

- Security
- > [Fujitsu Patch & TA Information](#)
- > [Oracle Solaris Patch & TA Information](#)

## Applet security problem on the INTERSTAGE Application Server July 3rd, 2002

This bulletin provides security information about the reports to CERT/CC, the coordination center, or detected by Fujitsu's own examination by the published date.

Products developed by third parties may be included as subject products. Information about such third party products may be exactly the same as provided by the respective third party.

The contents of this bulletin are provided "AS IS" without warranties of any kind, either express or implied (including, without limitation, any implied warranty of merchantability, fitness for a particular purpose and non-infringement). In no event shall Fujitsu be liable for any direct, indirect, special, incidental, consequential, punitive, or any other damages of any kind, including, without limitation, loss of profits and loss of data incurred by a customer arising out of, or in connection with, the use or non-use of any information in this bulletin, even if Fujitsu has been advised of the possibility of such damages.

The information contained in this bulletin will be updated from time to time without notice. Therefore, all customers are advised to always ascertain the latest information. In case of redistribution of this security bulletin, the full text of this statement shall be reproduced.

[Outline]	
<b>Problem</b>	Applet security problem on the INTERSTAGE Application Server.
<b>Manufacturer</b>	Fujitsu Limited
<b>Corresponding products</b>	INTERSTAGE Standard Edition V2.0 (Windows) INTERSTAGE Enterprise Edition V2.0 (Windows) INTERSTAGE Standard Edition 2.1 (Solaris) INTERSTAGE Enterprise Edition 2.1 (Solaris) INTERSTAGE Standard Edition V2.1 (Windows) INTERSTAGE Enterprise Edition V2.1 (Windows) INTERSTAGE Application Server Standard Edition V3.0 (Windows) INTERSTAGE Application Server Enterprise Edition V3.0 (Windows) INTERSTAGE Application Server Standard Edition 3.0 (Solaris) INTERSTAGE Application Server Enterprise Edition 3.0 (Solaris) INTERSTAGE Application Server Standard Edition 3.0 (HP-UX) INTERSTAGE Application Server Standard Edition V4.0 (Windows) INTERSTAGE Application Server Enterprise Edition V4.0 (Windows) INTERSTAGE Application Server Standard Edition 4.0 (Solaris) INTERSTAGE Application Server Enterprise Edition 4.0 (Solaris) INTERSTAGE Application Server Standard Edition 4.1 (Linux) INTERSTAGE Application Server Enterprise Edition 4.1 (Linux) INTERSTAGE Application Server Standard Edition 4.1 (HP-UX)
<b>Corresponding systems</b>	Windows 98, Me, XP, NT, 2000 Solaris 2.51, 2.6, 7, 8
<b>Impact</b>	A local file on the client system may be damaged, or information in the local file may leak.
<b>Method to temporarily avoid the problem</b>	See 4.
<b>Patch</b>	None

[Top of Page](#) ↑

### 1. Background

The following problem was found on the INTERSTAGE Application Server (hereafter called INTERSTAGE in this manual).

When Java applet uses a service (function) provided by INTERSTAGE, security permission settings described in the manual are not correct.

Fujitsu provides information about this problem. Immediately take the corresponding corrective action.

### 2. Range of corresponding system(s)

Corresponding command/file	Products	Target OS
ODjava2.jar ODporb2_plugin.jar	INTERSTAGE Standard Edition V2.0 (CORBA Service, CORBA Service client, Portable-ORB)	Windows

