Intelligent Application Gateway

Application Aware™ Settings

December 2006

Version 3.7

TRADEMARKS

Application Aware, and Attachment Wiper are service marks, trademarks or registered trademarks of Whale Communications or its subsidiaries in the United States and other countries, or both.

Netscape, and Netscape Navigator are service marks, trademarks or registered trademarks of America Online, Inc. or its subsidiaries in the United States and other countries, or both.

AppGate, and MindTerm are service marks, trademarks or registered trademarks of AppGate Network Security AB or its subsidiaries in the United States and other countries, or both.

Carbon, Macintosh, Mac OS, and Safari are service marks, trademarks or registered trademarks of Apple Computer, Inc. or its subsidiaries in the United States and other countries, or both.

Tuxedo is a service mark, trademark or registered trademark of BEA Systems, Inc. or its subsidiaries in the United States and other countries, or both.

Citrix , Citrix NFuse, Citrix Presentation Server, Citrix MetaFrame, Citrix SecureGateway, and ICA, are service marks, trademarks or registered trademarks of Citrix Systems, Inc. or its subsidiaries in the United States and other countries, or both.

Debian is a service mark, trademark or registered trademark of Software in the Public Interest, Inc. or its subsidiaries in the United States and other countries, or both.

Documentum Webtop is a service mark, trademark or registered trademark of EMC Corporation or its subsidiaries in the United States and other countries, or both.

GNU, and GZip are service marks, trademarks or registered trademarks of Free Software Foundation, Inc. or its subsidiaries in the United States and other countries, or both.

Domino, Lotus, IBM Lotus, iNotes, Lotus iNotes, Lotus Domino, Notes, Sametime, and WebSphere are service marks, trademarks or registered trademarks of IBM Corporation or its subsidiaries in the United States and other countries, or both.

Linux is a service mark, trademark or registered trademark of Linus Torvalds or its subsidiaries in the United States and other countries, or both.

Active Directory, ActiveSync, ActiveX, Excel, Microsoft, Outlook, SharePoint, Visual Basic, Windows Mobile, Windows NT, Windows Server are service marks, trademarks or registered trademarks of Microsoft Corporation or its subsidiaries in the United States and other countries, or both.

Camino, Firefox and Mozilla are service marks, trademarks or registered trademarks of Mozilla Foundation or its subsidiaries in the United States and other countries, or both.

Novell, Novell Directory Services, Novell NetWare, and SUSE are service marks, trademarks or registered trademarks of Novell, Inc. or its subsidiaries in the United States and other countries, or both.

PGP is a service mark, trademark or registered trademark of PGP Corporation or its subsidiaries in the United States and other countries, or both.

DISCLAIMER

LIMITATION OF LIABILITY

Without limiting the effect of the preceding clauses, the Company's maximum liability, if any, for damages (including but not limited to liability arising out of contract, negligence, misrepresentation, strict liability in tort or warranty of any kind) shall not exceed the consideration paid to the Company for the product. The Company shall under no circumstances be liable for damages arising out of any claim (including but not limited to a claim for personal injury or property damage) made by any third person or party.

Document Name	Intelligent Application Gateway Application Aware Settings
Document Revision	3.7
Date	December 2006
Software Version No.	3.7

Contents

Introduction

The Intelligent Application Gateway (IAG) application aware technology enables it to address application-specific issues. This includes security concerns, as well as functionality requirements, which offer organizations the ability to customize the behavior of specific applications when accessed remotely.

The IAG provides out-of-the-box support for key applications, to allow for rapid optimization of most popular applications in use today. In addition, the application aware approach provides you with tools and interfaces that enable you to define features which are not supported out-of-the-box for each of your applications individually.

About This Guide

This Guide provides application aware instructions and information pertaining to some of the applications supported by the IAG, as follows:

- Application-specific requirements and, where applicable, configuration instructions.
- Information regarding application-specific temporary files that are deleted by the Attachment Wiper™, and instructions, where relevant, for defining Attachment Wiper parameters.

Conventions Used in This Guide

This section explains the conventions used throughout this Guide.

Menu Item	Menu names and menu items.
Button	Buttons that you select with the mouse.
	Icons that you select with the mouse are represented graphically.
Procedure	Title of an operating procedure.
Computer text	System files and information that you type in.

Note
Important information you should note.

> **Tip**
> Helpful tips for working with the IAG.

> **Caution**
> Information needed to protect and to avoid damaging hardware or software.

All Domino® (Webmail 5.x/6.x/7.x and iNotes™) Interfaces

Application-Specific Settings

The application-specific settings for Lotus® Domino Web Access applications include the following options:

- Preventing users from sending email attachments unless their computer meets the defined security policy requirements, while blocking attachment sending at the client-side, as described in "Client-Side Attachment Blocking" on page 11. This option is applicable for Lotus Domino Web Access version 6.5 and higher.

- Preventing users from forwarding email attachments or replying with an attachment, as described in "Blocking Attachment Forwarding" on page 12. This option is applicable for Lotus Domino Web Access version 6.5 and higher.

- Enabling Domino Offline Services (DOLS) via the application, as described in "Enabling Domino Offline Services" on page 13. This option is applicable for Lotus Domino Web Access version 7.0, accessed via a Portal trunk.

- Running Sametime® Instant Messaging from within the Lotus Domino Web Access Interface, as described in "Sametime Instant Messaging" on page 13. This option is applicable for Lotus Domino Web Access version 6.5.x, accessed via a Portal trunk.

Client-Side Attachment Blocking

For Lotus Domino Web Access version 6.5 and higher, you can enhance the application's Upload policy, so that when end-users cannot send email attachments because their computer does not meet the security policy requirements, attachment sending is blocked at the client-side. When this option is used, a notification is displayed in the "Attachments" area of the Lotus Domino Web Access interface, and users cannot add attachments.

> ⚠️ **Caution**
>
> It is recommended to use this option in order to apply attachment blocking to the application. If you use the Default Web application Upload policy, attachment blocking at the server-side may cause problems on the endpoint computer. **For example:** the browser might stop functioning.

In order to enable this option, once you finish adding the application to the trunk, you need to assign a unique Upload policy to the application.

To block attachment sending at the client-side:

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

2. In the General tab, in the "Endpoint Policies" area, from the "Upload" drop-down list, select the policy "Domino Web Access 6 5 and 7 Upload".

3. By default, the value of the policy is "True", and it does not prevent uploads from any endpoint computer. If required, change the policy to comply with your corporate policy. For details, refer to the *Intelligent Application Gateway User Guide*, to the section "Endpoint Policies".

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

Attachments cannot be sent from endpoint computers.

Blocking Attachment Forwarding

For Lotus Domino Web Access version 6.5 and higher, you can enhance the application's Upload policy, so that end-users cannot forward email attachments or reply with an attachment. Blocking can be defined so that it is activated:

· If the endpoint computer does not comply with security policy requirements you define. For example, if the required antivirus or anti-spyware software, or the Attachment Wiper, are not installed on the computer.

Or,

· At all times.

To block attachment forwarding:

1. In the Configuration program, open the Application Properties dialog box, and, in the General tab, click `Edit Policies...`.

2. In the Policies dialog box, click the **+** sign to expand the Expressions group, select the expression "Enable Domino Web Access Forward and Reply with Attachments", then click `Edit...`.

3. In the Advanced Policy Editor, edit the expression as follows:

    · If you want to define the prerequisites that the computer must meet in order to enable attachment forwarding, remove the default value True, and add the appropriate variables to the expression.
    Attachment forwarding is then blocked on endpoint computers that do not comply with the defined criteria.
    For more information about editing policies, refer to the *Intelligent Application Gateway User Guide*, to the chapter "Endpoint Security", to the section "Configuration in the Advanced Policy Editor".

- If you want replying and forwarding with attachments to be blocked at all times, change the value from `True` to `False`.

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

When addressing incoming email messages, end-users cannot use these functions:

- *Forward*
- *Reply To Sender with History*
- *Reply To All with History*

Users are notified accordingly.

Enabling Domino Offline Services

This section describes the steps you need to take at the IAG in order to enables users to run DOLS from within the Domino interface. This option is applicable for Lotus Domino Web Access version 7.0 accessed via a Portal trunk.

