking Spool Cleanup	Yes	
MSMQ Receive Adapter Bytes Received	Yes	
MSMQ Receive Adapter Bytes/Sec	Yes	
MSMQ Receive Adapter Messages Received	Yes	
MSMQ Receive Adapter Messages Received/Sec	Yes	
MSMQ Send Adapter Bytes Sent	Yes	
MSMQ Send Adapter Bytes/Sec	Yes	
MSMQ Send Adapter Messages Sent	Yes	
MSMQ Send Adapter Messages Sent/Sec	Yes	

Orchestrations completed	Yes	
Orchestrations completed/sec	Yes	
Orchestrations Created	Yes	
Orchestrations Created/sec	Yes	
Orchestrations dehydrated	Yes	
Orchestrations dehydrated/sec	Yes	
Orchestrations discarded	Yes	
Orchestrations discarded/sec	Yes	
Orchestrations rehydrated	Yes	
Orchestrations rehydrated/sec	Yes	
Orchestrations resident in-memory	Yes	
Orchestrations suspended	Yes	
Orchestrations suspended/sec	Yes	
Orchestrations-% used physical memory	Yes	
Orchestrations-Database transactions	Yes	
Orchestrations-Database transactions/sec	Yes	
Orchestrations-Dehydratable orchestrations	Yes	
Orchestrations-Dehydrating orchestrations	Yes	
Orchestrations-Idle orchestrations	Yes	
Orchestrations-Megabytes allocated private memory-<All>-15.0-minutes	Yes	
Orchestrations-Megabytes allocated virtual memory	Yes	
Orchestrations-Pending messages	Yes	
Orchestrations-Pending work items	Yes	
Physical Disk %Idle Time BizTalk Servers	Yes	
Physical Disk Average Disk Queue Length BizTalk Server	Yes	

POP3 Receive Adapter Active Sessions	Yes	
POP3 Receive Adapter Bytes Received	Yes	
POP3 Receive Adapter Bytes/Sec	Yes	
POP3 Receive Adapter Messages Received	Yes	
POP3 Receive Adapter Messages Received/Sec	Yes	
Runnable orchestrations	Yes	
Running orchestrations	Yes	
SMTP Send Adapter Messages Sent	Yes	
SMTP Send Adapter Messages Sent/Sec	Yes	
SOAP Receive Adapter Messages Received	Yes	
SOAP Receive Adapter Messages Received /Sec	Yes	
SOAP Send Adapter Messages Sent	Yes	
SOAP Send Adapter Messages Sent/Sec	Yes	
SQL Receive Adapter Messages Received	Yes	
SQL Receive Adapter Messages Received/Sec	Yes	
SQL Send Adapter Messages Sent	Yes	
SQL Send Adapter Messages Sent/Sec	Yes	

Comparison Rule Name	**Enabled**	**Description**
Monitor Host Suspended Q Size	No	
Monitor HostQ Size	No	
Monitor HostQ Size - BizTalkServerApplication	No	
Monitor MessageBox Instances Size	No	
Monitor MessageBox Spool Size	No	
Monitor MessageBox Tracking Data Size	No	
Total TDDS Events Failed Exceeded Limit	No	

Total TDDS Failed Batches Exceeded Limit	No	
Warning: BizTalk Throttled on High Database Size for a significant period	Yes	
Warning: BizTalk Throttled on High Inprocess Message Count for a signiificant period	Yes	
Warning: BizTalk Throttled on High ProcessMemory for a significant period	Yes	
Warning: BizTalk Throttled on High Thread Count for a significant period	Yes	

How to Import the BizTalk Server Management Pack

Prerequisites

You must be logged on as a member of the MOM Administrators group to perform this procedure.

To Import the BizTalk Server Management Pack

1. Click **Start**, click **Programs**, click **Microsoft Operations Manager 2005**, and then click **Administrator Console**.

2. In the console tree, double-click the **Microsoft Operations Manager**, right-click **Management Packs**, and then click **Import/Export Management Pack**.

3. In the **Management Pack Import/Export Wizard**, on the **Welcome to the Management Pack Import/Export Wizard** page, click **Next**.

4. On the **Import or Export Management Packs** page, click **Import Management Packs and/or reports**, and then click **Next**.

5. On the **Select a Folder and Choose Import Type** page, browse to the location where you downloaded the BizTalk Server management pack, and then click **Next**.

6. On the **Select Management Packs** page, select **MicrosoftBizTalkServer2006.akm** and **MicrosoftEnterpriseSingleSignOn.akm**, and then click **Next**.

7. On the **Completing the Management Pack Import/Export Wizard** page, click **Finish**.

How to Mark BizTalk Server Databases as Critical in the SQL Server Management Pack

If you have installed the Microsoft SQL Server 2000 or Microsoft SQL Server 2005 management pack, you can designate the BizTalk Server databases as critical. This ensures that the SQL Server management pack monitors the following BizTalk Server databases:

- BAM Archive database (BAMArchive)
- BAM Primary Import database (BAMPrimaryImport)
- BAM Star Schema database (BAMStarSchema)
- BizTalk Tracking database (BizTalkDTADb)
- BizTalk Base EDI database (BizTalkEDIDb)
- HWS Administration database (BizTalkHwsDb)
- BizTalk Management database (BizTalkMgmtDb)
- BizTalk MessageBox database (BizTalkMsgBoxDb)
- Rule Engine database (BizTalkRuleEngineDb)
- Enterprise Single Sign-On database (SSODB)
- Trading Partner Management database (TPM)

Prerequisites

You must be logged on as a member of the Administrators group to perform this procedure.

To Mark BizTalk Server Databases as Critical in the SQL Server Management Pack

1. Click **Start**, click **Programs**, click **Microsoft Operations Manager 2005**, and then click **Administrator Console**.
2. In the console tree, double-click **Microsoft Operations Manager**, double-click **Management Packs**, double-click **Rule Groups**, and then double-click **Microsoft SQL Server**.
3. Depending on the version of SQL Server you are using, either double-click **SQL Server 2000** or double-click **SQL Server 2005**.
4. Double-click **State Monitoring and Service Discovery**, double-click **Event Rules**, and then double-click **SQL Server Database Health**.
5. In the **Event Rule Properties** dialog box, click the **Responses** tab, select the script in the **Response** box, and then click **Edit**.

6. In the **Launch a Script** dialog box, in the **Script parameters** boxes, click **HighSevDatabases**, and then click **Edit Parameter**.

7. In the **Edit Script Parameter** dialog box, in the **Value** box, add the BizTalk Server databases you want to monitor to the comma-separated list databases, and then click **OK**.

How to Add Enterprise Single Sign-On Computers to the List of Computers Monitored by the BizTalk Server Management Pack

You can add your Enterprise Single Sign-On computers to the list of computers monitored by the BizTalk Server 2006 management pack.

Prerequisites

You must be logged on as a member of the Administrators group to perform this procedure.

To add Enterprise Single Sign-On computers to the list of computers monitored by the BizTalk Server management pack

1. Click **Start**, click **Programs**, click **Microsoft Operations Manager 2005**, and then click **Administrator Console**.

2. In the console tree, double-click **Microsoft Operations Manager**, double-click **Management Packs**, and then double-click **Computer Groups**.

3. Right-click **BizTalk Server 2006**, and then click **Properties**.

4. In the **BizTalk Server 2006 Properties** dialog box, click the **Included Computers** tab.

5. On the **Included Computers** tab, click **Add**.

6. In the **Add Computer** dialog box, in the **Select one or more computers to add** box, select the computers running Enterprise Single Sign-On that you want to monitor, and then click **OK**.

7. If the Enterprise Single Sign-On computer you want to monitor is not listed in the **Select one or more computers to add** box, click **New**. In the **New Computer** dialog box, specify the domain name and computer name of the Enterprise Single Sign-On computer and then click **OK**.

Operations Tasks for the BizTalk Server 2006 Management Pack

The best practice is to review and prioritize all alerts on a daily basis. In addition, you should perform other tasks on an as-needed basis, depending on your environment. Many important problems do not cause alerts, but they still require periodic attention.

We recommend that you perform these tasks as specified. However, you can adjust the frequency of these tasks to meet the needs of your particular environment.

Daily Tasks

On a daily basis, you should perform the following tasks:

- Review all open alerts. Review all new alerts in the following order of priority:
  - Service Unavailable errors
  - Critical errors
  - Warnings (optional)
  - Informational messages (optional)

  Not all problems can be repaired in one day or less. For example, computer parts must be ordered or computers must be scheduled for restart. It is important that you follow up on open alerts to ensure that they are addressed in a timely manner.
- Verify that all servers running BizTalk Server are communicating with the MOM 2005 Administrator Console. Communication failure between the servers running BizTalk Server and the monitoring infrastructure prevents you from receiving alerts so that you can examine and resolve them.
- Review warnings (optional).

As Needed Tasks

It is recommended that you perform the following tasks as required to ensure the availability of BizTalk Server:

- Review all open alerts.
- Verify that all managed computers are communicating.

BizTalk Server Monitoring Scenarios

This section discusses the common problem scenarios and how to troubleshooting and resolve them using Microsoft Operations Manager 2005 and BizTalk Server 2006.

In This Section

- Resolving Suspended Message Alerts
- Resolving a BAM Technical Assistance Alert
- Monitoring BizTalk Messageboxes and Hosts

- Monitoring Throttling Conditions

Resolving Suspended Message Alerts

Monitoring and resolving suspended message issues is one of the common operational tasks in a BizTalk Server environment. The BizTalk Server 2006 Management Pack enables you to monitor and troubleshoot suspended message events in a streamlined fashion.

Two types of message suspension occur in BizTalk Server while processing messages.

1. Inbound Message Suspension

2. Outbound Message Suspension

In case of inbound messages, various types of processing failures or lack of subscription may cause a message to be suspended. Some transports can be configured to suspend the message or not suspend the message. In case of outbound messages, all processing failures will always lead to message suspension.

For every message suspension, a BizTalk MOM rule creates a new alert or increases repeat count for an existing message suspension alert. Once an alert is created, a MOM user can use two MOM tasks provided to deal with suspended message alerts. These are as follows:

- Open BizTalk Operations Query View

- Open BizTalk Message Flow View

On the MOM Operations console alert view, the user needs to select (by clicking on an alert in any of the alert views) an alert for which he or she decides to do further investigation. With the alert selected, clicking on “Open BizTalk Operations Query View”, will launch the BizTalk Server Administration Console with operations query for the suspended message performed. Clicking on “Open BizTalk Message Flow View”, will launch Health and Activity Tracking with the message flow query for the suspended message performed.

The first task can be used when BizTalk Service Instance associated with the alert is not completed – typically in cases when it got suspended. The second task can be used both for incomplete and complete service instances.

The MOM Alert rule linked to the suspended message event extracts the parameters from the event which are needed to launch the operations console. These parameters are

- Message Instance Identifier

- Service Instance Identifier

Another implicit parameter is the BizTalk Server group to which this computer belongs to. In order to perform the queries that the above tasks provide, it is also necessary to know the BizTalk Server group information i.e. the management database and the SQL Server hosting the database. The MOM task figures out the right BizTalk Server group to use based on the event source computer and performing a registry lookup. So if you have multiple BizTalk

Server groups being monitored from the same machine, the correct BizTalk Server group will be used to perform the query.

For the inbound messages, alert rules for suspension are written per adapter. The reason for this approach is to provide you with more flexibility to deal with message suspensions on the inbound side. You can add different response actions based on the adapter such as notification.

Further customization can be done on the existing rules to create finer grained alerts. This is discussed in the section on customization of rules.

For the outbound messages, all messages are always suspended on transmission time failure of any kind. They are covered with a single rule and the MOM tasks can be used in the same way as described above.

If multiple events have been suppressed under a single MOM alert, the MOM tasks will use Service Instance Id and Message Instance Id extracted from the latest event.

Alert Suppression Policy

MOM Rules for suspended messages employ different suppression policy in general applied for other rules. Alerts are suppressed based on the following:

Alert Name, Alert Source, Computer and Domain.

Suppression based on Alert Source deserves more explanation. Alert source for each suspended message rule also contains a parameter extracted from the suspended message event. This parameter is the URI on which the message was received or transmitted to.

Usually, errors that occur on the same URI are due to the same reason. Therefore, we recommend that you create a single alert for the same root cause even though there are multiple failure events associated. This moves us to the goal of “one alert, one root cause”. Streamlined alerts based on URIs reduces unnecessary alerts and facilitates efficient tracking of open issues. A new alert is created for a message suspension at a URI with no previous suspension alerts.

Resolving a BAM Technical Assistance Alert

BizTalk Server Business Activity Monitoring (BAM) Portal enables BAM Portal users to request technical assistance from the business activity level view of BizTalk Server. BAM Portal users, commonly referred to as business users, typically have an understanding of the business level indicators exposed through milestones and business activities. BAM Portal users typically monitor aggregate indicators, timely completion of in-process business transactions or search for transactions with particular properties to investigate further. During investigation of a given transaction, BAM Portal users typically enlist the help of the IT Operations staff to investigate transactions at the IT infrastructure level.

The BAM Portal enables this hand-off from the business user through a Technical Assistance request. For more information about the BAM Portal, see BAM Portal. Requesting Technical Assistance creates an entry in the Application log in Event Viewer of the computer where

the BAM Portal is hosted. This event contains details about the activity on which technical assistance is requested by the user. The details contain information about the Message Instance Identifier, Service Instance Identifier, and BizTalk Server group information.

The BizTalk Server 2006 Management Pack contains a Microsoft Operations Manager (MOM) rule to trigger a MOM alert on detection of a BAM Technical Assistance event. The rule that creates this alert is “Error: BAM Technical Assistance Required”.

A new alert is created for each request submitted from the BAM Portal and there is no suppression. In MOM, you can use the following MOM tasks provided to investigate further on the context of the alert:

- Open BizTalk Operations Query View
- Open BizTalk Message Flow View

The “Open BizTalk Operations Query View” task returns the details of the service instance. For more information, see Resolving Suspended Message Alerts. The “Open BizTalk Message Flow View” shows the associated message flow in Health and Activity Tracking. The first task can be executed for BizTalk Server service instances\message instances that are incomplete while the second one can be executed for both complete and incomplete service instances\message instances

Monitoring BizTalk Messageboxes and Hosts

BizTalk Server 2006 Management Pack incorporates performance threshold rules that provide a comprehensive view of the health of the BizTalk Server MessageBoxes and queues. Two different types of threshold rules are provided:

- Rules that apply generically i.e. to all BizTalk Hosts, all BizTalk MessageBoxes.
- Rules that are specific to either a particular BizTalk Host or a MessageBox

Generic rules monitor all the BizTalk Server Hosts or MessageBoxes based on a common threshold. For example, the rule: “Monitor HostQ Size” monitors the work queues of all BizTalk Server Hosts based on a common threshold. If there are three different Hosts, all of their work queues are monitored by the same rule and alerts occur when any of the host work queues cross the common threshold.

BizTalk Server Host-specific rules enable you to configure different thresholds for different hosts and MessageBoxes. For example, the rule "Monitor HostQ Size – BizTalkServerApplication" is a Host-specific rule that monitors the work queue of the BizTalkServerApplication Host. This is accomplished by defining a specific MOM provider for the particular performance counter instance and using that provider in the threshold rule. Due to this, it is not possible to define rules specific to each newly created Host or MessageBox out of the box.

Host\MessageBox-specific rules are provided as template rules to be used as a guide for creating rules that are applicable in your environment. All threshold monitoring rules are disabled by default:

- Generic Rules – need to be configured with threshold values specific to your environment

- BizTalk Host/MessageBox specific Rules – need to be created based on the template rules and appropriate thresholds

Thresholds for the different indicators – MessageBox queues and Host queues are different for different deployments based on your scenario and hardware. You should define your thresholds based on observations of the indicators over a period of time. A sound monitoring principle requires that the number of alerts are minimal, most alerts require operator intervention, and one root-cause is associated with one alert.

Your threshold values should therefore take into account average values of indicators, cyclic variations – like temporary maximums and performance under such conditions.

If you are using Host/MessageBox-specific threshold monitoring rules, it may be advisable to disable generic monitoring rules. This will prevent redundant alerts.

Monitoring Throttling Conditions

BizTalk Server 2006 incorporates self-throttling, which helps to prevent overloading of the server based on various parameters. A temporary overload that causes throttling to occur is not an operationally significant event. Persistent throttling, however, is not expected in a stable environment and could indicate underlying problems at the infrastructure level. The BizTalk Server 2006 management pack provides proactive monitoring of such persistent throttling conditions with performance threshold rules.

There are four separate rules that monitor for extended periods of throttling caused by four different conditions:

- BizTalk Server service process memory

- number of messages being processed

- number of threads in a BizTalk Server process

- size of the BizTalk database queues

These threshold rules use data providers based on four throttling state indicator performance counters. For more information about these performance counters,

These rules are configured to raise an alert if the average of over a certain number of samples(default – 30) crosses a particular threshold. For example, “Warning: BizTalk Throttled on High Database Size for a significant period” is a rule monitoring throttling state of all BizTalk Server processes in a given computer. This rule uses a data provider based on the throttling state indicator performance counter “BizTalk:Message Agent-High database size”. If this performance counter value is 1, then the associated process is throttling because of high database size.

The particular rule above is configured to take an average of 30 samples and raise an alert if the average of the samples is more than 0.6. Since, each sample is taken at an interval of one minute, this implies that over the past 30 minutes, at least one or more number of BizTalk Server processes in that computer were throttling because of high database size, 60% of the time.

This heuristic may not suit your particular application scenario. Based on the historical behavior in your environment as described before, you should configure these rules with the correct values – by adjusting samples, adjusting the threshold value or if necessary modifying the interval of sampling for the provider.

Tasks in the BizTalk Server 2006 Management Pack

The BizTalk Server 2006 management pack includes Microsoft Operations Manager (MOM) tasks that enable you to easily transition from an alert in MOM to appropriate BizTalk Server administration tool. These tasks use parameters extracted from event associated with the alert to perform queries based on the alert either in Health and Activity Tracking or in the BizTalk Server Administration Console.

The BizTalk Server 2006 management pack includes the following MOM tasks:

Open BizTalk Administration Console

Open BizTalk HAT Message Flow View

Use this task in the context of an alert related to a message suspended event to further troubleshoot the problem. This task enables you to open Health and Activity Tracking in Message Flow View directly from the Microsoft Operations Manager 2005 Operators Console with the instance information for the suspended message using a pre-canned query. This task is useful if the instance is already completed.

Open BizTalk Operations Query View

Use this task in context of an alert related to a message suspended event to further troubleshoot the problem. This task enables you to open the BizTalk Operations Query View directly from the Microsoft Operations Manager 2005 Operators Console with the instance information for the suspended message.

Start/Stop Enterprise Single Sign-On Service

Start/Stop IIS

Start/Stop Rule Engine Update Service

Views in the BizTalk Server 2006 Management Pack

The following table explains the public view hierarchy in the Microsoft BizTalk Server 2006 Management Pack. Microsoft BizTalk Server 2006 is top level folder for public views provided for BizTalk Server.

The public views are organized so that they:

- Provide shortcuts for the most used alert views. Four “Open Alerts” shortcuts are provided so that the views most frequently used are accessible easily.

- Provide specialized views. If a specific problem is being monitored, multiple views filter the alerts in a variety of ways to enable you to monitor in a more granular fashion. For example, if you are troubleshooting Business Activity Monitoring (BAM) problems or FILE problems, you can focus on the appropriate alert node.

Node	Type	Description
BizTalk Server 2006 Core Open Alerts	Alert View	Alerts from BizTalk Server engine. This is a shortcut to all open alerts related to BizTalk Server runtime.
BizTalk Server 2006 BAM Open Alerts	Alert View	Alerts from Business Activity Monitoring component of BizTalk. This is a shortcut to all open alerts from BizTalk BAM.
BizTalk Server 2006 BAS Open Alerts	Alert View	Alerts from Business Activity Services component of BizTalk Server.
BizTalk Server 2006 SSO Open Alerts	Alert View	Alerts from Enterprise Single-Sign On – a perquisite component for BizTalk Server.
Computer Groups	Computer Group View	Computer Group based summary of all computers running BizTalk Server.
Events	Event View	All events collected from monitored computers based on monitoring rules.
Performance	Performance Data View	Reserved for future use.
State-Overall	State View	Overall View of state components – on all BizTalk Server 2006 computers.
BizTalk Server 2006	Sub-Folder	BizTalk Server 2006 folder contains all the views specific to the BizTalk Server runtime.
Business Activity Monitoring	Sub-Folder	Folder contains all of the views specific to Business Activity Monitoring.
Business Activity Services	Sub-Folder	Folder contains all of the views specific to Business Activity Services.

The BizTalk Server 2006 sub-folder is organized as below:

Node	Type	Description
Alerts	Sub-Folder	Different alert views – based on alert resolution state and duration of alerts.
BizTalk Messagebox, Hosts	Sub-Folder	Alert Views and Performance Data Views related to the health of BizTalk Server MessageBoxes and Hosts.
BizTalk Messaging	Sub-Folder	Alert Views and Performance Data Views related to the health of the BizTalk Server engine, with sub-folders for a per adapter view.
BizTalk Orchestrations	Sub-Folder	Orchestration Performance data view – single point access to all orchestration performance data.
Server Resource usage	Sub-Folder	Views for additional non-BizTalk system parameters vital in determining health of a BizTalk Server system.

In addition to the standard default public views, the BizTalk Server 2006 management pack includes views in the following categories:

- State - BizTalk Server Core

  Overall view of BizTalk Server computers with role components defined for BizTalk Server.

Alerts
BizTalk Messagebox, Hosts
BizTalk Messaging
BizTalk Orchestrations
BizTalk Resource Usage

State Monitoring Definitions in the BizTalk Server 2006 Management Pack

The BizTalk Server 2006 management pack provides red, yellow, and green state monitoring based on the definitions detailed in the following table.

Item	Green	Yellow	Red

Securing BizTalk Server

This section discusses the user rights and user groups used with BizTalk Server, including Enterprise Single Sign-On.

In This Section

- Managing BizTalk Server Security
- Enterprise Single Sign-On

Managing BizTalk Server Security

Maintaining a secure Microsoft® BizTalk® Server 2006 environment requires that you manage accounts, certificates, and passwords. To ensure the security of the business documents handled by BizTalk Server, BizTalk administrators must manage the following accounts and certificates:

- **BizTalk Server Administrators group**. For users to perform administrative tasks either through the BizTalk Administration console or directly by using the Microsoft Windows® Management Instrumentation (WMI) provider, they must be granted the proper privileges in Microsoft SQL Server™ and Microsoft Windows®. The BizTalk Administrators group has the minimum privileges necessary to perform most administrative tasks. To perform administrative tasks for adapters, receive and send handlers, and receive locations, the BizTalk Administrators group must be added to the Single Sign-On Affiliate Administrators group.

  For information about adding users to the BizTalk Administrators group or removing users from the BizTalk Administrators group, see Managing the BizTalk Administrators Group .

  For more information about Enterprise Single Sign-On, see Using SSO .

- **BizTalk Server Operators group**. The BizTalk Server Operator is a low privilege role with access only to monitoring and troubleshooting actions.

  Members of the BizTalk Server Operators group can:

  - View service state and message flow.
  - Start or stop applications.
  - Start or stop orchestrations.
  - Start or stop send ports or send port groups.
  - Enable or disable receive locations. The changes do not take effect until the next cache refresh interval of 60 seconds, the default. The cache refresh interval is set at the BizTalk Server group level.
  - Terminate and resume service instances.

  Members of the BizTalk Server Operators group cannot:

  - Change configuration.

- View message context properties (classified as Personally Identifiable Information (PII)) or message bodies.
- Affect the course of message routing, such as removing or adding new subscriptions to the running system.

- **Hosts and service accounts**. When creating a host and host instances of that host, you must provide the Windows group for the host and the service account credentials for each host instance. You must ensure that the host instance service accounts are members of the Windows group for the host.

  Therefore, before creating a host and host instances you must:

  - Create the Windows group for the host.
  - Create service accounts for each host instance.
  - Add the service accounts to the host Windows group.

- **Signing certificates**. Signing certificates (private key certificates) are specified for the BizTalk group. These are optional and can be changed at any time by a BizTalk administrator.

In This Section

- Managing BizTalk Windows Groups and User Accounts
- Best Practices for Security, Accounts, and Certificates
- BizTalk Server User Rights

Best Practices for Security, Accounts, and Certificates

This section contains best practices and tips for managing security, accounts, and certificates.

Use service accounts for host instances

To ensure the security of your BizTalk Server environment, it is highly recommended that you use service accounts with the minimum privilege necessary to run host instances.

Use different user groups for authentication trusted and non-trusted hosts

To ensure that non-authentication trusted hosts have fewer privileges than authentication trusted hosts, you must use different service accounts for these hosts.

Use a different user group for each BizTalk Host

To maximize the security boundary between hosts, it is recommended that you use a different Windows user group for each BizTalk Host in your BizTalk group.

Use domain Windows groups and accounts in a multi-computer environment

If you install Microsoft BizTalk Server 2006 on multiple computers, you must specify domain groups and user accounts in the BizTalk Server Configuration Wizard. For example, if you install multiple BizTalk Server 2006 members of a BizTalk Server Group and if the Microsoft SQL Server that houses your BizTalk Server databases is on a remote machine, or if one of these cases is true, you must specify domain groups and user accounts.

Remove the installation user from the BizTalk Administrators group

The interactive user performing a BizTalk Server installation is automatically added to the BizTalk Administrators group so that that user can perform the tasks included in the Configuration Wizard.

If the user installing BizTalk Server will not be administering the BizTalk Server environment after installation, it is recommended that you remove this user from the BizTalk Administrators group after the Configuration Wizard is run.

Remove BUILTIN\Administrators from the SQL Server sysadmin group

After configuration, BUILTIN\Administrators remain members of the SQL Server sysadmin group.

It is recommended that at the very least, you remove BUILTIN\Administrators from the SQL Server sysadmin group. It is further recommended that you review all of the members of the SQL Server sysadmin group and remove any members who should not be members of the group.

Managing BizTalk Windows Groups and User Accounts

BizTalk Server 2006 uses a number of Windows groups and user accounts. For a complete list and description of the groups, and their affiliated user accounts in the BizTalk Server system, see Windows Group and User Accounts in BizTalk Server .

In This Section

- Managing the BizTalk Administrators Group
- Managing Hosts and Service Accounts
- Managing Signing Certificates

Managing the BizTalk Administrators Group

The BizTalk Server Administrators Group has the least privileges necessary to perform most administrative tasks. You can add users to the BizTalk Server Administrators group so that they can perform administrative tasks using the BizTalk Server Administration Console or the WMI provider. You should remove users from the BizTalk Server Administrators group when they no longer need to perform administrative tasks using the BizTalk Server Administration Console or the WMI provider.

Prerequisites

You must be logged on as a member of the Administrators group to perform this procedure.

To add users to the BizTalk Administrators group

1. Click **Start**, point to **Administrative Tools**, and then click **Computer Management**.
2. Expand **System Tools**, expand **Local Users and Groups**, and then click the **Groups** folder.

   The folder contents appear in the details pane.
3. In the details pane, click **BizTalk Server Administrators**.
4. On the **Action** menu, point to **All Tasks**, and then click **Add to Group**.
5. In the **BizTalk Server Administrators Properties** dialog box, click **Add**.
6. In the **Look in** list, select your domain or computer name.
7. In the list that contains the users and computers associated with the domain or computer you selected in step 6, select the user account to add, click **Add**, and then click **OK**.
8. Click **OK** to close the **BizTalk Server Administrators Properties** dialog box.

To remove users from the BizTalk Administrators group

1. Click **Start**, point to **Administrative Tools**, and then click **Computer Management**.
2. Expand **System Tools**, expand **Local Users and Groups**, and then click the **Groups** folder.

   The folder contents appear in the details pane.
3. In the details pane, click **BizTalk Server Administrators**.
4. On the **Action** menu, click **Properties**.

5. In the **BizTalk Server Administrators Properties** dialog box, select the user account you want to remove, and then click **Remove**.

6. Click **OK**.

Managing Hosts and Service Accounts

Before you create a host and host instances you must:

- Create the Windows group for the host.
- Create service accounts for each host instance.
- Add the service accounts to the host Windows group.

Required user rights for managing hosts and service accounts

You must be a Windows administrator to perform the following tasks:

- Create a host Windows group
- Create service accounts for each host instance
- Add the service accounts to the host Windows group
- Modify the Windows group associated with the host

Creating a Host Windows Group

In local group environment, the group name that you specify for the Host should not include the computer name. However, if you specify <*computer name*>\ as the prefix, it will only work if the <*computer name*> is the name of the SQL Server computer. Do not specify <*computer name*>\ as the prefix in local group environment setup.

Creating service accounts for each host instance

This content is not available in this preliminary release.

Adding the service accounts to the host Windows group

This content is not available in this preliminary release.

Updating the host Windows group credentials

This content is not available in this preliminary release.

To setup host to use local group in multi boxes environment

1. Create local groups and users on both Runtime and MgmtDb SQL computers.

2. Ensure that the local user is a member of the local group on both the Runtime and MgmtDb SQL computers.

3. When you create a host, do not specify <*computer name*>\ as the prefix for the group name.

4. Do not specify <*computer name*>\ as prefix for the host instance name.

Managing Signing Certificates

You must be a member of the BizTalk Server Administrators group to specify or change signing certificates. You can specify signing certificates (private key certificates) for the BizTalk group. Signing certificates are optional and you can change them at any time.

Windows Group and User Accounts in BizTalk Server

This section provides information about BizTalk Server local and domain group and user accounts. The Configuration Wizard creates the necessary BizTalk group accounts for you by default if you install BizTalk Server and all prerequisite software on a single computer. The information contained in this section applies to multiple computer topologies.

Procedures

To create Windows Group and User Accounts in BizTalk Server

1. Using Active Directory, from the **Start** menu, point to **Programs**, point to **Administrative Tools**, and select **Active Directory Users and Computers**.

2. In the Active Directory Users and Computers window, right-click at the bottom of the right pane, or right-click the **Users** folder in the navigation tree in the left pane.

3. Select **New**, then select **Group** or **User**.

4. Enter the group or user information outlined in the following table.

The following table lists the Windows group and their associated user accounts used by BizTalk Server. It also identifies the SQL Server/Analysis Server membership roles for the group. You can assign any name for the user accounts identified in brackets in the table.

Group	Group Description	User	User Description	SQL Server/Analysis Server Role Membership for the Group
SSO Administrator(s)*	Administrator of the Enterprise Single Sign-On (SSO) Service. The default name for the Windows	<Enterprise Single Sign-On Service> <SSO Administrator>	Account name under which the Single Sign-On (SSO) service should run. User account	Member of the db_owner SQL Server role for the Credential database.

	account created for this group is SSO Administrators.		for the SSO Administrator.	
SSO Affiliate Administrator(s)	Must be able to create affiliate applications. The BizTalk Administrator must be a member of this group. The default name for the Windows account created for this group is SSO Affiliate Administrators.	<SSO Affiliate Administrators>	User accounts for SSO Affiliate Administrators	

BizTalk Administrators Group	Has the least privileges necessary to perform administrative tasks in the Configuration Wizard and to administer the BizTalk Server environment after installation.
	
	The default name for the Windows account created for this group is BizTalk Server Administrators.
		<BizTalk Server Administrator>
		
		<BizTalk BAS Management Web Service Account>
			User accounts for BizTalk Server Administrators.
			
			BAS Management Web service runs under this service account.
				• Member of BTS_ADMIN_USERS SQL Server role in the following databases:
				  • BizTalk Management (also known as the Configuration database)
				  • MessageBox
				  • Rule Engine
				  • Tracking
				  • BAM Primary Import
				• Member of HWS_ADMIN_USER SQL Server role in the following databases
				  • Human Workflow Services

				• Tracking • Member of the db_owner SQL Server role for the following databases: • BAM Archive • BAM Primary Import • BAM Star Schema • Member of the OLAP Administrator group on the computer hosting the BAM Analysis database
BizTalk Host Users Group	Windows group for accounts with access to the In-Process BizTalk hosts (hosts processes in BizTalk Server). Use one BizTalk Host Group for each In-Process host in your environment. The default name for the Windows account created for the first Host Users group is BizTalk Application Users.	<BTS Host Instance account>	Windows account with access to a specific In-Process BizTalk host instance. This account has Log on as Service rights.	• Member of the BTS_HOST_USERS SQL Server role in the following databases: • BizTalk Management (also known as the Configuration database) • MessageBox • Rule Engine • Tracking • BAM Primary Import • Member of the BTS_<in-process host name>_USERS SQL Server role for the MessageBox database • Member of the BAM_EVENT_WRITER

				SQL Server role in the BAM Primary Import database.

BizTalk Isolated Host Users Group	Windows group for accounts with access to the Isolated BizTalk hosts (hosts processes not running on BizTalk Server, such as HTTP and SOAP).
	
	Use one BizTalk Isolated Host Group for each Isolated Host in your environment.
	
	The default name for the Windows account created for the first Isolated Host Users group is BizTalk Isolated Host Users.
		<BTS Isolated Host Instance Account>
		
		<Human Workflow Services User Account>
			Windows account with access to a specific Isolated BizTalk host instance. This account has Log on as Service rights.
			
			Windows account that the Human Workflow Services runtime services run under.
				• Member of the BTS_HOST_USERS SQL Server role in the following databases:
				  • BizTalk Management (also known as the Configuration database)
				  • MessageBox
				  • Rule Engine
				  • Tracking
				  • BAM Primary Import
				• Member of the BTS_<isolated host name>_USERS SQL Server role for the MessageBox database.
				• The Human Workflow Services User Account must be a member of the HWS_WS_USER SQL Server role in the following databases:
				  • BizTalk Management (also known as the Configuration database)
				  • Tracking
				  • Human Workflow Services

BizTalk Base EDI	Windows NT	<BizTalk Base	Handles all	Member of the

Users group	group that has access to the EDI database. The default name for the Windows account created for this group is EDI Subsystem Users.	EDI service>	EDI-related transactions for BizTalk Server.	edi_admin_users SQL Server role in the Base EDI database.
BizTalk BAS Web Services Group**	For non-interactive user accounts under which BAS Web services run. The default name for the Windows account created for this group is BizTalk BAS Web Services Group.	<BizTalk BAS Management Web Service Account>** <BizTalk BAS Publishing Web Service Account>**	BAS Management Web service runs under this service account. Business Activity Publishing Web service runs under this service account.	Member of the tpm_user SQL Server role in the TPM database.
BizTalk BAS Users**	Has the fewest privileges necessary to perform basic tasks in BAS not requiring the capability to configure business processes (for example, read access to partner profiles and agreements). The default name for the Windows account created for this group is BizTalk BAS Users.	<BAS user accounts>**		

BizTalk BAS Managers**	Has higher privileges than BAS Users group, including tasks to configure business processes such as deploy and activate partners and agreements. The default name for the Windows account created for this group is BizTalk BAS Managers.	<BAS manager user accounts>**		
BizTalk BAS Administrators**	Has privileges to perform all tasks and operations in BAS including administrative tasks such as Business Activity Site repair and synchronization. The default name for the Windows account created for this group is BizTalk BAS Administrators.	<BAS administrative user accounts>**		

*Ensure that the service account running the Enterprise Single Sign-On (SSO) service is a member of the SSO Administrators group on each computer.