ODjava2.jar ODporb2_plugin.jar	INTERSTAGE Enterprise Edition V2.0 (CORBA Service, CORBA Service client, Portable-ORB)	Windows
ODjava2.jar ODporb2_plugin.jar	INTERSTAGE Standard Edition 2.1 (CORBA Service, CORBA Service client, Portable-ORB)	Solaris
ODjava2.jar ODporb2_plugin.jar	INTERSTAGE Enterprise Edition 2.1 (CORBA Service, CORBA Service client, Portable-ORB)	Solaris
ODjava2.jar ODporb2_plugin.jar	INTERSTAGE Standard Edition V2.1 (CORBA Service, CORBA Service client, Portable-ORB)	Windows
ODjava2.jar ODporb2_plugin.jar	INTERSTAGE Enterprise Edition V2.1 (CORBA Service, CORBA Service client, Portable-ORB)	Windows
ODjava2.jar ODporb2_plugin.jar	INTERSTAGE Application Server Standard Edition V3.0 (CORBA Service, CORBA Service client, Portable-ORB)	Windows
ODjava2.jar ODporb2_plugin.jar	INTERSTAGE Application Server Enterprise Edition V3.0 (CORBA Service, CORBA Service client, Portable-ORB)	Windows
ODjava2.jar ODporb2_plugin.jar	INTERSTAGE Application Server Standard Edition 3.0 (CORBA Service, CORBA Service client, Portable-ORB)	Solaris
ODjava2.jar ODporb2_plugin.jar	INTERSTAGE Application Server Enterprise Edition 3.0 (CORBA Service, CORBA Service client, Portable-ORB)	Solaris
ODjava2.jar ODporb2_plugin.jar	INTERSTAGE Application Server Standard Edition 3.0 (CORBA Service, CORBA Service client, Portable-ORB)	HP-UX
ODjava2.jar ODporb2_plugin.jar ODporbROI2_plugin.jar	INTERSTAGE Application Server Standard Edition V4.0 (CORBA Service, CORBA Service client, Portable-ORB)	Windows
ODjava2.jar ODporb2_plugin.jar ODporbROI2_plugin.jar	INTERSTAGE Application Server Enterprise Edition V4.0 (CORBA Service, CORBA Service client, Portable-ORB)	Windows
ODjava2.jar ODporb2_plugin.jar ODporbROI2_plugin.jar	INTERSTAGE Application Server Standard Edition 4.0 (CORBA Service, CORBA Service client, Portable-ORB)	Solaris
ODjava2.jar ODporb2_plugin.jar ODporbROI2_plugin.jar	INTERSTAGE Application Server Enterprise Edition 4.0 (CORBA Service, CORBA Service client, Portable-ORB)	Solaris
ODjava2.jar ODporb2_plugin.jar ODporbROI2_plugin.jar	INTERSTAGE Application Server Standard Edition 4.1 (CORBA Service, CORBA Service client, Portable-ORB)	Linux
ODjava2.jar ODporb2_plugin.jar ODporbROI2_plugin.jar	INTERSTAGE Application Server Enterprise Edition 4.1 (CORBA Service, CORBA Service client, Portable-ORB)	Linux
ODjava2.jar ODporb2_plugin.jar	INTERSTAGE Application Server Standard Edition 4.1 (CORBA Service, CORBA Service client, Portable-ORB)	HP-UX

[Top of Page](#) 

### 3. Detected problem(s)

If all of the following conditions are met, any of the problems listed below may occur:

1. The INTERSTAGE CORBA service client function, the CORBA service function, and the Portable-ORB function are used with JDK/JRE 1.2.x or JDK/JRE 1.3.x.
2. A malicious Java applet using the above-listed functions is created, or a Java applet includes a creation failure.
3. The malicious Java applet is signed with a digital signature.
4. In the client machine, the security permission settings are performed for the digital signature of the malicious Java applet according to the INTERSTAGE manual.
5. A client machine with the settings describes in 4 accesses the Web site on which the malicious Java applet is posted.

<Possible problems>

- A file in the client may be damaged.
- The contents of a file in the client may leak.
- User-specific information in the client may leak.
- The native library (dynamic link library) of the client may be used by the Java applet.

### 4. Method to temporarily avoid the problem

<INTERSTAGE Standard/Enterprise Edition V2.0/2.1/V2.1>

[If the CORBA service or the CORBA service client is used]

Delete the permissions currently set for the Java applets and the preinstalled type Java libraries. Then make the settings according to the descriptions in 1. Settings and "2. Setting for use specific functions below.

