## Table of Contents

### Chapter 1
**Getting Started with Collaboration Services**

- Introduction ......................................................... 2
- Security Considerations ........................................... 2
- Authentication ...................................................... 2
- Authorization through Administrative Groups and Internet Information Server (IIS) ..................................................... 2
- Web Management Console ......................................... 3
- Connection Modes ................................................... 4
- Configuring Collaboration Services ................................. 5
  - Configure Secure Data Communication .......................... 6
  - Assign a Service Mailbox ........................................ 8
  - Select Recipient Update Service (RUS) .......................... 8
  - Configure Active Directory Access ............................... 9
  - Set Up Logging .................................................... 10
  - Configure Alerting ................................................ 11
  - Configure Synchronization Partners .............................. 11
  - Check License Information ...................................... 15

### Chapter 2
**Organizing Objects for Synchronization**

- Introduction ......................................................... 18
- Creating a Collection for Publication .............................. 18
  - Publish Collection Wizard .................................... 18
- Enabling or Disabling a Collection ................................ 26
- Editing a Collection ................................................ 26
- Subscribing to a Collection ....................................... 27
  - Modifying Subscription Properties ............................. 28
- Unsubscribing from a Collection .................................. 29
- Removing a Collection ............................................ 29
- Viewing Collection Settings and Synchronization Statistics ......................................................... 30
CHAPTER 3
RESOLVING SYNCHRONIZATION CONFLICTS ................. 31
WHAT CAN CAUSE SYNCHRONIZATION CONFLICTS? ........ 32
HOW CAN CONFLICTS BE RESOLVED? .................. 32
AUTOMATIC CONFLICT RESOLUTION ....................... 33
DELETION ............................................. 34
MATCHING ............................................. 36
PRE-MATCHING ....................................... 37
MANUAL CONFLICT RESOLUTION ......................... 40
APPLYING APPROVED OBJECTS ......................... 41

CHAPTER 4
MANAGING THE SYNCHRONIZATION PROCESS ............... 43
CONFIGURING THE SYNCHRONIZATION PROCESS ........... 44
GENERAL SETTINGS ................................ 45
SYNCHRONIZATION SETTINGS FOR ACTIVE DIRECTORY
OBJECTS ............................................ 46
FREE/BUSY INFORMATION SYNCHRONIZATION SETTINGS 50
CALENDAR INFORMATION SYNCHRONIZATION SETTINGS 53
USING THE PACKET QUEUE AS INTERIM DATA STORAGE . 54
SUSPENDED OBJECT STORAGE .......................... 56
MANUAL OPERATIONS .................................. 56

CHAPTER 5
TRANSPORT MANAGEMENT ............................... 59
OVERVIEW ........................................... 60
SEND .................................................. 60
RECEIVE .............................................. 61
SCHEDULING ........................................ 62
LIMITING TRAFFIC RATES .................................. 62
OUTGOING TRAFFIC .................................. 63
INCOMING TRAFFIC .................................... 63

CHAPTER 6
FINE-TUNING AND MAINTENANCE .......................... 65
ACTIVE DIRECTORY SYNCHRONIZATION PERFORMANCE 66
RESOURCE THROTTLING ............................... 66
Getting Started with Collaboration Services

- Introduction
- Security Considerations
- Web Management Console
- Configuring Collaboration Services
Introduction

Quest® Collaboration Services™ securely synchronizes Active Directory and Exchange data (such as users, groups, distribution lists, contacts, calendar, and free/busy information) between isolated forests in a multi-forest/multi-organization deployment of Active Directory. Collaboration Services allows companies to establish secure collaboration between users in forests separated across the public internet. Used on a continuous basis, it reduces the costs and complexities associated with managing a decentralized, multi-forest network.

Security Considerations

Authentication

The first security level for Quest Collaboration Services is authentication. The authentication type should be specified by an administrator according to the company’s environment and policy.

Authorization through Administrative Groups and Internet Information Server (IIS)

The second security level is authorization through Collaboration Services administrative groups and IIS.

To restrict access to administration tasks, Collaboration Services automatically creates and uses two local groups on every Collaboration Services server:

- ACS Administrator
  Members of this group have unrestricted access to the service configuration and can perform all service administration tasks.
- ACS Users
  Members of this group can only view current service settings and statistics; they do not have permission to change any settings or to invoke re-publication.

When the service is installed on a member server or a workstation, local computer groups are created. The administrator can redefine group membership using the Computer Management tool.
If the service is installed on a domain controller, domain local groups are created. Users can be added to or removed from these groups using the Active Directory Users and Computers administrative tool.

Members of the local Administrators group on the Collaboration Services server are also implicitly allowed to perform all synchronization service administration tasks, even if they are not members of the Collaboration Services Administrators group.

Web Management Console

To perform administrative tasks, you need to connect to the Collaboration Services service using the web management console. This interface provides secure access to Collaboration Services from any computer connected to the intranet or internet.

To open the Collaboration Services web management console on the computer where the Collaboration Services service is installed

- Select Start | Programs | Quest Software | Collaboration Services.

  To connect to the console from a remote computer, a web interface package must be installed, as described in the Quest Collaboration Services Installation Guide.
Figure 1: The web management console main window

Connection Modes

Using the web console, administrators can connect to Collaboration Services either locally or remotely using the Internet Explorer browser. When you connect to the service, the most suitable connection type is selected automatically.

To change the connection mode manually

1. Select the **Collaboration Services** node in the management tree and select **Connection Options** from the shortcut menu.

You can change the connection mode only if you are accessing Collaboration Services locally (not if you are accessing it from a remote computer).

2. Select the required connection option. The following modes are available:
   a) Local
Use this option if you need to connect to the service locally from the Collaboration Services server (the computer where the Collaboration Services instance is installed).

- Local Online. This is the default local connection mode. All changes made to the configuration are applied immediately.
- Local Offline. This mode should be used only for troubleshooting, for example if the Collaboration Services service is down and cannot be started due to invalid settings. Changes made to the configuration will be applied the next time the service starts.

It is strongly recommended to use the Local Offline mode for troubleshooting purposes only (not when the service is running normally).

b) Remote

Use this option if you need to connect from a remote computer through the Collaboration Services web interface. The web interface package will be automatically installed on the computer on first use. If you establish a remote connection to the Collaboration Services computer, you must enter the appropriate credentials for authorization.

When establishing a remote connection to Collaboration Services through the web interface, you are prompted to enter credentials for authentication. If you provide invalid credentials, Internet Explorer will not allow another attempt and will display a message that you have no appropriate rights to establish a connection. In order to log on, you need to restart Internet Explorer.

Configuring Collaboration Services

The Configure Branches Wizard, which allows for registering branches in the collaboration structure, automatically displays when you first open the user interface at the HQ forest. It is described in detail in the HQ Forest Administrator Activity section of this document (see, "HQ Forest Administrator Activity" on page 12).

All the branches and the HQ forest are called synchronization partners.
Configure Secure Data Communication

Collaboration Services provides secure communication between forests by using data encryption and signing. Collaboration Services uses public key files. Each public key file contains the following:

- Data encryption key
- SMTP address of the service mailbox for one forest

During Collaboration Services setup, you specify the following:

- File name and location where the HQ public key file should be saved
- Password to protect the file

All messages from the HQ forest are encrypted using the encryption key in the HQ public key file.

The public key file of each branch forest is required for the administrator of the HQ forest to register the branch forests in the collaboration structure. The Export Key Wizard, which allows for exporting the branch public key, automatically appears when you first open the user interface in a branch.
To change the settings for data encryption

1. Right-click the Collaboration Services node in the tree, select Properties, and click General.

On the Properties dialog box you can do the following to configure secure data communication:

If for some security reason your encryption key cannot be used any longer, you should generate a new key by clicking the Generate New button.

After generating a new encryption key, you must generate a new public key file and distribute it to the other forests so they can update your forest’s key using the Configure Branches or Configure HQ wizard. Until then, communication with other synchronization partners will not be possible.

The HQ public key file is not created immediately; rather, it is automatically generated and saved upon setup completion, after the synchronization service is installed and started.

To export the existing public data encryption key to a public key file, click Export.
If running on Windows 2003 platform (or later), you can change the data encryption algorithm. By default, RC4 128 bit symmetric key encryption is used; you can choose to use an AES 256 bit encryption algorithm instead.

All synchronization partners should use the same data encryption algorithm. If it is changed, then after all partners make the same change to the selection on this dialog box, all keys must be re-exported and re-registered, and then all collections must be re-published (as described in the Collection Re-publication section of this document).

**Assign a Service Mailbox**

Instances of Collaboration Services installed in the HQ and branch forests communicate with each other using the Simple Mail Transfer Protocol (SMTP), which is a native protocol for Exchange 2000/2003. All communications between partners are performed through administrative mailboxes, one mailbox per forest. The data packets are compressed, grouped in regular email messages, and sent to another service mailbox.

**To configure the service mailbox**

1. Right-click the Collaboration Services node in the tree, select Properties, select General.
2. Enter the name of Exchange server where this forest's service mailbox should reside.
3. Enter the mailbox name.
4. Click Test to find out whether the specified mailbox exists on the Exchange server and whether it can be accessed by Collaboration Services.

