Permissions Requested

A Java applet has requested the permissions displayed in the Security Alert dialog box. In order for a Java applet to run, it may require file access and other resources on your computer. Each of these actions requires a specific permission in order to be carried out. Your network administrator may have already specified which permissions to allow. For those which are allowed, your network administrator can specify whether to notify you when those permissions are requested. Otherwise, you will only be notified when a Java applet requests more permissions than are automatically allowed by your network administrator.

Given what you know about the software publisher, and the permissions this program is requesting, you must decide whether to install and run this Java applet. If you don't feel comfortable, click **OK** in the Security Alert dialog box, and then click **No** in the Security Warning dialog box.

Click a permission below for more information about that permission:

FileIO

NetIO

Thread

Property

Execution

Reflection

Printing

Registry

Security

ClientStore

UI

System Streams

User Directed File IO

Multimedia

Custom

For information about viewing the settings for permissions on your computer, see the Related Topics below.

{button ,AL("A_IDH_SEC_ALERT_VIEW_JAVA_CUSTOM_SETTINGS")} Related Topics

Displays the type of access you are viewing or making changes for. You can click a type of access and then specify the settings below for that type of access.

Provides a space for you to type the name of a file you want to add to the list of files for which you will allow the specified access. You can type specific files, or you can use wildcards, such as *.exe.

Lists the files for which you will allow the specified access.

Adds the item to the list to include with these permissions.

Removes the selected item from the list.

Provides a space for you to type the name of a file to exclude from the list of files for which you will allow the specified access.

Lists the files for which you will not allow the specified access.

Specifies whether you want to allow access to file URL code base.

Displays the type of access you are viewing or making changes for.

Provides a space for you to type a registry entry to add to the list of registry entries for which you will allow the specified access.

Lists the registry entries for which you will allow the specified access.

Provides a space for you to type a registry entry to exclude from the list of registry entries for which you will allow the specified access.

Lists the registry entries for which you will not allow the specified access.

Specifies whether to allow Java applets to create dialog boxes.

Specifies whether to allow Java applets to create a top level window.

Specifies whether to display a warning when a Java applet requests to create a top-level window.

Specifies whether to allow a Java applet to use your computer's clipboard to cut, copy, or paste information.

Specifies to allow Java applets unrestricted access to system properties.

Specifies to allow access to system properties and suffixes you specify, and deny access to the system properties you exclude.

Provides a space for you to type suffixes which you allow Java applets access.

Provides a space for you to type the system properties you allow Java applets access to.

Provides a space for you to type the system properties you do not want to allow Java applets access to.

Specifies whether to allow a loader type that has been associated with this public permission object.

Specifies whether to allow a loader type that refers to any loaders other than the one associated with this public permission object.

Specifies whether to allow a loader type that refers to public system classes.

Specifies whether to allow a loader type that has been associated with this permission object.

Specifies whether to allow a loader type that refers to any loaders other than the one associated with this permission object.

Specifies whether to allow a loader type that refers to declared system classes.

Specifies whether to let Java applets read files if the user allows it.

Specifies whether to let Java applets write to files if the user allows it.

Specifies how much storage space on the user's computer to allow Java applets to use.

Specifies whether to allow Java applets to ignore storage limits specified by the user for all Internet files.

Specifies whether roaming files can be created. Roaming files are created in the user's profile and are present on any computer the user is logged on to.

Specifies whether the applications specified in **Allow execution** can be run.

Specifies which programs are allowed to run.

Specifies which programs are not allowed to run.

Specifies whether to allow unrestricted thread access.

Specifies whether to allow unrestricted thread group access.

Specifies whether the permission object allows the System.in stream to be set.

Specifies whether the permission object allows the System.out stream to be set.

Specifies whether the permission object allows the System.err stream to be set.

Specifies whether the classes that possess the PrintingPermission will be able to use the printing services.

Specifies whether to allow access to extended aspects of the DirectX APIs.

Specifies whether to allow access to the JDK security classes **java.lang.security**.

Displays the type of communication you are viewing or making changes for. You can click a type of communication and then specify the settings below for that type of communication.

Click this	To specify settings for this
Connect Addresses	General communication to specific hosts
Bind Addresses	Connections on specific interfaces and ports
Multicast Addresses	Joining specific multicast groups
Global Ports	Settings that supercede any individual port rules

Provides spaces for you to type a host and port to add to the list of hosts and ports for which you will allow the specified communication.

Lists the hosts and ports for which you will allow the specified communication.

Provides spaces for you to type a host and port to exclude from the list of hosts and ports for which you will allow the specified communication.

Lists the hosts and ports for which you will not allow the specified communication.

Specifies whether you want to connect to a file URL.

Specifies whether you want to connect to a non-file URL.

Provides spaces for you to type the name and data for permissions you want to add to the list of custom permissions settings.

Lists the name and data for the custom permission settings you have added.

Click this to set the security level to High (most secure).

Click this to set the security level to Medium.

To view custom settings

The permissions are set by the network administrator through the Internet Explorer Administration Kit. You cannot edit these settings, but you can view them.