Replace the descriptions in the following manual with these descriptions:

- The table described in the 5th item of the following manual. INTERSTAGE Distributed Application Development Guide (CORBA Service Edition)
  - + "4.20.2 Client Setup"
  - + "Setting Java library permission"
  - + "(1) Pre-installation type Java client"

If V2.0 is used, the table in procedure 13 is described in Section 9.5, "Caution Item for Java," in the readme.txt file.  
The readme.txt file is stored in %OD\_HOME% in the CORBA service installation directory.

- Permissions corresponding to the Pre-installed Java Library in Table A.5, "Permissions," in the following manual:  
 INTERSTAGE Distributed Application Development Guide (CORBA Service Edition)
  - + "Appendix A Digital Signatures of Java Applets"
  - + "A.1.2 Digital Signatures using JDK tools"
  - + "(5) Setting up the Competence for the Certificate"

#### 1. Settings

Set the permissions as described in the table below. Do not use other settings for normal operation.

Permission type	Permission to be set		
	Permission	Target Name	Actions
Runtime Permission	RuntimePermission	loadLibrary.DLL name (See note)	None

Note: loadLibrary.DLL name

Specify the dynamic link libraries (DLL) listed in the table below according to the installed functions and JDK/JRE to be used. The file extension is not required for the specified DLL name.

Installed function	JDK/JRE to be used	Specified DLL
CORBA Service client (Client function)	JDK/JRE1.2.x	ODjava2 ODjvas2
CORBA Service (Server function)	JDK/JRE1.2.x	ODjvas2

#### 2. Settings to use specific functions.

If the functions below are used, in addition to the permissions set in the above section 1.Settings, the following permissions are required:

- To collect log information

To collect information in the internal CORBA service log, set the permissions in the table below. For more information about CORBA service internal log, refer to Appendix D.1 (or Appendix F.1), "config," in Appendix D (or Appendix F), "CORBA Service Environment Definition," in the INTERSTAGE Operations Guide.

Permission type	Permission to be set		
	Permission	Target Name	Actions
Property permission	PropertyPermission	user.dir java.class.path	read read
File permission	FilePermission	\${user.dir}* %OD_HOME%\etc\config	read, write read

Note: After the log is collected, delete the added permissions. Specify CORBA service installation directory or CORBA service client as %OD\_HOME%. The default installation folder is C:\INTERSTAGE\ODWIN.

[Top of Page](#) 

[If the Portable-ORB is used]

Delete the permissions currently set for the Java applets and the Portable-ORB. Then make the settings according to the descriptions in 1. Settings and 2. Setting for using specific functions.

Replace the descriptions in the following manual with these descriptions:

- The table described in the 5th item of the following manual:  
 INTERSTAGE Distributed Application Development Guide (CORBA Service Edition)
  - + "4.20.2 Client Setup"
  - + "Setting Java library permission"
  - + "(2) Portable-ORB (operation that does not download Portable-ORB)"

If the V2.0 is used, the table in procedure 15 is described in Section 9.5, "Caution Item for Java," in the readme.txt file.  
 The readme.txt is stored in %OD\_HOME% in the CORBA service installation directory.

- Permissions corresponding to the Portable-ORB in Table A.5, "Permissions," in the following manual:  
 INTERSTAGE Distributed Application Development Guide (CORBA Service Edition)
  - + "Appendix A Digital Signatures of Java Applets"
  - + "A.1.2 Digital Signatures using JDK tools"
  - + "(5) Setting up the Competence for the Certificate"

#### 1. Settings

Set the permissions as described in the table below. Do not use other settings for normal operation.

Permission type	Permission to be set		
	Permission	Target Name	Actions
Communication permission	SocketPermission	Communication destination server name (See note)	connect

Note: Communication destination server name

If the web server that downloaded the Java applet is only used to perform communications as a server machine, you do not need to set this permission.

To communicate with a server machine that is not a web server and that downloaded the Java applet, specify as many communication destination server names as the number of communication destination servers.

If serverA.interstage.co.jp and serverB.interstage.co.jp are used as the communication destination servers, two communication permissions are set for serverA.interstage.co.jp and serverB.interstage.co.jp as the communication destination server names. If the specified range

can be verified as reliable, a wild card (\*) can be used to set one communication permission as \*.interstage.co.jp.