If you change the service mailbox, you must generate a new public key file and distribute it to the other forests so they can update your forest's key using the Configure Branches or Configure HQ wizard. Until then, communication with other synchronization partners will not be possible.

**Select Recipient Update Service (RUS)**

If your Exchange organization version is earlier than 2007, or if you have mixed environment, then native Exchange RUS will be used to stamp mail attributes on the stub objects.
In most cases, the Exchange Server's built-in Recipient Update Service should be used to stamp mail attributes such as the Legacy Exchange DN. After installation, this should be enabled in the RUS Options section of the Collaboration Services properties dialog box. If not selected, published objects will not appear in the Global Address List.

To prevent possible conflicts with Exchange RUS, it is strongly recommended not to use this option if your Exchange organization is of earlier version or if you have a mixed environment.

Configure Active Directory Access

To configure Active Directory access settings

1. Right-click the Collaboration Services node in the tree, select Properties, select General, and AD Options.
   The General account is used to read and update Active Directory data. By default, the service account is used as the general account, but you can use a different account if you want.

Permissions required for that account are described in the Rights and Permissions section of the Quest Collaboration Services Installation Guide.

2. Use the Test button to test whether the newly specified account has sufficient permissions.

By default, Collaboration Services uses any available domain controller (DC) to read or update Active Directory data. To optimize the traffic and reduce the load on mission-critical DCs, you can configure the service to connect only to a particular DC (for example, you can choose to set up a dedicated DC for Collaboration Services to use).

For connection with a particular DC

1. Select the Use preferred domain controllers check box.
2. Select the domain, then click Load.
3. In the list of DCs loaded, select the check box next to the DC the service should use.

If the selected DC is down, Collaboration Services will not be able to access the Active Directory data. A corresponding event will be logged to the event log in this case.
Set Up Logging

Collaboration Services service logs its activity to its own log, ACSAlerts.log, which is located in the ACSLOGS subfolder of the service installation directory, and (optionally) to the Windows System log.

To instruct Collaboration Services to write events to the System log

1. In the management console, right-click Collaboration Services and select Properties.
2. Click Logging | General, and select whether to write events to the System log.
3. Adjust the level of events to be logged.

By default, all events are logged. It is recommended not to lower this setting soon after installation of Collaboration Services because log files are extremely helpful for troubleshooting. You can reduce the logging level after you are confident that the synchronization between partners is established correctly.

To clear the ACSAlerts.log

- Right-click Collaboration Services node in the tree, and use the corresponding shortcut menu command.

For Collaboration Services events details, see "Appendix B: Collaboration Services Events" on page 79.
Configure Alerting

To receive notifications about important service activities, configure the notification method you need on the Logging | E-mail tab, the Logging | Net send tab, or both.

<table>
<thead>
<tr>
<th>NOTIFICATION METHOD</th>
<th>USED TO</th>
<th>CONFIGURATION REQUIRED</th>
</tr>
</thead>
</table>
| email               | Send events of the selected types and notifications to the specified email address. | 1. Select the mailbox to which the email messages will be sent.  
2. Select whether you wish to receive Error and Warning events, Information events, or both.  
3. Specify the subject for the email message. |
| Net Send            | Send the events of the selected types and notifications using net send to the specified computers. | 1. Specify the NetBIOS names, DNS names, or IP addresses of the computers to which net send should deliver messages. Separate multiple entries by semicolons.  
2. Make sure the Messenger service is running on the Collaboration Services server and on the recipient computer. |

For example, you can configure email notifications to be sent when a specified percentage of free disk space is exceeded.

Configure Synchronization Partners

Using the Synchronization partners node of the management tree, you can:

- Configure new partners in the collaboration
- Track current synchronization partners and their statistics
- Manage the current collaboration structure and its forests
HQ Forest Administrator Activity

The HQ administrator can manage the current collaboration structure in the following ways:

- Add or remove branch forests
- Include branch forests in the data synchronization process, or exclude them from it
- Update the data encryption key (if it was changed by a branch) and provide an update for the appropriate public key file

To manage the collaboration structure

1. Select the Synchronization Partners node in the management tree.
2. From its shortcut menu, select Configure.
The Configure Branches Wizard is started.

   On the Specify Branches step, you can add partners to or remove partners from the list of registered branch forests:

3. To add a partner, click Add and browse for the key file (.AKF) of the branch you need. Supply the authentication password and click OK.
4. To specify whether each branch is currently enabled (involved in synchronization), use the Enabled check box.
   Clearing the box temporarily excludes the branch from collaboration. All statistics and configuration information related to the branch will be preserved until the branch is enabled again.

   When you decide to re-enable the branch, be sure to request re-publication for all collections it is subscribed to; otherwise, all data included in updates sent during the time while the branch was disabled will be missing.

5. To specify whether upgrade packets should be sent to each branch, use the Send Upgrades check box.
   For details about upgrading the product and about this option, refer to the Quest Collaboration Services Installation Guide.

Upgrade packages will not be sent to a disabled branch.

6. If any branch forest has changed its encryption key, you can update it by selecting the branch, clicking the Update Key button, and providing the appropriate public key file.
7. To remove a branch from the collaboration structure, select it in the list and click **Remove**.

If you remove a branch, all statistics and settings related to it will be lost. If you want to temporarily exclude a branch forest from the collaboration, clear the Enable check box instead of removing the branch.

*Alternatively, to add, edit, or remove synchronization partners, you can use the Branches page of the Collaboration Services Properties dialog box.*

**Branch Forest Administrator Activity**

Branch forest administrators can run the Configure HQ Wizard to edit, remove, or update HQ forest information.

Alternatively, the same settings can be changed using the HQ page of the Collaboration Services Properties dialog box.

**Synchronization Partner Statistics**

Collaboration partners involved in collaboration are displayed under the Synchronization Partners node in the management tree; the statistics report is shown in the right pane.

- To view statistics information for all collaboration partners, select the Synchronization Partners node of the management tree.
To view statistics for a particular branch forest, expand this node and select the forest you are interested in.

![Transport statistics](image)

**Figure 2: Synchronization Partners Report**

The following information is displayed in the statistics pane of the Collaboration Services web interface:

<table>
<thead>
<tr>
<th>STATISTICS SECTION</th>
<th>CAN BE USED FOR</th>
<th>DISPLAYS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transport</td>
<td>Estimating transport service performance</td>
<td>Information about traffic bandwidth, current branch forest quotas, history load, last operation time, last operation result, last operation status, and transport status.</td>
</tr>
<tr>
<td>Sent messages</td>
<td>Estimating traffic size</td>
<td>Number and total size of service messages sent and received per specified period of time.</td>
</tr>
<tr>
<td>Received messages</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Quota</td>
<td>Verifying the bandwidth load and setting optimal transport options for the HQ forest</td>
<td>Information about currently assigned quotas.</td>
</tr>
</tbody>
</table>
Check License Information

The License page allows you to view the data on the license currently being used by this forest. (You can also view this information about the license in the statistics pane when the Collaboration Services node of the management tree is selected.)

**To change the license**

- Click **Browse** and select a new license file.
Organizing Objects for Synchronization

- Introduction
- Creating a Collection for Publication
- Enabling or Disabling a Collection
- Editing a Collection
- Subscribing to a Collection
- Unsubscribing from a Collection
- Removing a Collection
- Viewing Collection Settings and Synchronization Statistics
Introduction

The administrator of each forest can select which objects and attributes to publish to other synchronization partners. The objects to be synchronized are grouped into collections—sets of objects and their attributes. Administrators can either define the objects to be synchronized on a per-container (organizational unit) basis, or explicitly add groups, users, and contacts to collections. This information then becomes available to other forests. Administrators of synchronization partners can see new collections of objects and can choose whether to subscribe to them.

Publication settings can vary for different collections of objects. For example, you might choose to publish the mobile phone numbers of administrators so they can be contacted in case of emergency, while keeping the mobile phone numbers of other users (such as top executives) unlisted outside the organization. Predefined "Minimum" and "All" sets of attributes to be published are provided, and administrators can create their own predefined sets (presets).

Creating a Collection for Publication

Collaboration Services offers numerous methods for organizing objects into collections. For example, you can do any combination of the following:

- Publish a whole domain or some top-level OUs and exclude objects not to be published explicitly, through containers or using LDAP filters.
- Create a group with users to be published, and publish just this group with the Synchronize members option enabled. Later, if you want to add additional users to the synchronization, you can join them to the group and they will be published automatically.
- Select users and groups to be published explicitly.
- Import a list of objects to be published from a plain text file.

Publish Collection Wizard

The Publish Collection Wizard will help you create a new collection of objects and publish it.

To run the wizard

- Right-click the Publication node in the management tree and select Publish Collection.
Step 1: Specify Collection Name, Description, and Synchronization Type

In the first step of the wizard:

1. Specify the collection’s name and description.  
   *The name and description should be as informative as possible; this will be the only collection information available to the administrators of other forests until they subscribe to the collection.*

2. Select what information will be published and synchronized:
   - Active Directory objects (for GAL synchronization)
   - Free/busy information
   - Calendar information

   If you choose not to synchronize AD objects with Collaboration Services, use some other directory object synchronization tool to synchronize Active Directory objects between forests, such as Microsoft Identity Integration Server (MIIS).

