Microsoft Office SharePoint Server 2007

Note

The Microsoft Office SharePoint Server 2007 application is used to access both the Windows SharePoint Services (WSS) and the SharePoint Portal Server (SPS).

Application-Specific Settings

This section describes the required and optional application-specific settings for the Microsoft Office SharePoint Server 2007 application, as follows:

• Requirements on the Endpoint Computer.

• Additional configuration steps you may have to take in these cases:

• When more than one SharePoint Server application is defined on the same trunk.

• When one SharePoint Server application is defined on the trunk, with multiple servers.

These steps are described in Configuration in a Multiple-Address Setup.

• Preventing end-users from uploading, checking-in files, and saving files from Microsoft Office applications to the SharePoint Server, unless their computer meets the security policy requirements you define, as described in Blocking File Upload Operations.

• Preventing end-users from downloading files, exporting to a spreadsheet, or editing datasheets, unless their computer meets the security policy requirements you define, as described in Blocking File Download Operations.

• Restricting end-users' access to sensitive areas of the application, unless their computer meets the security policy requirements you define, as described in Restricting Access to Zones and Areas.

• Enabling the "Explorer View" option, as described in Enabling the Explorer View Option.

• Enabling access from the SharePoint Server to third-party applications, as described in Integration with Third-Party Applications.

Requirements on the Endpoint Computer

• For maximal integration, Microsoft Office 2003 SP1 or higher must be installed on the endpoint computer.

• In order to enable integration with Microsoft Office applications, the Attachment Wiper client component must be installed on the endpoint computer. On computers where the Attachment Wiper is not installed, Office documents will be displayed in the browser, and will not be cached.

Configuration in a Multiple-Address Setup

Note

• This section is not relevant in these cases:

• If there is only one SharePoint Server application in the trunk, with one server, defined by a single, plain-text IP address or hostname and a single port number.

• If there are two or more trunks, each with a single SharePoint application with one server.

• If you define more than one trunk with multiple addresses, you must repeat the instructions in this section for each of the trunks.

• When end-users access more than one SharePoint site from the same trunk, working with Office documents is only enabled from the first site accessed.

This section describes additional configuration steps that are relevant when you use the same IAG trunk to access more than one SharePoint Server. Such a multiple-address setup can be achieved in two different ways:

• One SharePoint Server application is defined on the trunk, with multiple servers. That is, the application's servers are defined using multiple IP addresses, a subnet, or regular expressions.

• More than one SharePoint Server application is defined on the same trunk.

In both these setups, it is recommended that all SharePoint Servers in the trunk are defined with port 80. If another port number is defined, this may impede the functionality of Microsoft Office applications when accessed via the SharePoint Server application.

The first time you add a SharePoint Server application to the trunk, the system automatically creates two dynamic Manual URL Replacement rerouting rules, that reroute the requests to the application server. Each rule includes two server definitions:

• A dynamic parameter, *DynamicSharepointServer*, which is used to determine the destination server to which the request is rerouted.

• A fallback server, to which requests are rerouted in case the dynamic parameter cannot be resolved.

The fallback server is the first server that is defined for the first SharePoint Server application you add to the trunk, regardless of any servers you later add to the application. In addition, since the same fallback server is used for all the SharePoint Server applications in a trunk, if you later add more SharePoint Server applications to the trunk, they will all use the server you initially defined as the fallback server.

For example: If the trunk includes one SharePoint Server application with two servers, ServerA and ServerB, and ServerA is the fallback server, and you then add a new SharePoint Server application to the trunk, with ServerC, the fallback server for the new application is ServerA.

If you create a different trunk with SharePoint Server applications, a new set of dynamic Manual URL Replacement rerouting rules is created for that trunk, independently of the existing trunk.

Note

If you edit the definition of the server that is used as the fallback server, or if you delete that server, you must redefine the fallback server, as described in this procedure.

Tip

• Once you add an application to the trunk, the configuration of the application servers can be seen and edited in the Web Servers tab of the Application Properties dialog box.

• Manual URL Replacement rules are visible in the Application Access Portal tab of the Advanced Trunk Configuration window. For a full description of this feature, refer to the Intelligent Application Gateway Advanced Configuration guide, to the chapter "Optimizing Portal Performance".