To enable DOLS:

1. In the Configuration program, use the Add Application Wizard to add the Domino Offline Services 7.0 (Single/Multi Servers) application to the trunk (from the "Client/Server and Legacy Applications" group).
2. Define the application you added in step 1 as a prerequisite application to the All Domino application, as follows:
   a) Access the Application Properties dialog box of the All Domino application.
   b) In the General tab, in the "Prerequisite Applications" list, check the box next to the Sametime Domino Offline Services application, then click OK.

3. In the Configuration program, click ⚙ to activate the configuration.

Whenever users launch the All Domino application, the prerequisite Domino Offline Services application is launched, as well. Launching this application opens a relay from the endpoint computer to the DOLS server. Users can then run DOLS from within the Domino interface.

Sametime Instant Messaging

For Lotus Domino Web Access version 6.5.x, the IAG enables users to run Sametime Instant Messaging from within the Lotus Domino Web Access interface. This option is applicable if you are using Sametime Instant Messaging from within the Lotus Domino Web Access interface.

Some of the Sametime Instant Messaging tools require that the IAG's SSL Wrapper client component be installed on the endpoint computer, as follows:

- The Sametime Instant Messaging "Chat" tool, which is HTTP-based, does not require the SSL Wrapper client component.

- The Sametime Instant Messaging "Meeting Tools" require that the SSL Wrapper client component be installed.

> **Tip**
> The SSL Wrapper component is part of the Whale Client Components. For more information about the SSL Wrapper client component, including prerequisites on the endpoint computer, refer to the *Intelligent Application Gateway User Guide*, to the chapter "SSL Wrapper".

In order to enable Sametime Instant Messaging to run from within the Lotus Domino Web Access interface, in the Configuration program, use the Add Application Wizard to add the Sametime Plugin application to the trunk (from the Browser-Embedded Applications group). Note that if you are enabling the Sametime Plugin application only from within the Lotus Domino Web Access application, you do not need to add a link on the portal homepage for the Sametime Plugin application. In this case, in the Add Application Wizard, in the Portal Link step, uncheck the option "Add Link on Whale Portal and Toolbar".

Cleaning Application-Specific Temporary Files

When the option "Attachment Wiper Cleans Application-Specific Temporary Files" is activated, the Attachment Wiper deletes attachments from certain locations on the endpoint computer. This option is activated in the Session tab of the Advanced Trunk Configuration window.

> **Note**
> The Attachment Wiper deletes application-specific files only if the application is part of the IAG site.

The locations from which attachments are deleted, including all files and subfolders, are:

`%temp%\iNotes Web Access`

`%temp%\Domino Web Access` (Lotus Domino Web Access 6.5 and higher)

Where `%temp%` is the `temp` environment variable's value, as defined on the endpoint computer.

Citrix NFuse® FR2 (Direct)

> **Note**
> This application is not supported in version 3.7; the following instructions are intended for backward compatibility purposes only.

Cleaning Application-Specific Temporary Files

When the option "Attachment Wiper Cleans Application-Specific Temporary Files" is activated, the Attachment Wiper deletes the client's cache. This option is activated in the Session tab of the Advanced Trunk Configuration window.

> **Note**
> The Attachment Wiper deletes application-specific files only if the application is part of the IAG site.

The location and types of files that the Attachment Wiper deletes depend on the client that is used on the end-user computer, as described in the following sections.

Using ICA® Java® Client

Location

Bitmap cache folder, as defined in the Java Client Settings

File Type

`*.bv*`

Using ICA Web Client for 32-bit Windows®

Location

In setups where the ICA Web Client is configured to write to the cache, the IAG causes the Web Client to divert the cache to a folder it creates in the same location as the Desktop folder, named `whlcitrixcache`. During cleanup, the Attachment Wiper deletes the cache from this folder, including all subfolders.

File Type

All files

Citrix NFuse FR2 via SecureGateway

> **Note**
> This application is not supported in version 3.7; the following instructions are intended for backward compatibility purposes only.

Cleaning Application-Specific Temporary Files

When the option "Attachment Wiper Cleans Application-Specific Temporary Files" is activated, the Attachment Wiper deletes the client's cache. This option is activated in the Session tab of the Advanced Trunk Configuration window.

> **Note**
> The Attachment Wiper deletes application-specific files only if the application is part of the IAG site.

The location and types of files that the Attachment Wiper deletes depend on the client that is used on the end-user computer, as described in the following sections.

Using ICA Java Client

Location

Bitmap cache folder, as defined in the Java Client Settings

File Type

`*.bv*`

Using ICA Web Client for 32-bit Windows

Location

In setups where the ICA Web Client is configured to write to the cache, the IAG causes the Web Client to divert the cache to a folder it creates in the same location as the Desktop folder, named `whlcitrixcache`. During cleanup, the Attachment Wiper deletes the cache from this folder, including all subfolders.

File Type

All files

Citrix NFuse FR3 (Direct)

Cleaning Application-Specific Temporary Files

When the option "Attachment Wiper Cleans Application-Specific Temporary Files" is activated, the Attachment Wiper deletes the client's cache. This option is activated in the Session tab of the Advanced Trunk Configuration window.

> **Note**
> The Attachment Wiper deletes application-specific files only if the application is part of the IAG site.

The location and types of files that the Attachment Wiper deletes depend on the client that is used on the end-user computer, as described in the following sections.

Using ICA Java Client

Location

Bitmap cache folder, as defined in the Java Client Settings

File Type

`*.bv*`

Using ICA Web Client for 32-bit Windows

Location

In setups where the ICA Web Client is configured to write to the cache, the IAG causes the Web Client to divert the cache to a folder it creates in the same location as the Desktop folder, named `whlcitrixcache`. During cleanup, the Attachment Wiper deletes the cache from this folder, including all subfolders.

File Type

All files

Citrix NFuse FR3 via SecureGateway

> **Note**
> This application is not supported in version 3.7; the following instructions are intended for backward compatibility purposes only.

Cleaning Application-Specific Temporary Files

When the option "Attachment Wiper Cleans Application-Specific Temporary Files" is activated, the Attachment Wiper deletes the client's cache. This option is activated in the Session tab of the Advanced Trunk Configuration window.

> **Note**
> The Attachment Wiper deletes application-specific files only if the application is part of the IAG site.

The location and types of files that the Attachment Wiper deletes depend on the client that is used on the end-user computer, as described in the following sections.

Using ICA Java Client

Location

Bitmap cache folder, as defined in the Java Client Settings

File Type

`*.bv*`

Using ICA Web Client for 32-bit Windows

Location

In setups where the ICA Web Client is configured to write to the cache, the IAG causes the Web Client to divert the cache to a folder it creates in the same location as the Desktop folder, named `whlcitrixcache`. During cleanup, the Attachment Wiper deletes the cache from this folder, including all subfolders.

File Type

All files

Citrix Presentation Server™ (Web Interface 3)

Cleaning Application-Specific Temporary Files

When the option "Attachment Wiper Cleans Application-Specific Temporary Files" is activated, the Attachment Wiper deletes the client's cache. This option is activated in the Session tab of the Advanced Trunk Configuration window.

> **Note**
> The Attachment Wiper deletes application-specific files only if the application is part of the IAG site.

The location and types of files that the Attachment Wiper deletes depend on the client that is used on the end-user computer, as described in the following sections.

Using ICA Java Client

Location

Bitmap cache folder, as defined in the Java Client Settings

File Type

All files

Using ICA Web Client for 32-bit Windows

Location

In setups where the ICA Web Client is configured to write to the cache, the IAG causes the Web Client to divert the cache to a folder it creates in the same location as the Desktop folder, named `whlcitrixcache`. During cleanup, the Attachment Wiper deletes the cache from this folder, including all subfolders.

File Type

All files

Using ICA Local Client

Location

Bitmap cache folder, as defined in the ICA local client settings

File Type

All files

Using ICA ActiveX Client

Location

Bitmap cache folder, as defined in the ICA ActiveX client settings, including all subfolders.

> **Note**
>
> The Attachment Wiper will delete the bitmap cache from the location specified in the local client settings `*.ini` file only if it is an absolute path. If the location specified in the file is a relative path, the Attachment Wiper will always attempt to delete the bitmap cache from the following location, including all subfolders:
>
> `%programfiles%\citrix\icaweb32\cache`

File Type

All files

Using TSAC Web Client on Windows® 2000/XP Systems

Location

`%userprofile%\Local Settings\Application Data\Microsoft\ Terminal Server Client\Cache`

Where `%userprofile%` is the `userprofile` environment variable's value, as defined on the endpoint computer.