Step 2: Select Objects to Publish

Select the objects you want to include in the collection. Consider that only mail-enabled or mailbox-enabled objects can be published.

You can populate a collection in the following ways:

- Add a container; all objects in that container will be included in the collection.
- Add objects (user, groups, and contacts).
- Import a list of objects from a file. This file should list the distinguished names (DNs) of the objects, one DN per line.

To add a container

1. Click **Add Container**.
2. Click **Load** to view AD containers.
3. Select the containers you need, and click **Add**.

To add objects

1. Click **Add Objects**.
2. To display the objects you need, use filtering:
   - Domain—displays objects of the selected domain only.
• Additional filter—specifies an additional LDAP filter to reduce the scope of displayed objects. For example, to display only users from the list of AD objects, specify the following LDAP filter: (objectClass=user).
• Maximum number of displayed objects—specifies the maximum number of objects to display.

If you add a group to a collection, group members are not synchronized automatically by default. If you want them to be synchronized, select the added group, click Settings, and then choose the Synchronize members option in the Settings dialog box.

Nested groups are not included in a collection. For example, suppose Group 2 is a member of Group 1. If Group 1 is included in the collection, Group 2 will not be published. To publish Group 2, you must include it in the collection explicitly.

**Configuring Synchronization Settings**

From the Select Objects dialog box, you can configure synchronization options by clicking Settings. For example, for AD containers, you can select object classes to be synchronized.

It is recommended that you use this dialog box to configure synchronization of group members (they are not synchronized automatically by default).
To synchronize group members

- Select the group you have added, click Settings, and then choose the Synchronize members option.

Step 3: Specify Additional LDAP Filters

If you have added containers to be published, you may need to specify additional LDAP filters for each class of objects included in these containers.

Creating LDAP filters is a fairly complex task that should be performed by advanced users only. LDAP filters must be RFC2254-compliant.

For example, to exclude from publication all users who either belong to the HR department of your company or are members of the HRGroup group, apply the following filter to the User class:

```plaintext
(!(| (department=HR) (memberOf=CN=HRGroup,OU=Groups, DC=acme,DC=com)))
```
Step 4: Exclude Well-Known Objects

Specify if any built-in accounts, containers, or single objects should be excluded from the collection.

- To exclude built-in groups or accounts (such as Domain Admins and Guest), select Exclude well-known users and groups.
- To exclude a container (and all objects inside), select the Exclude the following objects check box and click Add Containers. All objects in the containers you select will be excluded from the collection.
- To exclude particular objects, click the Add Objects button, and select the objects from the list.

Step 5: Select Object Attributes to Be Synchronized

Specify which attributes should be synchronized for each object class. You can do the following:

- Select attributes manually from the list
- Use predefined sets of attributes: All Attributes set or Minimum set
- Save the set of selected attributes for the future use as a preset
  The Minimum set includes the only attributes required to create a stub object in another forest.

**To see what attributes comprise the Minimum set for the certain class**

- Expand the node for that class and click Minimum.

All object attributes in the Minimum set are mandatory, so you are not allowed to clear the check boxes next to them. If any object attribute included in the Minimum set is not valid, the object cannot be published.

**To save a set of selected attributes for a future use**

- Click Save Preset. If you need to publish an object with the set of attributes saved as a preset, click the Load Preset button.

**To use an extended AD schema**

- Click Add Attributes and select the necessary attributes from the list.

To synchronize extended schema attributes to other forests, their schemas must be extended with the same attributes as well.
Step 6: Select Calendar Attributes

On the Calendar Details page, specify which appointment attributes should be published and synchronized.

This page is skipped if Calendar information was not selected on the Step 1 of the wizard.

By default, if the Synchronize appointment details check box is cleared, Collaboration Services publishes to other synchronization partners only the time to start and end the appointment.

Select the Synchronize appointment details check box to allow publication of the following additional parameters for each appointment:

- Time zone
- Location
- Recurrence attributes
- Appointment subject

The Location and Subject appointment details will become available in Free/Busy information.

If you select the Synchronize appointment details option, then the Reviewer permission will be set for the Calendar folder (for Default on the subscriber side), so any user from the subscribed organization will be able to view synchronized calendar details.

Step 7: Apply Mappers

Sometimes the publishing or subscribing administrators might want to change the format or appearance of the data they publish or subscribe to. To do that, they can use mappers. A mapper is a plug-in component that changes the appearance of data that you publish or subscribe to. For example, a mapper can be used to set the AD objects’ attributes values to those specified in the .ini file.

In this step of the Publish Collection Wizard, you can apply mappers to the published objects.

For more information about what mappers are available, see “Appendix A: Customizing the Format of Synchronized Data” on page 75.
Step 8: Allow for Subscription and Synchronization

In this step you can:

- Allow other synchronization partners to subscribe to the collection you are creating or prohibit partners from subscribing.
- Specify whether synchronization of collection members should start immediately after the collection is published (after you finish the wizard).

**To allow or prohibit subscription**

1. Click the **Add** button.
2. Check or clear the **Allow** or **Deny** check box for a partner in the list.

Deny always overrides Allow. Thus, Deny selected for Everyone overrides all explicitly set Allow permissions.

Because the HQ forest operates as the service data packet distributor, it is allowed to subscribe to all collections in the collaboration structure by default.

If you do not want collection members to be involved in synchronization immediately after the collection is published, select the **Collection is disabled** check box. For details on enabling or disabling collections, see "Enabling or Disabling a Collection" on page 26.
Step 9: Apply Settings

Wait until the collection is created and its settings are saved to the configuration database.

Collaboration Services will notify allowed synchronization partners that the collection is available for subscription. As soon as a collection is published, the administrators of other branch forests who have appropriate permissions will be able to subscribe to the collection.

If a collection was created as enabled, then as soon synchronization partners subscribe to it, the collection’s data will start being synchronized to the other forests.
Enabling or Disabling a Collection

Enabling a collection means all objects included in it should be immediately synchronized by Collaboration Services. By default, a collection is created as enabled and synchronization starts right after the Publication Wizard is completed.

However, you may need to create a collection without enabling it (that is, synchronization does not start upon publication), and other branches subscribe to it as required in advance. Then on the day when the synchronization needs to be started, all you need to do is enable the collection.

**To enable a collection during creation**

- Ensure that the **Collection is disabled** check box on the Set Permissions step of the Publication Wizard is cleared.

**To enable an existing collection**

- Right-click it in the management tree and clear the **Disabled** check box.

**To disable a collection during creation**

- Select the **Collection is disabled** check box on the Set Permissions step of the Publication Wizard.

**To disable an existing collection**

- Select the **Disabled** check box on its shortcut menu.

Editing a Collection

After a collection is published, you may need to add objects to it, remove objects from it, or change some of its properties.

**To update a collection**

- Run the Edit Collection Wizard by selecting the **Edit Collection** command from collection's shortcut menu.

  *Its steps are similar to those of Publish Collection Wizard. For details, see “Publish Collection Wizard” on page 18.*
Organizing Objects for Synchronization

To access a collection's properties

- Right-click the collection and select Properties.

On the Advanced tab, you can select whether to Apply approved objects only. For details, refer to Resolving Synchronization Conflicts section of this guide.

After you edit a collection, the updates are automatically sent to the HQ forest and distributed to all branch subscribers; then the modified collection is automatically re-republished.

Subscribing to a Collection

To receive collection data, synchronization partners need to subscribe to collections. As soon as a forest subscribes to a collection, the Collaboration Services instance creates the following items for each member of the collection in this forest:

- Stub objects in the GAL. (For each original object, Collaboration Services creates a stub object in the forests that subscribe to the collection. The mail received by this stub should be redirected to the original object's email address.)
- Free/busy information.
- Calendar information.

Use the Subscribe Wizard to subscribe to the collections published by the HQ and branch forests.

To subscribe to a collection

1. Select the Subscription node in the management tree, and select Subscribe from the Action menu.
   Alternatively, you can use the toolbar button or the Subscribe shortcut menu command to start the wizard.
2. Select the collection you want to subscribe to from the list.
3. You can change the format or appearance of the objects in a collection you have subscribed to by applying mappers.

Before applying a mapper to a collection you are subscribing to, check with the collection originator to make sure this mapper was not already applied to the collection. Applying the same mapper twice is not necessary, and sometimes it can lead to undesired results, such as a suffix being added twice.
a) Select the collection you need and click the **Properties** button.

b) Select the **Apply mappers to synchronized objects** check box.

c) Click **Add** and select the mappers you want from the list of available mappers. For more information about mappers, see “Appendix A: Customizing the Format of Synchronized Data” on page 75.

4. Wait for the wizard to apply your changes.

5. Review the summary log of the subscription process, and click **Finish**.

### Modifying Subscription Properties

*To configure the collection to which you have subscribed*

1. Right-click the subscription and open its properties.

2. On the Mappers tab, configure the mappers you want to apply. For details, see “Appendix A: Customizing the Format of Synchronized Data” on page 75.

3. On the Advanced tab, select whether to Apply approved objects only. For details, refer to the Manual Conflict Resolution section of this document.

4. If you subscribe to a collection for calendar information synchronization, you should also select the **Always create mailbox** check box and specify the Exchange server and mailbox store that mailbox will be created on.