*The account you are using when you install BizTalk Server must also be a member of the SSO Administrators group, if the installation is also a SSO master secret server.

**These groups and user accounts are required for access to Business Activity Services (BAS).

The following table identifies the SQL Server membership roles for the user. You can assign any name for the user accounts identified in brackets in the table.

Group	Group Description	User	User Description	SQL Server Role Membership for the User
BizTalk BAS Administrators**	Has privileges to perform all tasks and operations in BAS including administrative tasks such as Business Activity Site repair and synchronization. The default name for the Windows account created for this group is BizTalk BAS Administrators.	<Rule Engine Update Service>	Notifies for deployment/undeployment of policies. No group affiliation.	Member of the RE_HOST_USERS SQL Server role in the Rule Engine database.
		<BizTalk BAM Query Web service user>	Windows account with permission to access the data in the BAM Primary Import database during Business Activity searches. No group affiliation.	Member of the BAM_QueryWS SQL Server role in the BAM Primary Import database.
		<BizTalk Server BAS Application Pool Account>	For application pools that host SharePoint Services, Trading Partner Manager (TPM) Web services and the STSReceive Web service. No group affiliation.	

**These groups and user accounts are required for access to Business Activity Services (BAS).

In This Section

- Local Groups
- Domain Groups

Local Groups

The Configuration Wizard creates the necessary Windows group and user accounts for you by default if you install BizTalk Server and all prerequisite software on a single computer. BizTalk Server supports local group and user accounts only in single computer configurations. BizTalk Server supports domain group and user accounts in both single and multiple computer configurations. For multiple computer configurations, you must observe the requirements provided in this section and in the Minimum Security Privileges and Requirements topic in the Installation Guide. For more information, see http://go.microsoft.com/fwlink/?linkid=22120.

For information about working with domain and local SSO accounts, see **Enterprise Single Sign-On Scenarios**.

If you configure Business Activity Services (BAS) without BizTalk Server (runtime) on your computer, disable Windows Message Queuing (MSMQ) signing for BAS if you want to use a local account for the BizTalk BAS Users Group. If you are using domain accounts, no changes are required.

Domain Groups

Use domain groups for all BizTalk Server installations. For multiple computer configurations using domain groups, observe the following requirements. The minimum security privileges and requirements for BizTalk Server appear in the BizTalk Server Installation Guide.

- If the domain group already exists, you must be a member of this group.
- If you are configuring your computer using domain group and/or user accounts, create them before installing BizTalk Server.
- You must create the group and/or user accounts in the domain to which the computer belongs before configuring them in the Configuration Wizard. The Configuration Wizard cannot create domain groups.
- If you use domain groups, you must add the BizTalk Host Instance Account to the BizTalk Host Users Group. You must add all domain accounts used for the Host and Isolated Host Instances to the appropriate Host Users Group.
- Before configuring BizTalk Server, you can create the Single Sign-On (SSO) Administrators Group, SSO Affiliate Administrators Group, BizTalk Administrator Group, BizTalk Host Users Group, BizTalk Isolated Host Users Group, BizTalk Base Electronic Data Interchange (EDI) Users Group, and BizTalk Business Activity Services (BAS) Users Group on the domain controller. For more information, see Windows Group and User Accounts in BizTalk Server
- You can create the domain group automatically if you specify a domain group during configuration for the SSO Administrators Group and SSO Affiliate Administrators Group, and you have sufficient privileges. If you do not have sufficient privileges, ensure that these groups already exist.

- Use <*DomainName*>\<*UserName*> when specifying domain account information in the Configuration Wizard.

- BizTalk Server requires domain accounts for all clustering scenarios. You cannot use local accounts with clustered SQL Server or clustered SSO Server (master secret server).

- When using a distributed topology in a domain, create the Windows groups used by BizTalk Server and add the appropriate users to the groups in the domain to which the SQL Server computers belong. For more information, see Windows Group and User Accounts in BizTalk Server.

- The administrator installing and configuring BizTalk Server must be a member of the following groups: SSO Administrators (only when configuring the master secret server); Windows administrator; SQL Server administrator; OLAP administrator.

BizTalk Server User Rights

This section provides information about the user rights required when using the various features in BizTalk Server.

In This Section

- Required User Rights for Administering BizTalk Server Objects
- Required User Rights for Managing Orchestrations
- Required User Rights for Managing Send Ports and Send Port Groups
- Required User Rights for Managing Receive Locations
- Required User Rights for Managing BizTalk Hosts and Host Instances
- Required User Rights for Managing a MessageBox Database
- User Accounts for Database Backups
- Security Considerations for Health and Activity Tracking

Required User Rights for Administering BizTalk Server Objects

You must be a member of the BizTalk Server Administrators group to administer BizTalk Server objects. For information about Windows groups and user accounts, see Windows Group and User Accounts in BizTalk Server .

In addition to being a member of the BizTalk Server Administrators group, you may need to have additional SQL Server permissions to complete certain administrative tasks such as creating host instances. For more information about these additional permissions, see **Minimum Security User Rights**.

The following table provides links to the user rights information for managing BizTalk Server objects.

BizTalk Server object	User rights information
Hosts and host instances	Required User Rights for Managing BizTalk Hosts and Host Instances
MessageBox databases	Required User Rights for Managing a MessageBox Database
Orchestrations	Required User Rights for Managing Orchestrations
Receive locations	Required User Rights for Managing Receive Locations
Send ports and send port groups	Required User Rights for Managing Send Ports and Send Port Groups

Required User Rights for Managing Orchestrations

Administrators who manage orchestrations must have the required user rights. You must be a member of the BizTalk Administrators Windows group to manage orchestrations.

Required User Rights for Managing Send Ports and Send Port Groups

Administrators who manage send ports and send port groups must have the required user rights. You must be a member of the BizTalk Administrators Windows group to manage orchestrations.

Required User Rights for Managing Receive Locations

Administrators who manage receive locations must have the required user rights. You must be a member of the BizTalk Administrators Windows group to manage orchestrations.

Required User Rights for Managing BizTalk Hosts and Host Instances

Administrators who manage BizTalk hosts and host instances must have the required user rights. The user rights required to manage hosts are slightly different from the user rights required to manage host instances.

User rights required to manage hosts

You must have the following user rights to create hosts, modify host properties, and delete hosts:

- You must be a member of the BizTalk Server Administrators group. For information about adding users to the BizTalk Server Administrators group,
- You must have the following rights in SQL Server:
  - You must be either a SQL Server administrator, or a member of the db_owner or db_securityadmin SQL Server database roles in the BizTalk Tracking database (BizTalk DTADb), MessageBox databases (BizTalkMsgBoxDb), and the BAM Primary Import database (BAMPrimaryImport).
  - You must be a member of the sysadmin SQL Server role on all the computers where there are MessageBox databases, or a member of the db_owner or db_ddladmin SQL Server role for all the MessageBox databases.

User rights required to manage host instances

You must have the following user rights to create host instances, modify host instance properties, start a host instance, stop a host instance, and delete host instances:

- You must be a member of the BizTalk Server Administrators group. For information about adding users to the BizTalk Administrators group,
- You must be a member of the Administrators group on the run-time computer.
- You must be a SQL Server administrator (a member of the sysadmin SQL Server role) on the computer running SQL Server.
- You must be a member of the db_accessadmin and db_securityadmin SQL Server database roles for the following databases:
  - BizTalk MessageBox (BizTalkMsgBoxDb) (all)
  - BizTalk Tracking (BizTalk DTADb)
  - Rule Engine (BizTalkRuleEngineDb)
  - BizTalk Management (BizTalkMgmtDb)
  - BAM Primary Import (BAMPrimaryImport)

Required User Rights for Managing a MessageBox Database

Administrators who manage MessageBox databases must have the required user rights. You must have the following user rights to manage MessageBox databases and disable new message publication:

- You must be logged on as a member of the BizTalk Server Administrators group.
- You must be a SQL Server Administrator on the computer where the database exists.

User Accounts for Database Backups

To back up your BizTalk Server 2006 databases, you must be logged on with a user account that has access to each of the databases you are backing up.

BizTalk Server includes a SQL Server role named BTS_BACKUP_USERS so that the user account you use to back up your databases does not require System Administrator permissions within SQL Server, except for the primary server controlling the backup process.

When setting up the user account that you are using to back up your databases, note the following:

- You must configure the SQL Server Agent service to run under a domain account or a local account with a mapped user on each instance of SQL Server.
- You must configure a SQL Server logon account for this user, and assign this user to the BizTalk BTS_BACKUP_USERS role on each server.
- You must assign this user to the System Administrators role within SQL Server for the BizTalk Management database server.

Security Considerations for Health and Activity Tracking

For security reasons, Health and Activity Tracking (HAT) does not use browsers or URLs as in previous releases of BizTalk Server. This monitoring option is now included as a part of HAT, which is installed as part of BizTalk Server when you install the administrative tools.

For backward compatibility, BizTalk Server still hosts Microsoft Internet Explorer. BizTalk Server hosts Internet Explorer inside a shell for security reasons. When you install BizTalk Server, you set up a Web site portal for HAT to use exclusively for displaying ASP pages.

Using HAT, you can access the technical details necessary to troubleshoot and optimize your BizTalk Server environment. Because HAT is a powerful tool, you should limit access to it in your production environment so that malicious or unauthorized users do not cause damage. It is recommended you follow these guidelines for securing and using HAT in your environment.

- You must be logged on as a member of the BizTalk Server Operators group to view data using Health and Activity Tracking (HAT). To access message bodies you must be logged on as a member of the BizTalk Server Administrators group.

  Ensure that HAT uses the minimum credentials to perform Health and Activity Tracking tasks. For more information, see **Minimum Security User Rights**.

  When you use HAT, you can access the following databases:

Database	User Group/Permissions
BizTalk Management (BizTalkMgmtDb)	BizTalk Server Administrators, BizTalk Server Operators
BizTalk MessageBox (BizTalkMsgBoxDb)	BizTalk Server Administrators, BizTalk Server Operators, or read-write permissions
BizTalk Tracking (BizTalkDTADb)	BizTalk Server Administrators, BizTalk Server Operators, or read-only permissions

- HAT generates reports about all hosts in the BizTalk Server environment based on the parameters of a query. To minimize the potential of information disclosure, only members of the BizTalk Server Administrators group can use HAT. However, if you do not want all BizTalk Server Administrators to have access to the reports HAT produces, you can limit their access to the data by adding/removing users from the HM_EVENT_WRITER and BAM_EVENT_WRITER SQL Server roles in the BizTalk Tracking (BizTalkDTADb) database.

- BizTalk uses the BAM_EVENT_WRITER and HM_EVENT_WRITER SQL Server roles to grant/deny their members permissions to read/write the tracking data in the Tracking database, but not through role membership. Do not remove these SQL Server roles. When you change a host from hosting to not hosting tracking (or vice versa), the adm_ChangeHostTrackingPrivilege stored procedure is called. This stored procedure reads the definition of the BAM_EVENT_WRITER and HM_EVENT_WRITER SQL Server roles and apply the corresponding GRANT/DENY statements to the Host Windows group. This achieves the same effect as adding the Host Windows group to these SQL roles.

- When you configure the HAT preferences to view data from an archived database, HAT connects to the databases that hold the archived data, not to the currently active BizTalk Tracking (BizTalkDTADb) database.

- You cannot debug live orchestrations across Network Address Translation (NAT) firewalls. You must have an administration computer on the Processing domain in order to debug live orchestrations.

- Depending on how you configure HAT and the pipelines, BizTalk Server may store sensitive information contained in the message context. If you use WMI or HAT to save message bodies to a file location, ensure that the location has a strong discretionary access control list (DACL) so that only BizTalk Server Administrators have read permissions to these message bodies. Apply the same DACL to any location you save the message bodies, including non-BizTalk databases where you may archive and restore them.

- You must manually grant permissions to the BizTalk Server Administrators group to access the Tracking Analysis Server (BizTalkAnalysisDb) database; by default, only OLAP administrators have permissions to it.

Enterprise Single Sign-On

Enterprise Single Sign-On (SSO) provides services to enable single sign-on to end users for enterprise application integration (EAI) solutions. The SSO system maps Microsoft Windows accounts to back-end credentials. SSO simplifies the management of user IDs and passwords, both for users and administrators. It enables users to access back-end systems and applications by logging on only once to the Windows network.

The following new features are included in this release:

- Graphical user interface for system operations, affiliate applications, Password Synchronization, and client utility
- Expanded developer features
- 64-bit support
- Watson support
- Ticketing enhancements
- Multiple access accounts for SSO roles
- Back up secret capability in ConfigFramework user interface
- Backward compatibility of master secret server and credential database with SSO v. 2.0 and SSO 1.0 servers
- Group type affiliate application enhancement to specify multiple mappings

In This Section

Understanding SSO Installing SSO Using SSO Securing Your Deployment of SSO Password Synchronization

Understanding SSO

To understand Enterprise Single Sign-On, it is useful to look at the three types of Single Sign-On services available today: Windows integrated, extranet, and intranet. These are described below, with Enterprise Single Sign-On falling into the third category.

Windows Integrated Single Sign-On

These services enable you to connect to multiple applications within your network that use a common authentication mechanism. These services request and verify your credentials after you log into the network, and use your credentials to determine the actions that you can perform based on your user rights. For example, if applications integrate using Kerberos, after the system authenticates your user credentials you can access any resource in the network that is integrated with Kerberos.

Extranet Single Sign-On (Web SSO)

These services enable you to access resources over the Internet by using a single set of user credentials. The user provides a set of credentials to log on to different Web sites that belong to different organizations. An example of this type of Single Sign-On is Microsoft .NET Passport for consumer based applications. For federated scenarios, Microsoft Active Directory Federation Services enables Web SSO.

Server-Based Intranet Single Sign-On

These services enable you to integrate multiple heterogeneous applications and systems within the enterprise environment. These applications and systems may not use common authentication. Each application has its own user directory store. For example, in an organization, Windows uses Active Directory directory service to authenticate users, and mainframes use IBM's Resource Access Control Facility (RACF) to authenticate the same users. Within the enterprise, middleware applications integrate the front-end and back-end applications. Enterprise Single Sign-On enables users in the enterprise to connect to both the front end and back end while using only one set of credentials. It enables both Windows Initiated Single Sign-On (in which the initial request is made from the Windows domain environment) and Host Initiated Single Sign-On (in which the initial request is made from a non-Windows domain environment) to access a resource in the Windows domain.

In addition, **Password Synchronization** simplifies administration of the SSO database, and keeps passwords in sync across user directories. This is done through the use of password synchronization adapters, which you can configure and manage using the Password Synchronization tools.

The Enterprise Single Sign-On System

Enterprise Single Sign-On (SSO) provides services to store and transmit encrypted user credentials across local and network boundaries, including domain boundaries. SSO stores the credentials in the SSO database. Because SSO provides a generic single sign-on solution, middleware applications and custom adapters can leverage SSO to securely store and transmit user credentials across the environment. End users do not have to remember different credentials for different applications.

The Single Sign-On system consists of an SSO database, a master secret server, and one or more Single Sign-On servers.

The SSO system contains affiliate applications that an administrator defines. An affiliate application is a logical entity that represents a system or sub-system such as a host, back-end system, or line of business application to which you are connecting using Enterprise Single Sign-On. Each affiliate application has multiple user mappings; for example, it has the mappings between the credentials for a user in Active Directory and their corresponding RACF credentials.

The SSO database is the SQL Server database that stores the information about the affiliate applications, as well as all the encrypted user credentials to all the affiliate applications.

The master secret server is the Enterprise Single Sign-On server that stores the master secret. All other Single Sign-On servers in the system get the master secret from the master secret server.

The SSO system also contains one or more SSO Servers. These servers do the mapping between the Windows and back-end credentials, look up the credentials in the SSO database, and administrators use them to maintain the SSO system.

In This Section

SSO User Groups SSO Components SSO Server Master Secret Server SSO Affiliate Applications SSO Mappings SSO Tickets Configuring SSO

SSO User Groups

To configure and manage the Enterprise Single Sign-On (SSO) system, you must create certain Windows groups and accounts for each of these roles. When configuring the access accounts in Enterprise SSO, you can specify more than one account for each of these roles. This section describes these roles.

Single Sign-On Administrators

SSO administrators have the highest level user rights in the SSO system. They can:

- Create and manage the SSO database
- Create and manage the master secret
- Enable and disable the SSO system
- Create password synchronization adapters
- Enable and disable password synchronization in the SSO system
- Enable and disable host initiated SSO
- Perform all administration tasks

The SSO administrators account can be either a Windows group account or an individual account. The SSO administrators account can also be either a domain or local group or individual account. When using an individual account, you cannot change this account to another individual account. Therefore, it is recommended that you do not use an individual account. You can change this account to a group account as long as the original account is a member of the new account.

Single Sign-On Affiliate Administrators

The SSO affiliate administrator defines the affiliate applications that the SSO system contains. Affiliate applications are a logical entity that represents the back-end system to which you are connecting using SSO. SSO affiliate administrators can:

- Create, manage, and delete affiliate applications
- Specify the application administrators account for each affiliate application
- Perform all the administration tasks that the application administrators and application users can

The SSO Affiliate Administrator account can be either a Windows group account or an individual account. The SSO Affiliate Administrator account can also be either a domain or local group or account.

Application Administrators

There is one application administrators group per affiliate application.

Members of this group can:

- Change the application users group account
- Create, delete, and manage credential mappings for all users of the specific affiliate application
- Set credentials for any user in that specific affiliate application users group account
- Perform all the administration tasks that the application users can

Application Users

There is one application users group account for each affiliate application. This account contains the list of end users in an Enterprise Single Sign-On environment. Members of this account can:

- Look up their credentials in the affiliate application
- Manage their credential mappings in the affiliate application

SSO Components

The sub services of the Enterprise Single Sign-On (SSO) service are as follows:

- **Mapping.** This component maps the user account in the Windows system to the user accounts in the back-end systems.
- **Lookup.** This component looks up the user credentials in the SSO database in the back-end system. This is the SSO runtime component.
- **Administration.** This component manages the affiliate applications and the mappings for each affiliate application.

- **Secret.** This component generates the master secret and distributes it to the other SSO servers in the system. It is only active on the Single Sign-On server that is acting as the master secret server.

- **Password Synchronization.** This component simplifies administration of the SSO database, and keeps passwords in sync across user directories

SSO Server

The Enterprise Single Sign-On (SSO) server can perform any of the following tasks:

- **Functions as the master secret server.** The master secret server holds a persisted copy of the master secret, or key, used to encrypt all the credentials in the SSO system. Though the master secret server can act as a server for lookups and administration, it is recommended to use this server to act only as a master secret server for security reasons. For more information about the functions the master secret server performs,

- **Performs administrative operations.** SSO administrators can use any of the Single Sign-On Servers to perform administrative tasks such as managing affiliate applications, setting user credentials, and managing user mappings.

- **Performs lookup operations.** The SSO server uses the runtime component to look up the user credentials.

- **Issues and Redeems Tickets.** The SSO server also issues and redeems SSO tickets.

- **Password Synchronization.** You can create and manage password synchronization adapters on the SSO Server.

Master Secret Server

The master secret server is the Enterprise Single Sign-On (SSO) server that stores the master secret (encryption key). The master secret server generates the master secret when an SSO administrator requests it. The master secret server stores the encrypted master secret in the registry. Only Single Sign-On administrators can access the master secret.

The other Single Sign-On servers check every 30 seconds to see whether the master secret has changed. If it has changed, they read it securely; otherwise, they continue to use the master secret they already have cached in memory. The SSO service uses the master secret to encrypt and decrypt the user credentials.

You cannot use the SSO system until an SSO administrator configures the master secret server and generates the master secret. The master secret server generates the master secret during configuration. Only SSO administrators can generate the master secret. An SSO administrator must configure the master secret server and the SSO database before an application can use the SSO service.

When an SSO administrator needs to regenerate the master secret, for example, if the SSO administrator wants to change the master secret periodically, the master secret server stores both the old and new master secret. The master secret server then goes through all the mappings, decrypts them using the old master secret, and encrypts them again using the new master secret.

If the master secret server fails, all runtime operations already running will continue to run, but SSO servers will not be able to encrypt new credentials.

SSO Affiliate Applications

The Enterprise Single Sign-On (SSO) Affiliate applications are logical entities that represent a system or sub-system such as a host, back-end system, or line of business application to which you are connecting using SSO. An affiliate application can represent a back-end system such as a mainframe or UNIX computer. It can also represent an application such as SAP, or a subdivision of the system, such as the "Benefits" or "Pay stub" sub-systems.

When the SSO administrator or the SSO Affiliate administrator defines an affiliate application, they must also determine who will administer the affiliate application (the application administrator), who the users of the affiliate application are (the application users), and what parameters the SSO system will use to authenticate the users of this affiliate application (the user ID, passwords, PIN numbers, and so on). For more information about application administrators and application users,

Affiliate Application Types

Enterprise SSO defines several different application types. The different application types support different types of mappings between the Windows account and the account on the non-Windows system.

The application types are:

Individual Individual applications support one-to-one mappings between the Windows account and the non-Windows account. In an Individual type application, one Windows account is mapped to one, and only one, non-Windows account. The mapping can be used in either direction, from Windows to non-Windows, or from non-Windows to Windows, or both, depending on the flags that have been set for this application. Thus, Individual applications may be used for Windows initiated SSO, Host initiated SSO, or both.

Group Group applications support mappings between one Windows group to one single non-Windows account. The Application Users account is used to define the Windows group that will be used for this Group application. Only one mapping can be defined for a Group application, and that mapping must be between the Windows group and the single non-Windows account that will be used by all members of this Windows group to access the non-Windows system. Group applications may only be used for Windows initiated SSO.

Host Group Host Group applications are conceptually the reverse of Group applications. They support mappings between a defined group of non-Windows accounts to a single Windows account. The single Windows account that will be used by the non-Windows accounts is defined by the Application Users account for the application. The group of non-

Windows accounts that is allowed to access this application is defined by creating a mapping for each non-Windows account. Host Group applications may only be used for Host initiated SSO.

Designing an Affiliate Application

Before creating an affiliate application, the SSO affiliate administrator or the SSO administrator has to make the following decisions:

1. **What will this affiliate application represent?** You need to know the non-Windows application that the affiliate application will represent in the SSO system. For example,

   Application name: APP1

   Description: Application for Pay stub department

   Contact: administrator@companyname.com

2. **Who will administer this affiliate application?** You need to determine the administrators for this affiliate application. These form the Windows administrators group for this affiliate application. For example, Domain\APP1AdminGroup

3. **Who will use this affiliate application?** You need to determine who the end-users are for this affiliate application. These users represent the Windows users group for this affiliate application; for example, Domain\DomainUsers. In the case of the application for Pay stubs, you might want all users to access their pay stub information, so you can specify the domain users group as the user group for this application.

4. **What credentials does the affiliate application use to authenticate its users?** Different applications user different credentials to authenticate users. For example, some applications may use user IDs, passwords, PINs, or a combination of these. You must also determine whether the system needs to mask these credentials as the user provides them.

5. **Will you use individual mappings or a group mapping for this affiliate application?** Does each Windows user have an account in the back-end system, or does the back-end system have one account for all Windows users? In the case of the pay stub system, each user has their own account to access their pay stub information, and you would need to use individual mappings.

After you create an affiliate application, you cannot modify the following properties:

- Name of the affiliate application
- Fields associated with the affiliate application
- Affiliate application type (host group, individual, or configuration store)

- Administration account same as affiliate administrators group. (If you select this property, then the affiliate administrators group is used as the application administrators account for this affiliate application.)

Affiliate Application Properties

The following table lists the properties you need to define for each affiliate application you create.

Property	Description
Application name	Name of the affiliate application. You cannot change this property after you create the affiliate application
Description	Brief description of the affiliate application
Contact	The main contact for this affiliate application that users can use. (Can be an e-mail address.)
appUserAccount	The Windows group that contains the user accounts of end-users that will be using this affiliate application
appAdminAccount	The Windows group that contains the administrator accounts that will manage this affiliate application.

Application Flag	Description
enableApp	The status of this affiliate application.
groupApp	Determines whether this application uses a group mapping (yes) or individual mappings (No.) You cannot change this property after you create the application.
configStoreApp	Determines whether this affiliate application is a Configuration Store type application (yes). You cannot change this property after you create the application.
hostInitiatedSSO	Enable this if it is a host initiated SSO type application. Default is No.
windowsInitiatedSSO	Enable this if it is a Windows initiated SSO type application. Default is Yes.
validatePassword	This applies only to host initiated SSO applications. When the application attempts to retrieve credentials, it must provide the password in the SSO database which is used for validation by SSO services. Default is Yes.
disableCredCache	The SSO Server stores credentials in a cache to expedite access.

	Default is No.
allowTickets	Determines whether the SSO system uses tickets for this affiliate application. **Security** You must be an SSO administrator to set this flag.
validateTickets	Determines whether the SSO system validates tickets when the user redeems them. **Security** You must be an SSO administrator to set this flag.
appTicketTimeOut	Specifies a ticket timeout specific to the affiliate application. This can be set only when updating an affiliate application, not when creating it. If ticketing is enabled for this application and this property is not, the timeout specified at the SSO System (Global) level is used. **Security** You must be an SSO administrator to set this flag.
timeoutTickets	Determines whether tickets have an expiration time. Default is Yes. **Security** Unless it is required, do not disable ticket timeouts (No.). **Security** You must be an SSO administrator to set this flag.
allowLocalAccounts	Determines whether you allow the use of local groups and accounts in the SSO system. You can only configure this flag to Yes in single-computer scenarios.
adminAccountSame	Determines whether to use the SSO affiliate administrator group as the application administrator group. You cannot change this property after you create the application. **Security** You must be an SSO administrator or SSO affiliate administrator to set this flag.

Application Fields	**Description**	**Description**
Field [0]	<*credential*>: Masked/Unmasked	Determines the type of credential (user ID, password, smartcard) that end users must provide to connect to the affiliate application, and whether this credential is masked (that is, whether the characters that the user types are displayed on the screen) or not. You can enter as many fields as there are credentials for the affiliate application, but the first field must be the user ID.

		You cannot change this property after you create the application.

SSO Mappings

When an Enterprise Single Sign-On (SSO) administrator or an SSO affiliate administrator defines an affiliate application, the administrator can define it either as an application with individual mappings, or as an application with a group mapping.

Individual Mappings

SSO individual mappings enable administrators and users to create a one-to-one mapping between Windows users and their corresponding non-Windows credentials. When using individual mappings, users can manage their own mappings. The SSO system maintains the one-to-one relation for the user's Windows account and the user's non-Windows account.

Windows End-users can create and manage their own mappings for individual type applications. The same affiliate application can act as a Windows Initiated SSO and a Host Initiated SSO type application.

Group Mapping

SSO group mapping consists of mapping a Windows group, which contains multiple Windows users, to a single account in the affiliate application.

You can also specify multiple accounts for the SSO Application Users role. Each account you specify can be associated with an external account. For example, you can map a domain group account to EXTERNALUSER1 and an individual domain account to EXTERNALUSER2. If the same user has more than one mapping, the first mapping in the order of SSO Application Users is used.

Only an application administrator, SSO affiliate administrator, or SSO administrator can create or manage a group mapping.

You cannot specify the same group application for Windows initiated SSO and Host Initiated SSO.

SSO Tickets

In an enterprise environment, where a user interacts with various systems and applications, it is very likely that the environment does not maintain the user context through multiple processes, products, and computers. This user context is crucial to provide single sign-on capabilities, as it is necessary to verify who initiated the original request. To overcome this problem Enterprise Single Sign-On (SSO) provides an SSO ticket (not a Kerberos ticket) that applications can use to get the credentials that correspond to the user who made the original request. SSO tickets are not enabled by default. For more information about enabling tickets,.

The SSO system issues a ticket when requested by an authenticated Windows user. The SSO system can issue a ticket for the user making the request or for a remote user. A ticket contains the encrypted domain and username of the current user, and the ticket expiration time. After the SSO system issues a ticket, it expires in two minutes by default. SSO administrators can modify the expiration time for tickets. The SSO Administrator can also set the ticket timeout at the Affiliate Application level. For more information,

After an application verifies the identity of the original requestor, the application redeems the ticket to obtain the credentials of the user who initiated the request affiliate application. An application can redeem tickets from the SSO system in one of two ways:

- **Redeem only.** When an application initiates a request to redeem a ticket, the request must contain the name of the affiliate application to connect to, and the ticket itself. Only application administrators for the specific affiliate application, SSO affiliate administrators, or SSO administrators can redeem a ticket. You should use **Redeem only** when there is a trusted sub-system between the application that issued the ticket and the application redeeming the ticket. Only an application administrator for the specified affiliate application can redeem the ticket for a user.

- **Validate and redeem.** Tickets contain information about the user for whom the SSO system is performing the credential look-up. In this case, the SSO service verifies that the sender of the original message and the user of the ticket are the same before the system redeems the ticket. Microsoft BizTalk Server adapter scenarios leverage this mechanism.

An SSO administrator can disable ticket timeouts on a per affiliate application basis. While this was not recommended in previous releases, this release supports the use of per affiliate application ticket timeout. This option allows you to set the ticket timeouts at the Affiliate Application level. If this is not specified, the ticket timeout specified at the global level is used.

An SSO affiliate administrator can specify that tickets are allowed and that validation of the ticket is required on a per affiliate application basis. However, if the SSO administrator specifies at the SSO system level that the validation of tickets is required, the SSO affiliate administrator cannot turn off this option at the affiliate application level.

Configuring SSO

You can configure Enterprise Single Sign-On by using command line utilities, UI tools, or COM or Microsoft .NET interfaces.

SSO command line utilities

You use three different command line utilities to perform Enterprise Single Sign-On tasks:

SSOConfig. Enables an SSO administrator to configure the SSO database and to manage the master secret.

SSOManage. Enables SSO administrators, SSO affiliate administrators, and application administrators to update the SSO database to add, delete and manage applications,

administer user mappings, and to set credentials for the affiliate application users. Some operations can be performed only by the SSO administrators, or, only by the SSO administrators and SSO affiliate administrators. All operations that can be performed by the Application Administrators can also be performed by the SSO Administrators and the SSO Affiliate Administrators.

SSOClient. Enables Single Sign-On users to manage their own user mappings and set their credentials.

For more information about the SSO accounts,

SSO UI tools

Enterprise SSO MMC Snap-in. Enables SSO Administrators, SSO Affiliate Administrators, and Application Administrators to update the SSO database, to add, delete and manage applications, administer user mappings, and to set credentials for the affiliate application users. Some operations can be performed only by the SSO administrators, or only by the SSO administrators and SSO affiliate administrators. All operations that can be performed by the Application Administrators can also be performed by the SSO Administrators and SSO Affiliate Administrators.

SSO Client Utility. Enables end users to manage their own mappings and set their credentials using the UI tool.

SSO COM and .NET interfaces

Enterprise Single Sign-On provides COM and .NET programmatic interfaces that enable you to create custom components, and to create scripts to facilitate the administration of the SSO system.

Installing SSO

The following sections contain information regarding installation of the Enterprise Single Sign-On feature. Because of this features complex relationships to other features and systems, and because of its importance to system security, you should read this section carefully before installing Enterprise Single Sign-On.

It is also recommended that you review the latest software prerequisites for installing Enterprise Single Sign-On.

In This Section

- Upgrading from a Previous Version of SSO
- Standard Installation Options
- High-Availability Installation Options
- How to Remove SSO

Upgrading from a Previous Version of SSO

If you are installing the Enterprise Single Sign-on feature and you already have a previous version deployed on your computer (for example, from Microsoft BizTalk Server 2006), you must complete the steps below.

- Back up the SSODB to a secure location
- Back up the master secret key on the master secret server
- Update the master secret server by running BizTalk Server 2006 setup, choosing **Custom Installation**, and then selecting **Enterprise Single Sign-On**. Select **Reuse** when the Configuration Wizard prompts you with the question: Do you want to reuse the existing configuration?

It is not necessary to update the other SSO Servers (non-master secret servers) from your BizTalk Server 2006 installation. However, if you want the new Enterprise Single Sign-On features to be available on those servers, you must update them by using the same procedures outlined above.

If you are installing Host Integration Server 2004 on a computer where BizTalk Server 2006 is already installed, do not select the Enterprise Single Sign-On feature. Host Integration Server Single Sign-On scenarios can leverage the newer (2006) version of Enterprise Single Sign-On already on that computer.

In This Section

- Using Host Initiated SSO Functionality
- Processing Servers for SSO

Using Host Initiated SSO Functionality

Host Initiated Single Sign-On uses the protocol transition feature of Windows Server 2003 to perform Single Sign-On for the non-Windows user. This feature requires Windows Server 2003 and must be in a domain that has its **Domain Functional Level** set to **Windows Server 2003**.

Processing Servers for SSO

In a multi-computer environment, after the master secret server and SSO database have been created, you can install Enterprise Single Sign-On on subsequent computers. These are typically the computers on which either BizTalk Server or Host Integration Server is installed as well.

The initial installation process is the same as on the first computer. Configuration, however, becomes slightly different. Since the master secret server and the SSO database are already in place, select **Join** when the Configuration Wizard asks, **Create a new SSO system or Join an existing system**.

Standard Installation Options

BizTalk Server 2006 leverages the Enterprise Single Sign-On (SSO) capabilities for securely storing credentials to enable single sign-on scenarios.

BizTalk Server also uses SSO to store custom configuration data of Adapters securely. To do this, BizTalk Server runtime and administration features install SSO as a dependent feature. The default installation of BizTalk Server installs Enterprise SSO.

The default installation only installs the Enterprise SSO Administration feature. To install the Enterprise SSO Services, it is necessary to use custom installation of BizTalk Server and select the Enterprise SSO feature.

List of installation options

- Run the BizTalk Server 2006 setup program. Select **Custom Installation**, and then select the appropriate option from the list below:
  - **Enterprise Single Sign-On Master Secret Server —** Acts as the Master Secret Server in the SSO System. This is the first server in the SSO System that needs to deployed and this allows you to create the SSO Credential Database.
  - **Enterprise Single Sign-On Administration —** Administration and client tools for mapping and connecting to Enterprise Single Sign-On Services.
  - **Server Runtime —** Core services to enable single sign-on and to store/access configuration data securely.
  - **Enterprise Single Sign-On Services with Password Synchronization —** Services to enable the Password Synchronization feature in the Enterprise SSO System. These services also integrate with the Microsoft Password Change Notification Service. Once you have installed the core Enterprise Single Sign-On services, you can install the Password Synchronization feature of Enterprise SSO from the BizTalk Server package by launching the \Platform\SSO\Setup.exe and selecting the Password Synchronization feature.
  - **Enterprise Single Sign-On Services —** Provides the core services to enable single sign-on and to store/access configuration data securely. Can act as the Master Secret Server in the SSO system.
  - **Enterprise Single Sign-On Services with Password Synchronization —** Provides the services to enable the Password Synchronization feature in the Enterprise SSO System. These services also integrate with the Microsoft Password Change Notification Service.
  - **Enterprise Single Sign-On Administration —** Administration and client tools for mapping and connecting to Enterprise Single Sign-On Services.
  - When running the HIS Client package, you have the following options:

- **Enterprise Single Sign-On Administration —** Administration and client tools for managing and connecting to Enterprise Single Sign-On Services.