File Type

`*.bmc`

Citrix® Secure Access Manager (Direct)

Application-Specific Settings

The application-specific settings that are required for the Citrix Secure Access Manager include:

- "Defining the Application URL" on page 21
- "Accessing Citrix Secure Access Manager CDAs/Portlets" on page 21

Defining the Application URL

When you add an application in the Add Application Wizard, the Application URL is inserted automatically in the Portal Link step of the wizard. When configuring the Citrix Secure Access Manager, you must add the Secure Access Manager site folder after the URL in the "Application URL" field.

For example:

If the automatically inserted Application URL is `http://192.168.1.90/` and the site folder is called "sam22", you must add the site folder after the URL as follows:

`http://192.168.1.90/sam22`

> (!) **Tip**
> If the site folder was not included in the Application URL while adding the application to the trunk, you can add it later, in the Portal Link tab of the Application Properties dialog box.

Accessing Citrix Secure Access Manager CDAs/Portlets

In order to enable access to some of the Citrix Secure Access Manager CDAs/portlets via the IAG, you need to add a corresponding web application to the Whale portal, in the Configuration program, as follows:

- For the **Adapter for Lotus Domino Web Access** CDA/portlet, add the "All Domino (Webmail 5.x/6.x/7.x and iNotes) Interfaces" application to the Whale portal.
- For the **Adapter for Microsoft® Outlook® WebAccess** CDA/portlet, add the "Microsoft Outlook Web Access 2000 SP2/SP3" application to the Whale portal.

Cleaning Application-Specific Temporary Files

When the option "Attachment Wiper Cleans Application-Specific Temporary Files" is activated, the Attachment Wiper deletes the client's cache. This option is activated in the Session tab of the Advanced Trunk Configuration window.

> **Note**
> The Attachment Wiper deletes application-specific files only if the application is part of the IAG site.

The location and types of files that the Attachment Wiper deletes depend on the client that is used on the end-user computer, as described in the following sections.

Using ICA Java Client

Location

Bitmap cache folder, as defined in the Java Client Settings

File Type

All files

Using ICA Web Client for 32-bit Windows

Location

In setups where the ICA Web Client is configured to write to the cache, the IAG causes the Web Client to divert the cache to a folder it creates in the same location as the Desktop folder, named `whlcitrixcache`. During cleanup, the Attachment Wiper deletes the cache from this folder, including all subfolders.

File Type

All files

Using ICA Local Client

Location

Bitmap cache folder, as defined in the ICA local client settings

File Type

All files

Using ICA ActiveX Client

Location

Bitmap cache folder, as defined in the ICA ActiveX client settings, including all subfolders.

> **Note**
> The Attachment Wiper will delete the bitmap cache from the location specified in the local client settings `*.ini` file only if it is an absolute path. If the location specified in the file is a relative path, the Attachment Wiper will always attempt to delete the bitmap cache from the following location, including all subfolders:
>
> `%programfiles%\citrix\icaweb32\cache`

File Type

All files

Domino iNotes

Cleaning Application-Specific Temporary Files

When the option "Attachment Wiper Cleans Application-Specific Temporary Files" is activated, the Attachment Wiper deletes attachments from certain locations on the endpoint computer. This option is activated in the Session tab of the Advanced Trunk Configuration window.

> **Note**
> The Attachment Wiper deletes application-specific files only if the application is part of the IAG site.

The locations from which attachments are deleted, including all files and subfolders, are:

`%temp%\iNotes Web Access`

`%temp%\Domino Web Access` (Lotus Domino Web Access 6.5 and higher)

Where `%temp%` is the `temp` environment variable's value, as defined on the endpoint computer.

Domino iNotes (Multi Servers)

Application-Specific Settings

This section describes how you prepare the IAG for the Domino iNotes (Multi Servers) application. The steps you take depend on whether you are adding the application to a Portal trunk, or as a separate Webmail trunk, as follows:

- For an application added to a Portal trunk, see "Setup For a Domino iNotes (Multi Servers) Application in a Portal Trunk" on page 25.

- For a separate Webmail trunk, see "Setup For a Domino iNotes (Multi Servers) Webmail Trunk" on page 26.

Setup For a Domino iNotes (Multi Servers) Application in a Portal Trunk

This section describes how you prepare the IAG when you add the Domino iNotes (Multi Servers) application to the trunk, in setups where the Socket Forwarding component of the SSLWrapper is not used.

> **Note**
>
> Although the procedure described here is required only if the Socket Forwarding component is not used, we recommend that you implement it even if the application is configured to operate in Socket Forwarding Mode, as a fallback for cases where the Socket Forwarding client component is not installed on the endpoint computer.

To prepare the IAG for the Domino iNotes (Multi Servers) application:

1. Access the following folder:

   `…\Whale-Com\e-Gap\von\InternalSite\inc\customUpdate`

2. Under the `customUpdate` folder, create an authentication "hook", which will be activated before the `PostValidate.asp` reaches the client side:

   `PrePostValidate.inc`
   Or,
   `PostPostValidate.inc`
   Name the file as follows:

   `<Trunk_Name><Secure(0=no/1=yes)><Hook_Name>`

   For example:

   For an HTTPS trunk named "OurTrunk", create a "PostPostValidate" hook, create the file:

   `OurTrunk1PostPostValidate.inc`

> **!** **Tip**
> If a file by this name already exists, you can use the existing file; you do not need to create a new file in this case.

3. In the file you defined in step 2, add the following lines:

```
<%
  SetSessionParam g_cookie,"RelayPort1352","<NotesServer>"
%>
```

Where `NotesServer` is a variable containing the name of the server that hosts the mailbox of the logged-in user.

4. In the Configuration program, click ⚙ to activate the configuration, select the option "Apply changes made to external configuration settings", and click ⟨Activate >⟩.

End-users can now access the Domino iNotes (Multiple Servers) application via the Portal trunk.

Setup For a Domino iNotes (Multi Servers) Webmail Trunk

This section describes how you prepare the IAG for a Domino iNotes (Multi Servers) Webmail trunk.

To prepare the IAG for a Domino iNotes (Multi Servers) Webmail trunk:

1. Copy the sample authentication "hook" file:

   `site_secure_PostPostValidate_for_notes.inc`

   From this location:

   `...\Whale-Com\e-Gap\von\InternalSite\samples`

   To the following custom folder:

   `...\Whale-Com\e-Gap\von\InternalSite\inc\customUpdate`

2. Rename the file as follows:

   `<Trunk_Name><Secure(0=no/1=yes)><Hook_Name>`

   For example:

   For an HTTPS trunk named "OurTrunk", rename the file to:

   `OurTrunk1PostPostValidate.inc`

3. In the file you defined in step 2, enter the values of the following fields:

   - `domain`: domain of the user
   - `url`: URL of the mail server

4. In the same file, add the following lines:

```
<%
  SetSessionParam g_cookie,"RelayPort1352","<NotesServer>"
%>
```

Where `NotesServer` is a variable containing the name of the server that hosts the mailbox of the logged-in user.

5. In the Configuration program, click ⚙ to activate the configuration, select the option "Apply changes made to external configuration settings", and click `Activate >`.

   End-users can now access the Domino iNotes (Multiple Servers) application via the Webmail trunk.

Cleaning Application-Specific Temporary Files

When the option "Attachment Wiper Cleans Application-Specific Temporary Files" is activated, the Attachment Wiper deletes attachments from certain locations on the endpoint computer. This option is activated in the Session tab of the Advanced Trunk Configuration window.

> **Note**
>
> The Attachment Wiper deletes application-specific files only if the application is part of the IAG site.

The locations from which attachments are deleted, including all files and subfolders, are:

`%temp%\iNotes Web Access`

`%temp%\Domino Web Access` (Lotus Domino Web Access 6.5 and higher)

Where `%temp%` is the `temp` environment variable's value, as defined on the endpoint computer.