   *In this case, mail-enabled object on the subscriber side will be created, and the Calendar information will be presented as the corresponding Free/Busy.*
Unsubscribing from a Collection

To unsubscribe from a collection

- Select the **Collection** node in the management tree and select **Unsubscribe**.

  *If you unsubscribe from a collection, the stub objects created in your forest for that collection's members are hidden from the GAL in your forest. Then the stub objects will be automatically deleted after the time interval specified by the corresponding Collaboration Services parameter. To change the retention period for these objects:*

  a) Open the Collaboration Services Properties dialog box.
  b) Go to the Synchronization | Active Directory | General page.
  c) Modify the Retention time for removed objects parameter.

By configuring the Retention time for removed objects parameter, you can delay deleting the stubs for a specified number of days; this will help improve overall collaboration performance and decrease the load on the production environment because if the object is added to another collection during this period, the stub objects will be re-used.

Removing a Collection

To remove a collection you published

- Right-click the collection name in the management tree and select **Remove**.

  A collection can be removed only by its publisher.

When a collection is removed by publisher, the following is performed:

1. All subscribing partners get a notification.
2. The stub objects created by Collaboration Services are immediately removed from the Global Address List in all subscribing forests.
3. Then the stub objects are automatically deleted after the time interval specified by the Retention time for removed objects parameter.
Viewing Collection Settings and Synchronization Statistics

The collection settings and synchronization statistics are displayed in the right pane when you select a collection in the management tree. To see the overall statistics for all collections currently published or subscribed to by your forest, select the Publication or Subscription nodes.

The report shows, in particular:

- General information about the collection: collection name, description, publisher, creation date.
- Collection membership information: number of objects included in the collection and membership scan statistics.
- Statistics on Active Directory objects synchronization (if it is configured for the collection): the number of objects added, modified or deleted per week, month, or year; synchronization status and state; and the date and time of the last synchronization.
- Statistics on Calendar and Free/busy information synchronization (if it is configured for the collection): the number of objects for which this information was synchronized, the number of updates sent, the synchronization status and state, and the date and time of the last synchronization. For more details on synchronization, see “Managing the Synchronization Process” on page 43.
Resolving Synchronization Conflicts

- What Can Cause Synchronization Conflicts?
- How Can Conflicts Be Resolved?
- Automatic Conflict Resolution
- Manual Conflict Resolution
What Can Cause Synchronization Conflicts?

A conflict occurs when two or more objects from different forests have the same email address. Most conflicts are due to manually-created contacts pointing to users in other forests.

While creating a stub object in the target forest, Collaboration Services populates the proxyAddresses attribute and the mail attribute of the stub with the appropriate attribute values of the corresponding source object. However, if existing contacts or other objects already have their properties populated with the same values, valid stub object cannot be created.

Therefore, before creating a stub, Collaboration Services checks whether any of the proxy addresses or mail attributes of the existing forest objects are already populated with the same values as the attribute planned for a stub object. If a conflict is detected, Collaboration Services cannot create a stub object until the conflict is resolved.

How Can Conflicts Be Resolved?

There are several different ways to resolve a conflict, object deletion, object matching, and pre-matching.

- **Object Deletion**
  The recommended method of resolving conflicts is to delete the conflicting object and create a stub object that inherits deleted object’s properties. This is the simplest way to resolve conflicts, and it is the only option available for resolving conflicts between objects of different classes (for example, user and contact).

- **Object Matching**
  If both the conflicting object and the published object are of the same class (for example, both are users), then you can choose to match the published object into the existing one. In this case, the existing object is used as a stub for the time of synchronization. One significant
difference between such a "temp stub" object and a regular stub object is that the user object’s account state remains unchanged. For example, if the account was enabled, it remains enabled after Collaboration Services makes a stub of it.

Matching needs to be used for deployment scenarios where some users have active user accounts in multiple forests. With matching, you can use active user accounts as stubs, so the users will still be able to log on in multiple forests with Collaboration Services deployed.

When specifying rules for matching published objects into existing ones, you can also define attribute synchronization rules. They allow you to specify which attributes of the objects you match into should be overwritten by the published object’s attributes and which should be left intact.

Attribute synchronization is useful if the user account is updated by the provisioning system in one of the forests and those changes need to be propagated to the same user’s accounts in other forests.

• Pre-Matching
  This method instructs Collaboration Services to match published objects into specified objects automatically in the selected OUs.

Forest administrators can configure Collaboration Services to handle conflicts using the following options: deletion, matching, and pre-matching. For that, the automation rules should be configured, and then the synchronization service will attempt to automatically resolve every conflict it encounters according to these rules.

**Automatic Conflict Resolution**

*To set up automatic conflict resolution*

• Open the Collaboration Services Properties dialog box, select **Synchronization | Automation**, and then select the conflict resolution method you need.
Deletion

Use this option to make Collaboration Services automatically delete conflicting objects in the selected OUs before creating the stub objects.

To configure the deletion

1. Select the Allow deletion of conflicting objects from the following containers: check box.
2. Click Add, and then Load the list of containers from Active Directory; select the ones from which conflicting objects will be deleted.
   
   You can also import a list of containers from a text file. Click the Import button and choose the file containing the list of containers. The file should list the distinguished names (DNs) of the containers, one DN per line.

3. For each container, specify how the attributes of deleted objects should be handled. To configure attribute handling:
Resolving Synchronization Conflicts

a) Select the container and click **Settings**.

b) Select the attribute synchronization rule for each attribute.

You can choose from among the following rules:

- Leave—Preserve the attribute of the deleted object.
- Replace—Overwrite the attribute with the published object’s attribute (you can click Replace All if this rule should be applied to all selected attributes).
- Merge—Merge the attributes of the deleted and published objects (this option is available for multi-valued attributes only).

A stub object created after deletion of the conflicting object will inherit the following attributes from the conflicting object: LegacyExchangeDN, X500 addresses. Preserving these attributes prevents users from getting non-delivery receipts (NDRs) when replying to older email from a deleted object.

c) You can also do the following:

- Save the configuration for future use by clicking Save Preset.
- Load a preset.
- Restore default settings.

d) Click **OK** to apply your changes.

With the default settings, a stub object created by matching into the conflicting object will replace the targetAddress attribute value of the target object with the redirector address. If you choose to leave the targetAddress attribute of the target object intact, mail redirection might not function properly.
4. To delete the conflicting objects not only in the selected OUs but in the sub-containers as well, select the **Apply to all sub-containers** check box. In that case, parent OU settings will be propagated to child OUs settings.

**Matching**

Use this method to make Collaboration Services automatically match published objects into conflicting objects in the selected OUs, thus resolving the conflict.

![Collaboration Services properties](image)

**Figure 5: Matching objects**

**To configure matching**

1. Select the **Allow matching to objects from the following containers** check box. Follow the procedure for configuring object attributes found within the Deletion section of this guide. For details see, “To configure the deletion” on page 34. You can select containers and specify how the attributes of objects you match into are handled as described in Deletion section, and the same rules are available for the attributes of target objects.

Passwords cannot be synchronized across forests due to the secure nature of Collaboration Services. Therefore, passwords need to be managed separately in each forest.
With the default settings, a stub object created by matching into the conflicting object will replace the targetAddress attribute value of the target object with the redirector address. If you choose to leave targetAddress attribute of the target object intact, mail redirection might not function properly.

2. Select the **Apply to all sub-containers** check box to specify that the conflicting objects should be deleted not only in the selected OUs, but in the sub-containers also. In that case, parent OU settings will be propagated to child OUs settings.

**Pre-Matching**

On the Pre-matching page you can configure Collaboration Services to match published objects into specified objects automatically in the selected OUs. To match published objects into existing ones, pre-matching rules are used. A rule includes:

- Email address of the published object
- Distinguished names (DNs) of the object to match into

Whenever an object with a specified email is synchronized, it will be matched into the object whose DN is stated in the rule.

The incoming object and the object you are matching into must be of the same object class; in most cases, they are user objects.
**Quest Collaboration Services**

**To configure pre-matching**

- Select the **Use custom matching for the following objects**: check box to enable the option.

![Collaboration Services Properties](image)

**Creating a New Rule and the Pre-Matching Wizard**

**To create a new rule**

1. Click the **Add** button and follow the steps of the Pre-Matching Wizard.
2. On the Welcome page, click **Next**.
3. On the Email Address page, click **Browse** to specify the email address of published object using the Select recipient dialog box and click **OK**.

![Select recipient dialog box](image)

4. On the Select Object page, specify the object you want to match into and click **Next**.

5. On the Attribute Synchronization page, choose how to handle the attributes of objects you match into. Select the **Replace**, **Leave**, or **Merge** (for multi-valued attributes only) attribute synchronization rule for each attribute of the object to match into and click **Next**.

6. In the message box that appears, click **Yes** if you want to proceed with creating the new pre-matching rule.

7. View the Summary and click **Finish**.

For each pre-matching rule you add, you can perform the following actions:

- Click **Remove** to delete the rule from the list.
- Click **Settings** to change how to handle the attributes of objects you match into.
- Click **Import** to import a list of pre-matching rules from a text file. The file should contain a list of pairs, one pair per line. Each pair must include the email address of the published object and the distinguished name (DN) of the object to match into, separated by a space.
- Click **Detect** to scan Active Directory and update the list of rules if any changes were made to Active Directory (for example, objects were moved).
Manual Conflict Resolution

If no automation rules are specified, or no rules can be used to resolve a particular conflict, the synchronization service marks the published object as non-applied.