- **Enterprise Single Sign-On Client —** Client tools for end users to manage their mappings.

In This Section

- How to Install the SSO Administration Component

- How to Install the SSO Client Utility

How to Install the SSO Administration Component

It is possible to install the Enterprise Single Sign-On Administration component as a stand-alone feature. This is useful if you need to administer the SSO system remotely. The hardware and software requirements are the same as for a typical Enterprise SSO Runtime Services sinstallation.

After installing the administration component, you will need to use ssomanage.exe to specify the SSO Server to be used for management. Both processes are included in the procedure below.

Installing the SSO administrative utility (ssomanage.exe) does not create shortcuts on the Start menu to access the command line utilities. To run the SSO administrative utilities after installation, you must open a command prompt and navigate to the SSO directory located at Program Files\Common Files\Enterprise Single Sign-On.

The Enterprise SSO Administration feature also includes an MMC Snap-in. The Snap-in is installed on Windows Server 2003 and Windows XP. It is not supported on Windows 2000. You must also have MMC 2.1 installed on your computer for the Snap-in to function.

To open the Enterprise SSO MMC Snap-in click the **Start** menu, then click **Programs**, **Microsoft Enterprise Single Sign-On**, and **SSO Administration**.

To install the Enterprise Single Sign-On administrative component

1. Perform a custom installation of BizTalk Server, selecting only the Enterprise Single Sign-On Administration feature. For BizTalk Server, this can be found under **Additional Software**.

2. When the install program finishes, go to the **Start** menu, click **run**, and then type **cmd**.

3. At the command line prompt, go to the Enterprise Single Sign-On installation directory. The default installation directory is **<drive>**:\Program Files\Common Files\Enterprise Single Sign-On.

4. Specify the SSO Server by selecting one of the following options:

a. Type **ssomanage –server** to specify the SSO Server you want to connect to when performing administration operations.

- OR -

b. Type **ssomanage -serverall** to specify the SSO Server all users of this computer will connect to when performing administration operations.

How to Install the SSO Client Utility

The stand-alone SSO client utility (command-line utility and user interface-based) allows end users to configure their client mappings in the SSO database. You can install the client utility from a self-extracting file (SSOClientInstall.exe) which is installed with the SSO administration feature. Administrators can also make the installer package available to client users by placing a copy of the installer package on a network share.

To install the SSO client utility, you must be running one of the following operating systems on the client computer:

- Windows Server 2003
- Windows 2000 Server with Service Pack 4, or Windows XP Professional with Service Pack 1
- .NET Framework (only necessary if you are using the UI-based SSO Client Utility or for leveraging the managed interoperability component of Enterprise SSO).

To run the command line based SSO client utility after installation, you must open a command prompt and navigate to the SSO directory located at Program Files\Common Files\Enterprise Single Sign-On.

If you had .NET Framework installed on your computer, the UI-based SSO Client Utility is also installed. You can launch this utility from the **Start** menu by clicking **Programs**, **Microsoft Enterprise Single Sign-On**, and then **SSO Client Utility**.

To install the SSO client utility

1. Double-click the installer package SSOClientInstall.
2. The **WinZip Self-Extractor** program appears.
3. Select the folder where you want to unzip the files, and click **Unzip**.

   It is recommended to unzip the files in a temporary folder.

   The **Enterprise Single Sign-On Client Setup** program appears.
4. On **the Welcome to the Enterprise Single Sign-On Client** page, click **Next**.

5. On the License Agreement page, click **I accept the terms of this license agreement**, and then click **Next**.

6. On the **User Information** page, type your user name, organization name, and then click **Next**.

7. On the **Start Installation** page, click **Install**.

8. On the **Completing the Enterprise Single Sign-On Client Wizard** page, click **Finish**.

High-Availability Installation Options

The topics in this section describe installation focused on high availability of Enterprise Single Sign-On, such as multicomputer deployment.

In This Section

- How to Cluster the Master Secret Server
- How to Cluster the SQL Server
- How to Configure SSO in a Multicomputer Scenario

How to Cluster the Master Secret Server

It is strongly recommended that you follow the instructions in this section to cluster the Enterprise Single Sign-On (SSO) service on the master secret server successfully.

When you cluster the master secret server, the Single Sign-On servers communicate to the active clustered instance of the master secret server. Similarly, the active clustered instance communicates with the SSO database.

You must be an SSO administrator to perform this procedure.

To cluster the master secret server

1. Before you start configuring SSO in a cluster environment, it is recommended that you understand how clustering works. For more information, see **http://go.microsoft.com/fwlink/?LinkId=33180**.

2. Create Domain groups with the names SSO Administrators and SSO Affiliate Administrators. To create a clustered instance of the Enterprise SSO service, you must create the SSO Administrators and SSO Affiliate Administrators groups as Domain Groups.

3. Create or designate a Domain account. The Enterprise SSO service on each node will be configured to log on as this Domain account. This account must have the Log on as a service right on each node in the cluster. This account must also be granted Full Control access to the cluster. To grant Full Control access to this account, follow these steps:

    a. Start the **Cluster Administrator**. To do this, click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Cluster Administrator**.

b. Select the cluster.

c. On the **File** menu, click **Properties**.

d. On the **Security** tab, grant the **Domain account Full Control access** to the cluster.

4. Perform a custom installation of BizTalk Server to install the master secret server on the first node (active) of the cluster. For more information about how to perform a custom installation of BizTalk Server, see the BizTalk Server Installation Guide that is located at the following Microsoft Web site:

   http://go.microsoft.com/fwlink/?linkid=22120

   Note that the master secret server must be configured on a cluster that is separate from the BizTalk Server or BizTalk Servers. Do not cluster the master secret server on the same computer or computers that you are running BizTalk Server on. If you create a clustered instance of the master secret server on the same computer that your BizTalk Server is running on, the BizTalk Server will not function correctly when the clustered instance of the master secret server is moved to a different node.

5. Set the following options in the BizTalk Server Configuration Wizard:

   Configuration Questions dialog box

   Click **Yes** in the **Will this Single Sign-On server (SSO) hold the master secret key?** list, and then click **Next**.

   Windows Accounts dialog box

   Specify the service account credentials for the SSO service that you configured in step 2. Make sure that this account is a member of the Domain SSO Administrators group.

   Database Configurations dialog box

   Specify the location of the SQL Server and SSO database (SSODB).

6. Back up the master secret on the active node.

7. Perform a custom installation to install the master secret server on the second node (passive) of the cluster. Configure the SSO server on the second node of the cluster by using the **BizTalk Configuration Wizard**. Because this is not the initial installation of the master secret server, in the Configuration Questions dialog box in the **BizTalk Configuration Wizard**, click **No** in the **Is this the master secret server?** list. Then, click **Next**.

8. Create a new cluster group in the **Cluster Administrator** that will contain the clustered Enterprise SSO service. Add an IP Address resource and a Network Name resource to this cluster group. For a valid IP address to use for the new IP Address

resource, contact your network administrator. Use a unique network name for the Network Name resource. For example, name the Network Name resource SSOCLUSTER.

9. At a command prompt, type **net start entsso** to ensure that the SSO service is running.

10. After you install and configure SSO on both the active and the passive cluster nodes, change the master secret server name in the SSO database to the cluster name. The cluster name is the Network Name resource that you have created in the cluster group that will contain the clustered Enterprise SSO service. For example, the name may be SSOCLUSTER. To do this, follow these steps:

    a. Paste the following code into a text editor:

    b. Save the file as an .xml file. For example, save the file as SSO CLUSTER.xml.

    c. At a command prompt, change to the Enterprise SSO installation folder. By default, the installation folder is Drive:\Program Files\Common Files\Enterprise Single Sign-On.

    d. Type **ssomanage -updatedb XMLFile** to update the master secret server name in the database, where XMLFile is the name of the .xml file that you saved in step b.

11. If you receive runtime error messages, ignore them for now. The Microsoft Distributed Transaction Coordinator (MSDTC) detects an internal inconsistency. MSDTC was not configured to run on a cluster. Therefore, MSDTC cannot start. To resolve these error messages, configure the MSDTC to run on a cluster. To do this, follow these steps:

    a. On the active cluster node, type **comclust -a** at a command prompt.

    b. In the **Services** console, right-click **Distributed Transaction Coordinator**, and then click **Restart**.

    c. On the inactive cluster node, type **comclust -a** at a command prompt.

    d. In the **Services** console, right-click **Distributed Transaction Coordinator**, and then click **Restart**.

To configure the service and resource parameters for the cluster

1. Start **Cluster Administrator**.

2. Click the cluster group that you created for the clustered Enterprise SSO service.

3. On the **File** menu, point to **New**, and then click **Resource**.

4. In the **New Resource** window, follow these steps:

    a. In the **Name** box, type the name of the SSO resource. For example, ENTSSO.

b. In the **Resource** type list, click **Generic Service**.

c. Click **Next**.

5. In the **Possible Owners** dialog box, include each cluster node as a possible owner of the ENTSSO resource.

6. In the **Dependencies** dialog box, add a dependency to the **Name** resource that you created for this group, and then click **Next**.

7. In the **Generic Service Parameters** dialog box, type **entsso** for the **Service** name, leave **Start parameters** blank, click to select the **Use Network Name for computer name** check box, click **Next**, and then click **Finish in the Registry Replication** dialog box.

   If you do not click to select the Use Network Name for computer name check box, SSO client computers will generate an error similar to the following when they try to contact this clustered instance of the Single Sign-On Service:

   Failed to retrieve master secrets. Verify that the master secret server name is correct and that it is available. Secret Server Name: ENTSSO Error Code: 0x800706D9, There are no more endpoints available from the endpoint mapper.

To restore the master secret on the second node

1. In **Cluster Administrator**, right-click the cluster group that includes the master secret server cluster, and then click **Move group**. This step moves the master secret server resources from the first node to the second node.

2. At a command prompt, change to the Enterprise SSO installation folder. By default, the installation folder is Drive:\Program Files\Common Files\Enterprise Single Sign-On.

3. Type **ssoconfig -restoresecret RestoreFile**, where RestoreFile is the name of the backup file that contains the master secret.

How to Configure SSO in a Multicomputer Scenario

This section contains instructions for configuring Enterprise Single Sign-On (SSO) in a three-computer scenario.

In the following scenario, computer A is the master secret server, computer B is the Single Sign-On server, and computer C holds the Credential database. Computer B can act as a runtime server, as an administration server (administration sub services of SSO use this server for managing the Credential database), or as a mapping server (administration and client sub services of SSO use this server to manage mappings).

- If you want to add more SSO servers to your environment, follow the steps for configuring computer B. Any new SSO servers will point to the existing Credential database, and cannot be the master secret server.

To configure the master secret server and create the Credential database on Computer A

1. Perform a custom installation of BizTalk Server, and install only the Enterprise Single Sign-On Master Secret Server component.

2. Run the Configuration Wizard to configure SSO on the master secret server. On the **Configuration Questions** page, select the option to **Create a new SSO system**.

3. On the **Windows Accounts** page, specify the service account credentials for the SSO service. This must be a member of the SSO Administrators group.

4. On the **Database Configurations** page, specify the location of the SQL Server (computer C) and the name of the Credential database (SSODB).

5. Specify the options to back up the Master Secret.

6. Complete the configuration.

To configure the SSO server on Computer B

1. Install Enterprise Single Sign-On on Computer B.

2. Run the Configuration Wizard to configure SSO. On the **Configuration Questions** page, select the option to **Join an existing SSO system**.

3. On the **Windows Accounts** page, specify the service account credentials for the SSO service. This must be a member of the SSO Administrators group.

4. On the **Database Configurations** page, point to the location of the SQL Server (computer C) and the name of the Credential database (SSODB).

How to Remove SSO

If you remove BizTalk Server, Enterprise Single Sign-On (SSO) is no longer configured unless a dependent product is using it. However, it is not removed. You must remove SSO separately. You can also restore configuration information including the master secret to reuse existing data. For more information.

To remove Enterprise Single Sign-On

1. Back up the master secret key. For more information,

2. Uninstall BizTalk Server 2006.

3. On the **Start** menu, point to **Settings**, and then click **Control Panel**.

4. Click **Add/Remove Programs**.

5. In the **Add/Remove Programs** dialog box, click **Microsoft Enterprise Single Sign-On**, and then click **Remove**.

6. Click **Yes** when prompted to confirm the removal of Microsoft Enterprise Single Sign-On.

7. **Note** If you have BizTalk Server Runtime, Development, or Administration features installed, or Host Integration Server Administration features installed, you will not be able to uninstall the SSO Runtime or Administration components until all dependencies are removed.

Using SSO

You can use either the MMC Snap-in or the command line management utility (ssomanage) to manage the SSO system. This includes activities such as updating the SSO database, adding, deleting, and managing applications, and administering user mappings.

Only Single Sign-On Administrators can perform these tasks.

In This Section

- How to Set the SSO Server
- How to Enable SSO
- How to Change the Master Secret Server
- How to Disable SSO
- How to Update the SSO Database
- How to Display the SSO Database Information
- How to Configure the SSO Tickets
- How to Audit SSO
- How to Enable SSL for SSO
- Managing the Master Secret
- How to Specify SSO Administrators and Affiliate Administrators Accounts
- Managing Affiliate Applications
- Managing User Mappings
- Host Initiated SSO

How to Set the SSO Server

Each time you use ssomanage, you must first point the user to the Single Sign-On server you want to connect to.

You can do this in one of two ways:

- Individual users can point themselves to the correct Single Sign-On Server.

- A local computer administrator for the Single Sign-On server can point all the members of the Single Sign-On Users account to this server.

To set the Enterprise Single Sign-On Server using the MMC Snap-In

1. Click **Start**, click **Programs**, click **Microsoft Enterprise Single Sign-On**, and then click **SSO Administration**.

2. In the MMC Snap-In under the **Console Root**, right-click **Enterprise Single Sign-On**, and click **Select**.

3. Browse to the desired server.

4. If appropriate, select the **Set SSO Server for all users** check box.

5. Click **OK**.

To set the Enterprise Single Sign-On Server for a single user using the command line

1. On the **Start** menu, click **run**, and then type **cmd**.

2. At the command line prompt, go to the Enterprise Single Sign-On installation directory. The default installation directory is **<drive>**:\Program Files\Common Files\Enterprise Single Sign-On.

3. Type **ssomanage –server <Single Sign-On Server>**, where **<Single Sign-On Server>** is the computer name of the Single Sign-On Server the user wants to connect to.

To set the Enterprise Single Sign-On Server for all users using the command line

1. On the **Start** menu, click **run**, and then type **cmd**.

2. At the command line prompt, go to the Enterprise Single Sign-On installation directory. The default installation directory is **<drive>**:\Program Files\Common Files\Enterprise Single Sign-On.

3. Type **ssomanage –serverall <Single Sign-On Server>**, where **<Single Sign-On Server>** is the computer name of the Single Sign-On Server all members of the Single Sign-On Users account will be pointed to.

To determine the Enterprise Single Sign-On Server to which a user is connected using the command line

1. On the **Start** menu, click **run**, and then type **cmd**.

2. At the command line prompt, go to the Enterprise Single Sign-On installation directory. The default installation directory is **<drive>**:\Program Files\Common Files\Enterprise Single Sign-On.

3. Type **ssomanage –showserver**.

How to Enable SSO

You can enable the entire Enterprise Single Sign-On (SSO) system by using either the MMC Snap-In or the command line.

After you run the enabling command, there is a short delay before all Single Sign-On Servers are enabled, as each polls the SSO database for the latest global information.

If you want to configure affiliate applications and mappings in the SSO system, you must also create an affiliate application. After an SSO affiliate administrator creates an affiliate application, an application administrator can make changes to it, and application users (end-users) can create their own mappings. For more information, see Managing Affiliate Applications and Managing User Mappings .

To enable the SSO system using the MMC Snap-In

1. Click **Start**, click **Programs**, click **Microsoft Enterprise Single Sign-On**, and then click **SSO Administration**.

2. In the scope pane of the ENTSSO MMC Snap-In, expand the **Enterprise Single Sign-On** node.

3. Right-click **System**, and then click **Enable**.

To enable the SSO system using the command line

1. Click **Start**, click **run**, and then type **cmd**.

2. At the command line prompt, go to the Enterprise Single Sign-On installation directory. The default installation directory is **<drive>**:\Program Files\Common Files\Enterprise Single Sign-On.

3. Type **ssomanage –enablesso**.

To enable SSO to create affiliate applications and mappings

1. Log on as an SSO administrator or SSO affiliate administrator to the SSO Server, or on a computer that has the SSO administration sub services of SSO.

2. On the **Start** menu, click **run**, and then type **cmd**.

3. At the command line prompt, go to the Enterprise Single Sign-On installation directory. The default installation directory is <*drive*>:\Program Files\Common Files\Enterprise Single Sign-On.

4. Type **ssomanage -enablesso** to enable the Enterprise Single Sign-On service.

5. Log on as an SSO affiliate administrator.

6. Type **ssomanage -createapps <*application file*>** to create an affiliate application, where <application file> is the XML file that contains definitions for the affiliate applications.

How to Change the Master Secret Server

After you set up the master secret server and configure the SSO database, you can change the master secret server if the original master secret server fails and cannot be recovered. To change the master secret server, you need to promote an SSO server to become the master secret server.

To change the Master Secret Server using the MMC Snap-in

1. On the **Start** menu, click **Programs**, click **Microsoft Enterprise Single Sign-On**, and then click **SSO Administration**.

2. In the scope pane, right click **System**, and then click **Properties**. The Master secret server is displayed on the **General** tab of the **SSO System Properties** dialog box.

3. Click **Change** to select a new Master secret server.

To promote a Single Sign-On Server to master secret server using the command line

1. Create an XML file that includes the name of the SSO server you want to promote to master secret server. For example,

2. On the **Start** menu, click **run**, and then type **cmd**.

3. At the command line prompt, go to the Enterprise Single Sign-On installation directory. The default installation directory is <*drive*>:\Program Files\Common Files\Enterprise Single Sign-On.

4. Type **ssomanage –updatedb** <***update file***>, where <*update file*> is the name of the XML file you create in step 1.

5. Restart the Master Secret Server.

6. Type **ssoconfig –restoresecret <*restore file*>**, where <*restore file*> is the path and name of the file where the master secret is stored.

How to Disable SSO

You can disable the entire Single Sign-On system by using either the MMC Snap-In or the command line.

There will be a short delay for all Single Sign-On Servers to be disabled, as they poll the SSO database for the latest global information.

To disable Enterprise Single Sign-On using the MMC Snap-In

1. On the **Start** menu, click **Programs**, click **Microsoft Enterprise Single Sign-On**, and then click **SSO Administration**.

2. In the scope pane of the ENTSSO MMC Snap-In, expand the **Enterprise Single Sign-On** node.

3. Right-click **System**, and then click **Disable**.

To disable Enterprise Single Sign-On using the command line

1. On the **Start** menu, click **run**, and then type **cmd**.

2. At the command line prompt, go to the Enterprise Single Sign-On installation directory. The default installation directory is <*drive*>:\Program Files\Common Files\Enterprise Single Sign-On.

3. Type **ssomanage –disablesso**.

How to Update the SSO Database

You can change the global information in the SSO database, such as the master secret server identification, the account names, auditing in the database, ticket timeout, and credential cache timeout, by using either the MMC Snap-In or the command line.

Changing timeouts for the SSO System

You can modify two timeouts at the Enterprise Single Sign-On (SSO) system level:

Ticket timeout. This property specifies the length of time for which a ticket SSO issues is valid. To satisfy most of the scenarios in an enterprise that use SSO, the default ticket timeout is 2 minutes. The SSO administrator can change this based on the application requirements.

Credential Cache timeout. This property specifies the credential cache timeout for all SSO Servers. SSO Servers cache the credentials after the first lookup. By default, the credential cache timeout is 60 minutes. The SSO administrator can change this to a suitable value based on the security requirements.

You change both of these timeouts by updating the SSO database.

A sample XML file for updating the SSO database is:

To change timeouts using the MMC Snap-In

1. On the **Start** menu, click **Programs**, click **Microsoft Enterprise Single Sign-On**, and then click **SSO Administration**.

2. In the scope pane of the ENTSSO MMC Snap-In, expand the **Enterprise Single Sign-On** node.

3. Right-click **System**, and then click **Properties**.

4. On the **SSO System Properties** dialog box, click the **General** tab.

5. Enter the appropriate settings, and click **OK**.

To update the SSO database using the MMC Snap-In

1. On the **Start** menu, click **Programs**, click **Microsoft Enterprise Single Sign-On**, and then click **SSO Administration**.

2. In the scope pane of the ENTSSO MMC Snap-In, expand the **Enterprise Single Sign-On** node.

3. Right-click **System**, and then click **Update**.

To update the SSO database using the command line

1. Click **Start**, click **run**, and then type **cmd**.

2. At the command line prompt, go to the Enterprise Single Sign-On installation directory. The default installation directory is <*drive*>:\Program Files\Common Files\Enterprise Single Sign-On.

3. Type **ssomanage –updatedb <*update file*>**, where <*update file*> is the path and name of the file.

How to Display the SSO Database Information

You can view SSO database information by using the MMC Snap-In or the command line (ssomanage) utility.

To display the SSO database information using the MMC Snap-In

1. On the **Start** menu, click **Programs**, click **Microsoft Enterprise Single Sign-On**, and then click **SSO Administration**.

2. In the scope pane of the ENTSSO MMC Snap-In, expand the **Enterprise Single Sign-On** node.

3. Right-click **System**, and then click **Properties**.

4. Click the tabs on the **SSO System Properties** dialog box to view SSO database information.

To display the SSO database information using the command line

1. On the **Start** menu, click **run**, and then type **cmd**.

2. At the command line prompt, go to the Enterprise Single Sign-On installation directory. The default installation directory is **<drive>**:\Program Files\Common Files\Enterprise Single Sign-On.

3. Type **ssomanage –displaydb**.

To display the SSO database the SSO Server is connected to using the command line

1. On the **Start** menu, click **run**, and then type **cmd**.

2. At the command line prompt, go to the Enterprise Single Sign-On installation directory. The default installation directory is **<drive>**:\Program Files\Common Files\Enterprise Single Sign-On.

3. Type **ssomanage –showdb**.

The following table describes the values displayed by these procedures.

Property	Value
SQL Server	**<SQL Server name>**
SQL Server database	**<SQL Server database name>**
Single Sign-On Secret Server name	**<Single Sign-On Server name>**
Single Sign-On Administrators account	Domain\account name
Single Sign-On Affiliate Administrators account	Domain\account name
Size of audit table for deleted applications (number of audit entries)	1,000 (default)
Size of audit table for deleted user mappings (number of audit entries)	1,000 (default)
Size of audit table for external credential lookups (number of audit entries)	1,000 (default)
Ticket timeout (in minutes)	2 (default) This value can be an integer from1 through 525,600
Credential cache timeout (in minutes)	60 (default)
Single Sign-On Status	Enabled/disabled
Tickets allowed	Yes/no (default)
Validate tickets	Yes (default)/no

How to Configure the SSO Tickets

You can use the MMC Snap-In or the command line to control ticket behavior for the entire Single Sign-On system, including whether to allow tickets, and whether the system must validate the tickets.

You can use Yes, No, On, or Off to indicate whether to allow and/or validate tickets. These words are case independent, and must be used regardless of your language settings.

If you have the SSO Administration feature installed on a remote computer, remote IssueTicket operation can be performed. Note that all traffic between the SSO Administration module and the Runtime module (ENTSSO service) is encrypted.

Using the command line utility, ssomanage.exe, you can specify the ticket timeout at the Affiliate Application level only when an update of the Application is performed, not at creation time.

Only an SSO Administrator can configure tickets at the SSO System level and at the Affiliate Application level.

If ticketing is disabled at the system level, it cannot be used at the Affiliate Application level either. It is possible to enable tickets at the system level and disable it at the Affiliate Application level.

If validation is enabled at the system level, validation of tickets are required at the Affiliate Application level as well. It is possible to disable validation at the system level and enable it at the Affiliate Application level.

If Ticket timeout is specified both at the System level and the Affiliate Application level, the one specified at the Affiliate Application level is used to determine the ticket expiry time.

For more information about tickets and tickets validation, see SSO Tickets.To configure the Enterprise Single Sign-On tickets using the MMC Snap-In for the Affiliate Application

1. On the **Start** menu, click **Programs**, click **Microsoft Enterprise Single Sign-On**, and then click **SSO Administration**.

2. In the scope pane of the ENTSSO MMC Snap-In, expand the **Affiliate Applications** node.

3. Right-click **Affiliate Application**, and then click **Properties**.

4. Click the **Options** tab.

5. Select **Allow Tickets** and configure the ticket timeout as appropriate.

To configure the Enterprise Single Sign-On system-level tickets using the command line

1. On the **Start** menu, click **run**, and then type **cmd**.

2. At the command line, go to the Enterprise Single Sign-On installation directory. The default installation directory is <*drive*>:\Program Files\Common Files\Enterprise Single Sign-On.

3. Type **ssomanage –tickets <*allowed yes/no*> <*validate yes/no*>**, where <*allowed yes/no*> indicates whether tickets will be allowed or not, and <*validate yes/no*> indicates whether tickets will need to be validated after they are redeemed.

How to Audit SSO

You can use the MMC Snap-In or the command line to set both the positive and negative auditing levels. Results of the auditing are stored in both the event logs and the audit logs of the database.

SSO administrators can set the positive and negative audit levels that suit their corporate policies. You can set positive and negative audits to one of the following levels:

0 = None

1 = Low

2 = Medium

3 = High. This level issues as many audit messages as possible.

The default value for positive auditing is 0 (none), and the default value for negative auditing is 1(low).

To change the database level auditing, you must update the SSO database using an XML file. A sample XML file for updating the SSO database is:

To audit Single Sign-On using the MMC Snap-In

1. On the **Start** menu, click **Programs**, click **Microsoft Enterprise Single Sign-On**, and then click **SSO Administration**.

2. In the scope pane of the ENTSSO MMC Snap-In, expand the **Enterprise Single Sign-On** node.

3. Right-click **System**, and then click **Properties**.

4. On the **SSO System Properties** dialog box, click the **Audits** tab.

5. Enter the appropriate settings, and click **OK**.

To audit Single Sign-On using the command line

1. On the **Start** menu, click **run**, and then type **cmd**.

2. At the command line prompt, go to the Enterprise Single Sign-On installation directory. The default installation directory is **<drive>**:\Program Files\Common Files\Enterprise Single Sign-On.

3. Type **ssoconfig –auditlevel < positive level> <negative level>**, where **<positive level>** is the level of auditing when actions succeed, and **<negative auditing>** is the level of auditing when actions fail.

To audit the SSO database

1. Click **Start**, click **run**, and then type **cmd**.

2. At the command line prompt, go to the Enterprise Single Sign-On installation directory. The default installation directory is **<drive>**:\Program Files\Common Files\Enterprise Single Sign-On.

3. Type **ssomanage –updatedb <update file>**, where **<update file>** is the path and name of the file.

How to Enable SSL for SSO

Use this command to enable Secure Sockets Layer (SSL) between all the Enterprise Single Sign-On (SSO) servers and the SSO database.

To enable SSL for Enterprise Single Sign-On

1. Click **Start**, click **run**, and then type **cmd**.

2. At the command line, go to the Enterprise Single Sign-On installation directory. The default installation directory is **<drive>**:\Program Files\Common Files\Enterprise Single Sign-On.

3. Type **ssoconfig –setSSL <yes/no>**, where <**yes/no**> indicates whether you want to enable SSL in the SSO system

Managing the Master Secret

The master secret is the key used to encrypt all the information stored in the SSO database. If the master secret server fails and you lose the secret, you will not be able to retrieve the information stored in the SSO database. Therefore, it is very important to back up the master secret as soon as you generate it.

In This Section

- How to Generate the Master Secret
- How to Back Up the Master Secret
- How to Restore the Master Secret
- How to Move the Master Secret

How to Generate the Master Secret

You must have administrator rights on the master secret server in order to perform this task. In addition, you must perform this task from the master secret server.

The first server where you install Enterprise Single Sign-On becomes the master secret server.

To generate the master secret using the MMC Snap-In

1. On the **Start** menu, click **Programs**, click **Microsoft Enterprise Single Sign-On**, and then click **SSO Administration**.

2. In the scope pane of the ENTSSO MMC Snap-In, expand the **Enterprise Single Sign-On** node.

3. Right-click **System**, and then click **Generate Master Secret**.

To generate the master secret using the command line

1. On the **Start** menu, click **run**, and then type **cmd**.

2. At the command line, go to the Enterprise Single Sign-On installation directory. The default installation directory is <*drive*>:\Program Files\Common Files\Enterprise Single Sign-On.

3. Type **ssoconfig –generatesecret <*backup file*>**, where <*backup file*> is the name of the file that contains the master secret.

   You will be prompted to enter a password to protect the file you just created.

How to Back Up the Master Secret

You can back up the master secret from the master secret server onto an NTFS file system or removable media, such as a floppy disk.

You must be a Single Sign-On Administrator and a Windows administrator to perform this task. The SSO system will prompt you for a password. To restore the secret later, you must specify the same password.

To back up the master secret using the MMC Snap-In

1. On the **Start** menu, click **Programs**, click **Microsoft Enterprise Single Sign-On**, and then click **SSO Administration**.

2. In the scope pane of the ENTSSO MMC Snap-In, expand the **Enterprise Single Sign-On** node.

3. Right-click **System**, and then click **Back up Master Secret**.

To back up the master secret using the command line

1. On the **Start** menu, click **Run**.

2. In the **Run** dialog box, type **cmd**, and then click **OK**.

3. At the command line, go to the Enterprise Single Sign-On installation directory. The default installation directory is <*drive*>:\Program Files\Common Files\Enterprise Single Sign-On.

4. Type **ssoconfig –backupsecret <*backup file*>**, where <*backup file*> is the path and name of the file where the master secret will be backed up. For example, A:\ssobackup.bak

5. Provide a password to protect this file. You will be prompted to confirm the password and to provide a password hint to help you remember this password.

How to Restore the Master Secret

As part of data recovery procedures, you may need to restore the master secret to re-use existing data. In order to perform this task, you must log on to the master secret server with an account that is both a Windows administrator and an SSO administrator.

To restore the master secret using the MMC Snap-In

1. On the **Start** menu, click **Programs**, click **Microsoft Enterprise Single Sign-On**, and then click **SSO Administration**.

2. In the scope pane of the ENTSSO MMC Snap-In, expand the **Enterprise Single Sign-On** node.

3. Right-click **System**, and then click **Restore Master Secret**.

To restore the master secret using the command line

1. On the **Start** menu, click **Run**.

2. In the **Run** dialog box, type **cmd**, and then click **OK**.

3. At the command line, go to the Enterprise Single Sign-On installation directory. The default installation directory is <*drive*>:\Program Files\Common Files\Enterprise Single Sign-On.

4. Type **ssoconfig –restoresecret <*restore file*>**, where <*restore file*> is the path and name of the file where the master secret is stored.

How to Move the Master Secret

This topic documents the steps you can follow to move the master secret from one server to another and the steps you can follow to move the master secret from one server to a Windows Server Cluster.

To move the master secret from one server to another server

1. Install Microsoft Enterprise Single Sign-On Server on the new master secret server if it is not already installed. Launch Microsoft Enterprise Single Sign-On Server setup from \Platform\SSO\setup.exe on the BizTalk Server 2006 CD.

2. Configure Enterprise SSO on the new master secret server if it is not already configured. Follow these steps to configure Enterprise SSO:

   - Open the Configuration tool. By default, the configuration tool is located at <drive>:\Program Files\Common Files\Enterprise Single Sign-On\Configuration.exe.
   - Click to select **Enterprise SSO** in the left pane.
   - Select the check box next to **Enable Enterprise Single Sign-On on this computer** in the right pane.
   - Click the option to **Join an existing SSO System**.
   - Specify the existing **Server Name** and **Database Name** for the SSO Database options.
   - Specify the existing Enterprise SSO service account for the **Enterprise Single Sign-On Server for the Windows Service** option.
   - Click the option to **Apply Configuration** and click **Configure** in the Configuration Wizard dialog box to complete the configuration.
   - Click **Finish** and close the Configuration tool.

3. Back up the existing master secret following the steps in How to Back Up the Master Secret

4. Change the master secret server name in the credential database to reference the new master secret server. For example, the name of the new master secret server may be **NewMSSServer**. To do this, follow these steps on the original master secret server:

   - Paste the following code in a text editor such as notepad.exe:
   - Save the file as an .xml file. For example, save the file as **NewMSSServer.xml**.
   - At a command prompt, change to the Enterprise SSO installation folder. By default, the installation folder is <drive>:\Program Files\Common Files\Enterprise Single Sign-On.
   - Type **ssomanage -updatedb XMLFile** to update the master secret server name in the database.

5. Set the SSO Server name for all users to the new master secret server with the ssomanage command line utility. This command should be run from the Enterprise SSO installation folder. For example, the following command line will set the SSO Server name for all users to the new master secret server:

6. Update the SSO Server name accessible in the **BizTalk Group Properties** page to reference the new master secret server. Launch **BizTalk Server Administration**,

right-click on the BizTalk Group and select the **Properties** menu item, then update the entry for **SSO Server name** and click **OK**.

7. Restart the Enterprise Single Sign-On service on the new master secret server.

8. Restore the backed-up master secret onto the new master secret server by following the steps in How to Restore the Master Secret on the new master secret server.

To move the Master Secret from one server to a Windows Server Cluster

1. Install and configure the Enterprise Single Sign-On service on a Windows Server cluster by following the steps in How to Cluster the Master Secret Server .

2. Back up the existing master secret following the steps in How to Back Up the Master Secret

3. Change the master secret server name in the credential database to reference the new clustered master secret server. Since the new master secret server exists as a cluster resource, the name of the new master secret server will be the same as the name resource in the cluster group that contains the clustered SSO service. For example, the name of the new master secret server may be **ClusteredSSOName**. To do this, follow these steps on the original master secret server:

   - Paste the following code in a text editor such as notepad.exe:

   - Save the file as an .xml file. For example, save the file as **ClusteredSSOName.xml**.

   - At a command prompt, change to the Enterprise SSO installation folder. By default, the installation folder is <drive>:\Program Files\Common Files\Enterprise Single Sign-On.

   - Type **ssomanage -updatedb XMLFile** to update the master secret server name in the database.