Domino iNotes (Single Server)

Cleaning Application-Specific Temporary Files

When the option "Attachment Wiper Cleans Application-Specific Temporary Files" is activated, the Attachment Wiper deletes attachments from certain locations on the endpoint computer. This option is activated in the Session tab of the Advanced Trunk Configuration window.

> **Note**
> The Attachment Wiper deletes application-specific files only if the application is part of the IAG site.

The locations from which attachments are deleted, including all files and subfolders, are:

`%temp%\iNotes Web Access`

`%temp%\Domino Web Access` (Lotus Domino Web Access 6.5 and higher)

Where `%temp%` is the `temp` environment variable's value, as defined on the endpoint computer.

Domino Offline Services 7.0 (Single/Multi Servers)

Application-Specific Settings

This section describes how you prepare the IAG when you add the Domino Offline Services 7.0 (Single/Multi Servers) application to the trunk.

To prepare the IAG for the Domino Offline Services 7.0 (Single/ Multi Servers) application:

1. Access the following folder:

   …\Whale-Com\e-Gap\von\InternalSite\inc\customUpdate

2. Under the `customUpdate` folder, create an authentication "hook", which will be activated before the `PostValidate.asp` reaches the client side:

   `PrePostValidate.inc`
   Or,
   `PostPostValidate.inc`
   Name the file as follows:

   `<Trunk_Name><Secure(0=no/1=yes)><Hook_Name>`

   For example:

   For an HTTPS trunk named "OurTrunk", to create a "PostPostValidate" hook, create the file:

   `OurTrunk1PostPostValidate.inc`

   > **!** **Tip**
   > If a file by this name already exists, you can use the existing file; you do not need to create a new file in this case.

3. In the file you defined in step 2, add the following lines:

   ```
   <%
     SetSessionParam g_cookie,"RelayPort1352","<NotesServer>"
   %>
   ```

   Where `<NotesServer>` is a variable containing the name of the server that hosts the mailbox of the logged-in user.

4. In the Configuration program, click ⚙ to activate the configuration, select the option "Apply changes made to external configuration settings", and click [Activate >].

   End-users can now access the Domino Offline Services 7.0 (Single/ Multi Servers) application via the trunk.

Cleaning Application-Specific Temporary Files

When the option "Attachment Wiper Cleans Application-Specific Temporary Files" is activated, the Attachment Wiper deletes attachments from certain locations on the endpoint computer. This option is activated in the Session tab of the Advanced Trunk Configuration window.

> **Note**
>
> The Attachment Wiper deletes application-specific files only if the application is part of the IAG site.

The locations from which attachments are deleted, including all files and subfolders, are:

`%temp%\iNotes Web Access`

`%temp%\Domino Web Access` (Lotus Domino Web Access 6.5 and higher)

Where `%temp%` is the `temp` environment variable's value, as defined on the endpoint computer.

FTP (Passive Mode)

Application-Specific Settings

In order for end-users to access the FTP (Passive Mode) application from a remote computer, the browser has to be configured to use Passive FTP mode.

For example: in Internet Explorer, in **Tools > Internet Options > Advanced**, the option "Use Passive FTP" must be selected.

Microsoft ActiveSync®

Application-Specific Settings

In order to enable access to Microsoft ActiveSync on handheld devices, configure a Webmail trunk, and in the "Webmail Application" step of the Create New Trunk wizard, select the application "Microsoft ActiveSync".

When creating the trunk, note the following:

- Since ActiveSync uses basic authentication only, it is highly recommended that you define the Microsoft ActiveSync trunk as an HTTPS trunk. If you use an HTTP trunk, users' credentials will not be secured.
- In the "Authentication" and "Application Login" steps of the Create New Trunk Wizard, the authentication server you select must be the authentication server that is used by the Exchange server, that is, the domain that is defined in ActiveSync on the handheld device.
- Most default trunk settings should not be changed. The settings you can optionally change include:
  - "Is SSL" option, relevant for HTTPS trunks. This option is activated either in the "Application Server" step of the Create New Trunk Wizard, or in the "Application Server" area of the Configuration program.
  - "Permitted Authentication Attempts" and "Block Period" authentication-related parameters. For details, refer to the *Intelligent Application Gateway Advanced Configuration* guide, to the chapter "Access Control", to the section "Configuration in the Authentication Tab".
  - Custom hooks, described in "Activating Custom Hooks" on page 32.

Activating Custom Hooks

There are two hooks that you can use with the ActiveSync trunk, to be run at different stages of the Login process, as follows:

- At the beginning of the Login process. This hook can be used, for example, to override original request parameters.
- At the end of the Login process. This hook can be used, for example, to analyze the authentication results.

To activate a custom hook:

1. At the IAG, access this folder; if it does not exist, create it:

    `…\Whale-Com\e-Gap\Von\InternalSite\inc\CustomUpdate`

2. Create a file containing the required script, as follows:
   - For a hook to be run at the beginning of the Login process, create a file named:

     `<Trunk_Name><Secure(0=no/1=yes)>ActiveSyncLoginStart.inc`

     For example: for an HTTPS trunk named "Handheld", name the file `Handheld1ActiveSyncLoginStart.inc`

   - For a hook to be run at the end of the Login process, create a file named:

     `<Trunk_Name><Secure(0=no/1=yes)>ActiveSyncLoginEnd.inc`

3. In the Configuration program, click ⚙ to activate the configuration, select the option "Apply changes made to external configuration settings", and click Activate >.

   The action you defined in the hook will be run when end-users access the Microsoft ActiveSync application.

Microsoft CRM 3.0

Application-Specific Settings

This section describes how you can prevent users from performing the following operations unless their computer meets the defined security policy requirements:

- Exporting to Excel.
- Printing.
- Adding attachments.
- Accessing the Settings area.

Users that are blocked are notified accordingly.

In order to enable this option, once you finish adding the application to the trunk, you need to define the security policy requirements using a dedicated endpoint policy: "Microsoft CRM 3 Enhanced Security". By default, the value of the policy is "True", and it does not prevent users from performing the operations listed above from any endpoint computer. If required, change the policy to comply with your corporate policy, as described here.

To prevent Enhanced Security operations from non-compliant endpoints:

1. In the Configuration program, open the Application Properties dialog box. In the General tab, click Edit Policies....
2. In the Policies dialog box, under the "Policies" group, select the policy "Microsoft CRM 3 Enhanced Security", then click Edit....
3. Use the Advanced Policy Editor to edit the policy according to your requirements. For details, refer to the *Intelligent Application Gateway User Guide*, to the section "Endpoint Policies".
4. In the Configuration program, click to activate the configuration.

   End-users accessing the Microsoft CRM 3.0 application from a non-compliant endpoint computer will not be able to perform Enhanced Security operations.

Microsoft Outlook Mobile Access 2003

Application-Specific Settings

These instructions are relevant for IAG trunks that include both the Microsoft Outlook Mobile Access 2003 and the Microsoft Outlook Web Access 2003 applications, where both applications use the same Exchange server.

In this case, make sure that the Microsoft Outlook Mobile Access 2003 application precedes the Microsoft Outlook Web Access 2003 application in the list of applications in the "Applications" area of the main window of the IAG Configuration program.

Microsoft Outlook Web Access 5.5

Application-Specific Settings

Once you finish adding a Microsoft Outlook Web Access 5.5 application to the trunk, you need to assign a unique Upload policy to the application.

> ⚠️ **Caution**
>
> Only the pre-defined policy can be used with Outlook Web Access 5.5. Do not use the Default Web Application Upload policy, or any other policy, with this application.

To assign a policy to the application:

1. In the Configuration program, access the Application Properties dialog box.
2. In the General tab, in the "Endpoint Policies" area, from the "Upload" drop-down list, select the policy "Microsoft Outlook Web Access 5 5 Upload".
3. By default, the value of the policy is "True", and it does not prevent uploads from any endpoint computer. If required, change the policy to comply with your corporate policy. For details, refer to the *Intelligent Application Gateway User Guide*, to the section "Endpoint Policies".

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

   Upload operations described in this section will be blocked on endpoint computers that do not comply with the security policy you defined here.