In other words, non-applied objects are the ones whose changes will not be automatically applied to your forest. These objects are displayed in the Non-Applied Objects node in the management tree.

For the listed objects, you have to resolve conflicts manually, either by using the method Collaboration Services suggests or by using your own method (custom action).

- To use the conflict resolution method suggested by Collaboration Services (for example, Create stub), you have to approve it manually. Simply select the objects in the list, right-click the selection, and click Approve Action.
- To resolve a conflict using a custom action, right-click the object and choose Advanced. This starts the Conflict Resolution wizard, which allows you to choose a custom action for resolving the conflict. In this wizard, you specify:
  - The email address of the published object
  - The DN of object you want to match into
  - How the attributes of objects you match into are to be handled

Custom actions created with this wizard are stored in the configuration as pre-matching rules; if the collection is republished, the custom action is re-applied automatically.
After you resolve the conflict, you should republish the objects by clicking Re-synchronize object in the shortcut menu. The objects will be re-published and applied.

**Applying Approved Objects**

You may want to manually resolve all conflicts for the objects your forest is subscribed to (that is, to approve objects applied to your forest manually), either one by one or all at once.

**To manually approve objects**

1. Right-click the collection of objects you need and select **Properties**.
2. Go to the **Advanced** tab and select the **Apply approved objects only** check box.
   
   All collection objects will appear in the Non-Applied Objects list, where you can choose which objects you allow to be applied to your forest.
Managing the Synchronization Process

- Configuring the Synchronization Process
- Using the Packet Queue as Interim Data Storage
- Suspended Object Storage
- Manual Operations
Configuring the Synchronization Process

The main task for Collaboration Services is keeping Active Directory data, calendar, and free/busy information synchronized between all synchronization partners so that users have access to up-to-date information about all objects participating in the collaboration. Use the synchronization settings to:

- Fine-tune the interaction between Active Directory, Exchange, and your Collaboration Services instance.
- Optimize the connectivity between the synchronization partners.

**To access the synchronization settings for Collaboration Services service in your branch:**

1. Right-click the **Collaboration Services** node in the management tree, and select **Properties**.
2. Under the Synchronization node, select the type of setting you need, as explained below.
Managing the Synchronization Process

General Settings

The General page of the Synchronization node contains common controls for all types of synchronization.

Figure 7: Synchronization general options

Collections Re-Scan Frequency

The regular scan (which uses Active Directory’s DirSync control) registers the majority of changes made to Active Directory objects. However, some changes cannot be registered by regular means, such as when an OU with collection members is moved to another domain or published objects are deleted.

Thus, a more thorough collections re-scan should be initiated periodically to register these types of changes; use the Scan collection for changes every option to specify how often the detailed re-scan should take place. The default period is 6 hours.

This type of scan uses significantly more resources than a normal scan, so it is recommended not to set this parameter to a low value.
Alerting and Notification

In the Notifications section, you can specify what percentage of any quota being filled should trigger notification of a forest administrator. The notification will state that the specified percentage of a quota is filled. The default value is 80%. For more information about quotas, see "Synchronization Settings for Active Directory Objects" on page 46.

Synchronization Settings for Active Directory Objects

The AD object synchronization process is as follows:

1. Collaboration Services periodically checks (scans) whether any changes were made to Active Directory objects in your forest.
2. When Collaboration Services finds that the properties of one or more published objects have changed, it creates update packages and sends them to the HQ for distribution to all branch forests that subscribe to the collections those objects belong to.
Use the Active Directory tab of the Synchronization node to adjust the synchronization settings for AD objects.

**Figure 8: Active Directory synchronization options**

**General Settings**

On the General page, you can set the time intervals for scanning Active Directory for changes and applying the changes received from collaboration partners, as explained below.

**Publication Settings**

At the time interval specified in the Query AD for changes every field, Collaboration Services checks whether any changes were made to Active Directory objects in your forest.

The sleep interval between the collection update sessions is specified in the Processing collections interval.

**Subscription Settings**

At the interval specified in the Update AD every field, Collaboration Services applies incoming updates to Active Directory in the forest.
Quest Collaboration Services

When an original object is removed from a collection you subscribe to, the deletion is automatically synchronized to the subscribing forests and the corresponding objects are hidden from the Global Address List. However, the stub objects themselves are not deleted immediately. Using the Retention time for removed objects option, you can delay deleting the stubs for a specified number of days; if the object is added to another collection during this period, the stub object will be re-used.

**Scheduling Access to Active Directory**

To avoid excessive load on the DCs during production hours, schedule Collaboration Services access to Active Directory for the least busy time periods.

> Active Directory access schedules must be thoroughly coordinated, especially when some of the collaboration partners are located in different time zones; otherwise, synchronization performance may be poor.

**To schedule AD access**

1. On the Scheduling page, select the **Use Active Directory access scheduling** check box.

![Collaboration Services Properties](image)

2. Specify the time intervals when the service is allowed to read and update data in Active Directory.
Managing the Synchronization Process

Limiting the Number of Active Directory Objects to Synchronize

When configuring Active Directory objects synchronization, you can specify the following limits on the Quotas page:

- Overall maximum number of synchronized Active Directory objects
- Maximum number of AD objects allowed to be synchronized daily

The maximum number of synchronized directory objects should be coordinated with the following:

- Hardware resources of the Collaboration Services server, and Active Directory and Exchange servers load in the HQ forest and in the branch forest.
- Number of the collaboration branches.
- Number of objects to be published in the collaboration structure.

When the specified maximum number of Active Directory objects is reached, no new objects will be added to Active Directory synchronization. In this case, it is recommended either to increase the specified value or to unsubscribe from some collections.

Namespace Usage

For each original object, Collaboration Services creates a stub object in the forests that subscribe to the collection. The mail received by this stub should be redirected to the original object’s email address.

Since mailbox-enabled object can have more than one proxy address, Collaboration Services should select which of them is to be used for mail redirection from stub object.

To choose the redirection address, Collaboration Services does the following:

1. If the object’s targetAddress attribute is populated, that will be used.
2. If the targetAddress attribute is not available, the primary SMTP address is used.
3. If neither address is available, redirection address will be set to the first matching proxy address found in the Namespaces page of the Collaboration Services Properties dialog box. The namespaces listed there are in priority order.

If none of the retrieved addresses is encountered in the specified namespace, no stub object will be created.

The Namespaces page of the Collaboration Services Properties dialog box allows you to add new namespaces or edit existing namespaces if your policy has changed since Collaboration Services setup.

![Namespaces Page](image)

### Free/Busy Information Synchronization Settings

Synchronized free/busy information is kept on the Exchange server that stores the free/busy public folder for the administrative group containing the Exchange server where the Collaboration Services service mailbox resides.

So, if your Exchange deployment contains multiple administrative groups, the groups must access free/busy information using either public folder referrals or free/busy folder replication. Please see the appropriate Microsoft Exchange server documentation for more information.
The free/busy information synchronization process is performed as follows:

1. Collaboration Services periodically checks whether any changes were made to the free/busy information of the published objects.
2. When the service detects such changes, it creates update data packets and sends them to the HQ forest for distribution to subscribers.
3. Collaboration Services applies the free/busy information changes to the stub objects of the collections the forest is subscribed to based on the frequency settings you select.

**General Settings**

Use the General page to adjust the frequency of scanning for updates and applying changes:

![Collaboration Services Properties](Image)

**Figure 9: Free/busy general options**

**Publication Settings**

- Query Free/Busy for changes every:
  Specify how often Collaboration Services should check for changes to the free/busy information of the published objects.
Subscription Settings

- Update Free/Busy every:
  Specify how often Collaboration Services should apply the free/busy information changes to the stub objects of the collections the forest is subscribed to.

Advanced Subscription Settings

- Wait for missing packets for:
  Specify how long the service should wait for missing data packets with free/busy information before automatically re-publishing this information.

Increasing this value lessens the load on Collaboration Services and the Exchange server, but makes the free/busy information less accurate.

In mixed collections (that is, intended for synchronization of several types of information), an object’s free/busy information may be received before the object itself. In such cases, the free/busy information cannot be published right away.

Use the Scan AD for required objects every: value to specify how often the service should scan Active Directory for the appearance of objects to which the free/busy information should be applied.

Scheduling

To avoid excessive load during production hours on the Exchange server where free-busy information is kept, schedule Collaboration Services to access the free/busy folder for the least busy time periods.

Free/busy access schedules must be thoroughly coordinated, especially when some of the collaboration partners are located in different time zones; otherwise, synchronization performance may be poor.

To schedule free/busy folder access

1. On the Scheduling page, select the Use Free/Busy access scheduling check box.
2. Specify the time intervals when the service is allowed to read and update free/busy information on the Exchange server.

If you allow access to the free/busy information in off hours only, the updated free/busy information will not be propagated to the other forests until the next day.