4. Set the SSO Server name for all users to the clustered master secret server with the ssomanage command line utility. This command should be run from the Enterprise SSO installation folder. For example, the following command line will set the SSO Server name for all users to the clustered master secret server:

5. Update the SSO Server name accessible in the **BizTalk Group Properties** page to reference the clustered master secret server. Launch **BizTalk Server Administration**, right-click on the BizTalk Group and select the **Properties** menu item, then update the entry for **SSO Server name** and click **OK**.

6. Restart the Enterprise Single Sign-On service on the clustered master secret server. Take the clustered SSO service offline and then bringing it back online in the cluster administrator.

7. Restore the backed-up master secret on each node of the Windows cluster that houses the clustered master secret server. Follow the steps in How to Restore the

Master Secret on each node of the Windows cluster that houses the clustered master secret server.

How to Specify SSO Administrators and Affiliate Administrators Accounts

The Enterprise Single Sign-On (SSO) Administrators and Affiliate Administrators accounts can be host group or individual accounts. You must create these accounts before you configure the SSO system.

When using domain accounts, you must create the SSO Administrators and SSO Affiliate Administrators accounts as a domain global security groups in the domain controller. The domain administrator must create these accounts.

You must specify the Single Sign-On Administrators and Affiliate Administrators accounts in the SSO database. You must disable the Single Sign-On system before you update the SSO database with the SSO Administrators group.

The following XML code shows a sample XML for updating the SSO database:

To disable the Enterprise Single Sign-On system using the MMC Snap-In

1. On the **Start** menu, click **Programs**, click **Microsoft Enterprise Single Sign-On**, and then click **SSO Administration**.

2. In the scope pane of the ENTSSO MMC Snap-In, expand the **Enterprise Single Sign-On** node.

3. Right-click **System**, and then click **Disable**.

To disable the Enterprise Single Sign-On system using the command line

1. On the **Start** menu, click **run**, and then type **cmd**.

2. At the command line, go to the Enterprise Single Sign-On installation directory. The default installation directory is <*drive*>:\Program Files\Common Files\Enterprise Single Sign-On.

3. Type **ssomanage** –**disablesso**.

To update the SSO database using the MMC Snap-In

1. On the **Start** menu, click **Programs**, **Microsoft Enterprise Single Sign-On**, and then **SSO Administration**.

2. In the scope pane of the ENTSSO MMC Snap-In, expand the **Enterprise Single Sign-On** node.

3. Right-click **System**, and then click **Update**.

To update the SSO database using the command line

1. On the **Start** menu, click **run**, and then type **cmd**.

2. At the command line, go to the Enterprise Single Sign-On installation directory. The default installation directory is <*drive*>:\Program Files\Common Files\Enterprise Single Sign-On.

3. Type **ssomanage –updatedb <*update file*>**, where <*update file*> is the path and name of the XML file.

To enable the Enterprise Single Sign-On system using the MMC Snap-In

1. On the **Start** menu, click **Programs**, **Microsoft Enterprise Single Sign-On**, and then **SSO Administration**.

2. In the scope pane of the ENTSSO MMC Snap-In, expand the **Enterprise Single Sign-On** node.

3. Right-click **System**, and then click **Enable**.

To enable the Enterprise Single Sign-On system using the command line

1. On the **Start** menu, click **run**, and then type **cmd**.

2. At the command line, go to the Enterprise Single Sign-On installation directory. The default installation directory is <*drive*>:\Program Files\Common Files\Enterprise Single Sign-On.

3. Type **ssomanage –enablesso**.

Managing Affiliate Applications

This section provides information about how to create and configure affiliate applications.

In This Section

- How to Create an Affiliate Application
- How to Delete an Affiliate Application
- How to Update the Properties of an Affiliate Application
- How to Enable an Affiliate Application
- How to Disable an Affiliate Application
- How to List Affiliate Applications
- How to List the Properties of an Affiliate Application
- How to Clear the Application Cache
- How to Set the SSO Server Using the Client Utility
- How to Display the SSO Server Using the Client Utility
- How to Set Credentials for the Affiliate Application Using the Client Utility

How to Create an Affiliate Application

You can use the MMC Snap-In or this command to create one or more applications, as specified by the XML file. An example XML file for Windows Initiated SSO is:

After you create an affiliate application, you cannot modify the following properties:

- Name of the affiliate application
- Fields associated with the affiliate application
- Affiliate application type (host group, individual, or configuration store)
- Administration account same as affiliate administrators group. (Specifying this flag will always use the affiliate administrators group as the administrator account for this affiliate application)

After you create the affiliate application, you must enable it. For more information, see How to Enable an Affiliate Application .

To create an affiliate application using the MMC Snap-In

1. On the **Start** menu, click **Programs**, click **Microsoft Enterprise Single Sign-On**, and then click **SSO Administration**.
2. In the scope pane of the ENTSSO MMC Snap-In, expand the **Enterprise Single Sign-On** node.
3. Right-click **Affiliate Applications**, and then click **New**.
4. Follow the instructions in the **Create New Affiliate Application** wizard.

To create an affiliate application using the command line

1. On the **Start** menu, click **run**, and then type **cmd**.
2. At the command line, go to the Enterprise Single Sign-On installation directory. The default installation directory is <*drive*>:\Program Files\Common Files\Enterprise Single Sign-On.
3. Type **ssomanage –createapps <*application file name*>**, where <*application file name*> is the XML file.

How to Delete an Affiliate Application

You can use the MMC Snap-In or the command line to delete the specified affiliate application from the SSO database.

To delete an affiliate application using the MMC Snap-In

1. On the **Start** menu, click **Programs**, click **Microsoft Enterprise Single Sign-On**, and then click **SSO Administration**.

2. In the scope pane of the MMC Snap-In, expand the **Enterprise Single Sign-On** node.

3. Right-click the affiliate application, and then click **Delete**.

To delete an affiliate application using the command line

1. On the **Start** menu, click **run**, and then type **cmd**.

2. At the command line, go to the Enterprise Single Sign-On installation directory. The default installation directory is <*drive*>:\Program Files\Common Files\Enterprise Single Sign-On.

3. Type **ssomanage –deleteapp <*application name*>**, where <*application name*> is the name of the affiliate application you want to remove from the SSO database.

How to Update the Properties of an Affiliate Application

You can use the MMC Snap-In or this command to update one or more application properties, as specified by the XML file. You must be an Affiliate Administrator to perform this task. The following is an example XML file that lists the fields you can update.

After you create an affiliate application, you cannot modify the following properties:

- Name of the affiliate application
- Fields associated with the affiliate application
- Affiliate application type (host group, individual, or configuration store)
- Administration account same as affiliate administrators group. (Specifying this flag will always use the affiliate administrators group as the administrator account for this affiliate application)

To update the properties of an affiliate application using the MMC Snap-In

1. On the **Start** menu, click **Programs**, click **Microsoft Enterprise Single Sign-On**, and then click **SSO Administration**.

2. In the scope pane of the ENTSSO MMC Snap-In, expand the **Enterprise Single Sign-On** node.

3. Right-click the affililate application, and then click **Update**.

To update the properties of an affiliate application using the command line

1. On the **Start** menu, click **run**, and then type **cmd**.

2. At the command line, go to the Enterprise Single Sign-On installation directory. The default installation directory is **<drive>**:\Program Files\Common Files\Enterprise Single Sign-On.

3. Type **ssomanage –updateapps <application file name>**, where the application file name is the XML file.

How to Enable an Affiliate Application

You can use the MMC Snap-In or the command line to enable the specified affiliate application.

To enable an affiliate application using the MMC Snap-In

1. On the **Start** menu, click **Programs**, click **Microsoft Enterprise Single Sign-On**, and then click **SSO Administration**.

2. In the scope pane of the ENTSSO MMC Snap-In, expand the **Enterprise Single Sign-On** node.

3. Right-click the affililate application, and then click **Enable**.

To enable an affiliate application using the command line

1. On the **Start** menu, click **run**, and then type **cmd**.

2. At the command line, go to the Enterprise Single Sign-On installation directory. The default installation directory is <*drive*>:\Program Files\Common Files\Enterprise Single Sign-On.

3. Type **ssomanage –enableapp <*application name*>**, where <*application name*> is the name of the affiliate application you want to enable.

How to Disable an Affiliate Application

You can use the MMC Snap-In or the command line to disable the specified affiliate application.

To disable an affiliate application using the MMC Snap-In

1. On the **Start** menu, click **Programs**, click **Microsoft Enterprise Single Sign-On**, and then click **SSO Administration**.

2. In the scope pane of the ENTSSO MMC Snap-In, expand the **Enterprise Single Sign-On** node.

3. Right-click the affiliate application, and then click **Disable**.

To disable an affiliate application using the command line

1. Click **Start**, click **run**, and then type **cmd**.

2. At the command line, go to the Enterprise Single Sign-On installation directory. The default installation directory is <*drive*>:\Program Files\Common Files\Enterprise Single Sign-On.

3. Type **ssomanage –disableapp <*application name*>**, where <*application name*> is the name of the affiliate application you want to disable.

How to List Affiliate Applications

Use this command to list all the affiliate applications. If the user is a member of the Application Administrators account, this command will only display the application for which the user is an administrator.

To list affiliate applications using the administration utility

1. On the **Start** menu, click **run**, and then type **cmd**.

2. At the command line, go to the Enterprise Single Sign-On installation directory. The default installation directory is <*drive*>:\Program Files\Common Files\Enterprise Single Sign-On.

3. Type **ssomanage -listapps [all]** where **all** is an optional parameter that will also display applications using the Configuration Store feature. If the user running this command is an Application administrator, it will only list the applications for which they are an administrator. If the user running this command is an Affiliate Administrator or an SSO Administrator, it will list all the affiliate applications.

To list affiliate applications using the client utility

1. On the **Start** menu, click **run**, and then type **cmd**.

2. At the command line, go to the Enterprise Single Sign-On installation directory. The default installation directory is <*drive*>:\Program Files\Common Files\Enterprise Single Sign-On.

3. Type **ssoclient –listapps** to list the affiliate applications. This will list only the affiliate applications that the user performing this task is a member of, i.e., they need to belong the application user group account for that affiliate application.

How to List the Properties of an Affiliate Application

This command shows the following information about the affiliate application. For more information about the properties for an affiliate application.

The SSO system obtains this information from the xml file that you used to update the affiliate application. For more information.

To display the properties of an affiliate application using the administration utility

1. On the **Start** menu, click **run**, and then type **cmd**.

2. At the command line, go to the Enterprise Single Sign-On installation directory. The default installation directory is <*drive*>:\Program Files\Common Files\Enterprise Single Sign-On.

3. Type **ssomanage –displayapp <*application name*>**, where <*application name*> is the name of the Affiliate Application you want to display the properties for.

To display the properties of an affiliate application using the client utility

1. On the **Start** menu, click **run**, and then type **cmd**.

2. At the command line, go to the Enterprise Single Sign-On installation directory. The default installation directory is <*install drive*>:\Program Files\Common Files\Enterprise Single Sign-On.

3. Type **ssoclient –displayapp <*application name*>**, where <*application name*> is the name of the Affiliate Application you want to display the properties for.

How to Clear the Application Cache

You can use the MMC Snap-In or the command line to remove the contents of the credential cache (all the information associated with the affiliate application) for the specified application on all of the Single Sign-On Servers.

To clear the cache using the MMC Snap-In

1. On the **Start** menu, click **Programs**, click **Microsoft Enterprise Single Sign-On**, and then click **SSO Administration**.

2. In the scope pane of the ENTSSO MMC Snap-In, expand the **Enterprise Single Sign-On** node.

3. Click **Affiliate Applications**.

4. In the results pane, right-click the affiliate application, and click **Clear**.

To clear the cache using the command line

1. On the **Start** menu, click **run**, and then type **cmd**.

2. At the command line, go to the Enterprise Single Sign-On installation directory. The default installation directory is <*drive*>:\Program Files\Common Files\Enterprise Single Sign-On.

3. Type **ssomanage –purgecache <*application name*>**, where <*application name*> is the name of the affiliate application you want to purge the cache for.

How to Set the SSO Server Using the Client Utility

Each time you use ssoclient, you must first point the user to the correct Single Sign-On server that contains their configuration information.

To set the SSO Server for a user using the client utility

1. On the **Start** menu, click **run**, and then type **cmd**.

2. At the command line, go to the Enterprise Single Sign-On installation directory. The default installation directory is <*drive*>:\Program Files\Common Files\Enterprise Single Sign-On.

3. Type **ssoclient –server <*Single Sign-On Server*>**, where <*Single Sign-On Server*> is the name of the Single Sign-On server the user wants to connect to.

How to Display the SSO Server Using the Client Utility

Use this command to display the Single Sign-On Server to which the user is currently pointing.

To display the SSO server using the client utility

1. On the **Start** menu, click **run**, and then type **cmd**.

2. At the command line, go to the Enterprise Single Sign-On installation directory. The default installation directory is <*drive*>:\Program Files\Common Files\Enterprise Single Sign-On.

3. Type **ssoclient –showserver**.

How to Set Credentials for the Affiliate Application Using the Client Utility

Use this command to set the credentials for a user so that the user is able to access a specific application. This command also automatically enables the mapping.

This command does not display the password as you type it.

If the user mapping already exists, this command will set the credentials for that existing mapping. If you have not created the user mapping, the SSO system will prompt you for the user ID for the application.

To set credentials for the affiliate application using the client utility

1. On the **Start** menu, click **run**, and then type **cmd**.

2. At the command line, go to the Enterprise Single Sign-On installation directory. The default installation directory is **<drive>**:\Program Files\Common Files\Enterprise Single Sign-On.

3. Type **ssoclient –setcredentials <application name>**, where **<application name>** is the specific application for which you want to set the credentials for.

4. When prompted for the user credentials, enter the user password for this application.

5. If you have not created the user mapping, the SSO system will prompt you for the user ID for the application.

Managing User Mappings

This section provides information on how to create and configure the Enterprise Single Sign-On mappings.

Administrators use the ssomanage utility to manage mappings, while the application users use the ssoclient utility to manage their mappings.

In This Section

- How to List User Mappings
- How to Create User Mappings
- How to Delete User Mappings
- How to Set Credentials for a User Mapping
- How to Enable a User Mapping
- How to Disable a User Mapping
-

How to List User Mappings

Use this command to list all the existing mappings for the specified user.

You must be an SSO administrator, application administrator, SSO affiliate administrator, or user to do this task.

Enabled user mappings appear as (E) <*domain*>\<*username*>, while disabled user mappings appear as (D) <*domain*>\<*username*>.

To list user mappings using the administration utility

1. On the **Start** menu, click **run**, and then type **cmd**.

2. At the command line, go to the Enterprise Single Sign-On installation directory. The default installation directory is <*drive*>:\Program Files\Common Files\Enterprise Single Sign-On.

3. Do one of the following:

To list user mappings using the client utility

1. On the **Start** menu, click **run**, and then type **cmd**.

2. At the command line, go to the Enterprise Single Sign-On installation directory. The default installation directory is <*drive*>:\Program Files\Common Files\Enterprise Single Sign-On.

3. Type **ssoclient –listmappings** to list all the mappings you have.

How to Create User Mappings

Use this command to create one or more user mappings, as specified in the XML file. The following is an example XML file.

If a user account is changed, you must use this command create a mapping for the new user account. You should also remove the old user mapping. For more information about removing a mapping,.

After you create a user mapping, you must enable it before you can use this mapping in the SSO system. For more information,.

To create user mappings using the administration utility

1. On the **Start** menu, click **run**, and then type **cmd**.

2. At the command line, go to the Enterprise Single Sign-On installation directory. The default installation directory is <*drive*>:\Program Files\Common Files\Enterprise Single Sign-On.

3. Type **ssomanage –createmappings <*mappings file name*>**, where <*mappings file name*> is the name of file that contains the user mapping(s) you want to create.

To create user mappings using the client utility

1. On the **Start** menu, click **run**, and then type **cmd**.

2. At the command line, go to the Enterprise Single Sign-On installation directory. The default installation directory is <*drive*>:\Program Files\Common Files\Enterprise Single Sign-On.

3. Type **ssoclient –setcredentials <*application name* >**, where <*application name* > is the name of affiliate application that the user wants to create a mapping for.

How to Delete User Mappings

Use these commands to delete one or more user mappings, as specified in the XML file. The following is an example XML file.

If a user is not a member of the Application Users account, or does not exist in Active Directory, you should use this command to remove the user mapping from the SSO database.

If a user account is changed, you must use this command to remove the old user mapping, and then create a new user mapping for the new user account. For more information about creating a mapping,

To delete user mappings using the administration utility

1. On the **Start** menu, click **run**, and then type **cmd**.

2. At the command line, go to the Enterprise Single Sign-On installation directory. The default installation directory is <*drive*>:\Program Files\Common Files\Enterprise Single Sign-On.

3. Type **ssomanage –deletemappings <*mappings file name*>**, where <*mappings file name*> is the name of the file that contains the user mapping(s) you want to delete.

To delete a specific user mapping using the administration utility

1. On the **Start** menu, click **run**, and then type **cmd**.

2. At the command line, go to the Enterprise Single Sign-On installation directory. The default installation directory is <*drive*>:\Program Files\Common Files\Enterprise Single Sign-On.

3. Type **ssomanage –deletemapping <*domain*>\<*username*> <*application name*>**, where <*domain*> is the Windows domain for the user account, <*username*> is the Windows user name, and <*application name*> is the specific application for which you want to remove the user mapping.

To delete a user mapping using the client utility

1. On the **Start** menu, click **run**, and then type **cmd**.

2. At the command line, go to the Enterprise Single Sign-On installation directory. The default installation directory is <*drive*>:\Program Files\Common Files\Enterprise Single Sign-On.

3. Type **ssoclient –deletemapping <*application name*>**, where <*application name*> is the name of the affiliate application you want to remove the user mapping for.

How to Set Credentials for a User Mapping

Use this command to set the credentials for a user to access a specific application.

This command does not display the password as you type it.

If the user mapping already exists, this command sets the credentials for that existing mapping. If you have not created the user mapping, the SSO system will prompt you for the user ID for the application.

To set credentials for a user mapping

1. On the **Start** menu, click **run**, and then type **cmd**.
2. At the command line, go to the Enterprise Single Sign-On installation directory. The default installation directory is **<drive>**:\Program Files\Common Files\Enterprise Single Sign-On.
3. Type **ssomanage –setcredentials <domain>\<username> <applicationname>**, where **<domain>** is the Windows domain for the user account, **<username>** is the Windows user name, and **<applicationname>** is the specific application for which you want to set the credentials for.
4. When the SSO system prompts you for the user credentials, enter the user password for this application.
5. If you have not created the user mapping, the SSO system will prompt you for the user ID for the application.

To set credentials for a user mapping from the client utility

1. On the **Start** menu, click **run**, and then type **cmd**.
2. At the command line, go to the Enterprise Single Sign-On installation directory. The default installation directory is **<drive>**:\Program Files\Common Files\Enterprise Single Sign-On.
3. Type **ssoclient -setcredentials <application name>**,where **<application name>** is the name of the affiliate application you want to remove the user mapping for.

How to Enable a User Mapping

You must enable a user mapping before it you can use the mapping in the Single Sign-On system.

When you enable a user mapping, it will appear as (E) **<domain>\<username>** when you list the user mappings.

Note that if you have set the credentials using the -setcredentials command, the mapping will already be enabled.

To enable a user mapping using the administration utility

1. On the **Start** menu, click **run**, and then type **cmd**.

2. At the command line, go to the Enterprise Single Sign-On installation directory. The default installation directory is **<drive>**:\Program Files\Common Files\Enterprise Single Sign-On.

3. Type **ssomanage –enablemapping <domain>\<username> <application name>**, where **<domain>** is the Windows domain for the user account, **<username>** is the Windows user name for which you want to enable the credentials, and **<application name>** is the name of the affiliate application you want to remove the user mapping for and then press ENTER.

To enable a user mapping using the client utility

1. On the **Start** menu, click **run**, and then type **cmd**.

2. At the command line, go to the Enterprise Single Sign-On installation directory. The default installation directory is **<drive>**:\Program Files\Common Files\Enterprise Single Sign-On.

3. Type **ssoclient –enablemapping <application name>**, where **<application name>** is the name of the affiliate application you want to remove the user mapping for.

How to Disable a User Mapping

You can disable a user mapping when you want to turn off all operations associated with a given mapping. You must disable a user mapping before you can remove it.

When you disable a user mapping, it will appear as (D) <*domain*>\<*username*> when you list the user mappings.

To disable a user mapping using the administration utility

1. On the **Start** menu, click **run**, and then type **cmd**.

2. At the command line, go to the Enterprise Single Sign-On installation directory. The default installation directory is <*drive*>:\Program Files\Common Files\Enterprise Single Sign-On.

3. Type **ssomanage –disablemapping <*domain*>\<*username*> <*application name*>**, where <*domain*> is the Windows domain for the user account, and <*username*> is the Windows user name for which you want to disable the credentials, and <*application name*> is the name of the affiliate application you want to remove the user mapping for.

To disable a user mapping using the client utility

1. On the **Start** menu, click **run**, and then type **cmd**.

2. At the command line, go to the Enterprise Single Sign-On installation directory. The default installation directory is <*drive*>:\Program Files\Common Files\Enterprise Single Sign-On.

3. Type **ssoclient –disablemapping <*application name*>**, where <*application name*> is the name of the affiliate application you want to remove the user mapping for.

Host Initiated SSO

Host initiated Single Sign-On enables a request from the host system to access a resource on a Windows system. The host system (for example, a RACF account) exists in a non-Windows environment and under the context of a non-Windows user. The Single Sign-On Credential Store maps host accounts to Windows accounts, enabling this access.

The following topics describe configuration specific to Host initiated SSO.

In This Section

- How to Configure Requirements for Host Initiated SSO
- How to Enable and Disable Host Initiated SSO
- How to Create Affiliate Applications for Host Initiated SSO
- Validating Passwords for Host Initiated SSO
- How to Manage User Mappings for Host Initiated SSO
- How to Use the Trace Utility in Host Initiated SSO

How to Configure Requirements for Host Initiated SSO

Although Enterprise SSO and host initiated SSO have certain aspects in common, certain platform and Active Directory requirements are unique to host initiated SSO. This topic discusses those requirements, and lists the steps to check or create them on your system.

- Host initiated SSO can be executed only on a native Windows 2003 domain environment.

- The service account for SSO Service that is performing host initiated SSO must be configured to have TCB privileges. (You can configure this for the service account in the domain security policy.)

In addition, certain requirements are necessary when using Transaction Integrator for Host Initiated Processing. TI for HIP leverages host initiated SSO to achieve Single Sign-On for non-Windows users.

For example, service account for TI for HIP service runs under a service account domainname\hipsvc. This service can host applications that want to access remote or local resources on Windows with the Windows account that correspond to the non-Windows account.

The domainname\hipsvc account must belong to the Application Administrator group account for the Affiliate Application that is being used for Single Sign-On.

The domainname\hipsvc account must have constrained delegation privileges to use host initiated Single Sign-On. This can be configured by the domain administrator in Active Directory. Delegation can be configured for accounts that have registered SPNs. Constrained delegation allows the service account to access only components that are specified by the administrator.

To check your domain function level

1. In your **Active Directory Domains and Trusts** MMC snap-in, right click the node **Active Directory Domains and Trusts**, and then click **Raise Forest Functional Level**.

2. Verify that the functional level is **Windows Server 2003**. If it is not, refer to your Active Directory documentation before you attempt to change the setting.

To create an SPN

1. Download the **setspn** utility from the following location: http://go.microsoft.com/fwlink/?LinkId=33178

2. On the **Start** menu, click **Run**.

3. In the **Run** dialog box, type **cmd**, and then click **OK**.

4. At the command line, go to the Enterprise Single Sign-On installation directory. The default is <drive>:\Program Files\Common Files\Enterprise Single Sign-On.

5. Type **setpsn -a hipsvc\computername.domain.com domain\hissvc**

   where **hipsvc\computername.domain.com** is the service that will perform the operation and the computer it is running on, and **domain\hissvc** is the service account for hipsvc.

After doing this, you can configure constrained delegation in Active Directory for this service account (domain\hissvc) to access the appropriate resource in the network.

To give TCB privileges for the SSO service account

- Under your **Domain Security Policy - Local Policies - User Rights Assignment**, add the SSO Service account to the **Act as part of operating system** policy.

How to Enable and Disable Host Initiated SSO

By default, host initiated Single Sign-On is not enabled in the Single Sign-On system, and must be enabled by the SSO Administrator.

To enable host initiated SSO using the MMC Snap-In

1. On the **Start** menu, click **Programs**, click **Microsoft Enterprise Single Sign-On**, and then click **SSO Administration**.
2. In the scope pane of the ENTSSO MMC Snap-In, expand the **Enterprise Single Sign-On** node.
3. Right-click **System**, and then click **Properties**.
4. Click the **Options** tab.
5. Select the **Enable host initiated SSO** box, and click **OK**.

To enable host initiated SSO using the command line

1. On the **Start** menu, click **Run**.
2. In the **Run** dialog box, type **cmd**, and then click **OK**.
3. At the command line, go to the Enterprise Single Sign-On installation directory. The default is <drive>:\Program Files\Common Files\Enterprise Single Sign-On.
4. Type **ssomanage -enable hisso**.

Disabling SSO applies to the entire SSO system, and all operations related to host initiated SSO are turned off.

To disable host initiated SSO using the MMC Snap-In

1. On the **Start** menu, click **Programs**, click **Microsoft Enterprise Single Sign-On**, and then click **SSO Administration**.
2. In the scope pane of the ENTSSO MMC Snap-In, expand the **Enterprise Single Sign-On** node.
3. Right-click **System**, and then click **Properties**.
4. Click the **Options** tab.
5. Clear the **Enable host initiated SSO** box, and click **OK**.

To disable host initiated SSO using the command line

1. On the **Start** menu, click **Run**.
2. In the **Run** dialog box, type **cmd**, and then click **OK**.

3. At the command line, go to the Enterprise Single Sign-On installation directory. The default is <drive>:\Program Files\Common Files\Enterprise Single Sign-On.

4. Type **ssomanage -disable hisso** as appropriate.

How to Create Affiliate Applications for Host Initiated SSO

You can define two types of applications:

- **Individual** There is a 1 to 1 relationship between Windows users and non-Windows users.

- **Host Group** Multiple non-Windows users can be mapped to the same Windows account.

To create an affiliate application using the MMC Snap-In

1. On the **Start** menu, click **Programs**, click **Microsoft Enterprise Single Sign-On**, and then click **SSO Administration**.

2. In the scope pane of the ENTSSO MMC Snap-In, expand the **Enterprise Single Sign-On** node.

3. Right-click **Affiliate Applications**, and then click **New** to open the **Create New Affiliate Application Wizard**.

4. Use the wizard to select the properties of your affiliate application.

To create an individual type affiliate application using the command line

1. On the **Start** menu, click **Run**.

2. In the **Run** dialog box, type **cmd**, and then click **OK**.

3. At the command line, go to the Enterprise Single Sign-On installation directory. The default is <drive>:\Program Files\Common Files\Enterprise Single Sign-On.

4. Type **ssomanage –createapps <AffApp.xml>**, where AffApp.xml is the name of the xml file.

To create a host group type affiliate application using the command line

1. On the **Start** menu, click **Run**.

2. In the **Run** dialog box, type **cmd**, and then click **OK**.

3. At the command line, go to the Enterprise Single Sign-On installation directory. The default is <drive>:\Program Files\Common Files\Enterprise Single Sign-On.

4. Type **ssomanage –createapps <AffApp.xml>**, where AffApp.xml is the name of the xml file.

To create an affiliate application supporting both Windows initiated SSO and host initiated SSO using the command line

1. On the **Start** menu, click **Run**.

2. In the **Run** dialog box, type **cmd**, and then click **OK**.

3. At the command line, go to the Enterprise Single Sign-On installation directory. The default is <drive>:\Program Files\Common Files\Enterprise Single Sign-On.

4. Type **ssomanage –createapps <AffApp.xml>**, where AffApp.xml is the name of the xml file

Validating Passwords for Host Initiated SSO

When an affiliate application for host initiated SSO is created, password validation for the non-Windows user is enabled by default. This means when applications call SSO to obtain the Windows user token to access resources, they must provide the non-Windows user account and the non-Windows password. If the password does not match the password in the SSO database for that non-Windows user, access is denied. If necessary, the password validation feature can be disabled for the affiliate application. The password validation feature applies to both individual and host group type affiliate applications for host initiated SSO.

How to Manage User Mappings for Host Initiated SSO

Use the following procedures to create mappings, set credentials, and enable or disable mapping.

To manage user mappings for host initiated SSO using the MMC Snap-In

1. On the **Start** menu, click **Programs**, click **Microsoft Enterprise Single Sign-On**, and then click **SSO Administration**.

2. In the scope pane of the ENTSSO MMC Snap-In, expand the **Enterprise Single Sign-On** node.

3. In the scope pane, click **Affiliate Applications**.

4. In the details pane, right-click the affiliate application, and then choose the appropriate menu item for your action.

To create mappings in host initiated SSO using the command line

1. On the **Start** menu, click **Run**.

2. In the **Run** dialog box, type **cmd**, and then click **OK**.

3. At the command line, go to the Enterprise Single Sign-On installation directory. The default is <drive>:\Program Files\Common Files\Enterprise Single Sign-On.

4. Type **ssomanage –createmappings <mapping file>**, where **mapping file>** is the name of the xml file.

When the Validate Password feature is enabled for the affiliate application, it is necessary to set credentials, as follows:

To set credentials for individual type affiliate applications using the command line

1. On the **Start** menu, click **Run**.
2. In the **Run** dialog box, type **cmd**, and then click **OK**.
3. At the command line, go to the Enterprise Single Sign-On installation directory. The default is <drive>:\Program Files\Common Files\Enterprise Single Sign-On.
4. Type **ssomanage -setcredentials <Windows account name> <application name>**.

To set credentials for host group type affiliate applications using the command line

1. On the **Start** menu, click **Run**.
2. In the **Run** dialog box, type **cmd**, and then click **OK**.
3. At the command line, go to the Enterprise Single Sign-On installation directory. The default is <drive>:\Program Files\Common Files\Enterprise Single Sign-On.
4. Type **ssomanage -setcredentials <external account name> <application name>**.

To enable mappings for individual type affiliate applications using the command line

1. On the **Start** menu, click **Run**.
2. In the **Run** dialog box, type **cmd**, and then click **OK**.
3. At the command line, go to the Enterprise Single Sign-On installation directory. The default is <drive>:\Program Files\Common Files\Enterprise Single Sign-On.
4. Type **ssomanage -enablemapping <Windows account name> <application name>**.

To disable mappings for individual type affiliate applications using the command line

1. On the **Start** menu, click **Run**.
2. In the **Run** dialog box, type **cmd**, and then click **OK**.
3. At the command line, go to the Enterprise Single Sign-On installation directory. The default is <drive>:\Program Files\Common Files\Enterprise Single Sign-On.

4. Type **ssomanage -disablemapping <Windows account name> <application name>**.

To enable mappings for host group type affiliate applications using the command line

1. On the **Start** menu, click **Run**.
2. In the **Run** dialog box, type **cmd**, and then click **OK**.
3. At the command line, go to the Enterprise Single Sign-On installation directory. The default is <drive>:\Program Files\Common Files\Enterprise Single Sign-On.
4. Type **ssomanage -enablemapping <external account name> <application name>**.

To enable mappings for individual type affiliate applications using the command line

1. On the **Start** menu, click **Run**.
2. In the **Run** dialog box, type **cmd**, and then click **OK**.
3. At the command line, go to the Enterprise Single Sign-On installation directory. The default is <drive>:\Program Files\Common Files\Enterprise Single Sign-On.
4. Type **ssomanage -disablemapping <external account name> <application name>**.

How to Use the Trace Utility in Host Initiated SSO

The primary method of troubleshooting is tracing.

Tracing

Use the Trace command line utility to enable tracing in SSO.

To use the trace utility

1. On the **Start** menu, click **Run**.
2. In the **Run** dialog box, type **cmd**, and then click **OK**.
3. At the command line, go to the Enterprise Single Sign-On installation directory. The default is <drive>:\Program Files\Common Files\Enterprise Single Sign-On.
4. Type **Trace –start –high** to set the tracing level to high and begin the trace.
5. Run the scenario with host initiated SSO.
6. Type **Trace –stop** to end the trace. A .bin file is generated in the directory above, which you can send to Microsoft for analysis.

Securing Your Deployment of SSO

This section outlines a typical scenario for secure deployment of Enterprise Single Sign-On. For detailed procedures on the actions to take in SQL Server, see your SQL Server documentation.

In This Section

- Deployment Overview
- Deployment Process

SSO Deployment Overview

The system in this example is deployed over three domains, containing the following computers:

Domain ORCH.com

- ORCH domain controller
- HIS1, the HISSO server
- HIS2, the Master Secret Server
- HIS3, the Admin database

Domain SQL.com

- SQL domain controller
- SQL2, the SSO database

Domain HIS.com

- HIS domain controller
- HIS4 database

The key points defining this deployment are as follows:

- Domain ORCH.com and domain SQL.com have a two-way selective trust relationship.
- Domain ORCH.com is configured as native Windows Server 2003 functional level.
- All SSO services are running on an ORCH.com domain user account (Orch\SSOSvcUser). The user is configured to have access permission on the SQL2 machine in the SQL.com domain. The user is configured for protocol transition and constrain delegation within the ORCH.com domain.

- Another ORCH.com domain user (Orch\TestAppUser) is set for running test programs. This user is also configured for protocol transition and constrain delegation.

Deployment Process

The following steps give a high-level overview of secure deployment of Enterprise Single Sign-On. For detailed procedures on the actions to take in SQL Server, see your SQL Server documentation.

1. On the SQL Server domain controller, use the New Trust Wizard to create a trust with the following properties:
   - **Name:** ORCH.com
   - **Direction:** Two-way
   - **Sides:** This domain only
   - **Outgoing Trust Authentication Level - Local Domain:** Selective authentication
   - **Password:** Choose a password
   - **Confirm Outgoing Trust:** Yes
   - **Confirm Incoming Trust:** No
2. On the ORCH.com domain controller, use the New Trust Wizard to create a trust with the following properties:
   - **Name:** SQL.com
   - **Direction:** Two-way
   - **Sides:** This domain only
   - **Outgoing Trust Authentication Level - Local Domain:** Selective authentication
   - **Password:** Must be the same as password for ORCH.com
   - **Confirm Outgoing Trust:** Yes
   - **Confirm Incoming Trust:** No
3. On the ORCH.com domain controller, set the domain wide trust for Incoming from SQL.COM.
4. On the SQL.com domain controller, set the domain wide trust for Outgoing from ORCH.COM.