If only the wild card is specified, any server can open communications. For security reasons, do not specify the wild card (\*) only.

As the communication destination server name, the following host names must be specified:

- The host name specified in the host information of the porbeditenv command.

For more details about the host information, refer to Section 1.9.1, "porbeditenv", in the INTERSTAGE Reference Manual.

- The host name stored in the object reference corresponding to the application that performs communications.

The host name stored in the object reference is the "Object host name" displayed when the -l option is specified in the odlistns command, which displays what has been registered with the Naming Service.

For more details about the odlistns command, refer to Section 1.2.7 (or 1.2.11), "odlistns", in the INTERSTAGE Reference Manual.

## 2. Settings to use specific functions.

If the functions below are used, in addition to the permissions set in the above section 1. Settings the following permissions are required:

- To collect log information

To collect log information, the permissions in the table below must be set. For more details about log information, refer to Section 1.9.1, "porbeditenv," in the INTERSTAGE Reference Manual.

Permission type	Permission to be set		
	Permission	Target Name	Actions
File permission	FilePermission	Log collection file (See note 1)	read, write, delete
File permission	FilePermission	Log collection folder (See note 2)	read

Note 1: Log collection file

Specify the directory name specified in Directory in the porbeditenv command by adding \\* to the path. For example, if the path c:\log\porb is specified in Directory, specify c:\log\porb\\*.

Note 2: Log collection folder

Specify the directory name specified in Directory in the porbeditenv command.

Note: The directory specified in Directory in the porbeditenv command must be created before the log is created. Do not store any user resources other than the log collection file in this Directory.

After the log has been collected, delete the added permissions.

- To use API to obtain user information

To use API to obtain user information on the server application, the permission in the table below must be set. For more details about the API for user obtaining information, refer to Section 3.12.6, "TD\_get\_user\_information," Section 4.14.7, "TD::get\_user\_information," and Section 6.14.7 (or 6.14.10), "TDGETUSERINFORMATION," in the INTERSTAGE Reference Manual.

Permission type	Permission to be set		
	Permission	Target Name	Actions
Property permission	PropertyPermission	user.name	read

[Top of Page](#) 

< INTERSTAGE Application Server Standard/Enterprise Edition V3.0/ 3.0>

[If the CORBA service or the CORBA service client is used]

Delete the permissions currently set for the Java applets and the preinstalled type Java libraries. Then make the settings according to the descriptions in 1. Settings and 2. Settings to use specific functions.

Replace the descriptions in the following manual with these descriptions:

- Permissions corresponding to the Pre-installed Java Library in Table 4-9, "Permissions," in the following manual:  
INTERSTAGE Application Server Distributed Application Development Guide (CORBA Service Edition)  
+ "Chapter 4: Java Programming Guide"  
+ "Digital Signatures in Applets"  
+ "Digital Signatures Using JDK Tools"  
+ "(6) Setting a Permission for the Certificate"
- The table described in the 5th item of the following manual:  
INTERSTAGE Application Server Distributed Application Development Guide (CORBA Service Edition)  
+ "Chapter 4: Java Programming Guide"  
+ "Execution of CORBA Applications"  
+ "Client Setup"  
+ "Setting Permission for Java Libraries"  
+ "Pre-installation Type Java Client"

## 1. Settings

Set the permissions as described in the table below. Do not use other settings for normal operation.

Permission type	Permission to be set		
	Permission	Target Name	Actions
Runtime Permission	RuntimePermission	loadLibrary.DLL name (See note)	None
Property permission	PropertyPermission	com.fujitsu.*	read

Note: loadLibrary.DLL name

Specify the dynamic link libraries (DLL) listed in the following table according to the installed functions and JDK/JRE to be used. The file extension is not required for the specified DLL name.

Installed function	JDK/JRE to be used	Specified DLL
CORBA Service client (Client function)	JDK/JRE 1.2.x, 1.3.x	ODjava2
CORBA Service (Server function)	JDK/JRE 1.2.x, 1.3.x	ODjavas2

## 2. Settings to use specific functions.

If the functions below are used, in addition to the permissions set in the above section 1. Settings the following permissions are required:

- To collect log information

To collect the CORBA service internal log, set the permissions in the table below.