The following procedure describes how you can change the fallback server defined in the rerouting rules. Note that:

• When the rules are created for a "Subnet" or "Regular Expression" address-type, there is no pre-defined fallback server, and you must define one.

• When the rules are created for a server that is defined by an "IP/Host" address-type, you can optionally change the fallback server.

Note

Make sure you implement the changes for both SharePoint Server rules.

To change the fallback server:

1. In the Configuration program, access the Advanced Trunk Configuration window.

2. In the Application Access Portal tab, in the "Manual URL Replacement" area, double-click the first SharePoint Server rule.

3. In the URL Change dialog box, edit the server definitions in the "Server Name" field as follows:

• For a server that is defined by a subnet or regular expression, the default value of "Server Name" is:

*DynamicSharepointServer*localhost

Change this value to

DynamicSharepointServer<fallback_server>

Where <fallback_server> is the IP address or hostname of the fallback server.

Do not change the parameter *DynamicSharepointServer*.

• For a server that is defined by an IP address or hostname, the default value of "Server Name" is:

DynamicSharepointServer<fallback_server>

Where <fallback_server> is the IP address or hostname of the first SharePoint Server that was defined on the trunk. You can change the value of <fallback_server> as required.

Do not change the parameter *DynamicSharepointServer*.

Note

Do not deselect the "Dynamic" option next to the "Server Name" field.

4. Repeat steps 2–3 for the second SharePoint Server rule.

5. In the Configuration program, click to activate the configuration.

If the dynamic parameter cannot be resolved, requests will be rerouted to the fallback server you defined here.

Blocking File Upload Operations

This section describes how you utilize the application's Upload policy, so that end-users cannot do the following, unless their computer meets the security policy requirements you define:

• Upload files.

• Save files from Microsoft Office applications to SharePoint Server.

Users that are blocked are notified accordingly.

To block file upload operations:

1. In the Configuration program, access the Application Properties dialog box.

2. Apply the policy on the client side:

a) Click [Edit Policies...] to open the Policies dialog box.

b) In the Policies dialog box, under the "Policies" group, select the policy "SharePoint 2007 Upload Checkin", then click [Edit...] to open the Advanced Policy Editor.

c) The "SharePoint 2007 Upload Checkin" policy affects the way in which the upload operations described in this section are handled on the client side only. By default, the value of the policy is "True", and it does not prevent upload operations from endpoint computers on the client side. You can:

• Edit the policy to comply with your corporate policy, so that non-complying computers are blocked. Note that you can use the "Default Web Application Upload" policy as a basis for your definitions.

Or,

• Change the policy value to "False" so that all endpoint computers are blocked.

For details, refer to the Intelligent Application Gateway User Guide, to the section "Endpoint Policies".

Once you activate the configuration, upload operations are blocked on the client side, according to your definitions.

3. Apply the policy on the server side: in the General tab of the Application Properties dialog box, in the "Endpoint Policies" area, from the "Upload" drop-down list, select the policy "SharePoint 2007 Upload Checkin".

4. In the Configuration program, click to activate the configuration.

The upload operations described in this section will be blocked, on both the client and the server side, on endpoint computers that do not comply with the security policy you defined here.

Note

The above steps ensure full correlation of the policy on the client and server sides. If you wish to cancel the policy, you must:

• Redefine the policy value as "True".

And

• Cancel selection of the policy in the General tab of the Application Properties dialog box.

Blocking File Download Operations

This section describes how you utilize the application's Download policy, so that end-users cannot do the following, unless their computer meets the security policy requirements you define:

• Download files.

• Use the Edit in Datasheet option.

Users that are blocked are notified accordingly.

To block file download operations:

1. In the Configuration program, access the General tab of the Application Properties dialog box.

2. Apply the policy on the client side:

a) Click [Edit Policies...] to open the Policies dialog box.

b) In the Policies dialog box, under the "Policies" group, select the policy "SharePoint 2007 Download", then click [Edit...] to open the Advanced Policy Editor.

c) The "SharePoint 2007 Download" policy affects the way in which the file download operations described in this section are handled on the client side only. By default, the value of the policy is "True", and it does not prevent download operations from endpoint computers on the client side. You can:

• Edit the policy to comply with your corporate policy, so that non-complying computers are blocked. Note that you can use the "Default Web Application Download" policy as a basis for your definitions.