5. On the ORCH.com domain controller, raise the domain functional level to Windows Server 2003.

6. In the ORCH domain, create the following new users:

   - ORCH\SSOSvcUser
   - ORCH\TestAppUser
   - ORCH\AffAppUser

7. Add **Act as part of the operating system** to SSOSvcUser and TestAppUser.

8. Add **Allowed to Authenticate** privilege to ORCH\TestAdmin.

9. Add ORCH\SSOSvcUser to SQL2 in the SQL domain. (This step requires using Advanced View in Active Directory MMC.)

10. On the SQL2 computer, create the following two new logins:

    - ORCH\TestAdmin
    - ORCH\SSOSvcUser

11. On the SQL2 domain, create two domain global groups:

    - ORCH\SSOAdminGroup
    - ORCH\SSOAffAdminGroup

12. Add **Allowed to Authenticate** privilege to the ORCH\SSOAdminGroup group.

13. On the SQL2 database, create the following new login:

    - ORCH\SSOAdminGroup

14. Install the Master Secret Server as follows:

    - Log on to NTS5 using ORCH\TestAdmin.
    - Install ESSO, using SQL2 as the Master Secret Server.

15. Log onto HIS1 using ORCH\TestAdmin, and install Enterprise Single Sign-On. Configure ESSO as SSO join HIS2, using database server name SQL2.

16. Install the Enterprise Single Sign-On Admin utility on HIS3 using ORCH\TestAdmin.

17. Add the following users to the following groups:

- Add ORCH\TestAppUser to ORCH\SSOAdminGroup
- Add ORCH\AffAppUser to ORCH\TestAffUserGroup

18. Install SQL Server 2000a Enterprise on HIS3, and add login ORCH\AffAppUser.

19. On the HIS1 computer, open a command prompt and use the following commands to set constrain delegation and protocol transition:

- **setspn -A MSSQLSvc/HIS3.ORCH.com:1433 ORCH\SSOSvcUser**
- **setspn -A MSSQLSvc/HIS3.ORCH.com:1433 ORCH\TestAppUser**

20. On the **ORCH\SSOSvcUser** and **ORCH\TestAppUser** property pages, set the proper delegation for both user accounts by selecting the following options:

- **Trust this user for delegation to specified services only**
- **Use any authentication protocol**

21. Using ORCH\TestAdmin on the HIS1 computer, perform the following:

- Add ORCH\TestAppUser to Remote Desktop User Group
- Grant **Impersonate after authenticated** privilege to ORCH\SSOSvcUser
- Grant **Impersonate after authenticated** privilege to ORCH\TestAppUser

22. Verify your deployment by logging onto HIS1 using ORCH\TestAppUser and running the following application configuration:

Password Synchronization

The purpose of Password Synchronization is to simplify administration of the SSO database, and to keep passwords in sync across user directories.

These two tasks are accomplished through the use of password synchronization adapters, and the topics in this section describe the command line utility for creating and managing those adapters.

There are three types of password synchronization sub-features.

The first type is **Windows to External** (for example, Active Directory to RACF). In this scenario, a Windows user's password change is captured and sent to the Enterprise SSO Server assigned to receive password changes from domain controllers. This then forwards the password change to an external system and the mapping in the SSO database is kept in sync with the change made on the external system.

The second type is **External to Windows - Full synchronization**. In this scenario, a password is captured on the External system and sent to the Enterprise Single Sign-On server assigned for Password Synchronization which then updates the password in the SSO database, and also updates the Windows user's password in Active Directory.

The third type is **External to Windows - Partial synchronization**. In this scenario a password is captured on the External system and sent to the Enterprise Single Sign-On server assigned for Password Synchronization which then updates the password in the SSO database.

In This Section

- How to Install Password Synchronization
- How to Administer Password Synchronization
- How to Configure Password Synchronization
- How to Manage Password Synchronization

How to Install Password Synchronization

As with the other Single Sign-On features, Password Synchronization is not installed in the default BizTalk Server 2006 installation, and must be specifically selected during setup.

To install Password Synchronization

1. On the BizTalk Server CD, browse to the **<CDRoot>\Platforms\SSO** folder.
2. Run **setup.exe** and follow the instructions in the wizard.
3. Select the **Password Synchronization** feature and proceed with the installation.

To addition to this, Password synchronization adapters are necessary to send and receive password changes to the external system. The topics in this section describe how to configure your own adapters. You can also view a list of currently available adapters at the following location:

http://go.microsoft.com/fwlink/?LinkId=30101

You can also contact support aliases to obtain information on these Password synchronization adapters.

Finally, to capture password changes made in Active Directory, in addition to installing the ENTSSO Password Sync feature, components need to be installed on the domain controllers to capture password changes.

Both the Windows Password Capture component and Password Change Notification Service (PCNS) must be installed on all domain controllers from which you will be capturing passwords. You can find these components in the following location:

<HIS CD ROOT>\Platform\PCNS

Read the accompanying documentation (also located in this folder) before you proceed with the installation on the domain controller.

How to Administer Password Synchronization

You can administer Password Synchronization through either the MMC Snap-In or the command line.

The MMC Snap-In displays a list of adapters and their properties. You can right-click an adapter and use the menu to perform the following commands:

- Create adapters
- Set properties
- Update
- Delete
- Enable
- Disable
- Add applications to an adapter
- Delete applications from an adapter
- Reset notification
- Add an adapter to an adapter group
- Delete an adapter from an adapter group

You can also use the SSOPS command line utility to administer your password synchronization. Most of commands in this section are intended for use by an administrator only.

For many commands, the command output is displayed on the screen in two columns. As certain screen settings may cause truncation of data, for best results you should change the screen buffer size/Windows size to 120 characters.

The SSOPS commands are listed in the following table. Procedures and further explanation are located throughout the rest of this topic.

Command	Function
-list	Lists existing adapters
-display	Displays adapter information

-create	Creates new adapter(s)
-setprops	Sets properties for adapter
-update	Updates existing adapter(s)
-delete	Deletes an existing adapter
-enable	Enables adapter
-disable	Disables adapter
-addapp	Adds application for adapter
-deleteapp	Deletes application for adapter
-reset	Resets notification or damping queues
-addtogroup	Adds adapter to adapter group
-deletefromgroup	Deletes adapter from adapter group

To list existing adapters

1. On the **Start** menu, click **Run**.
2. In the **Run** dialog box, type **cmd**, and then click **OK**.
3. At the command line, go to the Enterprise Single Sign-On installation directory. The default is <drive>:\Program Files\Common Files\Enterprise Single Sign-On.
4. Type **ssops -list** and press Enter.

   Adapters and descriptions will be listed. (E) denotes that the adapter is enabled, (D) denotes that it is disabled.

To display adapter information

1. On the **Start** menu, click **Run**.
2. In the **Run** dialog box, type **cmd**, and then click **OK**.
3. At the command line, go to the Enterprise Single Sign-On installation directory. The default is <drive>:\Program Files\Common Files\Enterprise Single Sign-On.
4. Type **ssops -display <adapter name>** and press Enter.

   The screen output will display information for the specified adapter.

In addition to name, type, description, computer, and accounts, the following information is displayed.

Adapter Flag	Details
Adapter enabled	Determines whether or not the adapter is enabled. Flag: SSO_FLAG_ENABLED Attribute Name: enableApp Default: No
Allow local accounts	Determines whether or not the App Admin or App Users accounts can be local accounts. Flag: SSO_FLAG_APP_ALLOW_LOCAL Attribute Name: allowLocalAccounts Default: No
Receive password changes from adapter	Determines whether or not the adapter is allowed to receive external password changes. Flag: SSO_FLAG_PARTIAL_SYNC_FROM_EXTERNAL_TO_DB Attribute Name: syncFromAdapter Default: No
Verify old password	Determines whether the adapter will verify the old password when an external password change is received. If this flag is set then with an external password change the external adapter must supply the old external password as well as the new external password. The old external password is then compared with the existing external password in the SSO database for that external account. If they match, the password change is accepted. If they do not match, the password change is rejected. Flag: SSO_FLAG_SYNC_VERIFY_EXTERNAL_CREDS Attribute Name: verifyOldPassword Default: Yes
Change Windows password	Determines whether or not the Windows password will also be changed when an external password change is received (full sync). ENTSSO always uses the old Windows password stored in the SSO database to change the Windows password to the new value (Windows requires both the old and new password to change a users password), so this must be initialized before the Windows

	password change can succeed. If password sync is configured for a particular mapping, then when the external credentials are set via administrative tools (ssomanage or ssoclient -setcredentials) the Windows password stored in the SSO database will also be set.Flag: SSO_FLAG_FULL_SYNC_FROM_EXTERNAL_TO_WINDOWS Attribute Name: changeWindowsPassword Default: No
Send Windows password changes to adapter	Determines whether or not Windows password changes will be sent to the external adapter. Flag: SSO_FLAG_FULL_SYNC_FROM_WINDOWS_TO_EXTERNAL Attribute Name: syncToAdapter Default: No
Send old password to adapter	If Yes, the old password value (from the SSO database) will also be sent to the external adapter as well as the new password value. Some external systems might require both the old and new password values to change the password. Flag: SSO_FLAG_SYNC_PROVIDE_OLD_EXTERNAL_CREDS Attribute Name: sendOldPassword Default: No
Allow mapping conflicts	Determines whether or not the adapter will allow mapping conflicts. A mapping conflict occurs when mappings are not unique. In a single SSO Individual application, mappings are always one-to-one: one Windows account is mapped to exactly one external account and vice versa. However, it is possible to assign more than one application to an adapter. Thus, it is possible to have a mapping in one application that conflicts with a mapping in the other. This purpose of this flag is to prevent this from occurring. It is more secure to not allow mapping conflicts unless there is a specific, well understood requirement for this behavior. Flag: SSO_FLAG_SYNC_ALLOW_MAPPING_CONFLICTS Attribute Name: allowMappingConflicts Default: No

Adapter Description	Details
Notification retry count	Default is 1.
Notification retry delay (in mins)	Default is 5.
Maximum pending notifications	Default is 8.
Store notifications (when offline)	True/False.
Server name	Server name.
Port number	Port number.
Applications for this adapter	List of applications currently assigned to the adapter.

To create new adapters

1. On the **Start** menu, click **Run**.
2. In the **Run** dialog box, type **cmd**, and then click **OK**.
3. At the command line, go to the Enterprise Single Sign-On installation directory. The default is <drive>:\Program Files\Common Files\Enterprise Single Sign-On.
4. Type **ssops -create <adapter file>** and press Enter.

   The screen output will display information for the newly created adapter.

To set properties for an adapter

1. On the **Start** menu, click **Run**.
2. In the **Run** dialog box, type **cmd**, and then click **OK**.
3. At the command line, go to the Enterprise Single Sign-On installation directory. The default is <drive>:\Program Files\Common Files\Enterprise Single Sign-On.
4. Type **ssops -setprops <adapter name>** and press Enter.

   The screen output will display the properties for the specified adapter. You can edit them if necessary, but new values are not validated.

To update existing adapters

1. On the **Start** menu, click **Run**.
2. In the **Run** dialog box, type **cmd**, and then click **OK**.
3. At the command line, go to the Enterprise Single Sign-On installation directory. The default is <drive>:\Program Files\Common Files\Enterprise Single Sign-On.

4. Type **ssops -update <adapter file>** and press Enter.

   Use this command to update the settings and flags for a specified adapter. Do not use this command to set properties; use instead the -setprops command.

To delete an existing adapter

1. On the **Start** menu, click **Run**.
2. In the **Run** dialog box, type **cmd**, and then click **OK**.
3. At the command line, go to the Enterprise Single Sign-On installation directory. The default is <drive>:\Program Files\Common Files\Enterprise Single Sign-On.
4. Type **ssops -delete <adapter name>** and press Enter.

   The specified adapter will be deleted.

To enable an adapter

1. On the **Start** menu, click **Run**.
2. In the **Run** dialog box, type **cmd**, and then click **OK**.
3. At the command line, go to the Enterprise Single Sign-On installation directory. The default is <drive>:\Program Files\Common Files\Enterprise Single Sign-On.
4. Type **ssops -enable <adapter name>** and press Enter.

   The specified adapter will be enabled.

To disable an adapter

1. On the **Start** menu, click **Run**.
2. In the **Run** dialog box, type **cmd**, and then click **OK**.
3. At the command line, go to the Enterprise Single Sign-On installation directory. The default is <drive>:\Program Files\Common Files\Enterprise Single Sign-On.
4. Type **ssops -disable <adapter name>** and press Enter.

   The specified adapter will be disabled.

To add an application to an adapter

1. On the **Start** menu, click **Run**.
2. In the **Run** dialog box, type **cmd**, and then click **OK**.
3. At the command line, go to the Enterprise Single Sign-On installation directory. The default is <drive>:\Program Files\Common Files\Enterprise Single Sign-On.

4. Type **ssops -addapp <adapter name> <application name>** and press Enter.

   The specified SSO application will be assigned to the specified adapter. This means that the passwords for the mappings in that application will now be synchronized using this adapter.

   While multiple applications can be assigned to one adapter, any given application can only be assigned to one adapter.

To delete an application from an adapter

1. On the **Start** menu, click **Run**.
2. In the **Run** dialog box, type **cmd**, and then click **OK**.
3. At the command line, go to the Enterprise Single Sign-On installation directory. The default is <drive>:\Program Files\Common Files\Enterprise Single Sign-On.
4. Type **ssops -deleteapp <application name>** and press Enter.

   The specified SSO application will be removed from an adapter. (Since an application can only be assigned to one adapter, it is not necessary to specify the adapter name.)

To reset notification

1. On the **Start** menu, click **Run**.
2. In the **Run** dialog box, type **cmd**, and then click **OK**.
3. At the command line, go to the Enterprise Single Sign-On installation directory. The default is <drive>:\Program Files\Common Files\Enterprise Single Sign-On.
4. Type **ssops -reset <adapter name | all | damping>** and press Enter.

   This command clears the damping table and/or notification queues for a single adapter or all adapters, as specified. The damping table stores a 10-minute history of password changes. Before the Enterprise SSO system accepts or sends a password change, it checks the damping table to see if it has performed the same change recently. If it has, the new change is discarded.

To add an adapter to an adapter group

1. On the **Start** menu, click **Run**.
2. In the **Run** dialog box, type **cmd**, and then click **OK**.
3. At the command line, go to the Enterprise Single Sign-On installation directory. The default is <drive>:\Program Files\Common Files\Enterprise Single Sign-On.
4. Type **ssops -addtogroup <adapter name> <adapter group>** and press Enter.

This command adds the specified adapter to the specified adapter group. While an adapter can belong to only one adapter group, an adapter group can contain multiple adapters.

To delete an adapter from an adapter group

1. On the **Start** menu, click **Run**.
2. In the **Run** dialog box, type **cmd**, and then click **OK**.
3. At the command line, go to the Enterprise Single Sign-On installation directory. The default is <drive>:\Program Files\Common Files\Enterprise Single Sign-On.
4. Type **ssops -deletefromgroup <adapter name> <adapter group>** and press Enter.

   This command deletes the specified adapter from the specified adapter group.

How to Configure Password Synchronization

Use the SSOCONFIG command line utility to configure your password synchronization settings.

To specify the directory for replay files

1. On the **Start** menu, click **Run**.
2. In the **Run** dialog box, type **cmd**, and then click **OK**.
3. At the command line, go to the Enterprise Single Sign-On installation directory. The default is <drive>:\Program Files\Common Files\Enterprise Single Sign-On.
4. Type **ssoconfig -replayfiles <replay files directory> | -default** and press Enter.

To display or change maximum password synchronization age

1. On the **Start** menu, click **Run**.
2. In the **Run** dialog box, type **cmd**, and then click **OK**.
3. At the command line, go to the Enterprise Single Sign-On installation directory. The default is <drive>:\Program Files\Common Files\Enterprise Single Sign-On.
4. Type **ssoconfig -syncage <maximum password age in hours>** and press Enter.

How to Manage Password Synchronization

Use the MMC Snap-in or the SSOMANAGE command line utility to enable or disable SSO features, and to display current SSO database settings.

To manage features or display settings using the MMC Snap-In

1. Right-click the appropriate feature or database.
2. Click the appropriate menu item.

To enable SSO features using the command line

1. On the **Start** menu, click **Run**.
2. In the **Run** dialog box, type **cmd**, and then click **OK**.
3. At the command line, go to the Enterprise Single Sign-On installation directory. The default is <drive>:\Program Files\Common Files\Enterprise Single Sign-On.
4. Type **ssomanage -enable** and press Enter.

To disable SSO features using the command line

1. On the **Start** menu, click **Run**.
2. In the **Run** dialog box, type **cmd**, and then click **OK**.
3. At the command line, go to the Enterprise Single Sign-On installation directory. The default is <drive>:\Program Files\Common Files\Enterprise Single Sign-On.
4. Type **ssomanage -disable** and press Enter.

To display current database settings using the command line

1. On the **Start** menu, click **Run**.
2. In the **Run** dialog box, type **cmd**, and then click **OK**.
3. At the command line, go to the Enterprise Single Sign-On installation directory. The default is <drive>:\Program Files\Common Files\Enterprise Single Sign-On.
4. Type **ssomanage -displaydb** and press Enter.

SSO Security Recommendations

With the Enterprise Single Sign-On (SSO) system, users can connect to different systems by using only one set of credentials. BizTalk Server leverages the SSO system as a store for sensitive information. Although BizTalk automatically installs whenever you install the BizTalk Server runtime, you can also install Enterprise Single Sign-On as a stand-alone component, independent of your BizTalk Server environment. For more information about

Enterprise Single Sign-On, see Using SSO . It is recommended you follow these guidelines for securing and deploying the Enterprise Single Sign-On (SSO) services and resources in your environment.

General deployment recommendations for SSO

- There must be only one master secret server and only one SSO database in the entire environment, even if you have multiple BizTalk groups in your environment. You must configure these two servers before you configure any other BizTalk and SSO servers.

- You must have a time server in your environment to ensure all SSO servers are synchronized. If the clocks on the SSO servers are not synchronized, this could compromise the security of your environment.

- Considering there is only one master secret server in your entire environment, it is recommended to use an active-passive cluster configuration for the master secret server. For more information about clustering the master secret server, see How to Cluster the Master Secret Server .

- The master secret server holds the encryption key the SSO systems uses to encrypt the information in the SSO database. It is recommended that you do not install or configure any other products or services on this computer.

- The master secret server should have access to a removable media or NTFS file system folder in order to back up and restore the master secret. If you use removable media, ensure you take appropriate measures to protect the removable media. If you back up the master secret to an NTFS file system, ensure you protect the file and the folder. Only the SSO Administrator should have access to this file.

- You should back up the master secret as soon as the master secret server generates it. This is so that you may recover the data in the SSO database in the event the master secret server fails. For more information about backing up the master secret, see Managing the Master Secret .

- Back up your current secret, or generate a new secret on a regular basis, for example, once a month. Without the secret, you cannot retrieve information from the SSO database. For more information about backing up and restoring the master secret, see Managing the Master Secret .

Security Recommendations for SSO Groups and Accounts

- It is recommended to use Windows groups, and not single user accounts, especially for the SSO Administrator and SSO Affiliate administrator groups. These groups must have at least two user accounts as members of the group at all times.

- The SSO runtime service accounts and the SSO administrator user accounts should be different accounts, even when they are members of the same SSO Administrators group. The SSO administrator users performing administrative tasks such as generating and backing up the secret need to be Windows administrators, while the SSO runtime service accounts do not need to be Windows administrators.

- If you use the SSO ticketing feature, you must use domain accounts that the computers in the processing domain (domain where the SSO servers are) recognize.

- It is recommended to use a unique service account for the SSO service corresponding to the master secret server.

- The SSO administrator account is a highly privileged account in the SSO system, which also is the SQL Server administrator account for the SQL server that has the SSO database. You should have dedicated accounts for SSO administrators, and should not use these accounts for any other purposes. You should limit the membership to the SSO administrators group only to those accounts responsible for running and maintaining the SSO system.

- You must manually add the BizTalk administrators group to the SSO Affiliate Administrators group so that the BizTalk administrators can leverage the SSO system to save the configuration information for the adapters in the SSO database. Only the BizTalk administrators managing adapters need to be members of the SSO Affiliate Administrators group. BizTalk administrators do not need to be SSO administrators.

Security Recommendations for an SSO Deployment

- If your network supports Kerberos authentication, you should register all SSO servers. When you use Kerberos authentication between the master secret server and the SSO database, you must configure Service Principal Names (SPN) on the SQL server where the SSO database is located. For more information about configuring Service Principal Names, see Microsoft Download Web site at http://go.microsoft.com/fwlink/?LinkId=20797.

- When running Windows Server 2003, if the master secret server is on a different domain from the other SSO servers and from the SSO database, you must disable RPC security (as used for Data Transaction Coordinator (DTC) authentication between computers) on the master secret server, on the SSO servers (processing computers in the processing domain), and on the SSO database. RPC security is a new DTC feature in Windows Server 2003. When you disable RPC security, the DTC authentication security level for RPC calls goes back to one available in Microsoft Windows 2000 Server. For more information about disabling RPC security, see the Microsoft Help and Support Web site at http://go.microsoft.com/fwlink/?LinkId=24774.

- SSO administrators should regularly monitor the event log in the master secret server and the SSO server for SSO auditing events.

- In addition to firewalls, it is recommended to use Internet Protocol security (IPSec) or Secure Sockets Layer (SSL) between all the SSO servers and the SSO database. For more information about SSL, see Microsoft Help and Support Web site at http://go.microsoft.com/fwlink/?LinkId=16731. For more information about using SSL between all the SSO servers and the SSO database, see How to Enable SSL for SSO .

Perimeter network

When running Internet Information Services (IIS) and Enterprise Single Sign-On, follow these recommendations:

- If IIS is in a perimeter network (also known as demilitarized zone, DMZ, and screened subnet), provide another IIS server behind the firewall to connect to the SSO system.

- Do not open the remote procedure calls (RPC) port on IIS.

SQL Server access

All SSO servers access the SQL Server SSO database. For more information about how to secure SQL Server databases, see http://go.microsoft.com/fwlink/?LinkId=33174 and http://go.microsoft.com/fwlink/?LinkId=33175.

It is recommended that you use Secure Sockets Layer (SSL) and/or Internet Protocol security (IPSec) to secure the transmission of data between the SSO servers and the SSO database. For more information about using SSL, see http://go.microsoft.com/fwlink/?LinkId=33176.

To enable SSL for only the connection between the SSO server and the SSO database, you can set SSL support on every SSO server using the ssoconfig utility. This option enables SSO to always use SSL when accessing the SSO database. For more information, see How to Enable SSL for SSO .

Strong passwords

It is very important that you use strong passwords for all accounts, especially the accounts that are members of the SSO Administrators group, because these users have control over the entire SSO system.

SSO administrator accounts

It is recommended that you use different service accounts for the SSO services running on different computers. You should not use the SSO administrator account that performs administration operations such as generating and backing up the secret for the SSO service. While the SSO service accounts should not be local administrators on that computer, the SSO administrator that is performing administration operations must be a local administrator on the computer for some operations.

Master secret server

It is highly recommended that you secure and lock down the master secret server. You should not use this server as a processing server. The only purpose of this server should be to hold the master secret. You should ensure the physical security of this computer and only SSO Administrators should have access to this computer.

Kerberos

SSO supports Kerberos, and it is recommended that you set up Kerberos for SSO. To set up Kerberos with SSO, you must register a Secure Principal Name (SPN) for the SSO service. By default, when you setup Kerberos, SSO uses that SPN to authenticate the components using the SSO Service. It is recommended you setup Kerberos authentication between the

SSO administrative sub services and the SSO server. You can also user Kerberos authentication between the SSO servers and between the SSO servers and the SQL Server where the SSO database is.

To set up and verify Kerberos, you use the utilities setspn and kerbtray. For more information about these utilities, see http://go.microsoft.com/fwlink/?LinkId=33178 and http://go.microsoft.com/fwlink/?LinkId=33179.

Delegation

When using Windows Server 2003, it is possible to use constrained delegation, but it is recommended that you do not use delegation to perform the tasks of the Single Sign-On Administrator. Similarly, it is recommended that you do not delegate additional tasks or user rights to the Single Sign-On administrator.

Auditing

Auditing is a critical mechanism for tracking information in your environment. Enterprise Single Sign-On (SSO) audits all operations performed in the SSO database. SSO uses event logs and audit logs of the database itself. SSO provides two audit levels for the Single Sign-On servers:

- Positive auditing levels audit successful operations
- Negative auditing levels audit operations that fail.

SSO administrators can set the positive and negative audit levels that suit their corporate policies.

You can set positive and negative audits to one of the following levels:

0 = None. This level issues no audit messages.

1 = Low

2 = Medium

3 = High. This level issues as many audit messages as possible.

The default value for positive auditing is 0 (none), and the default value for negative auditing is 1(low). You may want to change these values depending on the level of auditing you want for your SSO system.

Database-level auditing

For database-level auditing, the SSO system tracks the operations performed on the SSO database in the audit tables in the database. The size of these audit tables are defined at the SSO system level. You can audit for affiliate applications that are deleted, for mappings that are deleted, and for credential look-ups that are performed. By default, the audit size is

set to 1,000 entries. SSO administrators can change this size to meet their corporate policies.

Using SSO accounts

This section contains best practices when using domain and local groups and individual accounts in the Enterprise Single Sign-On (SSO) system.

Domain Windows groups and accounts

When working with domain Windows groups, the following recommendations apply:

- Use domain groups and domain accounts.
- Use a domain group for SSO administrators. You should not specify an individual domain account as the SSO administrator, because you cannot change this account from one individual account to another individual account.
- Although you can specify an individual domain account as the SSO affiliate administrator, you should use a domain group.
- Although you can specify an individual domain account as the application administrator, you should use a domain group.
- You must use domain groups for the application users account. The SSO applications users account does not support an individual account.
- Multiple accounts can be specified for each of these SSO access accounts.

Maintaining BizTalk Server

This section provides information about how to back up and restore the Microsoft BizTalk Server databases and how to archive and purge data from the BizTalk Tracking (BizTalkDTADb) database. It provides an overview of the backup and restoration process, as well as recommendations for maintaining the BizTalk Tracking database.

In This Section

- Backing Up and Restoring BizTalk Server
- Archiving and Purging the BizTalk Tracking Database

Backing Up and Restoring BizTalk Server

This section provides information about how to back up and restore the BizTalk Server databases. You should follow the procedures in this section to ensure your ability to restore a consistent BizTalk Server environment in the event of a hardware failure. BizTalk Server performs distributed transactions across databases, so it is critical that you back up and then restore all databases.

BizTalk Server requires a customized backup process that uses full database backups and transaction log backups in conjunction with log marking and distributed transactions. For information about this process, see Marked Transactions, Full Backups, and Log Backups.

In This Section

- Checklist: Back Up and Restore BizTalk Server
- Best Practices for Backup and Restore
- Backing Up and Restoring BizTalk Server Databases
- Backing Up and Restoring BAS
- Backing Up and Restoring BAM
- Backing Up and Restoring the Base EDI Adapter
- Resolving Data Loss
- Advanced Information About Backup and Restore

Checklist: Back Up and Restore BizTalk Server

Before attempting to back up or restore BizTalk Server, be sure to familiarize yourself with the processes involved.

Backing Up BizTalk Server

Step	Reference
Learn how to back up and restore BizTalk Server.	Best Practices for Backup and Restore Backing Up and Restoring BizTalk Server Databases
Ensure that you have appropriate permissions to back up and restore BizTalk Server.	User Accounts for Database Backups
Configure the Backup BizTalk Server job.	How to Configure the Backup BizTalk Server Job
Configure the server where backups will be stored.	How to Configure the Destination System for Log Shipping
If you are using Business Activity Services (BAS), back up the BAS site and database.	Backing Up and Restoring BAS
If you are using Business Activity Monitoring (BAM), back up the BAM databases.	Backing Up and Restoring BAM
If you are using the Base EDI adapter, back up the	Backing Up and Restoring the Base

Base EDI adapter.	EDI Adapter
If you are using Enterprise Single Sign-on, back up the master secret.	Managing the Master Secret

Restoring BizTalk Server

Step	Reference
Restore your databases.	**How to Restore the BizTalk Server Databases**
Restore the BAS site and database.	How to Restore Your BAS Site and Database
Update references to the BAM database names.	How to Update References to the BAM Analysis Server Database Name How to Update References to the BAM Archive Database Name How to Update References to the BAM Primary Import Database Name and Connection String How to Update References to the BAM Star Schema Database Name How to Update References to the TPM Database Name and Connection String How to Resolve Incomplete Activity Instances
Restore the Base EDI adapter Documentshome directory.	How to Restore the Documentshome Directory

Best Practices for Backup and Restore

Review the following best practices to help ensure that you can backup and restore your BizTalk Server databases.

- **Develop backup and restore strategies and test them.**

  With a good plan, you can quickly recover your data if it is lost due to hardware failure.

- **Train appropriate personnel.**

  In minimum-security and medium-security networks, assign backup rights to one user and restore rights to a different user. Train personnel with restore rights to perform all of the restore tasks if the administrator is unavailable.

  In a high-security network, make sure that only administrators can restore files.

- **Manage disk space and archive previous backup files.**

  The Backup BizTalk Server job does not delete outdated backup files, so you need to manage those backup files to conserve disk space. After you have created a new full backup of your databases, you should move the outdated backup files onto an archival storage device to reclaim space on the primary disk.

- **Do not store backups on the same computer that you are backing up.**

  You should specify a computer for your backup that is different from the computer with the original data.

- **Retain copies.**

  Keep at least three copies of the media. Keep at least one copy off-site in a properly controlled environment.

- **Perform trial restorations.**

  Perform a trial restoration at least once a month to verify that your files were properly backed up. A trial restoration can uncover hardware problems that do not show up when you verify that your software is functioning properly. Do not wait until your hard disk fails to see if you can restore your system and databases.

- **Secure devices and media.**

  Secure both the storage device and the backup media. It is possible for someone to access the data from a stolen medium by restoring the data to another server for which they are an administrator.

Backing Up and Restoring BizTalk Server Databases

You use the Backup BizTalk Server job to back up all of the databases in your BizTalk Server source system, except for those databases used by Business Activity Services (BAS) and Business Activity Monitoring (BAM). The source system is the server or group of servers that contain live data. Because the BAS and BAM databases have different backup and restore requirements, these databases are backed up and restored using other methods.

Backing up the BizTalk Server databases and restoring them involves the following steps:

1. **Configuring the Backup BizTalk Server job**

   Before you can back up the BizTalk Server databases, you must first configure the Backup BizTalk Server job on the source system, which directs backups to be automatically written to a folder where they can then be used to restore the databases on the destination system. The destination system is the server or group of servers that will be used to restore the database backups produced by the source system. For more information about this step, see How to Configure the Backup BizTalk Server Job.

2. **Configuring the destination system for log shipping**

You must also configure the destination system for log shipping, which provides standby server capabilities and reduces downtime in the event of a system failure. For more information about this step, see How to Configure the Destination System for Log Shipping.

3. **Restoring the databases**

When a hardware failure occurs, you can restore your databases by using the backups and logs sent to your destination system. For more information about this step, see How to Restore Your Databases.

BizTalk Server Databases

The following tables describe the databases used by BizTalk Server and identify which methods are used to back up the databases.

Databases Backed Up by the Backup BizTalk Server Job

The following table lists the databases that are backed up and restored as a part of the Backup BizTalk Server job. You can modify the Backup BizTalk Server job to back up custom databases by adding them to the adm_OtherBackupDatabases table. For more information, see How to Back Up Custom Databases.

Database	Default database name	Description
BAM Primary Import database	BAMPrimaryImport	This is the database where the Business Activity Monitoring (BAM) collects raw tracking data.
BAM Notification Services Application database	BAMAlertsApplication	This database contains alert information for BAM notifications. For example, when you create an alert using the BAM portal, entries are inserted in the database specifying the conditions and events to which the alert pertains, as well as other supporting data items for the alert.
BAM Notification Services Instance database	BAMAlertsNSMain	This database contains instance information specifying how the notification services connect to the system that BAM is monitoring.
HWS Administration database	BizTalkHwsDb	This database contains all administration information related to Human Workflow Services (HWS).
BizTalk Tracking database	BizTalkDTADb	This database stores business and health monitoring data tracked by the BizTalk Server tracking engine.
BizTalk Management database	BizTalkMgmtDb	This database is the central meta-information store for all instances of BizTalk Server.

BizTalk MessageBox database	BizTalkMsgBoxDb	This database is used by the BizTalk Server engine for routing, queuing, instance management, and a variety of other tasks.
Rule Engine database	BizTalkRuleEngineDb	This database is a repository for: • Policies, which are sets of related rules. • Vocabularies, which are collections of user-friendly, domain-specific names for data references in rules.
SSO database	SSODB	This Enterprise Single Sign-On credential database securely stores the configuration information for receive locations.
TPM database	TPM	This database stores trading partner data for Business Activity Services (BAS).
BizTalk Base EDI database	BizTalkEDIdb	This database stores state for the electronic data interchange (EDI) adapter.

Databases Backed Up by the BAS Backup Process

The following table lists the Microsoft Windows SharePoint Services databases that are backed up and restored using the procedures in Backing Up and Restoring BAS:

Database	Default database name	Description
Windows SharePoint Services configuration database	*User-defined*	This database contains all of the global settings for the server.
Windows SharePoint Services content database	*User-defined*	This database contains all of the site content, such as list items and documents.

Databases Backed Up by the BAM Backup Process

The following table lists the databases that are backed up and restored using the procedures in Backing Up and Restoring BAM:

Database	Default database name	Description
BAM Star Schema	BAMStarSchema	This database contains the staging table, and the measure and dimension tables.
BAM Analysis	BAMAnalysis	This database contains BAM OLAP cubes for both online and offline analysis.

BAM Archive	BAMArchive	This database archives old business activity data. Create a BAM Archive database to minimize the accumulation of business activity data in the BAM Primary Import database.
Tracking Analysis Server	BizTalkAnalysisDb	This database stores both business and health monitoring online analytical processing (OLAP) cubes.

How to Configure the Backup BizTalk Server Job

Before you can back up BizTalk Server 2006, you must configure the Backup BizTalk Server job by using SQL Server Enterprise Manager.

Prerequisites

To back up your BizTalk Server 2006 databases, you must be logged on with a user account that has access to each of the databases you are backing up.

BizTalk Server includes a SQL Server role named BTS_BACKUP_USERS so that the user account you use to back up your databases does not require System Administrator permissions within SQL Server, except for the primary server controlling the backup process.

When setting up the user account that you are using to back up your databases, note the following:

- You must configure the SQL Server Agent service to run under a domain account or a local account with a mapped user on each instance of SQL Server.
- You must configure a SQL Server logon account for this user, and assign this user to the BizTalk BTS_BACKUP_USERS role on each server.
- You must assign this user to the System Administrators role within SQL Server for the server that contains the BizTalk Management database.

To configure the Backup BizTalk Server job (SQL Server 2000)

1. On the computer that contains the BizTalk Management database, click **Start**, click **Programs**, click **Microsoft SQL Server**, and then click **Enterprise Manager**.
2. Open the appropriate server by clicking it, double-click **Management**, double-click **SQL Server Agent**, and then click **Jobs**.
3. In the details pane, right-click **Backup BizTalk Server**, and then click **Properties**.
4. In the **Backup BizTalk Server Properties** dialog box, click the **Steps** tab, click **BackupFull**, and then click **Edit**.