Limiting the Number of Free/Busy Messages to Synchronize

The Quotas page allows you to specify the following:

- Overall maximum number of synchronized free/busy messages.
- Maximum number of messages allowed to be synchronized daily.

Calendar Information Synchronization Settings

To support Exchange 2007 and 2010 deployments without public folders (where no free/busy information exists), Calendar information synchronization has been implemented in Collaboration Services.

Calendar Details data is not stored in the central location with free/busy information; rather, it is stored in the users' mailboxes.

Scan Frequency

Use the General page to adjust the frequency of scanning for updates and applying changes:

- Query Calendar for changes every:
  Specify how often Collaboration Services should check for changes to the Calendar information of the published objects.
- Update Calendar every:
  Specify how often Collaboration Services should apply the calendar information changes to the stub objects of the collections the forest is subscribed to.
Scheduling

To avoid excessive load on the Exchange server during production hours, schedule Collaboration Services access to the Calendar information for the least busy time periods.

Calendar information access schedules must be thoroughly coordinated, especially when some of the collaboration partners are located in different time zones; otherwise, synchronization performance may be poor.

To schedule Calendar access

1. On the Scheduling page, select the Use Calendar scheduling check box.
2. Specify the time intervals when the service is allowed to read and update Calendar information on the Exchange server.

If you allow access to the Calendar information in off hours only, the updated Calendar information will not be propagated to the other forests until the next day.

Using the Packet Queue as Interim Data Storage

Collaboration Services use SMTP as a transport protocol. Though this protocol has many advantages and is a native protocol for Exchange, it introduces one problem: it does not provide guaranteed delivery. For Collaboration Services, this means that synchronization data packets do not necessarily arrive in the order in which they were sent. In fact, sometimes a packet may not arrive at its destination at all, and needs to be sent again.

To deal with this problem, Collaboration Services use a Packet Queue. This is a special location where all received data packets are kept until all the other data required to create a particular object arrive. After all data is received, the service extracts the necessary data from the queue and creates an object.

The Packet Queue is also used to store the value of linked attributes, such as the Manager attribute of a user object. The link cannot be applied until the object it points to is created, so the link is stored in the Packet Queue until then.

In addition to Active Directory data, the Packet Queue stores an object’s free/busy information until the object is created and the free/busy information can be applied.
Packet Queue processes are fully automated and do not have to be managed. However, it is possible to fine-tune the packet queue behavior using the Packet Queue page.

**Figure 10: Packet queue options**

*To adjust the time when the packet should be marked as obsolete*

1. On the Packet Queue page, select the appropriate time interval from the Mark synchronization packet as obsolete if it could not be processed within.

   *Packets marked as obsolete will be deleted automatically if you select the Delete obsolete packets automatically check box. Otherwise, you can clean up the Packet Queue manually by clicking the Clean Up Now button.*
Suspended Object Storage

Suspended Object Storage contains objects excluded from synchronization due to various problems. If some objects are missing from the synchronization, you should first examine the log for errors and fix the problems that led to the objects being excluded from processing. Then open the Suspended Objects page of Collaboration Services properties and click Purge to empty the storage and add the excluded objects back into the synchronization.

![Suspended Object Options](image)

**Figure 11: Suspended object options**

Manual Operations

Synchronization

Manual synchronization is recommended when you need your collaboration partners to get the modifications made to objects in your forest before automatic synchronization is due.

Usually, Collaboration Services automatically synchronizes and updates collection data according to the time intervals specified on the Synchronization page and all sub-pages of the Collaboration Services properties. When you perform manual synchronization, all timeouts are minimized for a short period of time on both the publishing and subscribing forests, so all changes in published objects are synchronized much faster. This mode affects all available collections.

**To start manual synchronization**

1. Select the **Publications** node in the management tree.
2. Go to the **Action** menu and select **All Tasks**.
3. Click **Synchronize Now**.
   
   You can select whether to synchronize:
   
   - Everything (Active Directory objects, Calendar information, and free/busy data)
   - AD objects only
   - Free/Busy only
   - Calendar only

### Collection Re-publication

Re-publication is performing the entire data publication over—published objects’ data will be sent again from the publisher.

Initial synchronization is very resource consuming and may take significant time depending on the collection size. Therefore, re-publication should be performed only when you need to fully resynchronize all the data that was previously synchronized.

For example, you might need to re-publish data when Collaboration Services detects that an unrecoverable failure occurred. In this case, you will be prompted that re-publication is needed. You should not perform re-publication until you are sure what happened and have fixed the cause of the error.

**To re-publish a single collection**

1. Select the collection in the management tree.
2. Open the **Action** menu, point to **All Tasks**.
3. Point to Re-publish, and choose what data you want to republish:
   
   - Everything (Active Directory objects, Calendar information, and free/busy data)
   - AD objects only
   - Free/Busy only
   - Calendar only
   
   *Alternatively, to run the Re-publish command, you can use the toolbar button or collections' shortcut menu commands.*

**To re-publish all collections**

1. Select the **Publication** node in the management tree.
2. Open the **Action** menu, point to **All Tasks**.
3. Point to Re-publish, and choose what data you want to republish:
   
   - Everything (Active Directory objects, Calendar information, and free/busy data)
   - AD objects only
Initiating Re-publication from the Subscriber Side

To initiate re-publication when you are a subscriber, select either the Subscription node or a particular collection and then use the Request Re-publication command from the shortcut menu.

Re-publication of a collection may take significant time depending on its size and should be performed only when required.

Configuration Database Clean-Up

In case of intensive Active Directory updates, your collections may turn out to contain some objects that have become obsolete. For example, your published collections may include a number of user accounts that have been already removed from AD.

To prevent from synchronization conflicts that might occur due to obsolete objects still kept in the collections, you can periodically clean up Collaboration Services configuration data (new data will be stored to the configuration database at the next scan).

To perform a clean-up

- Right-click the Publication node in the management tree and select Clean Up Database.
Transport Management

- Overview
- Send
- Receive
- Scheduling
- Limiting Traffic Rates
Overview

Instances of Collaboration Services installed in the HQ and branch forests communicate with each other using the Simple Mail Transfer Protocol (SMTP), which is a native protocol for Exchange organization.

All communications between partners is performed through administrative mailboxes, one mailbox per forest. The data packets are compressed, grouped in regular email messages, and sent to another service mailbox.

To ensure optimal data flow between synchronization partners, you can adjust the transport settings to suit your needs. To view or edit transport settings, use the Transport page of Collaboration Services Properties dialog box.

Send

The Send page allows you to specify settings for sending messages to other synchronization partners. After a data packet to be sent is generated and compressed, the service performs the following procedure:

1. First, if the packet size exceeds the maximum allowed size, it is divided into multiple messages of the default size.
2. Then the messages are put in the message queue, from which they are sent to the designated synchronization partner.
3. A message is kept in the queue until the service receives an acknowledgement of successful message delivery from the partner.

![Figure 12: Transport send options](image-url)
Collaboration Services guarantees data delivery by checking the delivery status of every message and re-sending any message for which delivery is not confirmed.

- The time interval at which Collaboration Services sends new messages from the queue can be specified with the Send messages every option.
- You can specify the number of messages that may be sent before confirmation of delivery of a given message in the Send without confirmations option.
- Use the Stop creating new messages if queue exceeds option to specify the maximum queue size. Once this value is reached, no more new messages will be created. This option prevents you from running out of disk space due to long queues if a partner is not responding. As soon as a partner comes back online and starts processing the incoming messages, the queue will clean up and then new messages can be created.
- The time interval after which a message will be re-sent if its delivery is not confirmed is specified in the Initial timeout option. Each time the message is re-sent, the timeout is automatically increased.
- Use the Maximum timeout option to specify the maximum timeout allowed.

**Receive**

The Receive page allows you to specify the settings for receiving incoming messages.

- The time interval for checking the service mailbox for new messages is specified in the Check for new messages every option.
- To specify a maximum number of messages that can be retrieved from the mailbox during one session, use the Retrieve per session option.
- If the specified Session timeout value is more than 0, then after retrieving the specified number of messages, Collaboration Services will stop the current session and wait for the specified length of time. Having an interval between sessions may help decrease the load on the Exchange server.
- If the Session timeout value is 0, then Collaboration Services will retrieve messages continuously until all available messages are retrieved from the mailbox.
Quest Collaboration Services

Scheduling

Message exchange between synchronization partners can be scheduled in order to decrease the load on the Exchange servers during production hours.

To schedule exchanges

- Select the **Use SMTP transport scheduling** check box and select the time intervals when the service is allowed to send and receive messages containing synchronization data.

Transport is the key to successful implementation of inter-forest synchronization. Transport, Active Directory, Calendar, and Free/Busy schedules should be carefully coordinated (especially if collaboration forests are located in different time zones) and provide a sufficient time interval for Collaboration Services to perform its activities (sending messages, accessing Active Directory, and accessing free/busy information). Otherwise, synchronization performance may be poor.

Limiting Traffic Rates

The Quotas page allows you to control the incoming and outgoing traffic while messages are being exchanged between forests.