For more information about the CORBA service internal log, refer to "config," in "CORBA Service Environment Definition," in Chapter 2, "Definition Syntax," in the INTERSTAGE Application Server Reference Manual.

Permission type	Permission to be set		
	Permission	Target Name	Actions
Property permission	PropertyPermission	user.dir java.class.path	read read
File permission	FilePermission	\${user.dir}* %OD_HOME%\etc\config	read, write read

Note: After the log is collected, delete the added permissions. Specify the CORBA service installation directory or CORBA service client installation directory to %OD\_HOME%. The default installation folder is C:\INTERSTAGE\ODWIN.

[Top of Page](#) 

[If the Portable-ORB is used]

Delete the permissions currently set for the Java applets and the Portable-ORB. Then make the settings according to the descriptions in 1. Settings and 2. Setting for using specific functions.

Replace the descriptions in the following manual with these descriptions:

- Permissions corresponding to the Portable-ORB in Table 4-9, "Permissions," in the following manual:  
INTERSTAGE Application Server Distributed Application Development Guide (CORBA Service Edition)
  - + "Chapter 4: Java Programming Guide"
  - + "Digital Signatures in Applets"
  - + "Digital Signatures Using JDK Tools"
  - + "(6) Setting a Permission for the Certificate"
- The table described in the 5th item of the following manual:  
INTERSTAGE Application Server Distributed Application Development Guide (CORBA Service Edition)
  - + "Chapter 4: Java Programming Guide"
  - + "Execution of CORBA Applications"
  - + "Client Setup"
  - + "Setting Permission for Java Libraries"
  - + "When Portable-ORB is Not Downloaded"

## 1. Settings

Set the permissions as described in the table below. Do not use other settings for normal operation.

Permission type	Permission to be set		
	Permission	Target Name	Actions
Communication permission	SocketPermission	Communication destination server name (See note)	connect

Note: Communication destination server name

If the web server that downloaded the Java applet is only used for communications as a server machine, you do not need to set this permission.

To communicate with a server machine that is not a web server and that downloaded the Java applet, specify as many communication destination server names as the number of communication destination servers.

If serverA.interstage.co.jp and serverB.interstage.co.jp exist as the communication destination servers, two communication permissions are set for serverA.interstage.co.jp and serverB.interstage.co.jp as the communication destination server names. If the specified range can be verified as reliable, a wild card (\*) can be used to set one communication permission as \*.interstage.co.jp.

If only the wild card is specified, any server can open communications. For security reasons, do not specify the wild card (\*) only.

As the communication destination server name, the following host names must be specified:

- The host name specified in the host information of the porbeditenv command.

For more details about host information, refer to Chapter 1, "porbeditenv," in the INTERSTAGE Application Server Reference Manual.

- The host name stored in the object reference corresponding to the application that performs communications.

The host name stored in the object reference is the "Object host name" displayed when the -l option is specified in the odlistns command, which displays what has been registered with the Naming Service.

For more details about the odlistns command, refer to Chapter 1, "odlistns", in the INTERSTAGE

- The host name specified in the URL schema

For more details about the URL schema, refer to Chapter 8, "Naming Service Programming" and Chapter 14, "Obtaining Naming Service Initial References," in the INTERSTAGE Application Distributed Application Development Guide (CORBA Service Edition).

2. Settings to use specific functions.

If the functions below are used, in addition to the permissions set in the above section 1. Settings the permissions in the table below are required.

- To collect log information

To collect log information, set the permissions in the following table. For more details about log information, refer to Chapter 1, "porbeditenv," in the INTERSTAGE Application Server Reference Manual.

Permission type	Permission to be set		
	Permission	Target Name	Actions
File permission	FilePermission	Log collection file (See note 1)	read, write, delete
File permission	FilePermission	Log collection folder (See note 2)	read

Note 1: Log collection file

Specify the directory name specified in Directory in the porbeditenv command and add \\* to the path. For example, if the path c:\log\porb is specified in Directory, specify c:\log\porb\\*.