5. On the **General** tab, in the **Command** box, replace '<*destination path*>' with the full path (the path must include the single quotes) to the computer and folder where you want to back up the BizTalk Server databases, and then click **OK**.

6. On the **Steps** tab, click **MarkAndBackupLog**, and then click **Edit**.

7. On the **General** tab, in the **Command** box, replace **'**<*destination path*>**'** with the full path (including single quotes) to the computer and folder where you want to store the BizTalk Server database logs and then click **OK**. The <*destination path*> may be local or a UNC path to another server.

8. On the **Steps** tab, click **Clear Backup History**, and then click **Edit**.

9. On the **General** tab, in the **Command** box, change **DaysToKeep=**<*number*> to the number of days you want to keep the backup history, and then click **OK** twice to close the **Backup BizTalk Server Properties** dialog box.

10. Change the backup schedule, if desired. For more information, see How to Schedule the Backup BizTalk Server Job.

11. In the details pane, right-click the **Backup BizTalk Server** job, and then click **Enable Job**.

    In the **Enabled** column, the status changes to **Yes**.

To configure the Backup BizTalk Server job (SQL Server 2005)

1. On the computer that contains the BizTalk Management database, click **Start**, click **Programs**, click **Microsoft SQL Server 2005**, and then click **SQL Server Management Studio**.

2. In the **Connect to Server** dialog box, specify the name of the SQL Server where the BizTalk Server databases reside and the appropriate authentication type, and then click **Connect**.

3. In **Microsoft SQL Server Management Studio**, double-click **SQL Server Agent**, and then click **Jobs**.

4. In the details pane, right-click **Backup BizTalk Server (BizTalkMgmtDb)**, and then click **Properties**.

5. In the **Job Properties - Backup BizTalk Server (BizTalkMgmtDb)** dialog box, under **Select a page**, click **Steps**.

6. In the **Job step list**, click **BackupFull**, and then click **Edit**.

7. On the **General** page, in the **Command** box, replace '<*destination path*>' with the full path (the path must include the single quotes) to the computer and folder where you want to back up the BizTalk Server databases, and then click **OK**.

8. In the **Job step list**, click **MarkAndBackupLog**, and then click **Edit**.

9. On the **General** page, in the **Command** box, replace **'**<*destination path*>**'** with the full path (including single quotes) to the computer and folder where you want to store the BizTalk Server database logs and then click **OK**. The <*destination path*> may be local or a UNC path to another server.

10. In the **Job step list**, click **Clear Backup History**, and then click **Edit**.

11. On the **General** page, in the **Command** box, change **DaysToKeep=**<*number*> to the number of days you want to keep the backup history, and then click **OK** twice to close the **Job Properties - Backup BizTalk Server (BizTalkMgmtDb)** dialog box.

12. Change the backup schedule, if desired. For more information, see How to Schedule the Backup BizTalk Server Job.

13. In the details pane, right-click the **Backup BizTalk Server** job, and then click **Enable**.

    In the **Enable Jobs** dialog box, the status changes to **Success**.

How to Configure the Destination System for Log Shipping

Log shipping provides standby server capabilities, which reduces downtime in the event of a system failure. Log shipping works in both single server and distributed server environments. The server or group of servers that contain live data is known as the source system. The server or group of servers that are used to restore the database backups produced by the source system are known as the destination system.

You can use the following instructions to create a destination system that consists of one server for a single source system. If the destination system contains multiple servers, repeat the steps on each destination server.

Prerequisites

You must be logged on as a member of the BizTalk Server Administrators group to perform this procedure.

To configure the destination system for log shipping (SQL Server 2000)

1. On the computer or computers that you have identified as the destination system, click **Start**, click **Run**, type **isqlw.exe**, and then click **OK**.

2. Click **File**, click **Open**, and then browse to the following SQL script:

3. Click **Query**, and then click **Execute**.

4. Click **File**, click **Open**, and then browse to the following SQL script:

5. Click **Query**, and then click **Execute**.

6. On the computer or computers you have identified as the destination system, open **SQL Query Analyzer**. Click **Start**, click **Run**, type **isqlw.exe**, and then click **OK**.

7. Press **Ctrl + N** to open a new query window.

8. In the query window paste the following command:

9. In the command, replace <*MyLogShippingSolution*> with a meaningful description, surrounded by single quotes. Replace <*BizTalkServerManagementDatabaseName*> and <*BizTalkServerManagementDatabaseServer*> with the name and location of your source BizTalk Management database, surrounded by single quotes.

10. Click **Query**, and then click **Execute**.

11. On the destination system, open SQL Server Enterprise Manager. Click **Start**, click **Run**, type **"SQL Server Enterprise Manager.msc"** and then click **OK**.

12. Open the appropriate server by clicking it, click **Management**, click **SQL Server Agent**, and then click **Jobs**.

13. In the details pane, you will see three new jobs:

- **BizTalk Server Log Shipping Get Backup History**

  The BizTalk Server Log Shipping Get Backup History job moves backup history records from the source to the destination. It is scheduled by default to run every minute. This job runs as frequently as possible in order to move history records from the source to the destination. In the event of a system failure to the source system, the server that you identified as the destination system will continue to process the history records that have already been imported.

- **BizTalk Server Log Shipping Restore Databases**

  The BizTalk Server Log Shipping Restore Databases job restores backup files for the given databases for the source to the destination server. It is scheduled by default to run every minute. This job runs continuously without completing as long as there are backup files to restore.

- **BizTalk Server Log Shipping Restore To Mark**

  The BizTalk Server Log Shipping Restore To Mark job restores all of the databases to a mark in the last log backup. This ensures that all of the databases are in a transactionally consistent state. In addition, this job re-creates all of the SQL Server Agent jobs on the destination system that had been on the source system.

14. On a computer running BizTalk Server 2006, browse to the following folder: **%SystemRoot%\Program Files\Microsoft BizTalk Server 2006\Schema\Restore**.

15. Right-click **SampleUpdateInfo.xml**, and then click **Edit**.

16. Replace all instances of **"SourceServer"** with the name of the source system, and then replace all instances of **"DestinationServer"** with the name of the destination system.

17. If you are using BAM, HWS, SSO, the Rules Engine, EDI, uncomment these lines as appropriate.

18. If you have any custom databases, add them as appropriate under the **<OtherDatabases>** section. For more information, see How to Back Up Custom Databases.

19. When you are finished editing the file, save it and exit.

To configure the destination system for log shipping (SQL Server 2005)

1. On the computer or computers that you have identified as the destination system, click **Start**, click **Programs**, click **Microsoft SQL Server 2005**, and then click **SQL Server Management Studio**.

2. In the **Connect to Server** dialog box, specify the name of the SQL Server on the destination computer, and then click **Connect** to connect to the appropriate SQL Server.

3. In **Microsoft SQL Server Management Studio**, click **File**, click **Open**, and then click **File**.

4. In the **Open File** dialog box, browse to the following SQL script:

5. Click the **Query** menu, and then click **Execute**.

6. In **Microsoft SQL Server Management Studio**, click **File**, click **Open**, and then click **File**.

7. In the **Open File** dialog box, browse to the following SQL script:

8. Click the **Query** menu, and then click **Execute**.

9. On the computer or computers you have identified as the destination system, click **Start**, click **Programs**, click **Microsoft SQL Server 2005**, and then click **SQL Server Management Studio**.

10. In the **Connect to Server** dialog box, specify the name of the SQL Server on the destination computer, and then click **Connect** to connect to the appropriate SQL Server.

11. In **Microsoft SQL Server Management Studio**, click **New Query**.

12. In the query window paste the following command:

13. In the command, replace <*MyLogShippingSolution*> with a meaningful description, surrounded by single quotes. Replace <*BizTalkServerManagementDatabaseName*> and <*BizTalkServerManagementDatabaseServer*> with the name and location of your source BizTalk Management database, surrounded by single quotes.

14. Click the **Query** menu, and then click **Execute**.

15. On the destination system, in **SQL Server Management Studio**, double-click the appropriate server, double-click **SQL Server Agent**, and then double-click **Jobs**.

16. In the details pane, you will see three new jobs:

- **BizTalk Server Log Shipping Get Backup History**

  The BizTalk Server Log Shipping Get Backup History job moves backup history records from the source to the destination. It is scheduled by default to run every minute. This job runs as frequently as possible in order to move history records from the source to the destination. In the event of a system failure to the source system, the server that you identified as the destination system will continue to process the history records that have already been imported.

- **BizTalk Server Log Shipping Restore Databases**

  The BizTalk Server Log Shipping Restore Databases job restores backup files for the given databases for the source to the destination server. It is scheduled by default to run every minute. This job runs continuously without completing as long as there are backup files to restore.

- **BizTalk Server Log Shipping Restore To Mark**

  The BizTalk Server Log Shipping Restore To Mark job restores all of the databases to a mark in the last log backup. This ensures that all of the databases are in a transactionally consistent state. In addition, this job re-creates all of the SQL Server Agent jobs on the destination system that had been on the source system.

17. On a computer running BizTalk Server 2006, browse to the following folder: **%SystemRoot%\Program Files\Microsoft BizTalk Server 2006\Schema\Restore**.

18. Right-click **SampleUpdateInfo.xml**, and then click **Edit**.

19. Replace all instances of **"SourceServer"** with the name of the source system, and then replace all instances of **"DestinationServer"** with the name of the destination system.

20. If you are using BAM, HWS, SSO, the Rules Engine, EDI, uncomment these lines as appropriate.

21. If you have any custom databases, add them as appropriate under the **<OtherDatabases>** section. For more information, see How to Back Up Custom Databases.

22. When you are finished editing the file, save it and exit.

How to Restore Your Databases

You must restore all databases to the same mark to ensure a consistent transactional state among the databases.

If there is only one server in the destination system, make sure that all of the log backup sets (except for the most recent set) have been restored. For more information, see Viewing the History of Restored Backups. If all the log backup sets have not been restored, and the restore job is not currently running, run the restore job (manually if necessary). If there are outstanding backup sets that can be restored, the job will process them until they are all restored.

If there are multiple servers in the destination system, all servers must be restored to the same backup set. You must view the restore history on each server and make sure that the most recent log backup set restored is the same on all servers. If it is not, you must manually run the restore job on each server that needs the most recent log backup set restored. After all of the servers are on the same backup set, the final set can be manually restored.

The adm_BackupHistory table is the central history point for the log shipping process for the source system. All backup work performed is recorded to this table. All servers in your destination system read from this table to receive the information needed to perform their restore work.

Prerequisites

You must be logged on as a member of the BizTalk Server Administrators group to perform this procedure.

To restore your databases (SQL Server 2000)

1. On the computer or computers you have identified as the destination system, click **Start**, click **Programs**, click **Microsoft SQL Server**, and then click **Enterprise Manager**.

2. Open the appropriate server by clicking it. Double-click **Management**, double-click **SQL Server Agent**, and then click **Jobs**.

3. In the details pane, right-click **BTS Log Shipping - Get Backup History**, and then click **Disable Job**.

4. In the details pane, right-click **BTS Log Shipping - Restore Databases**, and then click **Disable Job**.

5. In the details pane, right-click **BTS Log Shipping - Restore To Mark**, and then click **Start Job**.

   SQL Server Agent jobs and BizTalk Server databases are restored to the destination system.

6. On the computer running BizTalk Server 2006, where you edited the SampleUpdateInfo.xml file, open a command prompt. Click **Start**, click **Run**, type **cmd** and then click **OK**.

7. Navigate to the following directory:
%SystemRoot%\Program Files\Microsoft BizTalk Server 2006\Schema\Restore.

8. At the command prompt, type:

cscript UpdateDatabase.vbs SampleUpdateInfo.xml

9. Copy the edited SampleUpdateInfo.xml file to the **%SystemRoot%\Program Files\Microsoft BizTalk Server 2006\Schema\Restore** directory on every computer running BizTalk Server 2006 that is part of the BizTalk Server group.

10. On each computer in the BizTalk Server group, open a command prompt. Click **Start**, click **Run**, type **cmd** and then click **OK**.

11. Navigate to the following directory:
%SystemRoot%\Program Files\Microsoft BizTalk Server 2006\Schema\Restore.

12. At the command prompt, type:

cscript UpdateRegistry.vbs SampleUpdateInfo.xml

13. Restart all of the BizTalk Server services. For more information about how to restart the BizTalk Server services.

14. On the computer you use to administer BizTalk Server, open the BizTalk Server 2006 Administration Console. Click **Start**, click **Run**, type **btsmmc.msc**, and then click **OK**.

15. In the console tree, right-click **BizTalk Server 2006 Administration**, and then click **Connect to Existing Group**.

16. In the **Connect to Existing BizTalk Server Configuration Database** dialog box, in the **SQL Server name** drop-down list box, select the name of the Microsoft SQL Server instance that hosts the BizTalk Management database. When you select the instance of SQL Server, BizTalk Server automatically attempts to detect BizTalk Server databases on that computer.

17. In the **Database name** drop-down list box, select the BizTalk Management database (**BizTalkMgmtDb**) to which you want to connect, and then click **OK**.

    The BizTalk Server Administration Console adds the BizTalk group to the console tree.

Your BizTalk server is now restored and should be running. You should now configure the Backup BizTalk Server job to start writing backups to a new destination server. You should also reconfigure a new destination system.

To restore your databases (SQL Server 2005)

1. On the computer or computers that you have identified as the destination system, click **Start**, click **Programs**, click **Microsoft SQL Server 2005**, and then click **SQL Server Management Studio**.

2. In the **Connect to Server** dialog box, specify the name of the SQL Server on the destination system, and then click **Connect** to connect to the appropriate SQL Server.

3. In **Microsoft SQL Server Management Studio**, double-click the appropriate server, double-click **SQL Server Agent**, and then double-click **Jobs**.

4. In the details pane, right-click **BTS Log Shipping - Get Backup History**, and then click **Disable**.

   In the **Disable Jobs** dialog box, the status changes to **Success**.

5. In the details pane, right-click **BTS Log Shipping - Restore Databases**, and then click **Disable**.

   In the **Disable Jobs** dialog box, the status changes to **Success**.

6. In the details pane, right-click **BTS Log Shipping - Restore To Mark**, and then click **Start Job**.

   SQL Server Agent jobs and BizTalk Server databases are restored to the destination system.

7. On the computer running BizTalk Server 2006, where you edited the SampleUpdateInfo.xml file, open a command prompt. Click **Start**, click **Run**, type **cmd** and then click **OK**.

8. Navigate to the following directory:
   %SystemRoot%\Program Files\Microsoft BizTalk Server 2006\Schema\Restore.

9. At the command prompt, type:

   cscript UpdateDatabase.vbs SampleUpdateInfo.xml

10. Copy the edited SampleUpdateInfo.xml file to the **%SystemRoot%\Program Files\Microsoft BizTalk Server 2006\Schema\Restore** directory on every computer running BizTalk Server 2006 that is part of the BizTalk Server group.

11. On each computer in the BizTalk Server group, open a command prompt. Click **Start**, click **Run**, type **cmd** and then click **OK**.

12. Navigate to the following directory:
    %SystemRoot%\Program Files\Microsoft BizTalk Server 2006\Schema\Restore.

13. At the command prompt, type:

    cscript UpdateRegistry.vbs SampleUpdateInfo.xml

14. Restart all of the BizTalk Server services. For more information about how to restart the BizTalk Server services, see How to Start, Stop, Pause, Resume, or Restart BizTalk Server Services.

15. On the computer you use to administer BizTalk Server, open the BizTalk Server 2006 Administration Console. Click **Start**, click **Run**, type **btsmmc.msc**, and then click **OK**.

16. In the console tree, right-click **BizTalk Server 2006 Administration**, and then click **Connect to Existing Group**.

17. In the **Connect to Existing BizTalk Server Configuration Database** dialog box, in the **SQL Server name** drop-down list box, select the name of the Microsoft SQL Server instance that hosts the BizTalk Management database. When you select the instance of SQL Server, BizTalk Server automatically attempts to detect BizTalk Server databases on that computer.

18. In the **Database name** drop-down list box, select the BizTalk Management database (**BizTalkMgmtDb**) to which you want to connect, and then click **OK**.

    The BizTalk Server Administration Console adds the BizTalk group to the console tree.

Your BizTalk server is now restored and should be running. You should now configure the Backup BizTalk Server job to start writing backups to a new destination server. You should also reconfigure a new destination system.

Backing Up and Restoring BAS

This section provides information about how to back up and restore the BAS Web site and database.

In This Section

- How to Back Up Your BAS Site and Database
- How to Restore Your BAS Site and Database
- How to Update References to the TPM Database Name and Connection String

How to Back Up Your BAS Site and Database

The Business Activity Services (BAS) environment consists of the following:

- A Web site hosted in Microsoft Windows SharePoint Services and Microsoft Office InfoPath 2003 templates. Windows SharePoint Services and InfoPath provide a common user interface for all of the services included in BAS.

- A Trading Partner Management database (TPM database). This database stores trading partner data for BAS. It is not a run-time database.

Prerequisites

You must be logged on as a member of the BizTalk Server Administrators group to perform this procedure.

To back up your BAS site and database

1. After you set up BAS, back up all the changes you made to the Web application configuration files and Windows SharePoint Services site templates so these can be easily recovered later. In your backup you should also include modifications that you made in other places, for example, in client-side JavaScript files.

2. Use the Backup BizTalk Server job to back up the TPM database. For instructions, see How to Configure the Backup BizTalk Server Job.

3. Follow the instructions in the "Backing up and Restoring Databases by Using the SQL Server 2000 Tools" section of the Windows SharePoint Services Administrator's Guide to back up the Windows SharePoint Services configuration and content databases.

How to Restore Your BAS Site and Database

If you backed up your BAS site (which is a Microsoft Windows SharePoint Services site) and the Windows SharePoint Services configuration and content databases, you can use the following procedure to restore those backups to another computer in the event of a hardware failure.

Prerequisites

You must be logged on as a member of the BizTalk Server Administrators group to perform this procedure.

To restore your BAS site and database

1. Using the SQL Server backup and restore tools, restore the Windows SharePoint Services configuration and content databases.

2. Click **Start**, point to **Settings**, click **Control Panel**, double-click **Administrative Tools**, and then double-click **SharePoint Central Administration**.

3. On the **Windows SharePoint Services Central Administration** page, click **Configure virtual server settings**.

4. On the **Virtual Server List** page, click your Windows SharePoint Services virtual server.

5. On the **Virtual Server Settings** page, under **Virtual Server Management**, click **Remove Windows SharePoint Services from virtual server**, click **Remove and**

delete content databases to unextend Windows SharePoint Services virtual server, and then click **OK**.

6. Under **Server Configuration**, click **Set configuration database server**.

7. On the **Set Configuration Database Server** page, in **Database server**, enter the name of the server hosting the database. Then, in **SQL Server database name**, enter the name of the database, select **Connect to existing database**, and then click **OK**.

8. Under **Virtual Server Configuration**, click **Extend or upgrade virtual server**.

9. In the **Virtual Server List**, click **Default Web Site**.

10. Under **Provisioning Options**, click **Extend and map to another virtual server**.

11. In **Extend and Map to Another Virtual Server**, select **Use an existing application pool**, and then click **OK**.

12. On the **Virtual Server Settings** page, under **Virtual Server Management**, click **Manage content databases**.

13. On the **Manage Content Databases** page, click **Add a content database**.

14. On the **Add Content Database** page, under **Database Information**, click **Specify database server settings**. In **Database server**, type the name of the restored database server name. In **Database name**, type the name of the restored data base.

15. On the **Manage Content Databases** page, click the previous content database. This is the database you backed up.

16. On the **Manage Content Database Settings** page, under **Remove Content Database**, click **Remove content database** to remove this old database link from the **Manage Content Databases** page.

    For more information about restoring Windows SharePoint Services databases, see "Restoring from a Backup" in "Backing Up and Restoring Databases by Using the SQL Server 2000 Tools" in the Windows SharePoint Services Administrator's Guide.

17. Open the **Internet Information Services Manager** snap-in. To do this, click **Start**, click **Run**, and then type **%SystemRoot%\system32\inetsrv\iis.msc**.

18. Click the local computer, click **Web Sites**, click **Default Web Site**, click **_layouts**, click the <*locale identifier*>, right-click **BAS**, and then click **Properties**.

19. In the **BAS Properties** dialog box, on the **Directory** tab, next to the **Application name** box, click **Create**, and then click **OK**. Verify that the BAS application pool is unchanged after you restore the BAS site and database.

20. In Windows SharePoint Services, apply all of your own customizations, including the ones made to the Web.config files, the JavaScript file, and the Windows SharePoint Services site templates.

Updating Windows SharePoint Services

You need to update Windows SharePoint Services in the following two scenarios:

- When you upgrade from a previous version of Windows SharePoint Services to a newer version.
- When you install service packs or hotfixes for Windows SharePoint Services.

In these scenarios, you must back up all modifications made to Web application configuration files and Windows SharePoint Services site templates after BAS setup so these can be easily applied later. To do this, perform the following steps:

- Follow the procedure in this topic to back up your BAS site in case you need to recover it later.
- Follow all the steps included in the Windows SharePoint Services upgrade guide or the instructions accompanying a software update.
- Apply your own modifications that you saved before the update.

How to Update References to the TPM Database Name and Connection String

If you backed up your Trading Partner Management (TPM) database, in the event of a system or data failure you can restore that backup to a different computer and you can rename the backup.

To restore the TPM database, perform the steps in How to Restore Your Databases. In addition, you must update other references to the TPM database name and the TPM connection string in your BizTalk Server environment.

Prerequisites

- You must be logged on as a member of the BizTalk Server Administrators group to perform this procedure.
- Download and install **aspnet_setreg.exe**. For information about how to do this, see How to use the ASP.NET utility to encrypt credentials and session state connection stringsHow to use the ASP.NET utility to encrypt credentials and session state connection strings.

To update references to the TPM database name and connection string

1. In the restored TPM database, in the SourceDef table, update the value of the ConnStr column with the new connection string:
2. If you registered BizTalk Server in BAS, you must update "Server" column of "BizTalkServer" table in the TPM database to use the new database server name.

3. On all servers where BAS is installed, update the **TpmDbConnStr** registry key with the TPM connection string in encrypted form:

   a. Open Registry Editor. To do this, click **Start**, click **Run**, and them type **regedit**.

   b. In Registry Editor, right-click the **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\BizTalk Server\3.0\TpmDbConnStr** registry key, click **Permissions**, and then click **Advanced**.

   c. In the **Advanced Security Settings for TpmDbConnStr** dialog box, write down the users and permissions currently configured on the **TpmDbConnStr** registry key. You need this information to reset permissions after the registry key is modified.

   d. To update the encrypted **TpmDbConnStr** registry key, click **Start**, click **Run**, type **cmd**, and then type the following command:

4. Reset the permission on the registry key by using the settings you wrote down in step c.

5. Open Registry Editor. To do this, click **Start**, click **Run**, and them type **regedit**.

6. In **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\BizTalk Server\3.0\TPM**, update the following registry keys with the new database server and database name:

   - TpmDbName
   - TpmTechGroupSql
   - TpmDbServer

7. Update the following Web.config files:

   - C:\Program Files\Microsoft BizTalk Server 2006\Business Activity Services\TPM\Management\Web.config
   - C:\Program Files\Microsoft BizTalk Server 2006\Business Activity Services\TPM\Publishing\Web.config

   Replace the <*ServerName*> string with the new server name and <*DatabaseName*> with the new database name. The following keys contain connection strings that must be updated:

8. Resynchronize the Business Activity Services (BAS) site with the TPM database:

   In Internet Explorer, in the **Address** box, type the URL of the Business Activity Services site, and then press ENTER.

On the **Business Activity Services Site Home** page, click **TPM Admin** at the top of the page.

. On the **TPM Administration** page, click **Resync**.

Backing Up and Restoring BAM

This section provides information about how to back up and restore the BAM Analysis, Tracking Analysis, BAM Star Schema, and BAM Archive databases.

In This Section

- How to Back Up the BAM Analysis and Tracking Analysis Server Databases
- How to Update References to the BAM Analysis Server Database Name
- How to Update References to the Tracking Analysis Server Database Name
- How to Update References to the BAM Star Schema Database Name
- How to Update References to the BAM Archive Database Name
- How to Update References to the BAM Primary Import Database Name and Connection String
- How to Update References to the BAM Notification Services Databases
- How to Resolve Incomplete Activity Instances

How to Back Up the BAM Analysis and Tracking Analysis Server Databases

The Business Activity Monitoring (BAM) Analysis database and the Tracking Analysis Server database store content in SQL Server Analysis Services cubes. The Backup BizTalk Server job does not back up these databases. Instead, to backup these databases, you must use SQL Server Analysis Manager.

After you back up these databases, you may want to purge the OLAP cubes. When you purge the OLAP cubes, you must also perform the following steps:

1. Before you purge the OLAP cubes, in the BAM Star Schema database, truncate the fact table(s) for the cube you want to purge. The table naming convention is "bam_<*CubeName*>_Facts".

2. After you purge the OLAP cubes, you must fully process active, completed, and virtual cubes.

For instructions about backing up the analysis databases, see "Archiving an Analysis Services Database" in SQL Server Books Online.

Scheduling backups for the BAM databases

If you are using BAM, verify that neither the BAM cube process nor data maintenance Data Transformation Services (DTS) packages are running when the backup package is scheduled to run.

To ensure consistent schema across all BAM databases, back up the BAM databases and DTS packages each time you deploy or undeploy a BAM activity.

Back up the BAM Analysis database and BAM Star Schema database each time you deploy or undeploy a BAM view.

Back up the BAM databases in the following order:

1. Back up the BAM Analysis database, and then the BAM Star Schema database.

2. Run the Backup BizTalk Server job to back up the BAM Primary Import database and your other BizTalk Server databases.

3. Run the BAM data maintenance DTS package for all activities.

   Incorporate these steps into a DTS package, and schedule the package to run on a regular basis. To ensure data integrity, make sure no other BAM cubing or data maintenance DTS packages run when this backup package is scheduled to run.

   To ensure that you can recover a complete set of archived data if the BAM Archive database fails, back up the BAM Archive database after you copy the partition into the BAM Archive database, but before you delete the partition from the BAM Primary Import database. To do this, modify the data maintenance DTS package for each activity to insert a step to back up the BAM Archive database before the last step in the DTS package, "End Archiving."

4. Get a copy of the .xml file used for restoring BAM:

   a. At the command prompt, type:

   b. Save the file on the destination system where you back up the BizTalk Server databases.

How to Update References to the BAM Analysis Server Database Name

If you backed up your BAM Analysis database, in the event of a system or data failure you can restore that backup to a different computer and you can rename the backup.

To restore the BAM Analysis Server database, perform the steps in How to Restore Your Databases. In addition, you must update the BAM Data Transformation Services (DTS) packages with the new server name and database name.

Prerequisites

You must be logged on as a member of the BizTalk Server Administrators group to perform this procedure.

To update references to the BAM Analysis Server database name (SQL Server 2000)

1. Stop any BAM cube update and data maintenance DTS packages, or prevent them from running until you have restored the BAM Analysis database.

2. Stop the BizTalk Application Service (which includes the BAM Event Bus service) so it does not try to import more data into the database.

3. Update the server and database names in all BAM analysis DTS packages, which are prefixed with "BAM_AN_" by following these steps:

   a. On the server hosting BAM, open SQL Server Enterprise Manager.

   b. Open the **Data Transformation Services** folder.

   c. Open the **Local Packages** folder, and then open the DTS packages.

   d. On the **Package** menu, click **Properties**.

   e. On the **Global Variables** tab, update the values for the primary import server and database.

   f. Change the following lines to match your new server and database:

      PrimaryImportServer= "<*ServerName*>"

      PrimaryImportDatabase = "<*DatabaseName*>"

4. Restart the BizTalk Application service.

5. Enable any BAM cube update and data maintenance DTS packages.

6. Open Analysis Manager and update the Data Sources connection strings in the BAMAnalysis database for the BAM_AN cube. Click **Start**, click **Programs**, click **Microsoft SQL Server**, click **Analysis Services**, and then click **Analysis Manager**.

7. In Analysis Manager, double-click **Analysis Services**, double-click the appropriate SQL Server, double-click **BAMAnalysis**, and then click **Data Sources**.

8. In the details pane, on the **Meta Data** tab, right-click the BAM_<*CubeName*> cube, and then click **Edit**.

9. Update the server name with the new server name.

To update references to the BAM Analysis Server database name (SQL Server 2005)

1. Stop any BAM cube update and data maintenance DTS packages, or prevent them from running until you have restored the BAM Analysis database.

2. Stop the BizTalk Application Service (which includes the BAM Event Bus service) so it does not try to import more data into the database.

3. Click **Start**, click **Microsoft SQL Server 2005**, and then click **SQL Server Business Intelligence Development Studio**.

4. In SQL Server Business Intelligence Development Studio, create a new project. Click **File**, click **New**, and then click **Project**.

5. In the **New Project** dialog box, in **Templates**, click **Integration Services Project**, and then click **OK**.

6. In the **Integration Services Project** dialog box, in **Solution Explorer**, right-click **SSIS Packages**, and then click **Add Existing Package**.

7. In the **Add Copy of Existing Package** dialog box, in the **Server** drop-down list box, select the server that contains the BAM_AN package.

8. In **Package Path**, click the ellipses button.

9. In the **SSIS Package** dialog box, select the BAM_AN package, click **OK**, and then click **OK**.

   The package is now listed in Solution Explorer.

10. In **Solution Explorer**, double-click the BAM_AN package. In **Connections Managers**, double-click database number 3 (MSDB database).

11. In the **Connection Manager** dialog box, in the **Server name** box, enter the name of the MSDB server, and then click **OK**.

12. Click the **Package Explorer** tab, double-click the **Variables** folder, and then update the values for the primary import server name and primary import database name.

13. Click **File**, and then click **Save All**.

14. In **Microsoft SQL Server Management Studio**, click **Connect**.

15. Click **Integration Services**, double-click **Stored Packages**, click **MSDB**, right-click the BAM_AN package, and then click **Import Package**.

16. In the **Import Package** dialog box, in **Package location**, select **File System**.

17. In **Package Path**, navigate to your saved project, select the BAM_AN*.dtsx file, and then click **Open**.

18. Click inside the **Package Name** box to automatically populate the box.

19. Click **OK**, and then click **Yes** to overwrite.

20. Restart the BizTalk Application service.

21. Enable any BAM cube update and data maintenance DTS packages.

How to Update References to the Tracking Analysis Server Database Name

The Tracking Analysis Server database is an optional database. It contains the online analytical processing (OLAP) cubes used by Health and Activity Tracking (HAT). These OLAP cubes are aggregations of data contained in the BizTalk Tracking database.

To restore the Tracking Analysis Server database, use SQL Server Analysis Manager to process the MessageMetrics and ServiceMetrics cubes. For instructions, see "Restoring an Analysis Services Database" in SQL Server Books Online.

To restore the Tracking Analysis Server database to an alternate computer, you must also update references to the database name in the BizTalk Management database using the following procedure.

Prerequisites

You must be logged on as a member of the BizTalk Server Administrators group to perform this procedure.

To update references to the Tracking Analysis Server database name (SQL Server 2000)

1. On the destination system, click **Start**, click **Programs**, click **Microsoft SQL Server**, and then click **Enterprise Manager**.

2. Open the appropriate server by clicking it, double-clicking **Databases**, double-clicking **BizTalkMgmtDb**, and then clicking **Tables**.

3. In the details pane, right-click **adm_Group**, point to **Open Table**, and then click **Return all rows**.

4. Modify the columns corresponding to the original database to reference the appropriate values for the new database.

5. Close the table to save the new values.

   <DBType>DBServerName and <DBType>DBName indicate the location of the database, where <DBType> corresponds to the type of the database: TrackingAnalysis.

To update references to the Tracking Analysis Server database name (SQL Server 2005)

1. On the destination system, click **Start**, click **Programs**, click **Microsoft SQL Server 2005**, and then click **SQL Server Management Studio**.

2. In the **Connect to Server** dialog box, specify the name of the SQL Server on the destination system, and then click **Connect** to connect to the appropriate SQL Server.

3. In **Microsoft SQL Server Management Studio**, double-click the appropriate server, double-click **Databases**, and then double-click **BizTalkMgmtDb**.

4. Double-click **Tables**, right-click **adm_Group**, and then click **Open Table**.

5. Modify the columns corresponding to the original database to reference the appropriate values for the new database.

6. Close the table to save the new values.

   <DBType>DBServerName and <DBType>DBName indicate the location of the database, where <DBType> corresponds to the type of the database: TrackingAnalysis.

How to Update References to the BAM Star Schema Database Name

If you backed up your BAM Star Schema database, in the event of a system or data failure you can restore that backup to a different computer, and you can rename the backup.

To restore the BAM Star Schema database, perform the steps in How to Restore Your Databases. In addition, you must update the BAM Data Transformation Services (DTS) packages with the new server name and database name.

Prerequisites

You must be logged on as a member of the BizTalk Server Administrators group to perform this procedure.

To update references to the BAM Star Schema database name (SQL Server 2000)

1. Stop any BAM cube update and data maintenance DTS packages, or prevent them from running until you have restored the BAM Star Schema database.

2. Stop the BizTalk Application service (which includes the BAM Event Bus service) so it does not try to import more data into the database.

   a. Click **Start**, click **Run**, and then type **services.msc**.

   b. Right-click the **BizTalk Service BizTalk Group: BizTalkServerApplication** service and then click **Stop**.

3. Update SQL Connection 2 to change the server and database name in all BAM analysis DTS packages, which are prefixed with "BAM_AN_", by following these steps:

   a. On the computer or computers you have identified as the destination system, click **Start**, click **Programs**, click **Microsoft SQL Server**, and then click **Enterprise Manager**.

   b. Double-click the server hosting BAM.

   c. Double-click **Data Transformation Services**, and then click **Local Packages**.

   d. In the details pane, double-click the DTS package, and then double-click **Connection 2** to open the connection.

   e. Select the new server and database name in the drop-down box.

4. Update the data source in the BAM Analysis database as follows:

   a. Click **Start**, click **Programs**, click **Microsoft SQL Server**, click **Analysis Service**, and then click **Analysis Manager**.

   b. Double-click **Analysis Servers**, and then expand the server hosting the BAM Analysis database.

   c. Double-click **BAMAnalysis**, and then double-click **Data Sources**.

   d. Right-click the data source for the cube, and then click **Edit**.

   e. On the **Connection** tab, type the new server name and database name for the BAM Star Schema database, and then click **OK**.

5. Restart the BizTalk Application service.

   a. Click **Start**, click **Run**, and then type **services.msc**.

   b. Right-click the **BizTalk Service BizTalk Group: BizTalkServerApplication** service and then click **Start**.

6. Enable any BAM cube update and data maintenance DTS packages.

To update references to the BAM Star Schema database name (SQL Server 2005)

1. Stop any BAM cube update and data maintenance DTS packages, or prevent them from running until you have restored the BAM Star Schema database.