![Collaboration Services Properties](image)

**Figure 13: Quota options**
Outgoing Traffic

To control outgoing traffic, the HQ and branch administrators can specify a maximum outgoing traffic size in megabytes per hour by selecting the Control outgoing traffic check box. As soon as the traffic exceeds the specified limit, sending of new packets is delayed until the traffic drops below the limit, and an appropriate message is logged to the Collaboration Services Event log.

Incoming Traffic

To control the incoming traffic, the branch forests and an HQ forest can limit the number of incoming messages and the overall size of the incoming traffic.

Use the Control incoming traffic and Control incoming traffic by number of messages options to protect the service from being overloaded with large amounts of synchronization data:

- If the Control incoming traffic check box is selected, the service will process only a limited amount of synchronization data per hour.
- If the Control incoming traffic by number of messages check box is selected, the service will process only a limited number of incoming messages every hour.

You can use these options to control incoming mail flow to ensure safe service functionality. However, the use of these options may impact the initial synchronization performance significantly, so it is recommended to turn them on only after the initial synchronization is over for all collections.

The HQ forest web interface includes two additional options that can be used to set the bandwidth and quotas for branch forests. These options let the HQ forest administrator specify which message and traffic quotas should be assigned each newly-registered branch forest.

To ensure optimal synchronization performance between all synchronization partners, HQ constantly redistributes the message quota and the bandwidth between the branch forests. The redistribution is performed every hour for each branch.

Collaboration Services uses an adaptive algorithm when redistributing available bandwidth and message quotas between branches. This algorithm is quite complex and takes into account statistical information, such as when the branch was added and its average bandwidth usage.
Fine-Tuning and Maintenance

- Active Directory Synchronization Performance
- Resource Throttling
Active Directory Synchronization Performance

To improve Collaboration Services performance, first register schmmgmt.dll (which is located in the \COMPUTERNAME\admin$\SYSTEM32 subfolder). Then, using the MMC console, add the Active Directory Schema Snap-In into the program group of the Administrative Tool and make sure indexing is turned on for the following object attributes:

- proxyAddresses
- mail
- targetAddress
- mailNickName
- Extension attribute used by Collaboration Services for storing data (selected during the Collaboration Services setup procedure—by default, extensionAttribute10)

Resource Throttling

To ensure safe service functionality, Collaboration Services always monitors the usage of system memory and disk space. Using the Resource Usage page of Collaboration Services properties, you can adjust the related settings according to your needs.

Memory Usage

This page allows you to specify whether the service memory usage should be limited on the Collaboration Services server. This helps you protect the system resources from being overloaded. Use the Available memory slider to adjust the maximum amount of system memory that can be used by Collaboration Services.

Though the Available memory slider can be set to the minimum value, there is a minimum amount of memory that the service is allowed to use. This amount is based on the system requirements and cannot be changed. Also, the memory usage for the first 60 seconds after the service starts is not limited to prevent the service from being cyclically restarted.
Fine-Tuning and Maintenance

Figure 14: Memory usage information

Decreasing the memory usage limit worsens the service performance, so this is not recommended unless other software is running on the same computer with Collaboration Services.

Disk Usage

This page allows you to specify the service behavior if the computer the service is installed on runs out of free disk space.

Figure 15: Disk usage options
• Select the Limit disk usage to make the service monitor the disk space usage on the volume where the service is installed.

   It is highly recommended to have this option turned on.

• To receive notifications when a specified percentage of free disk space is exceeded, select Send notifications if used disk space is more than option.

   The notification format and the notification service to be used can be configured on the Logging page of the Collaboration Services Properties dialog box.

• To specify the notification time interval, use the Re-send notification every drop-down box.

• The Switch the service to suspend mode if free disk is less than option allows you to choose the minimum amount of free disk space for the service to be allowed to run. If the free disk space drops below this threshold, the service is automatically switched to suspend mode. When the service runs in suspend mode, no synchronization is performed. The service will automatically switch to normal mode as soon as the specified minimum amount of disk space is free.

**Resource Usage Statistics Report**

To view statistics information on resource usage, select the Resource Usage node in the management tree. The following information is displayed in the statistics pane of the Collaboration Services web interface:

<table>
<thead>
<tr>
<th>STATISTICS SECTION</th>
<th>CAN BE USED FOR</th>
<th>DISPLAYS</th>
</tr>
</thead>
</table>
| General information | Checking the status of the synchronization service | Service state, which can have the following values:  
  • Running  
  • Suspended |
### Statistics Update Frequency

Use the UI Settings page to configure whether and how often Collaboration Services should automatically refresh the synchronization statistics. It is not recommended to set the refresh period to a low value, because the refresh may take significant time on slow connections or if the Collaboration Service server is too busy processing synchronization data.

By default, the automatic refresh is disabled in remote connection mode because it is assumed that the remote connection speed is low. If this is not the case, you can enable the refresh. Otherwise, you need to refresh statistics manually using the Refresh button in the user interface.

<table>
<thead>
<tr>
<th>STATISTICS SECTION</th>
<th>CAN BE USED FOR</th>
<th>DISPLAYS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory resources</td>
<td>Checking the amount of memory currently used by the synchronization service</td>
<td>• The time of last memory usage information update</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Service memory usage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Service handles usage</td>
</tr>
<tr>
<td>Disk resources</td>
<td>Checking the amount of the available free disk space</td>
<td>• The time of last disk usage information update</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Working directory</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Disk usage statistics</td>
</tr>
<tr>
<td>Storage integrity</td>
<td>Checking the condition of the configuration database</td>
<td>Configuration database integrity, which can have the following values:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• OK</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Recoverable error detected</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Fatal error detected</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The time of last disk usage information update</td>
</tr>
</tbody>
</table>
Backup, Restore, and Troubleshooting

- Backup and Restore Options
- Troubleshooting
- Repair or Uninstall
Backup and Restore Options

To protect the configuration database from power and hardware failures, Collaboration Services is by default configured to perform automatic configuration backup and restore. All mission-critical information is saved in the database file containing all currently existing collections, statistics, and the service configuration information. If a failure occurs, the service will automatically detect whether any configuration data is corrupted and perform an automatic restore.

It is highly recommended to have both automatic backup and restore always enabled (this is the default state).

Use the Backup & Restore page of the Collaboration Service Properties dialog box to adjust the backup and restore options.

Figure 16: Backup and restore general options

In particular, you can specify:

- Whether and how often the automatic backup should be performed.
- How many backup files should be kept.

If you have applied significant changes to the Collaboration Services configuration, you may want to perform an immediate configuration backup. To do this, click the Backup Now button.

The restore options allow you to:

- Enable automatic restore (recommended).
• Select what backups should be used if restore from the latest backup fails.

## Troubleshooting

This section describes the some issues you may face during Collaboration Services operations and explains how to resolve them:

<table>
<thead>
<tr>
<th>SYMPTOMS</th>
<th>POSSIBLE REASONS</th>
<th>SOLUTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>You see the following message in a particular synchronization partner's statistics: “Synchronization partner is not responding”</td>
<td>The SMTP connection between forests is configured incorrectly, - OR - The encryption key was changed for one of the forests.</td>
<td>Check whether the SMTP channel is working by sending a test email between the service mailboxes of both forests in both directions. Export the forests’ public key files and re-register both forests using the newly-generated public key files.</td>
</tr>
<tr>
<td>While creating or editing a collection in remote connection mode, you get the following error: “Unspecified error: The size of the request exceeds the limit allowed by the server”</td>
<td>There is a limit on the amount of data that can be sent from client to server using SOAP protocol. You can exceed this default limit when you try to add more than 100 containers or groups to the collection.</td>
<td>Either connect to the web interface locally, or increase the following value in the registry on the computer where you open the web interface: HKLM\SOFTWARE\Microsoft\MSSOAP\SOAPISAP MaxPostSize : REG_DWORD This value is the maximum size, in kilobytes, of a SOAP message that you can POST to the server. The default setting is 100.</td>
</tr>
<tr>
<td>Some objects are not available from a collection your forest subscribes to.</td>
<td>The initial synchronization is still being performed.</td>
<td>Wait until the initial synchronization is completed. It could take up to a few days for large collections, depending on the servers’ hardware and network conditions.</td>
</tr>
</tbody>
</table>
**Repair or Uninstall**

*To repair or remove Collaboration Services*

1. From the Start menu, select **Control Panel | Add/Remove Programs | Quest Collaboration Services**, and select **Change**.
2. If you need to Repair, click the **Options** button, select the check boxes next to the required repairs, and then click **OK**.

   *The repair wizard will guide you through the repair process.*

   **– OR –**

   To completely remove the application, select **Remove**.

   *Collaboration Services and the web management console (if installed locally) will be uninstalled.*

   **– OR –**

   To remove a Collaboration Service web console remotely connected to Collaboration Services, go to **Control panel | Add/Remove Programs | Quest Collaboration Services User Interface** and select **Remove**.