Note 2: Log collection folder

Specify the directory name specified in Directory in the porbeditenv command.

Note: The directory specified in Directory in the porbeditenv command must be created before the log is created. Do not store user resources other than the log collection file in this directory.

After the log has been collected, delete the added permissions.

- To use API to obtain user information

To use API to obtain user information on the server application, the permission in the table below must be set. For more details about the API to obtain user information, refer to Chapter 3, "TD\_get\_user\_information," Chapter 4, "TD::get\_user\_information," and Chapter 6, "TDGETUSERINFORMATION," in the INTERSTAGE Application Server Reference Manual.

Permission type	Permission to be set		
	Permission	Target Name	Actions
Property permission	PropertyPermission	user.name	read

[Top of Page](#) 

<INTERSTAGE Application Server Standard/Enterprise Edition V4.0/ 4.0/ 4.1>

[If the CORBA service or the CORBA service client is used]

Delete the permissions currently set for the Java applets and the preinstalled type Java libraries. Then make the settings according to the descriptions in 1. Settings and 2. Settings to use specific functions.

Replace the descriptions in the following manual with these descriptions:

- Permissions corresponding to the Pre-installed Java Library in Table, "Permissions," in the following manual:  
INTERSTAGE Application Server Distributed Application Development Guide (CORBA Service Edition)  
+ "Chapter 4: Java Programming Guide"  
+ "Digital Signatures in Applets"  
+ "Digital Signature Procedures"  
+ "(6) Setting a Permission for the Certificate"  
+ "Setting Authorization"
- The table described in the 5th item of the following manual:  
INTERSTAGE Application Server Distributed Application Development Guide (CORBA Service Edition)  
+ "Chapter 4: Java Programming Guide"  
+ "Execution of CORBA Applications"  
+ "Client Setup (Pre- Installed Library/Pre-installed Version Java Library)"  
+ "Setting Permission for Java Libraries"

1. Settings

Set the permissions as described in the table below. Do not use other settings for normal operation.

Permission type	Permission to be set		
	Permission	Target Name	Actions
Runtime Permission	RuntimePermission	loadLibrary.DLL name (See note)	None
Property permission	PropertyPermission	com.fujitsu.*	read

Note: loadLibrary.DLL name

Specify the dynamic link libraries (DLL) listed in the table below according to the installed functions and JDK/JRE to be used. The file extension is not required for the specified DLL name.

Installed function	JDK/JRE to be used	Specified DLL
CORBA Service client (Client function)	JDK/JRE1.2.x, 1.3.x	ODjava2
CORBA Service (Server function)	JDK/JRE1.2.x, 1.3.x	ODjavas2

2. Settings to use specific functions.

If the functions below are used, in addition to the permissions set in the above section 1. Settings the following permissions are required.

- To collect log information

To collect the CORBA service internal log, set the permissions in the table below.

For more information about CORBA service internal log, refer to "config, " in Chapter 3, "CORBA Service Environment Definition," in the INTERSTAGE Application Server Reference Manual (Definition Edition).

Permission type	Permission to be set		
	Permission	Target Name	Actions
Property permission	PropertyPermission	user.dir java.class.path	read read
File permission	FilePermission	\${user.dir}*\ %OD_HOME%\etc\config	read, write read

Note: After the log is collected, delete the added permissions. Specify the CORBA service installation directory or CORBA service client installation directory to %OD\_HOME%. The default installation folder is C:\INTERSTAGE\ODWIN.

[Top of Page](#) 

[If the Portable-ORB is used]

Delete the permissions currently set for the Java applets and the Portable-ORB. Then make the settings according to the descriptions in 1. Settings and 2. Settings to use specific functions.