2. Stop the BizTalk Application service (which includes the BAM Event Bus service) so it does not try to import more data into the database.

   a. Click **Start**, click **Run**, and then type **services.msc**.

b. Right-click the **BizTalk Service BizTalk Group: BizTalkServerApplication** service and then click **Stop**.

3. Update SQL Connection 2 to change the server and database name in all BAM analysis DTS packages, which are prefixed with "BAM_AN_", by following these steps:

a. On the computer or computers you have identified as the destination system, click **Start**, click **Programs**, click **Microsoft SQL Server**, and then click **Enterprise Manager**.

b. Double-click the server hosting BAM.

c. Double-click **Data Transformation Services**, and then click **Local Packages**.

d. In the details pane, double-click the DTS package, and then double-click **Connection 2** to open the connection.

e. Select the new server and database name in the drop-down box.

4. Update the data source in the BAM Analysis database as follows:

a. Click **Start**, click **Programs**, click **Microsoft SQL Server**, click **Analysis Service**, and then click **Analysis Manager**.

b. Double-click **Analysis Servers**, and then expand the server hosting the BAM Analysis database.

c. Double-click **BAMAnalysis**, and then double-click **Data Sources**.

d. Right-click the data source for the cube, and then click **Edit**.

e. On the **Connection** tab, type the new server name and database name for the BAM Star Schema database, and then click **OK**.

5. Restart the BizTalk Application service.

a. Click **Start**, click **Run**, and then type **services.msc**.

b. Right-click the **BizTalk Service BizTalk Group: BizTalkServerApplication** service and then click **Start**.

6. Enable any BAM cube update and data maintenance DTS packages.

How to Update References to the BAM Archive Database Name

If you backed up your BAM Archive databases, in the event of a system or data failure you can restore that backup and rename it.

To restore the BAM Archive databases, perform the steps in How to Restore Your Databases. In addition, you must perform these general steps, which are followed by a procedure that describes the steps in detail:

- Update the connection string in all BAM Microsoft Excel files with real-time aggregation pivot tables or OLAP tables.
- Update the BAM DTS packages with the new server name and database name.

Prerequisites

You must be logged on as a member of the BizTalk Server Administrators group to perform this procedure.

To update references to the BAM Archive database name (SQL Server 2000)

1. Stop any BAM cube update and data maintenance DTS packages, or prevent them from running until you have restored the BAM Archive database.
2. Stop the BizTalk Application service (which includes the BAM Event Bus service) so it does not try to import more data into the database.
   a. Click **Start**, click **Run**, and then type **services.msc**.
   b. Right-click the **BizTalk Service BizTalk Group: BizTalkServerApplication** service and then click **Stop**.
3. Unregister the BizTalk Application Service by running the following command:
   a. Click **Start**, click **Run**, type **cmd**, and then click **OK**.
   b. Navigate to **C:\Program Files (x86)\Microsoft SQL Server Notification Services\v2.0.3008.0\Bin**.
   c. At the command prompt, type: **nscontrol unregister -name BamAlerts**
4. Register the new BizTalk Application Service with the new server:
   a. Click **Start**, click **Run**, type **cmd**, and then click **OK**.
   b. Browse to **C:\Program Files (x86)\Microsoft SQL Server Notification Services\v2.0.3008.0\Bin**.
   c. At the command prompt, type: **nscontrol register -name BamAlerts -server** <*ServerName*> -service -serviceusername "<*ServiceUserName*>" -servicepassword "<*ServicePassword*>"
5. Update the SQL Connection 2 to change the connection string in all BAM Microsoft Excel files with real-time aggregation pivot or OLAP tables.

   For each file, perform the following steps:

a. Open the Excel file.

b. On the **Tools** menu, click **Macro**, and then click **Visual Basic Editor**.

c. When prompted for the password, type **Microsoft**.

d. Click **VBAProject**, and then click **ConnectionInfoHiddenSheet**.

e. Set the **Visible** property of **ConnectionInfoHiddenSheet** to **xlSheetVisible**.

f. On the **File** menu, click **Close and Return to Microsoft Excel**.

g. Click the **ConnectionInfoHiddenSheet** worksheet.

h. Find the column titled **Connection String**, and make changes to the data source and initial catalog settings on the correct type of row. There are two types of rows, one for RTA and another for OLAP determined by the RTAExists column. Modify the database references that have changed.

i. For the OLAP connection strings (the rows with no information in the RTAName column), the original string has the following format: AOLEDB; Provider=MSOLAP.2; Data Source=<*ServerName*>;Initial Catalog=<*DatabaseName*>.

   Replace <*ServerName*> with the new analysis server name, and <*DatabaseName*> with the new analysis database name.

j. For the RTA connection string (rows with information in the RTAName column), the string has the following format: Source_DSN="DRIVER=SQL Server;SERVER=<server name>; DATABASE=<database name>;Trusted_Connection=Yes";

   Replace the <*ServerName*> with the new primary import server name, and replace <*DatabaseName*> with the new primary import database name. Click **OK**.

k. On the **Tools** menu, click **Macro**, and then click **Visual Basic Editor**.

l. When prompted for the password, type **Microsoft**.

m. Click **VBAProject**, and then click **ConnectionInfoHiddenSheet**.

n. Set the **Visible** property of **ConnectionInfoHiddenSheet** to xlSheetHidden.

o. On the **File** menu, click **Close and Return to Microsoft Excel**.

p. On the **File** menu, click **Save**.

6. Update SQL Connection 2 in all BAM data maintenance packages (prefixed with "BAM_DM_") as follows:

a. Using SQL Enterprise Manager, open the server hosting BAM.

b. Open the **Data Transformation Services** folder.

c. Open the **Local Packages** folder.

d. Double-click to open the DTS package.

e. Double-click **Connection 2** to open the connection.

f. Select the new server and database name in the drop-down box.

7. Restart the BizTalk Application Service.

a. Click **Start**, click **Run**, and then type **services.msc**.

b. Right-click the **BizTalk Service BizTalk Group: BizTalkServerApplication** service and then click **Start**.

8. Enable any BAM cube update and data maintenance DTS packages.

To update references to the BAM Archive database name (SQL Server 2005)

1. Stop any BAM cube update and data maintenance DTS packages, or prevent them from running until you have restored the BAM Archive database.

2. Stop the BizTalk Application service (which includes the BAM Event Bus service) so it does not try to import more data into the database.

a. Click **Start**, click **Run**, and then type **services.msc**.

b. Right-click the **BizTalk Service BizTalk Group: BizTalkServerApplication** service and then click **Stop**.

3. Unregister the BizTalk Application Service by running the following command:

a. Click **Start**, click **Run**, type **cmd**, and then click **OK**.

b. Navigate to **C:\Program Files (x86)\Microsoft SQL Server Notification Services\v2.0.3008.0\Bin**.

c. At the command prompt, type: **nscontrol unregister -name BamAlerts**

4. Register the new BizTalk Application Service with the new server:

a. Click **Start**, click **Run**, type **cmd**, and then click **OK**.

b. Browse to **C:\Program Files (x86)\Microsoft SQL Server Notification Services\v2.0.3008.0\Bin**

c. At the command prompt, type: **nscontrol register -name BamAlerts -server** <*ServerName*> -service -serviceusername "<*ServiceUserName*>" -servicepassword "<*ServicePassword*>"

5. Update the SQL Connection 2 to change the connection string in all BAM Microsoft Excel files with real-time aggregation pivot or OLAP tables.

For each file, perform the following steps:

a. Open the Excel file.

b. On the **Tools** menu, click **Macro**, and then click **Visual Basic Editor**.

c. When prompted for the password, type **Microsoft**.

d. Click **VBAProject**, and then click **ConnectionInfoHiddenSheet**.

e. Set the **Visible** property of **ConnectionInfoHiddenSheet** to **xlSheetVisible**.

f. On the **File** menu, click **Close and Return to Microsoft Excel**.

g. Click the **ConnectionInfoHiddenSheet** worksheet.

h. Find the column titled **Connection String**, and make changes to the data source and initial catalog settings on the correct type of row. There are two types of rows, one for RTA and another for OLAP determined by the RTAExists column. Modify the database references that have changed.

i. For the OLAP connection strings (the rows with no information in the RTAName column), the original string has the following format: AOLEDB; Provider=MSOLAP.2; Data Source=<*ServerName*>;Initial Catalog=<*DatabaseName*>.

Replace <*ServerName*> with the new analysis server name, and <*DatabaseName*> with the new analysis database name.

j. For the RTA connection string (rows with information in the RTAName column), the string has the following format: Source_DSN="DRIVER=SQL Server;SERVER=<server name>; DATABASE=<database name>;Trusted_Connection=Yes";

Replace the <*ServerName*> with the new primary import server name, and replace <*DatabaseName*> with the new primary import database name. Click **OK**.

k. On the **Tools** menu, click **Macro**, and then click **Visual Basic Editor**.

l. When prompted for the password, type **Microsoft**.

m. Click **VBAProject**, and then click **ConnectionInfoHiddenSheet**.

n. Set the **Visible** property of **ConnectionInfoHiddenSheet** to xlSheetHidden.

o. On the **File** menu, click **Close and Return to Microsoft Excel**.

p. On the **File** menu, click **Save**.

6. Update SQL Connection 2 in all BAM data maintenance packages (prefixed with "BAM_DM_") as follows:

a. Using SQL Enterprise Manager, open the server hosting BAM.

b. Open the **Data Transformation Services** folder.

c. Open the **Local Packages** folder.

d. Double-click to open the DTS package.

e. Double-click **Connection 2** to open the connection.

f. Select the new server and database name in the drop-down box.

7. Restart the BizTalk Application Service.

a. Click **Start**, click **Run**, and then type **services.msc**.

b. Right-click the **BizTalk Service BizTalk Group: BizTalkServerApplication** service and then click **Start**.

8. Enable any BAM cube update and data maintenance DTS packages.

How to Update References to the BAM Primary Import Database Name and Connection String

If you backed up your BAM Primary Import database in the event of a system or data failure, you can restore that backup to a different computer and rename the backup.

The BAM Event Bus service moves event data from the MessageBox database to the BAM Primary Import database. The BAM Event Bus service includes fault tolerance logic that enables it to recover and restart from an unexpected failure without losing any data. For more information about the BAM Event Bus service,.

To restore the BAM Primary Import database, perform the steps in How to Restore Your Databases. In addition, you must perform these general steps, which are followed by a procedure that describes the steps in detail:

- Update the SQL Connection 1 in all BAM DTS packages to refer to the new database name.

- Update the web.config file with the new database name.

- Update the BAM Primary Import connection string in all BAM Microsoft Excel files with real-time aggregation pivot or OLAP tables.

Prerequisites

You must be logged on as a member of the BizTalk Server Administrators group to perform this procedure.

To update references to the BAM Primary Import database name and connection string

1. Stop any BAM cube update and data maintenance Data Transformation Services (DTS) packages, or prevent them from running until you have restored the BAM Primary Import database.

2. Stop the BizTalk Application Service (which includes the BAM Event Bus service) so it does not try to import more data into the database.

3. Restore the BAM Primary Import database, performing the steps in How to Restore Your Databases.

4. Update the following Web.Config files:

   - C:\Program Files\Microsoft BizTalk Server 2006\BAMPortal\BamManagementService\Web.Config.

     Replace the <*ServerName*> string with the new server name and <*DatabaseName*> with the new database name. Update the following connection strings:

     <appSettings>

     <add key="BamServer" value="<*ServerName*>" />

     <add key="BamDatabase" value="<*DatabaseName*>" />

     <add key="MaxResultRows" value="2000" />

     </appSettings>

   - C:\Program Files\Microsoft BizTalk Server 2006\BAMPortal\BamQueryService\Web.Config.

     Replace the <*ServerName*> string with the new server name and <*DatabaseName*> with the new database name. Update the following connection strings:

     <appSettings>

     <add key="BamServer" value="<*ServerName*>" />

     <add key="BamDatabase" value="<*DatabaseName*>" />

     <add key="MaxResultRows" value="2000" />

</appSettings>

5. In the BAM Primary Import database, in the Bam_metadata_configuration table, update the BAMConfigurationXml column with the contents of the newly modified BamConfiguration.xml file, as follows:

   a. Using SQL Query Analyzer, select the **BAM Primary Import Database**.

   b. Execute the following command, replacing the <BAMConfigurationXml> string with the contents of the BAMConfiguration.xml file:

   Update bam_Metadata_configuration set BamConfigurationXml = '<*BAMConfigurationXml*>'.

6. Update the connection string in all BAM Microsoft Excel files with real-time aggregation pivot or OLAP tables. For each file:

   . Open the Excel live data file. The file name ends with _LiveData.xls.

   a. On the **BAM** menu, click **BAM DB Connection**.

   b. In the **Select BAM Database** dialog box, enter the SQL Server and BAMPrimaryImport database, and then click **OK**.

   c. On the **File** menu, click **Close and Return to Microsoft Excel**.

   d. On the **File** menu, click **Save**.

7. Restart the BizTalk Application service so it can import data into the new database.

8. Enable any BAM cube update and data maintenance DTS packages.

9. To resolve any incomplete trace instance

How to Update References to the BAM Notification Services Databases

After you perform the steps necessary to restore the Business Activity Monitoring (BAM) Notification Services databases to the destination system, you must re-register the Notification Service on all computers in the BizTalk Server group that are running Notification Services (NSservice.exe). This enables Notification Services to connect to the databases in their new location.

Registering an instance of Notification Services creates the NS$instance_name service, creates performance counters on the local server, and adds information to the registry. You must register the instance on the following servers:

- Each server that runs the NS$instance_name service. The service runs the event provider host, generator, and distributor components. For scaled-out configurations, the service runs on multiple servers.

- Each server that runs a subscription management application. If the subscription management application runs on its own server, do not create the NS$instance_name service when registering the instance.

- Each server that runs an independent event provider. If the independent event provider runs on its own server or the database server, do not create the NS$instance_name service when registering the instance.

If the database server does not also run the Notification Services instance or the client components, do not register the instance on this server.

Prerequisites

You must be logged on as a member of the Administrators group to perform this procedure.

To update references to the BAM Notification Services databases

1. Click **Start**, click **Run**, type **cmd**, and then click **OK**.

2. At the command prompt, type: **bm.exe get-configxml**

3. Open the xml file created in step 2 to obtain the list of the computers on which you must re-register Notification Services.

   The computer names are listed in the **<Property Name=>** parameters in the **<DeploymentUnit Name="Alert">** section of the xml file:

4. On each computer listed in the xml file, stop the NS service and then unregister an instance of Notification Services:

   a. Click **Start**, click **Programs**, click **Microsoft SQL Server Notification Services**, and then click **Notification Services Command Prompt**.

   b. At the command prompt, type: **net stop NSservice.exe**

   c. Type the following command to unregister the instance:

      nscontrol unregister -name BamAlerts

      Unregistering an instance removes the registry entries, removes the NS$instance_name service (if present), and deletes the performance counters for the service.

5. Re-register the Notification Service:

   a. Click **Start**, click **Programs**, click **Microsoft SQL Server Notification Services**, and then click **Notification Services Command Prompt**.

b. At the command prompt, type: **nscontrol register -name BamAlerts -server** <*ServerName*> **-service -serviceusername "**<*ServiceUserName*>**" -servicepassword "**<*ServicePassword*>**"**

This enables Notification Services to log on to the correct database (this information is maintained in the registry of the service machine by nscontrol).

6. On the computer that hosts the BAM portal, open the Notification Services Command Prompt.

Click **Start**, click **Programs**, click **Microsoft SQL Server Notification Services**, and then click **Notification Services Command Prompt**.

7. At the command prompt, type:

nscontrol unregister -name BamAlerts

8. At the command prompt, type:

nscontrol register -name <*BamAlerts*> **-server**<*NotificationServicesDatabaseServer*>

How to Resolve Incomplete Activity Instances

BAM stores data for incomplete activity instances in a special *active instance* table in the BAM Primary Import database.

If some instance records were started before the last backup of the BAM Primary Import database but completed after the backup, those instance records remain in an active instance table. This is because after the BAM Primary Import database is restored, the completion records for these instances are lost.

Although the records in the active instance table do not prevent BAM from functioning properly, we recommend that you mark these records as "completed," and then move them out of the active instance table.

Prerequisites

You must be logged on as a member of the BizTalk Server Administrators group to perform this procedure.

To generate a list of incomplete ActivityIDs for an activity

1. Run the following query against the BAM Primary Import database:

2. If data from external systems indicates that the activity instance is in fact completed, run the following query to manually complete the instance:

Backing Up and Restoring the Base EDI Adapter

As part of your plan for backing up and restoring your BizTalk Server installation, you must include plans for backing up and restoring the Base EDI adapter. This is because the Base EDI adapter, unlike the other adapters in BizTalk Server, has its own database and stores files in a directory (Documentshome) during runtime.

Backing up the Base EDI adapter

While some parts of the Base EDI adapter, such as the BizTalk Base EDI database, are backed up in the recommended BizTalk Server system recovery plans, others are not. This section describes the procedures that you should follow to help ensure that all items related to the Base EDI adapter are protected in case of a hardware or software failure.

Restoring the Base EDI adapter

The steps you take to restore the Base EDI adapter to its last known good state depend on which component or components of your BizTalk Server deployment fail. This section describes how to recover from faults occurring with the BizTalk Server databases and the Documentshome directory.

When restoring your environment, you should follow a precise order of steps. Doing so ensures that when the system comes back online it is in a controlled fashion that allows the resumption of message processing and tracking from the point of failure with minimal risk of data loss.

In This Section

- Best Practices for Backing Up the Documentshome Directory
- How to Restore the Documentshome Directory
- How to Recover Data and Resynchronize the Audit Trail
- How to Generate an Engine Input File

Best Practices for Backing Up the Documentshome Directory

By default, the Documentshome directory is located on your file system in the <root>\Documents and Settings\All Users\Application Data\Microsoft\BizTalk Server 2006\EDI\Subsystem. The Subsystem folder contains four subfolders where the following items are stored:

- Sent and received documents in XML and EDI format
- Temporary and intermediate files created during translation
- The compiled engine input file (EIF)
- The Base EDI adapter settings file (esp.ini)

- All generated log files

At any given moment, the Documentshome directory can contain archived files, files that are in an intermediate stage between being ready to send to an external trading partner, ready to translate between EDI/XML format, ready to send to BizTalk Server, or in their final version.

Following are best practices for backing up and restoring the Documentshome directory:

Use file-based backups

Because the Documentshome directory is file-based, your solution should employ a robust and high storage capability backup solution that provides the frequent or instantaneous backing up of data.

One of the safest and most effective ways to safeguard disk-based data is to use disk mirroring. Disk mirroring schemes write data to two disks simultaneously, which guarantees that there are always two identical copies of the data available at any one time. There are many disk mirroring solutions available, such as RAID/MAID and EMC Symmetrix.

In the absence of a disk mirroring scheme, your backup strategy should involve frequent, regular backups that include accurate timestamps that are synchronized with the system that hosts the BizTalk Server databases.

Use disk mirroring for high availability failover

Disk mirroring software offers the further advantage of providing a seamless and instantaneous failover from the active disk to the mirrored disk in case the primary disk fails. Such a solution precludes the possibility of there being any significant downtime should the Documentshome directory fail or become corrupted.

Use disk mirroring for quick restore time

In the event of a failure of the hardware containing the Documentshome directory, the more quickly and efficiently the system can be restored to its last known, good state, the less time your deployment will be out of production. If you employ disk mirroring, the software that manages the system automatically switches to the mirrored disk in case the primary disk becomes unavailable. In such a solution, there will be little or no need to perform restore operations.

If you do not employ a disk mirroring solution, you should devise a backup scheme that regularly archives your data and from which you can quickly restore.

Maintain data separation

To provide the most protection for your data and to ensure that you can quickly recover from the failure of one or more components, we strongly recommend that in your production system you physically separate (on separate disks) the data stored in the Documentshome directory from the data saved in the tracking and tracing databases as well as the file system folders designated for the send port and receive location.

If you lose some or all of the data in your Documentshome directory or in the tracking and tracing database, the chances that you can recover from the problem are greatly increased. Additionally, you should never store the backed-up data on the same physical disk as the production data.

Back up your production data frequently

How often you back up your production data depends to a large extent on how often data in your system changes. Generally, the more often the data in your production environment changes, the more frequently you should back it up. If your production environment processes messages or a greater number of messages at a regularly scheduled time of day, the time of your backups should coincide closely with the more intensive processing.

Archive copies of incoming EDI messages

Depending on the legal agreements that exist between you and your trading partner and whether or how long your trading partner keeps sent EDI messages, you can archive copies of incoming EDI messages in case you need to recover from data loss. One way of doing this is to create an alternate receive location (pickup folder). When EDI messages are sent by your trading partner, they are first received in the alternate receive location and then automatically copied to the designated pickup location on the BizTalk Receive Location for processing. In such a scheme, if you need to recover from a loss of data due to a failure on the disk where the Documentshome directory is located, you will have archived copies of received EDI files that you can reprocess.

Consider the benefits of message body tracking

Message body tracking in BizTalk Server archives not only the status, ID, and details of the sender and receiver of a message, but it also keeps a copy of the message body itself. In case of a system or data failure that requires you to restore your system from backup, it is possible to reconstruct XML files in their entirety by extracting the message body from the tracking database. Keep in mind that message body tracking causes your database to grow to a substantial size over time. It does, however, provide a means of recovering data that you might not otherwise be able to recover.

How to Restore the Documentshome Directory

This topic describes the steps you should follow to restore the Documentshome directory. The basic steps are the same regardless of how old the backup is or the method you used for the backup, such as disk mirroring.

Prerequisites

To perform this procedure, you must be logged on as a member of the BizTalk Administrators group.

If the failure of the Documentshome directory coincides with a failure of one or more BizTalk Server databases, you must first restore the affected databases before restoring the Documentshome directory. For more information about restoring BizTalk Server databases, see How to Restore Your Databases.

To restore the Documentshome directory

1. Restore the BizTalk Server databases (if any) that were affected by the failure that resulted in the loss of the Documentshome directory.

2. On the computer that hosts the Documentshome directory in your production system, restore the archived Documentshome directory.

3. Follow the steps in How to Recover Data and Resynchronize the Audit Trail in order to recover lost data and/or resynchronize the audit trail with the files in the restored Documentshomedirectory.

How to Recover Data and Resynchronize the Audit Trail

This topic describes the steps you should follow to recover lost data and to resynchronize the Documentshome directory with the audit trail after a failure of the disk hosting the Documentshome directory. These steps break down the actions you must follow for incoming and outgoing messages according to their status in the audit trail at the time you restored the Documentshome directory, or at the time you restored the files in the Documentshome directory with no corresponding status in the audit trail.

After you have evaluated all the files in the Documentshome directory and the files listed in the audit trail and followed the recommended steps, you should restart the BizTalk Server services.

Prerequisites

To perform these steps, you must be logged on as a member of the BizTalk Administrators group.

List the files in the Documentshome directory and all subdirectories

- Make a list of all the files in the Documentshome directory and all subdirectories, as described in the following table.

Location	File naming convention	Description
System\External\Inbox	**audin.[icin].in**, where [icin] is the value from the icin column in the **audin** table.	EDI messages that were received from your trading partner. Note that messages containing multiple interchanges will be saved as multiple files, one for each transaction.
System\External\Outbox	**audout.[icout].out**, where [icout] is the value from the icout column in the **audout** table.	EDI messages that were sent, or are to be sent, to your trading partner.
System\Internal\Inbox	**audin.[msgin].imi**, where [msgin] is the value from the msgin column in the **audin** table.	XML messages that were sent to, or that are to be sent to, BizTalk Server.

System\Internal\Outbox	**audout.[msgout].imo**, where [msgout] is the value from the msgout column in the **audout** table.	XML messages that were received from BizTalk Server translated, or that are to be translated, into EDI format.

Evaluate the status of all messages

- Evaluate the status of all messages that are referenced in the audin and audout tables. Organize your list as shown in the following table.

Table	Status	Description
audin	In external format	EDI messages that were received from your trading partner and stored in the External\Inbox folder.
audin	In internal format	EDI messages that were translated to XML format and stored in the Internal\Inbox folder.
audin	Accepted by BizTalk Server	Messages that were successfully sent to BizTalk Server.
audin	Rejected by BizTalk Server	Messages that were not accepted by BizTalk Server.
audout	In internal format	XML messages that were received from BizTalk Server and stored in the Internal\Outbox folder.
audout	Translation in progress	Messages that are in an intermediate state between internal and external format.
audout	In external format	XML messages that were received from BizTalk Server translated to EDI format and stored in the External\Outbox folder.
audout	Sent	EDI messages that were sent to your trading partner.
audout	Communication failed	EDI messages that either could not be written to the Put folder designated on the BizTalk Server send port, or whose time-out for receiving a functional acknowledgement from your trading partner was exceeded.

Compare incoming message lists, resolve data loss, and resynchronize the audit trail

1. Compare the list of messages that you compiled in the second step ("Evaluate the status of all messages") with the list of files in the Internal and External Inbox/Outbox folders that you compiled in the first step ("List the files in the Documentshome directory and all subdirectories").

2. Resolve the missing or partially processed data and resynchronize the audit trail if necessary. Use the descriptions in the following table to work with incoming messages according to their status in the audit trail.

Incoming message status (audin table)	**Solution**
Accepted by BizTalk	Messages with the status "Accepted by BizTalk" were successfully sent to BizTalk Server. Depending on the backup method you employed for your Documentshome directory, the audit trail may not contain copies of some XML messages that were processed. If you archive incoming EDI messages from your trading partner before sending them to the receive location for the BizTalk Server receive port, you will have archived copies of the original EDI messages.
In internal format	Messages with the status "In internal format" are in one of two states: • The message has been successfully processed (accepted) by BizTalk Server but the audit trail was not updated. • The message must still be processed (accepted) by BizTalk Server. Perform the following tasks: c. Run an EDI report in HAT and compile a list of the most recent EDI messages written to the MessageBox and compare that list to the base names of the files stored in the Internal\Inbox folder. d. Delete all files with the status "In internal format" that appear in the recent message list from the Internal\Inbox folder. This prevents the creation of duplicate messages when you restart the services.
Rejected by BizTalk	The message was not accepted by BizTalk Server. This is a final status. You must evaluate the message to determine why BizTalk Server rejected it and then reprocess it through your back-end system.
In external format	Messages with the status "In external format" were successfully translated from XML to EDI format but the **audin** database may not have been updated to reflect the current status of the messages. Perform the following tasks: e. Make a list of all files in the External\Inbox folder with the file extension *.imi. f. Compare the base names of the *.imi files with the numbers listed in the icin column of the **audin** table. g. Rename or delete any *.imi file in the External\Inbox folder that

	does not appear in the **audin** table with the status "In external format."

Compare outgoing message lists, resolve data loss, and resynchronize the audit trail

1. Compare the list of messages referenced in the database that you compiled in the second step ("Evaluate the status of all messages") with the list of files in the Internal and External Inbox/Outbox folders that you compiled in the first step ("List the files in the Documentshome directory and all subdirectories ").

2. Resolve the missing or partially processed data and resynchronize the audit trail if necessary. Use the descriptions in the following table to work with outgoing messages according to their status in the audit trail.

Outgoing Message Status (audout Table)	Solution
Sent	Outgoing messages with the status "Sent" were successfully sent to your trading partner. Depending on the backup method you employed for your Documentshome directory, the audit trail may not contain copies of some XML and EDI messages that were processed. It is possible to reconstruct the XML message body if you enabled message body tracking in BizTalk Server.
Communication failed	Outgoing messages with the status "Communication failed" either could not be written to the designated Put folder assigned to the BizTalk Server send port, or the time-out for receiving a functional acknowledgement from your trading partner was exceeded. This is a final status. Depending on the backup method you employed for your Documentshome directory, the audit trail may not contain copies of some XML and EDI messages that were processed. You must evaluate the problem writing to the Put folder and then reprocess the XML message from BizTalk Server.
In internal format	Outgoing messages with the status "In internal format" were successfully received from BizTalk Server and written to the Internal\Outbox folder; however, the database may not have been updated. Perform the following tasks: a. Make a list of all messages in the Internal\Outbox folder with the extension *.imo. b. Evaluate the numbers in the msgout column of the **audout** table and find the numbers that match the base name of the *.imo files in the Internal\Outbox folder. c. Delete all *.imo files from the Internal\Outbox folder that

	do not have a match in the msgout column.
Translation in progress	Outgoing messages with the status of "Translation in progress" are in one of two states: • The file has been translated to external format but the database was not updated to reflect its status. • Translation of the file to external format did not conclude at the time the problem occurred. To reconcile messages with the status "Translation in progress," perform the following tasks: f. Make a list of all messages in the Internal\Outbox folder with the extension *.imo. g. Evaluate the numbers in the msgout column of the audout table. h. Delete all *.imo messages in the Internal\Outbox folder that have a corresponding match in the msgout column.
In external format	Outgoing messages with the status "in external format" can be in one of two states: • The messages were successfully translated into EDI format but have not been combined into a single interchange (in the case outbound batching) or sent to your trading partner. • The messages were successfully translated to EDI format and sent to the Put folder defined on the BizTalk Server send port; however, the database was not updated to reflect the status of "Sent." Perform the following tasks: k. Make a list of all the files in the External\Outbox with the extension *.out. l. Cross-reference the names of the *.out files with the numbers appearing in the icout column in the audout table. m. Delete all *.out files in the External\Outbox folder that do not have a matching reference number in the icout column. n. Make a list of all the files in the Put folder (as defined on the BizTalk Server send port) that match the defined file mask (#.edi by default).

	o. Cross-reference the messages appearing in the icout column of the audout table with the base file name of the files appearing in the designated Put folder for the send port. p. Delete all the messages in the Put folder that match the reference numbers in the icout column.

How to Generate an Engine Input File

After restoring the Base EDI Adapter, you must run the compeif.exe command and restart the BizTalk Base EDI Service. The Compeif.exe command uses the information in the BizTalk EDI database to generate an Engine Input File (EIF), which is used by the BizTalk Base EDI Service to parse and serialize EDI documents.

Prerequisites

You must be logged on as a member of the BizTalk Server Administrators group to perform this procedure.

To generate an Engine Input File

1. Click **Start**, click **Run**, and then type **cmd**.
2. At the command prompt, type:

   net start "edi subsystem"

3. At the command prompt, type **compeif.exe**.

   Compeif.exe recompiles the EDI repository

4. After the **compeif.exe** has completed, at the command prompt, type:

   net start "edi subsystem"

Resolving Data Loss

Recovering lost data can be difficult or impossible. The topics in this section describe processes you can follow to help minimize data loss.

In This Section

- Resolving Data Loss of In-Progress Orchestrations
- Identifying Lost HAT Data
- Marking In-Progress Transactions as Complete in BAM

Resolving Data Loss of In-Progress Orchestrations

MessageBox databases contain the state of orchestrations that are currently in progress. Although there is no way to tell exactly what data has been lost from the MessageBox databases, there are some steps you can take to gather information about the lost data:

- Determine what messages have been sent and received in the current orchestrations, and what external systems have been used after the point of recovery. For example, if your system maintains an external log of messages and events, you can examine that log. You may also need to manually review the external systems to see what activities have occurred.

- After you determine the cause of the data loss, you can begin to correct the restored system, deciding which processes can continue, which processes must be terminated and restarted (by resubmitting the lost activation messages), and which processes have completed successfully and can be terminated. This process depends largely on the architecture of your system and must be considered as part of your system recovery planning.

Identifying Lost HAT Data

BizTalk Server provides two sets of tools that you can use to identify which Health and Activity Tracking (HAT) data has been lost as a result of a system failure, the HAT operations tools and the HAT reporting tools.

HAT operations tools

You can use the HAT operations tools to determine which services were active at the time the MessageBox was recovered. One tool, the Operation View tool, enables you to see what is in the MessageBox database that you backed up before the system failure.

Because there is a gap between the time that the database was recovered and the time of the system failure, the state of these and other transactions that may have started is in doubt.

HAT reporting tools

You can use the HAT reporting tools for viewing system events. Use these tools to identify which service instances completed and started after the point of recovery, as follows:

- Look for which instances completed or started since the last time you backed up the database.

- If data in the BizTalk Tracking database indicates that the message started but did not complete, and the message is not in the database, then that message was sent after the last backup.

HAT can report on any service that completed, and it can indicate that a service started. Tracking data is first staged to the MessageBox and then moved to the BizTalk Tracking

database. The data that was staged may have been lost to the backlog of the BAM Event Bus service.

While all databases need to be restored to the same mark for operational reasons, you can use a BizTalk Tracking database (that was not lost) in Archive mode to see what happened after the mark.

If Reporting shows a service instance as having completed, you can terminate that instance. Reporting may show instances that started after the point of recovery. If so, you will need to compensate for any actions these instances took and then resubmit their initial activation messages.

You can use the Orchestration Debugger in Reporting to see the last shapes that executed, and then use Message Flow to see what message should have been sent or received.

If the BizTalk Tracking database was lost, all discovery of what happened past the point of recovery will need to be done by using the external systems reporting mechanisms.

Marking In-Progress Transactions as Complete in BAM

Business Activity Monitoring (BAM) keeps data for incomplete trace instances in a special active instance table. If some instance records were started before the last backup but completed after the backup, those records will remain in the active instance table. Although this does not prevent the system from functioning, you can manually mark these records as completed so that they can be moved out of the active instance table.

A list of incomplete ActivityIDs for a given activity can be determined by issuing the following query against the BAM Primary Import database:

Advanced Information About Backup and Restore

The topics in this section describe the backup and restore processes in more detail and are intended to be used by advanced users with a thorough understanding of BizTalk Server.

In This Section

- Marked Transactions, Full Backups, and Log Backups
- Log Shipping
- How to Schedule the Backup BizTalk Server Job
- How to Back Up Custom Databases
- How to Create a Linked Server
- Viewing the History of Restored Backups

Marked Transactions, Full Backups, and Log Backups

The Backup BizTalk Server Job creates synchronized backups of all BizTalk Server databases by using full database backups and transaction log backups, in conjunction with a type of transaction known as a *marked transaction*. Marked transactions are transactions that place a mark into the transaction log of all databases participating in the transaction. The marked transaction blocks new distributed transactions from starting, waits for the distributed transactions that are currently running to complete, and then executes to place the mark.

The mark represents a transaction point that is consistent across all databases; you can use the mark with subsequent log backups to restore your databases to that point.

For each BizTalk Server database, the Backup BizTalk Server job creates a marked transaction log backup every time it runs, and it creates a full backup based on a time period that you specify.

Full backups

When you run the Backup BizTalk Server job it runs the first backup process, *BackupFull*, once every period (not every time the job runs). For more information about how to schedule the Backup BizTalk Server job, see How to Schedule the Backup BizTalk Server Job.

The first time the Backup BizTalk Server job runs during a new period, it performs a full backup. For example, if you schedule the job to run every hour but configure the period to be daily, the Backup BizTalk Server job performs a full backup the first time it runs, and then every day at midnight.

Transaction log backups

The second process that the Backup BizTalk Server job performs is *MarkAndBackupLog*. This process places a mark in all BizTalk Server databases and performs a transaction log backup every time the job executes.