<table>
<thead>
<tr>
<th>SYMPTOMS</th>
<th>POSSIBLE REASONS</th>
<th>SOLUTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>One or more objects are not available from a collection your forest subscribes to, but the initial synchronization is already completed.</td>
<td>Some of the objects were accidentally deleted from the Collaboration Services container.</td>
<td>Initiate re-publication of the collection using the Request re-publishing command.</td>
</tr>
<tr>
<td>You cannot add newly-added custom attributes, or objects from a newly-added domain to the synchronization.</td>
<td>Collaboration Services reads a forest’s schema only once, during the service start-up. Thus, on-going changes to the schema cannot be detected.</td>
<td>Restart the synchronization service using the Services MMC snap-in.</td>
</tr>
</tbody>
</table>

**SYMPTOMS POSSIBLE REASONS SOLUTION**
Appendix A: Customizing the Format of Synchronized Data

Sometimes publishing or subscribing administrators might want to change the format or appearance of the data they publish or subscribe to. To do that, mappers can be used. A mapper is a plug-in component that changes the appearance of data that you publish or subscribe to.

If you use mappers when creating a collection, the mappers modify the data before it is published, so all subscribers get modified data. If you use mappers while subscribing to a collection, the mappers modify the published data before it is applied to your particular forest.

Mappers applied during publication do not modify the original Active Directory objects; only the information to be published is modified before it is distributed to other forests.

Collaboration Services is shipped with the following mappers:

- User to Contact mapper
- Group to Contact mapper
- Suffix mapper
- Attribute filter mapper
- SMTP address filter mapper

User to Contact Mapper

This mapper converts users and inetOrgPerson objects into contacts. Converting these objects to contacts might be required to meet internal regulations. This mapper can also be useful if you have software that is licensed by the number of user objects in Active Directory and you do not want to buy additional licenses.
In the Global Address List, contacts are marked with a globe next to their names, while users are not. To achieve full transparency, you should avoid using this mapper if possible, so that users from all forests look the same in the GAL. Otherwise, end users may be puzzled by the differences.

**Group to Contact Mapper**

This mapper converts groups into contacts, allowing you to hide group membership from other forests. This is useful if you want users from other forest to be able to send mail to your distribution groups but do not want the group members to be revealed.

When publishing a group as a contact, it is not necessary to publish all group members for distribution lists to function, as long as email messages sent to the contact are always redirected to the original group object in the group’s “home” forest.

**Mapping Groups from Exchange 2007**

If you want to use the Group to Contact Mapper for a source group from an Exchange 2007 organization, you must first turn off user authentication. Otherwise, message delivery to the target contact will fail.

*To Disable User Authentication in Exchange 2007*

2. On the Mail Flow Settings tab, double click Mail Delivery Restrictions, and clear the "Require that all senders are authenticated" check box.

**Suffix Mapper**

This mapper adds a specified suffix to the display name of the published objects so that the users can distinguish published objects from the objects of their own forest. For example, you may want to add the [PartnerCo] suffix to the display names of objects from a partner company in the subscribed collection to emphasize that they belong to the other company.
Appendix A: Customizing the Format of Synchronized Data

Attribute Filter Mapper

This mapper allows a subscribing forest's administrator to filter out unnecessary or undesired attributes, thus controlling exactly which attributes are applied to the forest.

![Attribute filter mapper](image)

**Figure 17: Attribute filter mapper**

SMTP Filter Mapper

This mapper allows a subscribing administrator to defend against "address stealing." By adding an SMTP address to the published object, the publishing administrator effectively assigns his forest's users email addresses from another forest. In a merger or acquisition scenario, this is usually a requirement and is done on purpose. However, the same action can also be performed by a malicious administrator in a partner collaboration scenario, causing unsanctioned email address usage with all associated risks, including possible information leaks. By using this mapper and filtering out your own forest's addresses from incoming objects, you protect your forest from this type of attack.
To configure the mapper, add all of your company’s SMTP email address namespaces (including the @ sign) to the list of namespaces to be filtered out. You can also import a list of namespaces from a text file by clicking the Import button and choosing the file. The file should list the SMTP namespaces, one namespace per line.

Figure 18: SMTP filter mapper
Appendix B: Collaboration Services Events

To view the service events in the Collaboration Services web interface, select the Event node in the management tree.

Figure 19: Collaboration Services web interface

You can filter, sort, and save events and search for particular items using the commands from the Events node’s shortcut menu.

To clear the current event view (all events displayed in the management console), use Clear All Alerts command (these records stay intact in the event log).

You can right-click any item in the right pane and use the following shortcut menu commands:

- **Find**—Enables you to search for specific things such as EventIDs, types.
- **Sort and Select Columns**—Changes the way the events are displayed.
- **Mark As Read**—Highlights the last viewed item.
- **Refresh**—Updates the event list being displayed.
- **Properties**—Enables you to view event details.
Quest Collaboration Services

Event Format

Collaboration Services events have the following format:

- **Type**—One of the following:
  - Informational
  - Warning
  - Error
- **Level**—Event severity level:
  - High
  - Normal
  - Low
- **ID**—Unique event ID
- **Date, Time**—When the event was generated
- **Header**—Event source
- **Description**—Detailed event description

*To explore an event’s details*

1. Right-click the event in the right pane and select **Properties**.
2. To view the details of the next or the previous item in the list, click the up or down arrow buttons in this dialog box. To copy event data to the clipboard, click the **Copy** button.

Using Event Filters

Predefined Filters

To help you view the events more efficiently, Collaboration Services allows you to use event filters. There are several predefined event filters:

- Critical errors
- Errors and Warning
- Important
- Informational

To use one of these filters, select the corresponding sub-node of the Events node in the management console.
Custom Filters

You can customize any filter by selecting it in the management tree under the Events node and selecting the Edit Filter command. The Create Events Filter wizard is started to help you with the procedure.

To create a new event filter

1. Run the Create Events Filter wizard.
2. Specify a name for the new event filter and select the template you want to base it on. The following templates are available:
   - Custom (allows you to make a filter of your own)
   - Informational
   - Important
   - Errors and Warnings
   - Critical Errors
3. Select which types, importance, levels, and IDs of events should be shown by the filter.
4. Set up the filter to include or exclude events with a specified header or description by using a corresponding mask.
   
   If the Exclude check box is cleared, events containing the specified header or description are included in the view; otherwise, they are excluded from it.

5. You can configure the filter to show only those events that occurred during a specified period of time. To specify the beginning of this period, either select Events on and specify a particular date and time, or choose to show all events starting from the first one by choosing First event. Similarly, to define the end of the period, you can either specify the end date and time or choose to show all events up to the last one.
INDEX

A
Active Directory
  limiting the objects to synchronize 49
  synchronization performance 66
attribute filter mapper 77
automatic conflict resolution 33

B
backup and restore 72

C
configure
  Active Directory access settings 9
  alerts 11
  collection 28
  service mailbox 8
  synchronization 44
  Synchronization Partners 11
conflicts 32
  delete 34
  manual resolution 40
  matching 36
  pre-matching 37
  resolving 32
connection options 4
create
  collection 18

D
data storage 54
  database clean up 58
  delete conflicts 34
  disable a collection 26
  disk usage 67

E
eedit
  collection 26
  subscription properties 28
  enable a collection 26
  events 79
Exchange 2007
  using group to contact mapper with 76

G
group to contact mapper 76

L
logging 10

M
mapper 75
  attribute filter 77
  group to contact 76
  SMTP filter 77
  suffix 76
  user to contact 75
matching 36
memory usage 66

P
pre-matching 37
Publish Collection Wizard 18

R
receive messages 61
Recipient Update Service 9
remove a collection 29
repair 74
resolving conflicts 32
resource throttling 66

S
send messages 60
SMTP mapper 77
subscribe to a collection 27
suffix mapper 76
synchronization
  Active Directory settings 46
  calendar information 53
  customizing the data format 75
  free/busy 50
  general settings 45
  manual settings 56
  performance 66

T
Third Party Contributions 86
transport
  quotas 62
  receive 61
  scheduling 62
  send 60
Quest Collaboration Services

transport management 60
troubleshooting 73

U
unsubscribe from a collection 29
usage statistics 68
user to contact mapper 75

V
view collection settings 30

W
web management console 3
About Quest Software

Now more than ever, organizations need to work smart and improve efficiency. Quest Software creates and supports smart systems management products—helping our customers solve everyday IT challenges faster and easier. Visit www.quest.com for more information.

Contacting Quest Software

Refer to our Web site for regional and international office information.

Email: info@quest.com
Mail:
Quest Software, Inc.
World Headquarters
5 Polaris Way
Aliso Viejo, CA 92656
USA
Web site: www.quest.com

Contacting Quest Support

Quest Support is available to customers who have a trial version of a Quest product or who have purchased a Quest product and have a valid maintenance contract. Quest Support provides unlimited 24x7 access to SupportLink, our self-service portal. Visit SupportLink at http://support.quest.com.

From SupportLink, you can do the following:

- Retrieve thousands of solutions from our online Knowledgebase
- Download the latest releases and service packs
- Create, update and review Support cases

View the Global Support Guide for a detailed explanation of support programs, online services, contact information, policies and procedures. The guide is available at: http://support.quest.com.
Quest Collaboration Services

Third Party Contributions

Quest Collaboration Services contains some third party components (listed below). Copies of their licenses may be found on our website at http://www.quest.com/legal/third-party-licenses.aspx

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>LICENSE OR ACKNOWLEDGEMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Synchronization Service</td>
<td>zlib 1.2.3</td>
</tr>
<tr>
<td>Synchronization Service</td>
<td>Boost 1.34.1</td>
</tr>
</tbody>
</table>