Or,

• Change the policy value to "False" so that all endpoint computers are blocked.

For details, refer to the Intelligent Application Gateway User Guide, to the section "Endpoint Policies".

Once you activate the configuration, download operations are blocked on the client side, according to your definitions.

3. Apply the policy on the server side: in the General tab of the Application Properties dialog box, in the "Endpoint Policies" area, from the "Download" drop-down list, select the policy "SharePoint 2007 Download".

4. In the Configuration program, click to activate the configuration.

The download operations described in this section will be blocked, on both the client and the server side, on endpoint computers that do not comply with the security policy you defined here.

Note

The above steps ensure full correlation of the policy on the client and server sides. If you wish to cancel the policy, you must:

• Redefine the policy value as "True".

And

• Cancel selection of the policy in the General tab of the Application Properties dialog box.

Restricting Access to Zones and Areas

This section describes how you utilize the application's Restricted Zone policy, so that end-users cannot access sensitive zones and areas of the application, such as administrative zones, if their computer does not meet the security policy requirements.

In order to enable this option, once you finish adding the application to the trunk, you need to assign a unique Restricted Zone policy to the application, as described below. The defined zones and areas are blocked on the server side, and users that are blocked are notified accordingly.

To restrict access to zones and areas:

1. In the Configuration program, access the Application Properties dialog box.

2. In the Web Settings tab, verify that the option "Activate Restricted Zone" is activated.

3. In the General tab, in the "Endpoint Policies" area, from the "Restricted Zone" drop-down list, select the policy "Default Web Application Restricted Zone".

4. Still in the General tab, click [Edit Policies...] to open the Policies dialog box.

5. In the Policies dialog box, under the "Policies" group, select the policy "Default Web Application Restricted Zone", then click [Edit...] to open the Advanced Policy Editor.

6. By default, the value of the policy is "True", and it enables access to all zones and areas of the application from all endpoint computers. You can:

• Edit the policy to comply with your corporate policy, so that non-complying computers are denied access to the administrative zones.

Or,

• Change the policy value to "False" to prevent any access to the administrative zones from endpoint computers.

For details, refer to the Intelligent Application Gateway User Guide, to the section "Endpoint Policies".

7. You can also use this feature to block access to additional areas of the application, such as the News area. In order to do so, take the following steps:

a) Access the Global URL Settings tab of the Advanced Trunk Configuration window, and, next to "Restricted Zone URLs", click [Configure...].

b) Use the Restricted Zone URLs Settings dialog box to add a rule with the URL of the area you wish to block. For example, to block access to the News area, add the following rule:

• Type: SharePoint 2007

• URL: .*/news/default\.aspx

• Method: GET

For details, refer to the Intelligent Application Gateway Advanced Configuration guide, to the section "Global URL Settings Tab—URL Settings".

c) Repeat steps a–b to add as many areas as required.

8. In the Configuration program, click to activate the configuration.

Access to the administrative zones, and to the areas you defined, will will be blocked on the server side, for endpoint computers that do not comply with the security policy you defined here.

Enabling the Explorer View Option

By default, the "Explorer View" option is blocked. You can enable this option as described in this section; note that this option may not function as expected.

To enable the Explorer View option:

1. In the Configuration program, access the Application Properties dialog box.

2. In the General tab, in the "Endpoint Policies" area, click [Edit Policies...] to open the Policies dialog box.

3. In the Policies dialog box, under the "Policies" group, select the policy "SharePoint 2007 Enable Explorer View", then click [Edit...] to open the Advanced Policy Editor.

4. By default, the value of the policy is "False". Change the policy value to "True" to enable the Explorer View option.

5. In the Configuration program, click to activate the configuration.

End-users can now access the "Explorer View" option.

Integration with Third-Party Applications

This section describes how you enable access from the SharePoint Server to third-party applications, via the SharePoint Server webparts, when the SharePoint Server is accessed through the IAG. This is required only for third-party applications that communicate directly with the application server, for example Outlook Web Access.

For applications of this type, you need to add a corresponding application to the Whale portal. In the Configuration program, use the Add Application Wizard to add the required applications to the trunk that enables access to the SharePoint Server.