The mark is the string created by using <*ServerName*>_<*DatabaseName*>_Log_<*LogMarkName*>_<*Timestamp*>.bak, where the <*Log Mark Name*> is configured in the SQL Server Agent job. This mark must be used when restoring the last log to each database.

For more information, see "Transaction Log Backups" and "Backup and Recovery of Related Databases" in SQL Server Books Online.

Log Shipping

Log shipping provides standby server capabilities, which reduces downtime in the event of a system failure.

Due to the distributed database design of BizTalk Server 2006, when you produce backups you must be certain to provide a consistent point to which the backups can be restored. Transactions can span multiple databases; if one database goes offline and must be

restored, then all related databases must be restored to a single point in time to ensure that the system is in a consistent state.

The Backup BizTalk Server job uses Microsoft SQL Server log marking to provide an automated process that produces database backup sets. These backup sets include synchronized points that are used during the restoration process. As part of the process of restoring a set of databases produced by the Backup BizTalk Server job, the last log backup file for each database is restored to a specific log mark. When the SQL Server implementation of log shipping is applied to BizTalk Server databases, there is no final log to restore to the mark.

How to Schedule the Backup BizTalk Server Job

The Backup BizTalk Server job runs as scheduled by the SQL Server Agent service. If you want to create more frequent or less frequent backups, you can change the schedule of the Backup BizTalk Server job by using SQL Server Enterprise Manager.

Prerequisites

You must be logged on as a member of the Administrators group to perform this procedure.

To schedule the Backup BizTalk Server job

1. On the computer that contains the BizTalk Management database, open SQL Server Enterprise Manager. Click **Start**, click **Run**, type **"SQL Server Enterprise Manager.msc"** and then click **OK**.

2. Open the appropriate server by clicking it, double-clicking **Management**, double-clicking **SQL Server Agent**, and then click **Jobs**.

3. In the details pane, right-click the **Backup BizTalk Server** job, and then click **Properties**.

4. In the **Backup BizTalk Server Properties** dialog box, click the **Steps** tab, click **BackupFull**, and then click **Edit**.

5. On the **General** tab, in the **Command** box, edit the command by changing the frequency to the desired interval at which to perform a full backup: **'h'** (hourly), **'d'** (daily), **'w'** (weekly), **'m'** (monthly), **'y'** (yearly), and then click **OK**.

6. On the **Schedules** tab, click **MarkAndBackupLogSched**, and then click **Edit**.

7. In the **Edit Job Schedule** dialog box, click **Recurring** (if it is not already selected), and then click **Change**.

   By default, the job is scheduled to run every 15 minutes.

8. In the **Edit Recurring Job Schedule** dialog box, update the schedule as desired, and then click **OK**.

9. In the **Edit Job Schedule** dialog box, click **OK**.

10. In the **Backup BizTalk Server Properties** dialog box, click **OK**.

How to Back Up Custom Databases

Because your custom databases are not installed with BizTalk Server 2006, they are not included in the default list of databases to be marked and backed up by the Backup BizTalk Server job. If you want the Backup BizTalk Server job to back up your custom databases, you must manually add the databases to the Backup BizTalk Server job.

Prerequisites

To back up your custom databases, you must be logged on with a user account that has access to each of the databases you are backing up.

BizTalk Server includes a SQL Server role named BTS_BACKUP_USERS so that the user account you use to back up your databases does not require System Administrator permissions within SQL Server, except for the primary server controlling the backup process.

When setting up the user account that you are using to back up your databases, note the following:

- You must configure the SQL Server Agent service to run under a domain account or a local account with a mapped user on each instance of SQL Server.
- You must configure a SQL Server logon account for this user, and assign this user to the BizTalk BTS_BACKUP_USERS role on each server.
- You must assign this user to the System Administrators role within SQL Server for the BizTalk Management database server.

To add custom databases to the Backup BizTalk Server job

1. Build the objects in the new database:
   - Browse to the <*installation directory*>\Program Files\Microsoft BizTalk Server 2006\Schema directory, and then run Backup_Setup_All_Procs.sql and Backup_Setup_All_Tables.sql in the destination database. This creates the necessary procedures, table, and role and assigns permissions to the stored procedures.
2. Perform the following configurations:
   - Link the SQL server that is hosting the BizTalk Management database to the SQL server hosting the new database. The account used to run the SQL Server Agent service on the Mgmt SQL Server must be either a domain account or a local account that is mapped to each computer holding a database to be backed up. If the

databases are on the same computer you can skip this step. This is done automatically.

- Add a login on the SQL server hosting the new database for the account running the SQL Server Agent service on the Mgmt SQL Server. If the databases are on the same computer you can skip this step.

- Add a user in the new database for the login created in the previous step and add them to the BTS_BACKUP_USERS role. This role is created and granted Execute permissions on the necessary procedures by the scripts in step 1.

3. Using SQL Server Enterprise Manager, in the BizTalk Management database, modify the **adm_OtherBackupDatabases** table to include a row for each of your custom databases.

4. Type the new server and database names in the corresponding columns, as shown in the following table.

Column	Value
DefaultDatabaseName	The friendly name of your custom database.
DatabaseName	The name of your custom database.
ServerName	The name of the computer running SQL Server.
BTSServerName	The name of the SQL Server database.

The next time you run the Backup BizTalk Server job, it will back up your custom databases.

How to Create a Linked Server

As a part of the backup and restore process, the Backup BizTalk Server job automatically creates linked servers. If necessary, however, you can manually create linked servers.

In a distributed BizTalk Server 2006 environment, where databases exist on multiple servers, you must configure linked servers from your BizTalk Management database server to all of the remote servers.

After you create the linked servers, you must configure them because the backup process for BizTalk Server uses four-part naming to execute stored procedures on all databases in the BizTalk Server environment.

On the BizTalk Management database server, you add the linked servers by using SQL Server Enterprise Manager.

Prerequisites

You must be logged on as a member of the Administrators group to perform this procedure.

To create a linked server

1. Open SQL Server Enterprise Manager. Click **Start**, click **Run**, type **"SQL Server Enterprise Manager.msc"** and then click **OK**.

2. In SQL Server Enterprise Manager, select the appropriate BizTalk server, and then click the **Security** folder.

3. Right-click the **Linked Servers** folder, and then click **New Linked Server**.

4. In the **Linked Server Properties - New Linked Server** dialog box, complete the dialog box as appropriate for your server.

Viewing the History of Restored Backups

To determine the last successful backup set restored, review the contents of the Master.dbo.bts_LogShippingHistory table. This table is populated by the Get Backup History job and updated by the Restore Databases job. When a backup is successfully restored, the Restored column is set to 1 and the RestoredDateTime is set to the current date and time.

When all of the databases being restored to the server from a particular backup set have been successfully restored, that backup set ID is written to the Master.dbo.bts_LogShippingLastRestoreSet table.

Gaps in the restore process

When reviewing records in the Master.dbo.bts_LogShippingHistory table, you may find gaps in the sets restored. This can occur for several reasons. However, you can still recover the stability of your destination system (which are your backup computers), even when gaps have occurred. A gap must be followed by a restore of a full backup set to repair the destination system. If a gap is not followed by a full backup set restore, the destination environment is not stable.

Archiving and Purging the BizTalk Tracking Database

As BizTalk Server processes more and more data on your system, the BizTalk Tracking (BizTalkDTADb) database continues to grow in size. Unchecked growth decreases system performance and may generate errors in the Tracking Data Delivery Service (TDDS). In addition to general tracking data, tracked messages can also accumulate in the MessageBox database, causing poor disk performance.

While previous versions of BizTalk Server included sample scripts for archiving tracked messages and purging the BizTalk Tracking database, BizTalk Server 2006 automates both processes using the DTA Purge and Archive job. By archiving and purging data from the BizTalk Tracking database, you can maintain a healthy system, as well as keep your tracking data archived for future use. Because BizTalk Tracking database archives accumulate over time and consume disk space, it is a good idea to move the BizTalk Tracking database archives to secondary storage on a regular basis.

When you purge data from the BizTalk Tracking database, the DTA Purge and Archive job purges different types of tracking information such as message and service instance information, orchestration event information, and rules engine tracking data.

In the DTA Archive and Purge job, you configure the LiveHours and LiveDays parameters. The sum of the LiveHours and LiveDays parameters is the live window of data you want to maintain in your BizTalk Server environment. All data associated with a completed instance older than this live window of data is deleted.

The age of a tracking data record is based on the time the tracking data was inserted into the BizTalk Tracking database. The DTA Purge and Archive job uses the timestamp to continuously verify whether the record is older than the live window of data. After every live window period, the BizTalk Tracking database is archived and all completed tracking data older than the live window period are purged.

Following is an example of how the purge feature works, and a description of a hard purge:

- **How purging works**: In this example, you configure the SQL Server Agent job to run every 10 minutes and you create an archive every 24 hours. The first time the SQL Server Agent job runs, it creates a backup of the database and creates the archive. All data associated with instances that completed over 24 hours ago is deleted. Each time the job runs, completed data over 24 hours old is deleted. On the 144th run (after 24 hours), a new archive is created that contains the next 24-hour segment.

  The time stamp of the last backup is stored in the BizTalk Tracking (BizTalkDTADb) database and is used in the purge logic to ensure that data is deleted only if it is in the previous archive. Archives are overlapped by approximately 10 minutes in order to reduce the chances that an instance has some data in one archive and the rest of the data in a second archive.

- **Hard purge**: Because only data associated with completed instances is deleted, if you have an infinite number of looping instances that run indefinitely, then your tracking database would grow and would never be able to purge. The hard purge date allows all information older than the specified date to be deleted except for information indicating a service's existence (that is, the row in the ServiceInstances table). The hard purge setting should always be greater than your normal purge setting.

Archiving and purging includes the features described in the following table:

Feature	Description
Hard purge option	Enables you to configure a time interval to delete information older than a specified date.
Copying tracked messages to tracking database	Using the CopyTrackedMessageToDTA option, you can directly copy tracked messages from the MessageBox servers to your BizTalk Tracking database using a linked server.
Archive validation	Enables you to optionally set up a secondary database server to validate the archives as they are created.
Health and Activity Tracking	Enables you to use the HAT with old BizTalk Tracking

(HAT) support for multiple BizTalk Tracking database versions	database archives even if the current and previous schemas are different.
Reduction of tracking data	Substantially reduces the amount of tracking data generated without reducing any tracking information stored. This results in slower growth of the tracking database.
Faster HAT operations, significant optimization in database schemas	Enables you to use HAT tasks for finding messages and service instances on large databases; this feature has been significantly optimized.

In This Section

- Checklist: Archiving and Purging the BizTalk Tracking Database
- How to Configure the BTS_BACKUP_USERS Role for Archiving and Purging Data from the BizTalk Tracking Database
- How to Configure the DTA Purge and Archive Job
- How to Purge Data from the BizTalk Tracking Database
- How to Manually Purge Data from the BizTalk Tracking Database
- How to Enable Automatic Archive Validation
- How to Copy Tracked Messages into the BizTalk Tracking Database

Checklist: Archiving and Purging the BizTalk Tracking Database

Step	Reference
Read the Archiving and Purging overview to become more familiar with the process of archiving and purging tracking data.	Archiving and Purging the BizTalk Tracking Database
Although you can run the DTA Purge and Archive job using your log on credentials, for added security, should configure the BTS_BACKUP_USERS role with the necessary SQL Server credentials to run the DTA Purge and Archive job. This helps to prevent elevation of privileges.	How to Configure the BTS_BACKUP_USERS Role for Archiving and Purging Data from the BizTalk Tracking Database
Configure the DTA Purge and Archive job.	How to Configure the DTA Purge and Archive Job
Run the DTA Purge and Archive job, which archives the data in your BizTalk Tracking (BizTalkDTADb) database	How to Purge Data from the

and purges old data.	BizTalk Tracking Database
Optionally, you can manually purge data from the BizTalk Tracking (BizTalkDTADb) database.	How to Manually Purge Data from the BizTalk Tracking Database
Enable automatic validation of the archived data from the BizTalk Tracking (BizTalkDTADb) database.	How to Enable Automatic Archive Validation
Copy tracked messages into the BizTalk Tracking (BizTalkDTADb) database.	How to Copy Tracked Messages into the BizTalk Tracking Database

How to Configure the BTS_BACKUP_USERS Role for Archiving and Purging Data from the BizTalk Tracking Database

The DTA Purge and Archive (BizTAlkDTADb) job normally runs using the credentials of the logged-on SQL Server Agent service account user. For added security, however, you can configure the DTA Purge and Archive (BizTalkDTADb) job to run using the credentials of an account which is a member of the BTS_BACKUP_USERS role. This helps to prevent elevation of privileges by running SQL Server Agent jobs under accounts with essential permissions.

Prerequisites

You must be logged on with an account that is a member of the SQL Server sysadmin fixed server role to perform this procedure.

To configure the BTS_BACKUP_USERS role for archiving and purging data from the BizTalk Tracking database (SQL Server 2000)

1. Click **Start**, click **Programs**, click **Microsoft SQL Server**, and then click **Enterprise Manager**.

2. Open the appropriate server by clicking it, double-click **Databases**, double-click **BizTalkDTADb**, and then click **Roles**.

3. In the details pane, double-click **BTS_BACKUP_USERS**.

4. In the **Database Role Properties – BTS_BACKUP_USERS** dialog box, click **Add**.

5. In the **Add Role Members** dialog box, select an account with SQL Server Agent Service credentials, and then click **OK**.

To configure the BTS_BACKUP_USERS role for archiving and purging data from the BizTalk Tracking database (SQL Server 2005)

1. Click **Start**, click **Programs**, click **Microsoft SQL Server 2005**, and then click **SQL Server Management Studio**.

2. In the **Connect to Server** dialog box, specify the name of the SQL Server where the BizTalk Tracking (BizTalkDTADb) database resides and the appropriate authentication type, and then click **Connect** to connect to the appropriate SQL Server.

3. In **Microsoft SQL Server Management Studio**, double-click **BizTalkDTADb**, double-click **Security**, double-click **Roles**, and then double-click **Database Roles**.

4. In the details pane, double-click **BTS_BACKUP_USERS**.

5. In the **Database Role Properties – BTS_BACKUP_USERS** dialog box, under **Members of this role**, click **Add**.

6. In the **Select Database User or Role** dialog box, enter a user account with SQL Server Agent Service credentials, and then click **OK**.

How to Configure the DTA Purge and Archive Job

Before you can archive or purge data from the BizTalk Tracking (BizTalkDTADb) database, you must configure the DTA Purge and Archive (BizTalkDTADb) job. This job is configured to call the stored procedure dtasp_BackupAndPurgeTrackingDatabase, which uses the six parameters you must configure in this job.

Prerequisites

You must be logged on with an account that is a member of the SQL Server sysadmin fixed server role to perform this procedure.

To configure the DTA purge and archive job (SQL Server 2000)

1. Click **Start**, click **Programs**, click **Microsoft SQL Server**, and then click **Enterprise Manager**.

2. Open the appropriate server by clicking it, double-click **Management**, double-click **SQL Server Agent**, and then click **Jobs**.

3. In the details pane, right-click **DTA Purge and Archive (BizTalkDTADb)**, and then click **Properties**.

4. In the **DTA Purge and Archive (BizTalkDTADb) Properties** dialog box, click the **Steps** tab, click **Archive and Purge**, and then click **Edit**.

5. On the **General** tab, in the **Command** box, edit the following parameters as appropriate, and then click **OK**.

   - @nLiveHours tinyint — Any completed instance older than the (live hours) + (live days). Default is 0 hours.

   - @nLiveDays tinyint — Will be deleted along with all associated data. Default interval is 1 day.

   - @nHardDeleteDays tinyint — All data (even if incomplete) older than this will be deleted. The time interval specified for HardDeleteDays should be greater than the live window of data. The live window of data is the interval of time for which you want to maintain tracking data in the BizTalk Tracking (BizTalkDTADb) database.

Anything older than this interval is eligible to be archived at the next archive and then purged. Default is 30 days.

- @nvcFolder nvarchar(1024) — Folder in which to put the backup files.
- @nvcValidatingServer sysname — Server on which validation will be done. NULL value indicates no validation is being done. Default is NULL.
- @fForceBackup int — Default is 0. This is reserved for future use.

6. In the details pane, right-click the **DTA Purge and Archive (BizTalkDTADb)** job, and then click **Enable Job**.

   In the **Enabled** column, the status changes to **Yes**.

To configure the DTA purge and archive job (SQL Server 2005)

1. Click **Start**, click **Programs**, click **Microsoft SQL Server 2005**, and then click **SQL Server Management Studio**.
2. In the **Connect to Server** dialog box, specify the name of the SQL Server where the BizTalk Tracking (BizTalkDTADb) database resides and the appropriate authentication type, and then click **Connect** to connect to the appropriate SQL Server.
3. In **Microsoft SQL Server Management Studio**, double-click **SQL Server Agent**, and then click **Jobs**.
4. In the details pane, right-click **DTA Purge and Archive (BizTalkDTADb)**, and then click **Properties**.
5. In the **Job Properties - DTA Purge and Archive (BizTalkDTADb)** dialog box, under **Select a page**, click **Steps**.
6. In the **Job step list**, click **Archive and Purge**, and then click **Edit**.
7. On the **General** page, in the **Command** box, edit the following parameters as appropriate, and then click **OK**.
   - @nLiveHours tinyint — Any completed instance older than the (live hours) + (live days). Default is 0 hours.
   - @nLiveDays tinyint — Will be deleted along with all associated data. Default interval is 1 day.
   - @nHardDeleteDays tinyint — All data (even if incomplete) older than this will be deleted. The time interval specified for HardDeleteDays should be greater than the live window of data. The live window of data is the interval of time for which you want to maintain tracking data in the BizTalk Tracking (BizTalkDTADb) database. Anything older than this interval is eligible to be archived at the next archive and then purged. Default is 30 days.

- @nvcFolder nvarchar(1024) — Folder in which to put the backup files.
- @nvcValidatingServer sysname — Server on which validation will be done. NULL value indicates no validation is being done. Default is NULL.
- @fForceBackup int — Default is 0. This is reserved for future use.

8. On the **Job Properties - DTA Purge and Archive (BizTalkDTADb)** dialog box, under **Select a page**, click **General**, select the **Enabled** check box, and then click **OK**.

How to Purge Data from the BizTalk Tracking Database

When you purge data from the BizTalk Tracking (BizTalkDTADb) database, the DTA Purge and Archive job purges different types of tracking information such rules engine artifacts, service instance information, and orchestration event information from the BizTalk Tracking (BizTalkDTADb) database.

Prerequisites

You must be logged on with an account that is a member of the SQL Server sysadmin fixed server role to perform this procedure.

To purge data from the BizTalk Tracking database (SQL Server 2000)

1. Click **Start**, click **Programs**, click **Microsoft SQL Server**, and then click **Enterprise Manager**.
2. Open the appropriate server by clicking it, double-click **Management**, double-click **SQL Server Agent**, and then click **Jobs**.
3. In the details pane, right-click **DTA Purge and Archive (BizTalkDTADb)**, and then click **Properties**.
4. In the **DTA Purge and Archive (BizTalkDTADb) Properties** dialog box, click the **Steps** tab, click **Archive and Purge**, and then click **Edit**.
5. On the **General** tab, in the **Command** box, change **exec dtasp_BackupAndPurgeTrackingDatabase** to **exec dtasp_PurgeTrackingDatabase**.
6. In the **Command** box, edit the following parameters as appropriate, and then click **OK**.
   - @nHours tinyint — Any completed instance older than (live hours) + (live days).
   - @nDays tinyint — Will be deleted along with all associated data. Default interval is 1 day.
   - @nHardDays tinyint — All data older than this day will be deleted, even if the data is incomplete. The time interval specified for HardDeleteDays should be greater

than the live window of data. The live window of data is the interval of time for which you want to maintain tracking data in the BizTalk Tracking (BizTalkDTADb) database. Anything older than this interval is eligible to be archived at the next archive and then purged.

- @dtLastBackup — Set this to NULL.

7. In the details pane, right-click the **DTA Purge and Archive (BizTalkDTADb)** job, and then click **Enable Job**.

8. In the **Enabled** column, the status changes to **Yes**.

To purge data from the BizTalk Tracking database (SQL Server 2005)

1. Click **Start**, click **Programs**, click **Microsoft SQL Server 2005**, and then click **SQL Server Management Studio**.

2. In the **Connect to Server** dialog box, specify the name of the SQL Server where the BizTalk Tracking (BizTalkDTADb) database resides and the appropriate authentication type, and then click **Connect** to connect to the appropriate SQL Server.

3. In **Microsoft SQL Server Management Studio**, double-click **SQL Server Agent**, and then click **Jobs**.

4. In the details pane, right-click **DTA Purge and Archive (BizTalkDTADb)**, and then click **Properties**.

5. In the **Job Properties - DTA Purge and Archive (BizTalkDTADb)** dialog box, under **Select a page**, click **Steps**.

6. In the **Job step list**, click **Archive and Purge**, and then click **Edit**.

7. In the **Job Step Properties - Archive and Purge** dialog box, on the **General** page, in the **Command** box, change **exec dtasp_BackupAndPurgeTrackingDatabase** to **exec dtasp_PurgeTrackingDatabase**.

8. In the **Command** box, edit the following parameters as appropriate, and then click **OK**.

- @nHours tinyint — Any completed instance older than (live hours) + (live days).

- @nDays tinyint — Will be deleted along with all associated data. Default interval is 1 day.

- @nHardDays tinyint — All data older than this day will be deleted, even if the data is incomplete. The time interval specified for HardDeleteDays should be greater than the live window of data. The live window of data is the interval of time for which you want to maintain tracking data in the BizTalk Tracking (BizTalkDTADb) database. Anything older than this interval is eligible to be archived at the next archive and then purged.

- @dtLastBackup — Set this to NULL.

9. On the **Job Properties - DTA Purge and Archive (BizTalkDTADb)** dialog box, under **Select a page**, click **General**, select the **Enabled** check box, and then click **OK**.

How to Manually Purge Data from the BizTalk Tracking Database

The DTA Archive and Purge SQL Server Agent job reduces the need to manually purge data from the BizTalk Tracking (BizTalkDTADb) database due to continuous purging of the database and compaction of stored tracking data. You might need to manually purge data if your BizTalk Tracking (BizTalkDTADb) database has grown so much that sustained performance degradation is occurring and the DTA Archive and Purge job is unable to keep up with the database growth.

Prerequisites

You must be logged on with an account that is a member of the SQL Server sysadmin fixed server role to perform this procedure.

To manually purge data from the BizTalk Tracking database (SQL Server 2000)

1. Backup your BizTalk Server databases.
2. Archive the BizTalk Tracking (BizTalkDTADb) database.
3. Open Services. Click **Start**, click **Run**, and then type **services.msc**.
4. Right-click each of the following services, and then click **Stop**:
   - BizTalk Base EDI Service
   - BizTalk Service BizTalk Group: BizTalkServerApplication
   - Enterprise Single Sign-On Service
   - Rule Engine Update Service
5. Click **Start**, click Run, type **cmd**, and then click **OK**.
6. At the command prompt, type:

   net stop iisadmin /y

   This stops the IIS Admin Service and all dependent services, one-by-one. Write down the list of services as each one is stopped. You will need to use this list of services later when you restart IIS.

Below is an example of the output you will see after issuing this command (the dependent services listed on your computer may vary):

7. Click **Start**, click **Run**, type **isqlw.exe**, and then click **OK**.

8. In the **Connect to SQL Server** dialog box, specify the name of the SQL Server where the BizTalk Tracking (BizTalkDTADb) database resides and the appropriate authentication type to connect to the appropriate SQL Server.

9. In SQL Query Analyzer, click the **BizTalkDTADb** database, click **Stored Procedures**, right-click **dbo.dtasp_PurgeAllCompletedTrackingData**, and then click **Open**.

10. In the **Execute Procedure** dialog box, click **Execute**.

    This stored procedure deletes all tracking data associated with completed instances regardless of their completion time.

11. Open Services. Click **Start**, click **Run**, and then type **services.msc**.

12. Right-click each of the following services, and then click **Start**:

    - BizTalk Base EDI Service
    - BizTalk Service BizTalk Group: BizTalkServerApplication
    - Enterprise Single Sign-On Service
    - Rule Engine Update Service

13. Click **Start**, click Run, type **cmd**, and then click **OK**.

14. At the command prompt, restart each of the IIS services that you stopped in step 6. Type:

    net start <*IISserviceName*>

    Where <*IISserviceName*> is the name of the IIS service you want to restart. You must repeat this command for each of the IIS services.

To manually purge data from the BizTalk Tracking database (SQL Server 2005)

1. Backup your BizTalk Server databases.

2. Archive the BizTalk Tracking (BizTalkDTADb) database.

3. Open Services. Click **Start**, click **Run**, and then type **services.msc**.

4. Right-click each of the following services, and then click **Stop**:

    - BizTalk Base EDI Service

- BizTalk Service BizTalk Group: BizTalkServerApplication
- Enterprise Single Sign-On Service
- Rule Engine Update Service

5. Click **Start**, click Run, type **cmd**, and then click **OK**.

6. At the command prompt, type:

   net stop iisadmin /y

   This stops the IIS Admin Service and all dependent services, one-by-one. Write down the list of services as each one is stopped. You will need to use this list of services later when you restart IIS.

   Below is an example of the output you will see after issuing this command (the dependent services listed on your computer may vary):

7. Click **Start**, click **Programs**, click **Microsoft SQL Server 2005**, and then click **SQL Server Management Studio**.

8. In the **Connect to Server** dialog box, specify the name of the SQL Server where the BizTalk Tracking (BizTalkDTADb) database resides and the appropriate authentication type, and then click **Connect** to connect to the appropriate SQL Server.

9. In **Microsoft SQL Server Management Studio**, double-click **Databases**, double-click the **BizTalkDTADb** database, double-click **Programmability**, and then click **Stored Procedures**.

10. In the details pane, right-click **dtasp_PurgeAllCompletedTrackingData**, and then click **Execute Stored Procedure**.

11. In the **Execute Procedure** dialog box, click **OK**.

    This stored procedure deletes all tracking data associated with completed instances regardless of their completion time.

12. Open Services. Click **Start**, click **Run**, and then type **services.msc**.

13. Right-click each of the following services, and then click **Start**:

    - BizTalk Base EDI Service
    - BizTalk Service BizTalk Group: BizTalkServerApplication
    - Enterprise Single Sign-On Service
    - Rule Engine Update Service

14. Click **Start**, click Run, type **cmd**, and then click **OK**.

15. At the command prompt, restart each of the IIS services that you stopped in step 6. Type:

    net start <*IISserviceName*>

    Where <*IISserviceName*> is the name of the IIS service you want to restart. You must repeat this command for each of the IIS services.

How to Enable Automatic Archive Validation

Archive validation enables to validate the archives as they are created. Before you can enable automatic archive validation, you must set up a secondary database server, also called a validation server. Because the archiving process is a simple backup, it is possible that the actual image stored on the disk can be corrupted due to a hardware issue.

Using the archive validation feature, you can ensure the archive (backup) was successful and can be restored. After an archive is created, the validation server is notified that a new archive has been created. The validation server attempts to restore the archive. A validation server must be another instance of SQL Server different from the one in which the job is running.

If the restore is successful, the validation server communicates this information back to the BizTalk Tracking (BizTalkDTADb) database. Until a successful restore is completed, the purge job will not purge any more data.

If the restore is not successful, the validation server communicates this information back to the BizTalk Tracking database. The purge job creates another archive and awaits validation of the new archive. This prevents the possibility of a corrupted archive causing you to lose tracking data.

Prerequisites

You must be logged on with an account that is a member of the SQL Server sysadmin fixed server role to perform this procedure.

To enable automatic archive validation (SQL Server 2000)

1. On the validation server, click **Start**, click **Run**, type **isqlw.exe**, and then click **OK**.
2. Click **File**, and then click **Connect**.
3. In the **Connect to SQL Server** dialog box, click the server from the list, or click the ellipsis button (**...**) to browse to the SQL server where you can validate the archive by performing a test of the restore process, and then click **OK**.
4. Click **File**, click **Open**, and then browse to the following SQL script:
5. Click **Query**, and then click **Execute**.
6. The BTS_Tracking_ValidateArchive.sql script creates a SQL Server Agent job called ValidateArchive.

7. Click **Start**, click **Programs**, click **Microsoft SQL Server**, and then click **Enterprise Manager**.

   The archiving and purging process potentially accesses\updates databases in different SQL Servers, so you must set up linked servers between the involved SQL Server instances. You must set up linked server between:

   - Each of your BizTalk MessageBox (BizTalkMsgBoxDb) databases and the BizTalk Tracking (BizTalkDTADb) database.
   - The BizTalk Tracking (BizTalkDTADb) database and the validating server for archive validation.

8. Open the appropriate server by clicking it, double-click **Security**, right-click **Linked Servers**, and then click **New Linked Server**.

9. In the **Linked Server Properties - New Linked Server** dialog box, in **Linked server**, enter the name of the server you want to link to.

   For example, the server hosting the BizTalk MessageBox (BizTalkMsgBoxDb) database, BizTalk Tracking (BizTalkDTADb) database, or the validation server.

10. Under **Server type**, click **SQL Server**, and then click **OK**.

11. In SQL Server Enterprise Manager, open the appropriate server by clicking it, double-click **Management**, double-click **SQL Server Agent**, and then click **Jobs**.

12. In the details pane, right-click **ValidateArchive**, and then click **Properties**.

13. In the **ValidateArchive Properties** dialog box, click the **Steps** tab, click **validate**, and then click **Edit**.

14. In the **Edit Job Step** dialog box, on the **General** tab, in the **Command** box, in the command, **exec dtasp_ValidateArchive null, null**, replace null, null with the name of the server hosting the BizTalk Tracking database, surrounded by single quotes, followed by the name of the BizTalk Tracking database, surrounded by quotes, and then click **OK**. For example:

    exec dtasp_ValidateArchive '<*TrackingServerName*>**', '**<*TrackingDatabaseName*>**'**

To enable automatic archive validation (SQL Server 2005)

1. On the validation server, click **Start**, click **Programs**, click **Microsoft SQL Server 2005**, and then click **SQL Server Management Studio**.

2. In the **Connect to Server** dialog box, specify the name of the SQL Server where you can validate the archive by performing a test of the restore process, and then click **Connect** to connect to the appropriate SQL Server.

3. In **Microsoft SQL Server Management Studio**, click **File**, click **Open**, and then click **File**.

4. In the **Open File** dialog box, browse to the following SQL script:

5. Click the **Query** menu, and then click **Execute**.

6. The BTS_Tracking_ValidateArchive.sql script creates a SQL Server Agent job called ValidateArchive.

7. The archiving and purging process potentially accesses\updates databases in different SQL Servers, so you must set up linked servers between the involved SQL Server instances. In **SQL Server Management Studio**, double-click **Server Objects**, right-click **Linked Servers**, and then click **New Linked Server**.

   You must set up linked server between:

   - Each of your BizTalk MessageBox (BizTalkMsgBoxDb) databases and the BizTalk Tracking (BizTalkDTADb) database.

   - The BizTalk Tracking (BizTalkDTADb) database and the validating server for archive validation.

8. In the **New Linked Server** dialog box, on the **General** page, in **Linked server**, enter the name of the server you want to link to.

   For example, the server hosting the BizTalk MessageBox (BizTalkMsgBoxDb) database, BizTalk Tracking (BizTalkDTADb) database, or the validation server.

9. Under **Server type**, click **SQL Server**, and then click **OK**.

10. In **Microsoft SQL Server Management Studio**, double-click **SQL Server Agent**, and then click **Jobs**.

11. In the details pane, right-click **ValidateArchive**, and then click **Properties**.

12. In the **Job Properties - ValidateArchive** dialog box, under **Select a page**, click **Steps**.

13. In the **Job step list**, click **validate**, and then click **Edit**.

14. On the **General** page, in the **Command** box, in the command, **exec dtasp_ValidateArchive null, null**, replace null, null with the name of the server hosting the BizTalk Tracking database, surrounded by single quotes, followed by the name of the BizTalk Tracking database, surrounded by quotes, and then click **OK**. For example:

    exec dtasp_ValidateArchive '<*TrackingServerName*>**', '**<*TrackingDatabaseName*>**'**

How to Copy Tracked Messages into the BizTalk Tracking Database

The archiving and purging process potentially accesses\updates databases in different SQL Servers, so you must set up linked servers between the involved SQL Server instances. You can directly copy tracked messages from the BizTalk MessageBox (BizTalkMsgBoxDb) database server to your BizTalk Tracking (BizTalkDTADb) database using a linked server. You must set up linked server between:

- Each of your BizTalk MessageBox (BizTalkMsgBoxDb) databases and the BizTalk Tracking (BizTalkDTADb) database.
- The BizTalk Tracking (BizTalkDTADb) database and the validating server for archive validation.

Prerequisites

You must be logged on with an account that is a member of the SQL Server sysadmin fixed server role to perform this procedure.

To copy tracked messages into the BizTalk Tracking database (SQL Server 2000)

1. Click **Start**, click **Programs**, click **Microsoft SQL Server**, and then click **Enterprise Manager**.
2. Open the appropriate server by clicking it, double-click **Management**, double-click **SQL Server Agent**, and then click **Jobs**.
3. In the details pane, right-click **CopyTrackedMessages_**<*msgboxname*>, and then click **Properties**.
4. In the **CopyTrackedMessages_**<*msgboxname*> **Properties** dialog box, click the **Steps** tab, click **Purge**, and then click **Edit**.
5. On the **Steps** tab, in the **Command** box, edit the tracking server and database names parameters as appropriate, and then click **OK**.
6. In the details pane, right-click the **CopyTrackedMessages_**<*msgboxname*> job, and then click **Enable Job**.

   In the **Enabled** column, the status changes to **Yes**. The messages will be copied to the BizTalk Tracking (BizTalkDTADb) database.

To copy tracked messages into the BizTalk Tracking database (SQL Server 2005)

1. Click **Start**, click **Programs**, click **Microsoft SQL Server 2005**, and then click **SQL Server Management Studio**.
2. In the **Connect to Server** dialog box, specify the name of the SQL Server where the BizTalk Tracking (BizTalkDTADb) database resides and the appropriate authentication type, and then click **Connect** to connect to the appropriate SQL Server.

3. In **Microsoft SQL Server Management Studio**, double-click **SQL Server Agent**, and then click **Jobs**.

4. In the details pane, right-click **TrackedMessages_Copy_BizTalkMsgBoxDb**, and then click **Properties**.

5. In the **Job Properties - TrackedMessages_Copy_BizTalkMsgBoxDb** dialog box, under **Select a page**, click **Steps**.

6. Under **Job step list**, click **Purge**, and then click **Edit**.

7. In the **Command** box, edit the tracking server and database names parameters as appropriate, and then click **OK**.

8. On the **Job Properties - TrackedMessages_Copy_BizTalkMsgBoxDb** dialog box, under **Select a page**, click **General**, select the **Enabled** check box, and then click **OK**.

The messages will be copied to the BizTalk Tracking (BizTalkDTADb) database.