Microsoft Outlook Web Access 2003 SP1/SP2

Application-Specific Settings

For organizations that use Everywhere Networks' SecureView for OWA Enterprise 3.0, the IAG provides a dedicated endpoint policy for secure handling of attachments via SecureView on Microsoft Outlook Web Access 2003 SP1/SP2. The "SecureView for OWA2003 SP1" policy defines the security level that is required on the endpoint computer in order to enable full functionality of the application. When an endpoint does not comply with the requirements of the policy, the following functionality is disabled when the user handles attachments in Microsoft Outlook Web Access 2003 SP1/SP2:

- Attachments open in a browser with a "view only" display- the menu bar, toolbar, address bar, and status bar are not displayed.
- When an attachment is open, the user cannot:
  - Right-click the attachment
  - Use the Ctrl+C keyboard combination in Internet Explorer
  - Use the "Print Version" option in Navigation View
- When a user right-clicks an attachment link, the following options are disabled:
  - Save Target As
  - Print View

If required, you can modify the default definition of the policy, to change the security level that is required on the endpoint computer.

To modify the "SecureView for OWA2003 SP1" policy:

1. In the Configuration program, access either the General tab of Application Properties dialog box or the Session tab of the Advanced Trunk Configuration window, and click Edit Policies....
2. In the Policies dialog box, under the Policies group, select the policy "SecureView for OWA2003 SP1", then click Edit....
3. In the Advanced Policy Editor, edit the expression as required.
4. In the Configuration program, click ⚙ to activate the configuration.

   The security level for access from on endpoint computers will depend on their compliance with the security policy you defined here.

Microsoft Outlook Web Access 2007

Application-Specific Settings

The application-specific settings for Microsoft Outlook Web Access 2007 (OWA) include the following options:

· Enabling access to documents via Microsoft Office SharePoint® Server 2007, in "Enabling Access to Sharepoint Server Via Outlook Web Access" on page 38.

· Preventing users from uploading or downloading files via OWA, unless their computer meets the defined security policy requirements, as described in "Blocking Uploads and Downloads" on page 38.

In addition, the behavior of the application when the Form Authentication Engine is defined to automatically reply to application-specific authentication requests is described in "Using Login Forms" on page 39.

Enabling Access to Sharepoint Server Via Outlook Web Access

Microsoft Outlook Web Access 2007 includes integration with Microsoft Office SharePoint Server 2007, where users can access documents via the SharePoint Server from within the OWA interface.

In order to enable this functionality, you need to add the SharePoint Server application to the portal. In the Configuration program, use the Add Application Wizard to add the "Microsoft Office SharePoint Server 2007" application to the trunk that enables access to OWA.

Blocking Uploads and Downloads

This section describes how you utilize the application's Upload and Download policies, so that end-users cannot upload files or download files via OWA, unless their computer meets the security policy requirements. Users that are blocked are notified accordingly.

In order to enable this option, once you finish adding the Microsoft Outlook Web Access 2007 application to the trunk, you need to assign a unique Upload or Download policy to the application, as described here.

To block uploads:

1. In the Configuration program, select the trunk where the Microsoft Outlook Web Access 2007 application is defined.

2. In the Applications list, select the Microsoft Outlook Web Access 2007 application, and click Edit… to access the Application Properties dialog box.

3. In the General tab, in the "Endpoint Policies" area, from the "Upload" drop-down list, select the policy "Microsoft OWA 2007 Upload".

4. By default, the value of the policy is "True", and it does not prevent uploads from any endpoint computer. If required, change the policy to comply with your corporate policy. For details, refer to the *Intelligent Application Gateway User Guide*, to the section "Endpoint Policies".

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

   File uploading will only be enabled on endpoint computers that comply with the security policy you defined here.

To block downloads:

1. In the Configuration program, select the trunk where the Microsoft Outlook Web Access 2007 application is defined.

2. In the Applications list, select the Microsoft Outlook Web Access 2007 application, and click Edit... to access the Application Properties dialog box.

3. In the General tab, in the "Endpoint Policies" area, from the "Download" drop-down list, select the policy "Microsoft OWA 2007 Download".

4. By default, the value of the policy is "True", and it does not prevent downloads via OWA. If required, change the policy to comply with your corporate policy. For details, refer to the *Intelligent Application Gateway User Guide*, to the section "Endpoint Policies".

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

   File downloading from the server will only be enabled on endpoint computers that comply with the security policy you defined here.

Using Login Forms

In the Authentication step of the Add Application Wizard, or in the Web Settings tab of the Application Properties dialog box, you can select the option "Automatically Reply to Application-Specific Authentication Requests". If the request form is an HTML form, that is, either "HTML Form" or "Both" is selected in the Web Settings tab, once users enter a set of credentials that is valid for the application, for example during the initial login, they are not requested to authenticate again, against the application server.

In the Microsoft Outlook Web Access 2007 application, this means that each time the authentication page is automatically processed, the application is accessed with the default settings of the login page. The main consequence of this for the end-user is that the computer type is automatically defined as "Public or shared", and thus the period of inactivity before the user is logged out is relatively short. The user cannot select the computer type "Private", or select the Outlook Web Access Light option.

Native Notes® Client (Multi Servers)

Application-Specific Settings

The application-specific settings for Native Notes Client Multiple Servers applications include the following options:

- Enabling access to the application from endpoint computers where the Socket Forwarding component of the SSL Wrapper is not used, as described in "Enabling Access Without the Socket Forwarding Component" on page 41.

- Enabling users to run Sametime Instant Messaging from within the Lotus Notes client, as described in "Enabling Sametime Instant Messaging" on page 43.

Enabling Access Without the Socket Forwarding Component

This section describes the steps you have to take on endpoint computers where the Socket Forwarding component of the SSL Wrapper is not used, in order to enable remote access to multiple corporate Lotus Notes servers from the portal via the IAG.

To enable access without the Socket Forwarding component:

1. At the computer where you wish to enable remote access to Lotus Notes, access the Lotus Notes Client. In the Lotus Notes screen, at the bottom right corner, select the profile through which you wish to remotely access the Notes application, for example: **Internet**.

    ```
    Home (Network Dialup)
    Home (Notes Direct Dialup)
    Internet
    Island (Disconnected)
    Office (Network)
    Travel (Notes Direct Dialup)
    Edit Current...
                      Internet          ▼
    ```
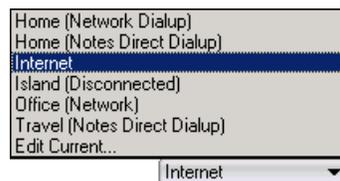
    The selected profile is displayed at the bottom right corner of the Lotus Notes screen.

2. Still from the menu at the bottom right corner, select **Edit Current…**

    The Lotus Notes screen displays the settings of the selected profile. In this example, Settings for location: Internet.
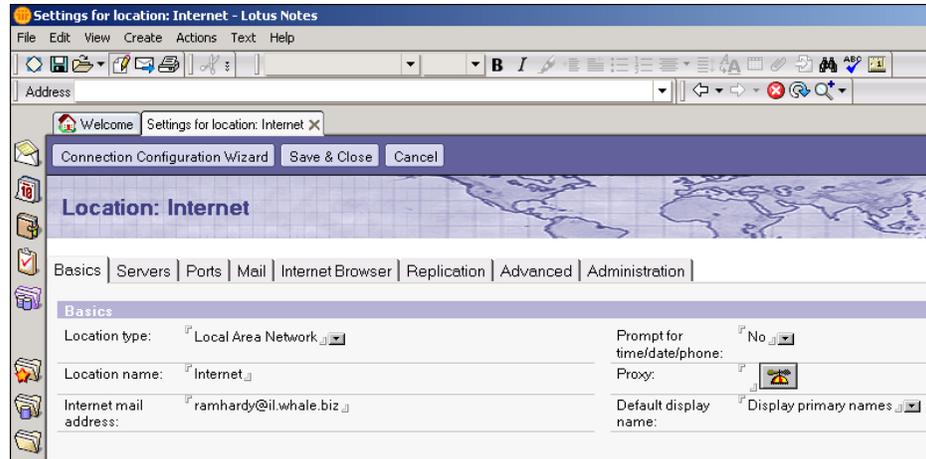
3. In the Basics tab click .

   The Proxy Server Configuration dialog box is displayed.