1 Right-click the **Internet** icon on your desktop, and then click **Properties**.

2 Click the **Security** tab, and then click **Custom**.

3 In the settings list, under **Java**, click **Custom**.

4 Click the **Java Custom Settings** button at the bottom of the dialog box.

Notes

- If an **Edit** button appears at the bottom of the Java settings dialog box, then you can change the settings.
- If an **Edit** button does not appear, and you need settings changed, see your network administrator.

{button ,AL("A_IDH_SEC_ALERT_MORE_INFO")} Related Topics

Closes this dialog box and saves any changes you have made.

Closes this dialog box without saving any changes you have made.

Zone Editor dialog box

Within this zone, you can assign permissions to Unsigned, Allowed, or Query/Deny. Any permission that is not assigned to Unsigned or Allowed is assigned to Query/Deny.

Within the permissions assigned to Query/Deny, you can assign specific permissions to Query, and any remaining permissions are assigned to Deny. Or you can assign specific permissions to Deny, and any remaining permissions are assigned to Query.

If you want to automatically allow all permissions without having to open the corresponding editing box and turning all of the permissions on, you can select **Allow full set of permissions**.

Custom Permissions dialog box

This dialog box displays what Java permissions have been specified by your network administrator.

In order for a Java applet to run, it may require file access and other resources on your computer. Each of these types of actions requires a specific permission to be granted before the action can be carried out. Your network administrator may have already specified which permissions to allow. For those which are allowed, your network administrator can specify whether to notify you when those permissions are requested. Otherwise, you will only be notified when a Java applet requests more permissions than are automatically allowed by your network administrator.

Each of the tabs represents the three types of permission sets:

Unsigned Permissions granted to unsigned downloaded content

Allowed Permissions that do not require user approval

Query/Deny Permissions that require user approval or are absolutely denied

The following permissions may be assigned to these tabs:

FileIO

NetIO

Thread

Property

Execution

Reflection

Printing

Registry

Security

ClientStore

UI

System Streams

User Directed File IO

Multimedia

Custom

File IO tab

Use this tab to specify files and file types that you will allow in this permission set for this zone. By default, all files are excluded, so you do not need to specify files to exclude, unless they are a subset of the files you are including. For example, if you include a multimedia file type (*.avi), you can exclude a specific file of that type (huge.avi). You can specify different permissions for different types of access: Read, Write, and Delete.

Note

- Help is available for each setting in this dialog box. Select or click the setting or button you want information about, and then press F1.

Registry tab

Use this tab to specify registry entries you will allow in this permission set for this zone. By default, all registry entries are excluded, so you do not need specify registry entries to exclude, unless they are a subset of the registry entries you are including. For example, if you include HKEY_CURRENT_USER, you can exclude a specific registry category underneath that entry (HKEY_CURRENT_USER\NETWORK). You can specify different permissions for different types of access: Read, Write, Delete, Open, and Create.

Note

- Help is available for each setting in this dialog box. Select or click the setting or button you want information about, and then press F1.

UI tab

Use this tab to specify permissions for some of the more visible actions a Java applet might request on a user's computer, such as creating a window or dialog box, accessing system properties (such as .ini files), or checking information to determine how it is structured, so that the program can query the information. These permissions may be listed in the user's Java custom settings, or in a Security Warning dialog box when a Java applet requests permissions that exceed those you automatically allow.

Note

- Help is available for each setting in this dialog box. Select or click the setting or button you want information about, and then press F1.

Misc tab

Use this tab to specify permissions for reading, writing, and storing files, running programs, threading, and other permissions. These permissions may be listed in the user's Java custom settings, or in a Security Warning dialog box when a Java applet requests permissions that exceed those you automatically allow.

Note

- Help is available for each setting in this dialog box. Select or click the setting or button you want information about, and then press F1.

Net IO tab

Use this tab to specify the type of connections you will allow, and to which hosts and ports. By default, all hosts and ports are excluded, so you do not need to specify hosts and ports to exclude, unless they are a subset of the hosts and ports you are including. You can specify different permissions for different types of connections: Connect Addresses, Bind Addresses, Multicast, and Global Ports.

Note

- Help is available for each setting in this dialog box. Select or click the setting or button you want information about, and then press F1.

Custom tab

Use this tab to specify Custom Permission settings by name or data type.

Note

- Help is available for each setting in this dialog box. Select or click the setting or button you want information about, and then press F1.

A request or permission to access or control access to files.

A request or permission to perform network operations or a network-related action.

A permission that controls the ability to create and manipulate threads and thread groups.

A request or permission to access or manipulate global system properties.

A request or permission to control or run other programs.

A request or permission to perform reflection operations or use reflection APIs to gain access to members of a specified class.

A permission that controls access to the printing APIs.

A permission that controls the ability to gain access to the registry, or a request for access to a registry key.

A permission that controls access to the JDK security classes **java.lang.security**.

A permission for controlling access to client-side storage that is available through the **ClientStore** class.

A request to use an extended aspect of the user interface APIs, or a permission that controls the ability to use some of the enhanced functionality of the AWT.

A permission that controls the ability to change the values of the system streams **java.lang.System.in**, **java.lang.System.out**, and **java.lang.System.err**.

A request or permission to perform or control user-directed I/O operations.

A permission to allow the use of enhanced multimedia functionality.

A permission or request to perform custom operations.