Replace the descriptions in the following manual with these descriptions:

- Permissions corresponding to the Portable-ORB in Table, "Permissions," in the following manual:  
INTERSTAGE Application Server Distributed Application Development Guide (CORBA Service Edition)  
+ "Chapter 4: Java Programming Guide"  
+ "Digital Signatures in Applets"  
+ "Digital Signature Procedures"  
+ "(6) Setting a Permission for the Certificate"  
+ "Setting Authorization"
- The table described in the 5th item of the following manual:  
INTERSTAGE Application Server Distributed Application Development Guide (CORBA Service Edition)  
+ "Chapter 4: Java Programming Guide"  
+ "Execution of CORBA Applications"  
+ "Client Setup (Portable-ORB)"  
+ "Setting Permission for Java Libraries"

#### 1. Settings

Set the permissions as described in the below. Do not use other settings for normal operation.

Permission type	Permission to be set		
	Permission	Target Name	Actions
Communication permission	SocketPermission	Communication destination server name (See note)	connect

Note: Communication destination server name

If the web server that downloaded the Java applet is only used to perform communications as a server machine, you do not need to set this permission.

To communicate with a server machine that is not a web server and that downloaded the Java applet, specify as many communication destination server names as the number of communication destination servers.

If server A.interstage.co.jp and server B.interstage.co.jp exist as the communication destination servers, two communication permissions are set for server A.interstage.co.jp and server B.interstage.co.jp as the communication destination server names. If the specified range can be verified as reliable, a wild card (\*) can be used to set one communication permission as \*.interstage.co.jp.

If only the wild card is specified, any server can open communications. For security reasons, do not specify the wild card (\*) only.

As the communication destination server name, the following host names must be specified:

- The host name specified in the host information of the porbeditenv command

For more details about host information, refer to Chapter 9 (or one of the following: 7, 10, or 11), "porbeditenv", in the INTERSTAGE Application Server Reference Manual (Command Edition).

- The host name stored in the object reference corresponding to the application that performs communications

The host name stored in the object reference is the "Object host name" displayed when the -l option is specified in the odlistns command, which displays what has been registered with the Naming Service.

For more details about the odlistns command, refer to Chapter 4 (or one of the following: 5, or 3), "odlistns", in the INTERSTAGE Application Server Reference Manual (Command Edition).

- The host name specified in the URL schema

For more details about the URL schema, refer to Chapter 8, "Naming Service Programming" and Chapter 14 (or 13), "Obtaining Naming Service Initial References," in the INTERSTAGE Application Distributed Application Development Guide (CORBA Service Edition).

#### 2. Settings to use specific functions.

If the functions below are used, in addition to the permissions set in the above section 1. Settings the permissions in the table below are required.



- To use the EJB application

To use the EJB application, the permission in the table below must be set. For more details about the EJB application, refer to the INTERSTAGE Application Server Distributed Application Development Guide (EJB Service Edition).

Permission type	Permission to be set		
	Permission	Target Name	Actions
Property permission	PropertyPermission	com.fujitsu.* java.class.path	read read

- To collect log information

To collect log information, set the permissions in the table below. For more details about log information, refer to Chapter 9 (or one of the following: 7, 10, or 11), "porbeditenv", in the INTERSTAGE Application Server Reference Manual (Command Edition).

Permission type	Permission to be set		
	Permission	Target Name	Actions
File permission	FilePermission	Log collection file (See note 1)	read, write, delete
File permission	FilePermission	Log collection folder (See note 2)	read

Note 1: Log collection file

Specify the directory name specified in Directory in the porbeditenv command with adding \\* to the path. For example, if the path c:\log\porb is specified in Directory, specify c:\log\porb\\*.

Note 2: Log collection folder

Specify the directory name specified in Directory in the porbeditenv command.

Note: The directory specified in Directory in the porbeditenv command must be created before the log is created. Do not store files other than user resources in log collection file in Directory.

After the log has been collected, delete the added permissions.

- To use API to obtain user information

To use API to obtain user information on the server application, the permission in the table below must be set. For more details about the API used to obtain user information, refer to Chapter 1, "TD\_get\_user\_information," Chapter 2, "TD::get\_user\_information", and Chapter 4, "TDGETUSERINFORMATION", in the INTERSTAGE Application Server Reference Manual (API Edition).

Permission type	Permission to be set		
	Permission	Target Name	Actions
Property permission	PropertyPermission	user.name	read

5. Patch information

- None.

6. Revision history

- July 3rd, 2002: Initial release

[Top of Page](#) 