4. In the Proxy Server Configuration dialog box enter the following:
   - HTTP Tunnel: 127.0.0.3:10080
   - Exceptions: 127.0.0.3
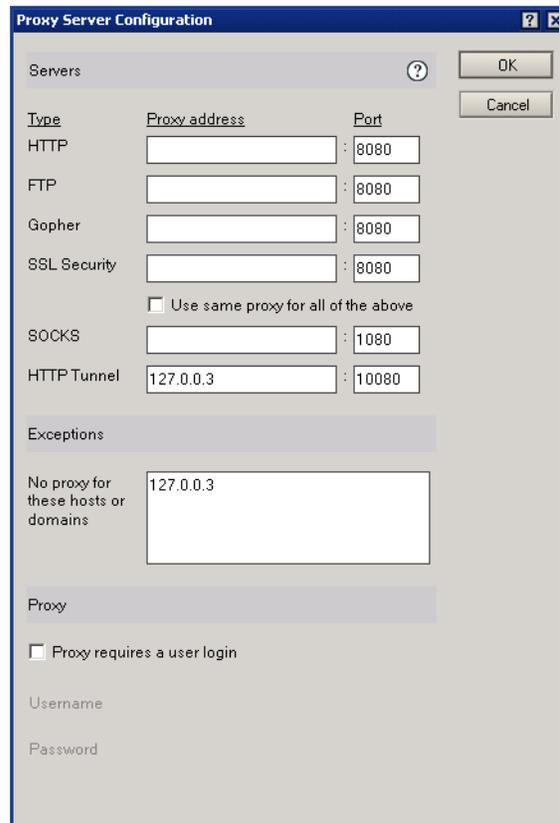
5. Click OK to close the Proxy Server Configuration dialog box.

6. In the Lotus Notes screen, click $\boxed{\text{Save & Close}}$ to save the profile.

   The Lotus Notes screen closes. The user can access the Lotus Notes server remotely via the IAG, using the profile configured here.

> (!) **Tip**
>
> When users don't need to work via the IAG, for example when working from the office, they can select another profile, for example: **Office (Network)**. To resume work via the IAG, users select the IAG profile again, in the example shown here: **Internet**.

Enabling Sametime Instant Messaging

This section describes how you enable users to run Sametime instant messaging from within the Lotus Notes client.

To enable instant messaging from within the Notes client:

1. In the Configuration program, use the Add Application Wizard to add the Sametime Native Relay (Chat Only) application to the trunk (from the "Client/Server and Legacy Applications" group).

2. Define the application you added in step 1 as a prerequisite application to the Native Notes application:

   a) Access the Application Properties dialog box of the Native Notes application.

   b) In the General tab, in the "Prerequisite Applications" list, check the box next to the Sametime Native Relay application, then click $\boxed{\text{OK}}$.

3. In the Configuration program, click 🔧 to activate the configuration.

   Once you activate the configuration, whenever users launch the Native Notes application, the prerequisite Sametime Native Relay application is launched, as well. Launching this application opens a relay from the endpoint computer to the Sametime server. Users can then run Sametime instant messaging from within the Lotus Notes client.

Native Notes Client (Single Server)

Application-Specific Settings

This section describes how you enable users to run Sametime instant messaging from within the Lotus Notes client.

To enable instant messaging from within the Notes client:

1. In the Configuration program, use the Add Application Wizard to add the Sametime Native Relay (Chat Only) application to the trunk (from the "Client/Server and Legacy Applications" group).

2. Define the application you added in step 1 as a prerequisite application to the Native Notes application:

    a) Access the Application Properties dialog box of the Native Notes application.

    b) In the General tab, in the "Prerequisite Applications" list, check the box next to the Sametime Native Relay application, then click OK.

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

    Once you activate the configuration, whenever users launch the Native Notes application, the prerequisite Sametime Native Relay application is launched, as well. Launching this application opens a relay from the endpoint computer to the Sametime server. Users can then run Sametime instant messaging from within the Lotus Notes client.

Outlook (Corporate/Workgroup Mode)

Application-Specific Settings

This procedure describes how you use the Microsoft RPC Proxy to enable remote access from Outlook 2000, 2003, and 2007 clients to corporate Exchange servers operating in Corporate or Workgroup mode via a Whale portal, in setups where the Socket Forwarding component of the SSL Wrapper is not used.

Installation and configuration of the Microsoft RPC Proxy must be implemented before you add the Outlook (Corporate/ Workgroup Mode) application to the trunk.

> **Note**
> It is recommended that you install and configure the Microsoft RPC Proxy even if the application is configured to operate in Socket Forwarding Mode, as a fallback for cases where the Socket Forwarding client is not installed on the endpoint computer.

The steps you take include:

- Installing a Microsoft RPC Proxy on a corporate server, as described in "RPC Proxy Installation" on page 45.

- Configuring the RPC Proxy as described in "RPC Proxy Configuration" on page 46.

RPC Proxy Installation

The Microsoft RPC Proxy can be installed on any Windows 2000 corporate server. It cannot be installed on the IAG.

> **Note**
> During the installation, you will be asked for the Windows 2000 Server CD.

To install the Microsoft RPC Proxy:

1. In the Windows desktop, click Start then point to **Settings > Control Panel** and select **Add/Remove Programs**.
    The Add/Remove Programs window is displayed.

2. In the Add/Remove Programs window, click **Add/Remove Windows Components**.
    The Windows Components Wizard is displayed.

3. In the Windows Components Wizard, in the Components list, check the component **Networking Services**, then click $\boxed{\text{Details}}$.

   The Networking Services dialog box is displayed.

4. In the Networking Services dialog box, check the sub-component **COM Internet Services Proxy** and click $\boxed{\text{OK}}$.

5. Follow the instructions on the screen to complete the installation.

   The RPC Proxy is installed. Proceed to "RPC Proxy Configuration" on page 46.

RPC Proxy Configuration

While configuring the RPC Proxy, you need to supply details of the following servers:

- All Exchange servers in the organization
- Windows 2000 Domain Controllers (DCs) and Global Catalogs (GCs)
- Windows NT domain controllers that serve as Primary Domain Controllers (PDCs)

For each of these servers, you configure two entries:

- NetBIOS hostname, for example: `owa2003`
- Fully Qualified Domain Name (FQDN), for example: `owa2003.whale.com`

> (!) **Tip**
> You will also need these server details when adding the Outlook (Corporate/Workgroup Mode) application to the trunk, in the Server Settings step of the Add Application Wizard.

To configure the RPC Proxy:

1. At the computer where you installed the RPC Proxy, use the Registry Editor to access the following location:

   `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Rpc\RpcProxy`

2. Verify that the value `Enabled` is set to `1`. If not, change it to `1`.

3. Modify the settings of the `ValidPorts` value to reflect the servers and port ranges listed at the beginning of this section.

   For each server, enter the server name with the suffix: `100-65535`.

   For example:

   `owa2003:100-65535`

   Separate between servers with a semi-colon.

   For example:

   `owa2003:100-65535;owa2003.whale.com:100-65535`

4. Click **OK**.

   The Edit String dialog box closes. In the Registry Editor, the value of `ValidPorts` *includes the servers and ports you configured here.*
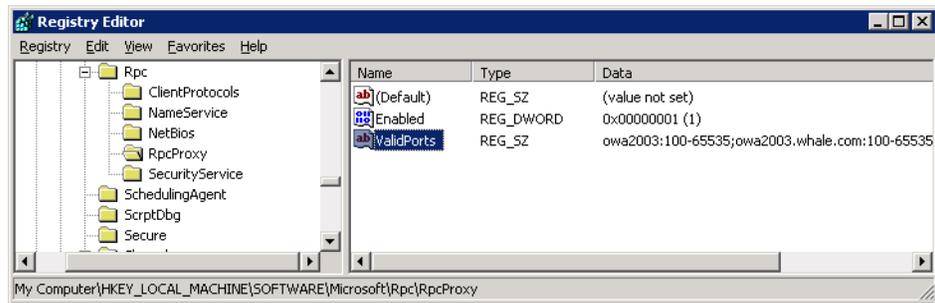
5. Restart the computer.

   The RPC Proxy is configured for the Outlook (Corporate/Workgroup Mode) application.

SAP® Enterprise Portal 6

Application-Specific Settings

The following sections describe additional options you can implement and which determine aspects of the behavior of SAP Enterprise Portal 6 when accessed from a remote computer via the IAG, including:

- Enabling access via the SAP portal to third-party applications that communicate directly with the application server, in "Integration with Third-Party Applications" on page 48.

- Preventing users from uploading attachments to the portal, or sending email attachments, unless their computer meets the defined security policy requirements, as described in "Blocking Uploads and Attachment Sending" on page 49.

- Preventing users from deleting documents or editing documents locally, unless their computer meets the defined security policy requirements, as described in "Blocking Document Deleting and Editing" on page 49.

> **Note**
>
> Some SAP implementation may generate URLs with a long path. By default, the IIS rejects URLs where the path is longer than 260 characters. For details, and for a description of the Registry key that controls this setting, access the following link:
>
> http://support.microsoft.com/kb/820129/en-us
>
> Note that this setting is global to all IIS sites on the computer.

Integration with Third-Party Applications

This section describes how you enable access from the SAP portal to third-party applications via the SAP portal iViews. This is required only for third-party applications that communicate directly with the application server, for example an Outlook Web Access server.

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 SAP portal.

Blocking Uploads and Attachment Sending

This section describes how you utilize the application's Upload policy, so that end-users cannot upload attachments to the portal, or send email attachments, if their computer does not meet the security policy requirements. Users that are blocked are notified accordingly.

In order to enable this option, once you finish adding the application to the trunk, you need to assign a unique Upload policy to the application, as described here.

To block uploads and attachment sending:

1. In the Configuration program, access the Application Properties dialog box.
2. In the General tab, in the "Endpoint Policies" area, from the "Upload" drop-down list, select the policy "SAP Enterprise Portal 6 Upload".
3. By default, the value of the policy is "True", and it does not prevent uploads from any endpoint computer. If required, change the policy to comply with your corporate policy. For details, refer to the *Intelligent Application Gateway User Guide*, to the section "Endpoint Policies".

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

   Attachment sending and uploading will only be enabled on endpoint computers that comply with the security policy you defined here.

Blocking Document Deleting and Editing

This section describes how you can prevent end-users from deleting documents, or editing documents locally, if their computer does not meet the defined security policy requirements. Users that are blocked are notified accordingly.

In order to enable this option, once you finish adding the application to the trunk, you need to define the security policy requirements using a dedicated endpoint policy: "SAP Enterprise Portal 6 Enhanced Security". By default, the value of the policy is "True", and it does not prevent document editing and deleting on any endpoint computer. If required, change the policy to comply with your corporate policy, as described here.

To block document editing and deleting:

1. In the Configuration program, open the Application Properties dialog box. In the General tab, click Edit Policies....
2. In the Policies dialog box, under the "Policies" group, select the policy "SAP Enterprise Portal 6 Enhanced Security", then click Edit....
3. Use the Advanced Policy Editor to edit the policy according to your requirements. For details, refer to the *Intelligent Application Gateway User Guide*, to the section "Endpoint Policies".

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

   Document deleting and local editing will only be enabled on endpoint computers that comply with the security policy you defined here.

Cleaning Application-Specific Temporary Files

When the option "Attachment Wiper Cleans Application-Specific Temporary Files" is activated, the Attachment Wiper deletes the client's cache. This option is activated in the Session tab of the Advanced Trunk Configuration window.

> **Note**
> The Attachment Wiper deletes application-specific files only if the application is part of the IAG site.

By default, the Attachment Wiper deletes the browser's cache. In addition, you can configure the IAG to delete attachments, including all files and sub-folders, from the following SAP-specific cache folder:

`%temp%\docservice\*.*\`

> **Caution**
> The "docservice" folder is where SAP saves temporary copies of documents that users edit locally. If the Attachment Wiper deletes the folder before the user checks in a document, all changes are lost.
>
> For a description of when the Attachment Wiper deletes attachments, refer to the *Intelligent Application Gateway User Guide*, to the section titled "Attachment Wiper".

To configure the Attachment Wiper to delete the "docservice" folder:

1. At the IAG, copy the following file:

   …\Whale-Com\e-Gap\von\conf\samples\SAPEP6_sample.txt

   Place it under the following location:

   …\Whale-Com\e-Gap\von\conf\wizarddefaults\AWPaths

2. Rename the file you copied in step 1 to SAPEP6.txt:

   …\Whale-Com\e-Gap\von\conf\wizarddefaults\AWPaths\SAPEP6.txt

3. In the Configuration program, click to activate the configuration, select the option "Apply changes made to external configuration settings", and click Activate > .

   When the Attachment Wiper deletes attachments, it will delete all data under the "docservice" folder.

> **Note**
>
> The file you copied in step 1 will be over-written when the IAG software is next upgraded or a patch is applied. In this case, you will have to run this procedure again.

Microsoft SharePoint Portal Server 2003

Note

The Microsoft SharePoint Portal Server 2003 application is used to access both Windows SharePoint Services (WSS) and SharePoint Portal Server (SPS).

Application-Specific Settings

This section describes the required and optional application-specific settings for the SharePoint Portal Server 2003 application, as follows:

- "Requirements on the Endpoint Computer" on page 53.

- 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" on page 53.

- 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" on page 55.

- 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" on page 57.

- Disabling end-users' ability to modify webparts, unless their computer meets the security policy requirements you define, as described in "Disabling Modification of Webparts" on page 58.

- 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" on page 59.

- Enabling access from the SharePoint Server to third-party applications, as described in "Integration with Third-Party Applications" on page 60.

Requirements on the Endpoint Computer

- For maximal integration, Microsoft Office 2003 SP1 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 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 dynamic rerouting 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.

- Check-in files.
- Save files from Microsoft Office applications to the 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 2003 Upload Checkin", then click `Edit...` to open the Advanced Policy Editor.

   c) The "SharePoint 2003 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 2003 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 achieve 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.
- Use the Export to Spreadsheet 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 2003 Download", then click `Edit...` to open the Advanced Policy Editor.
   c) The "SharePoint 2003 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 2003 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 achieve 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.

Disabling Modification of Webparts

This section describes how you prevent end-users from modifying webparts, including adding, editing, and deleting items in webparts, unless their computer meets the security policy requirements you define.

The webparts that are affected by this policy include:

• Announcements	• General discussion	• News
• Contacts	• Image library	• Shared documents
• Document library	• Links	• Tasks
• Events		

You prevent the modification of webparts by blocking end-users at the client side. This is achieved by activating the endpoint policy "SharePoint 2003 Enhanced Security" and defining it to comply with your corporate policy, as described in the procedure below.

> **Tip**
> In addition, you can optionally block users on the server side. For more details, contact your support channel.

To prevent the modification of webparts on the client side:

1. In the Configuration program, open the Application Properties dialog box. In the General tab, click [Edit Policies...] to open the Policies dialog box.

2. In the Policies dialog box, under the "Policies" group, select the policy "SharePoint 2003 Enhanced Security", then click [Edit...] to open the Advanced Policy Editor.

3. By default, the value of the policy is "True", and it does **not** prevent the modification of webparts from endpoint computers.

   You can:

   · Edit the policy to comply with your corporate policy, so that non-complying computers are blocked.

   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".

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

   Modification of webparts is blocked at the client side, on endpoint computers that do not comply with the security policy you defined here.

Restricting Access to Zones and Areas

This section describes how you utilize the application's Restricted Zone policy, so that end-users cannot access specific 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 "SharePoint 2003 Admin Zones".

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 "SharePoint 2003 Admin Zones", 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 2003
      - 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.

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 an Outlook Web Access server.

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.

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" on page 63.
- 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" on page 63.
- 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" on page 65.
- 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" on page 67.
- 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" on page 68.
- Enabling the "Explorer View" option, as described in "Enabling the Explorer View Option" on page 69.
- Enabling access from the SharePoint Server to third-party applications, as described in "Integration with Third-Party Applications" on page 70.

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.

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*`.

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.

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.

Terminal Services Web Client (Multi Servers)

Cleaning Application-Specific Temporary Files

When the option "Attachment Wiper Cleans Application-Specific Temporary Files" is activated, the Attachment Wiper deletes attachments from certain locations on the client. This option is activated in the Session tab of the Advanced Trunk Configuration window.

> **Note**
> The Attachment Wiper deletes application-specific files only if the application is part of the IAG site.

The location and types of files that the Attachment Wiper deletes are described below.

Location

Windows 2000 and Windows XP systems:

```
%userprofile%\Local Settings\Application
Data\Microsoft\Terminal Server Client\Cache
```

Where `%userprofile%` is the `userprofile` environment variable's value, as defined on the endpoint computer.

File Type

`*.bmc`

Terminal Services Web Client (Single Server)

Cleaning Application-Specific Temporary Files

When the option "Attachment Wiper Cleans Application-Specific Temporary Files" is activated, the Attachment Wiper deletes attachments from certain locations on the client. This option is activated in the Session tab of the Advanced Trunk Configuration window.

> **Note**
> The Attachment Wiper deletes application-specific files only if the application is part of the IAG site.

The location and types of files that the Attachment Wiper deletes are described below.

Location

Windows 2000 and Windows XP systems:

```
%userprofile%\Local Settings\Application
Data\Microsoft\Terminal Server Client\Cache
```

Where `%userprofile%` is the `userprofile` environment variable's value, as defined on the endpoint computer.

File Type

`*.bmc`

WebSphere® Portal 5.02

Application-Specific Settings

In order to enable access to some of the WebSphere Portal 5.02 portlets via the IAG, you need to add a corresponding web application to the Whale portal, in the Configuration program, as follows:

- For the **Domino Web Access** portlet, add the "Generic Web Application" to the Whale portal.

> **Note**
> Do not add a specific Domino application for this portlet.

- For the portlets listed below, add the "Microsoft Outlook Web Access 2000 SP2/SP3" application to the Whale portal:
  - Microsoft Exchange Contacts
  - Microsoft Exchange Mail
  - Microsoft Exchange Notes
  - Microsoft Exchange Calendar
  - Microsoft Exchange Tasks

Webtop® (Documentum)

Note

This application is not supported in version 3.7; the following instructions are intended for backward compatibility purposes only.

Application-Specific Settings

The following sections describe the settings required in order to enable full functionality of the Webtop portal when it is accessed from a remote computer via the IAG, including:

- Steps you need to take if the URL of the Webtop application does not start with "webtop", in "Changing the Application Name" on page 74.

- Enhanced security settings you can apply, which will prevent users from performing certain operations unless their computer meets the defined security policy requirements, in "Enhanced Security Settings" on page 75.

Changing the Application Name

This section describes the steps you need to take if the URL of the Webtop application, as defined during the installation of the application, does not start with "webtop". In this case, you need to change the name of the application in the Application Customization template that is used with the trunk that enables access to the Webtop portal.

Note

The steps described here are only required if the application name does not start with "webtop". If, for example the application name is "webtop1", no change is required.

To change the application name in the Application Customization template:

1. At the IAG, access the following folder:

    `…\Whale-Com\e-Gap\Von\Conf\Websites\<Trunk_Name>\Conf`

2. Under the `Conf` folder, create the following subfolder: `CustomUpdate`. If such a folder already exists, use the existing folder.

3. From the `Conf` folder, copy the following file to the `CustomUpdate` subfolder, depending on the trunk-type:

    `HTTP_WhlFiltAppWrap_ForPortal.xml` or

    `HTTPS_WhlFiltAppWrap_ForPortal.xml`

    If such a file already exists, use the existing file.

4. In the file you copied or accessed in step 3, locate the string:

    ```
    <!-- General connectivity section-->
    ```

    Under the <DATA_CHANGE> element, in <URL>, replace the string `webtop.*` with the URL of the Webtop application, as defined during the installation of the application.

    For example: if the URL of the application is "OurWebtop", the <URL> element should read:

    ```
    <URL case_sensitive="false">/OurWebtop/.*</URL>
    ```

    > **Note**
    >
    > • The application name is case insensitive.
    >
    > • The <UR> element takes regular expressions.

5. Access the Configuration program. Click 🔘 to activate the configuration. Select the option "Apply changes made to external configuration settings", and click Activate >.

    The Webtop (Documentum) application can now be accessed.

Enhanced Security Settings

This section describes how you can prevent users from performing the following operations unless their computer meets the defined security policy requirements:

• Using a pre-defined list of authentication repositories when logging in to the Webtop portal.

• Checkout.

• Checkin.

• Import.

• Export.

Users that are blocked are notified accordingly.

In order to enable this option, once you finish adding the application to the trunk, you need to define the security policy requirements using a dedicated endpoint policy: "Webtop Documentum 5 3 SP1 Enhanced Security". By default, the value of the policy is "True", and it does not prevent users from performing the operations listed above from any endpoint computer. If required, change the policy to comply with your corporate policy, as described here.

To prevent login, checkin, checkout, import, and export operations from non-compliant endpoints:

1. In the Configuration program, open the Application Properties dialog box. In the General tab, click `Edit Policies...`.
2. In the Policies dialog box, under the "Policies" group, select the policy "Webtop Documentum 5 3 SP1 Enhanced Security", then click `Edit...`.
3. Use the Advanced Policy Editor to edit the policy according to your requirements. For details, refer to the *Intelligent Application Gateway User Guide*, to the section "Endpoint Policies".
4. If you wish to define a list of repositories that users will not be able to use when running non-compliant computers, take the following additional steps:
   a) At the IAG, access the following folder:
      `…\Whale-Com\e-Gap\Von\Conf\Websites\<Trunk_Name>\Conf`
   b) Under the `Conf` folder, create the following subfolder: `CustomUpdate`. If such a folder already exists, use the existing folder.
   c) From the `Conf` folder, copy the following file to the `CustomUpdate` subfolder, depending on the trunk-type:
      `HTTP_WhlFiltAppWrap_ForPortal.xml` or
      `HTTPS_WhlFiltAppWrap_ForPortal.xml`
      If such a file already exists, use the existing file.

> (!) **Tip**
> For more information about these files, refer to the *Intelligent Application Gateway Advanced Configuration* guide, to the chapter titled "Application Customizers".

   d) In the file you copied or accessed in step c, locate the string:
      `list_of_unautorized_repositories =`
      `"repository_name1;repository_name2"`
      Replace the dummy repository names with the names of the repositories to which you wish to prevent access from non-compliant computers. Note that repository names are separated by a semi-colon.

e) Access the Configuration program. Click ⚙ to activate the configuration. Select the option "Apply changes made to external configuration settings", and click Activate >.

Checkin, checkout, import, and export operations will only be enabled on endpoint computers that comply with the security policy you defined here. If you defined a list of repositories, users running non-compliant computers will not be able to use those repositories when logging in to the Webtop portal, as well.

Cleaning Application-Specific Temporary Files

When the option "Attachment Wiper Cleans Application-Specific Temporary Files" is activated, the Attachment Wiper deletes the client's cache. This option is activated in the Session tab of the Advanced Trunk Configuration window.

> **Note**
> The Attachment Wiper deletes application-specific files only if the application is part of the IAG site.

By default, the Attachment Wiper deletes attachments, including all files and sub-directories, from the following locations:

```
c:\documentum\viewed\*.*\
```

```
c:\documentum\contentxfer\*.*\
```

In addition, you can configure the IAG to delete attachments from the following location:

```
c:\documentum\checkout\*.*\
```

> **Caution**
> The "checkout" folder is where Webtop saves temporary copies of documents that users check out, in order to edit them. If the Attachment Wiper deletes the folder before the user checks in a document, all changes are lost.
>
> For a description of when the Attachment Wiper deletes attachments, refer to the *Intelligent Application Gateway User Guide*, to the section titled "Attachment Wiper".

To configure the Attachment Wiper to delete the "checkout" folder:

1. At the IAG, open the following file:

    `...\Whale-Com\e-Gap\von\conf\samples\Webtop_sample.txt`

    Copy the content of the file.

2. Open the following file:

    `...\Whale-Com\e-Gap\von\conf\wizarddefaults\AWPaths\Webtop.txt`

    Paste the content of the file you copied in step 1 into this file, and save it.

3. In the Configuration program, click ⚙ to activate the configuration, select the option "Apply changes made to external configuration settings", and click Activate >.

    When the Attachment Wiper deletes attachments, it will delete all data under the "checkout" folder.

    Note

    Any changes you make to the `Webtop.txt` file in step 2 will be over-written when the IAG software is next upgraded or a patch is applied. It is therefore recommended that you back up the changes you made in an external file.