Citrix Access Gateway Enterprise Edition
Citrix Access Gateway Plugin for Windows User Guide

Citrix Access Gateway™ 9.0, Enterprise Edition

Copyright and Trademark Notice

Trademark Acknowledgements

Document Code: October 29, 2008 (KKW)

Contents

Chapter 1 **Welcome**

Chapter 2 **Getting Started with the Access Gateway Plugin**

Chapter 3 **Changing Settings in the Access Gateway Plugin**

Chapter 4 **Using the Citrix Access Gateway Plugin for ActiveX**

Chapter 5 Working with the Access Interface

Chapter 6 Troubleshooting

Appendix A Access Gateway Session Error Codes

Welcome

This chapter describes who should read the *Citrix Access Gateway Plugin for Windows User Guide*.

Before logging on using the Access Gateway Plugin, review this documentation to learn how your connections work and how to access network resources in the secure network.

How to Use this Guide

This user guide is intended for users who log on to the internal network through an Access Gateway appliance. This document assumes that the Access Gateway is connected to an existing network and that your system administrator configured the appliance for user connections.

Document Conventions

Access Gateway documentation uses the following typographic conventions for menus, commands, keyboard keys, and items in the program interface:

Convention	Meaning
Boldface	Commands, names of interface items such as text boxes, option buttons, and user input.
Italics	Placeholders for information or parameters that you provide. For example, *filename* in a procedure means you type the actual name of a file. Italics also are used for new terms and the titles of books.
%SystemRoot%	The Windows system directory, which can be WTSRV, WINNT, WINDOWS, or other name you specify when you install Windows.
`Monospace`	Text displayed in a text file or command-line interface.
{ braces }	A series of items, one of which is required in command statements. For example, **{ yes | no }** means you must type **yes** or **no**. Do not type the braces themselves.

Convention	Meaning
[brackets]	Optional items in command statements. For example, [/**ping**] means that you can type **/ping** with the command. Do not type the brackets themselves.
| (vertical bar)	A separator between items in braces or brackets in command statements. For example, **{ /hold | /release | /delete }** means you type **/hold** or **/release** or **/delete**.
… (ellipsis)	You can repeat the previous item or items in command statements. For example, **/route:***devicename*[,…] means you can type additional *devicenames* separated by commas.

Getting Started with the Access Gateway Plugin

The Access Gateway is a hardware appliance that provides communication between your device and an enterprise network. It does so by creating a secure connection between your device and the Access Gateway. This allows you to gain access to critical business resources such as email, shared file systems, and applications.

How the Access Gateway Works

To log on to a remote network, you need to log on to the Access Gateway. To do this, you use the Access Gateway Plugin. If you are trying to log on to your internal network, install the plugin on your computer and then log on.

The Access Gateway Plugin is installed on your computer when you log on for the first time. When the plugin is installed, you can log on using the icon on your desktop or connect using a Web portal page.

When the Access Gateway Plugin is downloaded to your computer and a connection is made, it creates a secure channel of communication between your computer and the Access Gateway, and allows you to access resources in the internal network that you are authorized to use.

Your system administrator can also configure the Access Gateway Plugin to ensure that certain personal firewalls and antivirus applications are running on your computer.

System Requirements

The Access Gateway Plugin runs on the following operating systems:

- Windows Vista
- Windows XP

The following Web browsers are supported:

- Internet Explorer
- Firefox

Creating Connections using the Access Gateway Plugin

To connect with and use the Access Gateway Plugin, your system administrator needs to provide you with the following information:

- Access Gateway Web address, such as https://*AccessGatewayFQDN*/.
- Any system requirements for running the plugin as determined by your system administrator. System requirements can include antivirus software or a personal firewall installed on your computer.

Depending on the configuration of your computer, you might also need additional information:

- To install the Access Gateway Plugin, you must be a local administrator or a member of the Administrators group to install programs on your computer.
- If you are using a personal firewall on your computer, when you first connect with the plugin, the firewall might prompt you for permission to allow the connection. If you receive this prompt, always allow the connection. For details for allowing connections, see the manufacturer's documentation.

Connecting Using a Web Address

If you are connecting using a Web page, you are either prompted to log on or are taken directly to a portal page where you can connect using the Access Gateway Plugin.

If the Access Gateway is configured to have you log on before making a connection with the plugin, type your user name and password and then log on. A Web page appears that allows you to download and install the plugin. When the Access Gateway Plugin is installed, the connection provides full access to the network resources that you have permission to use.

Connecting Using the Access Gateway Plugin

To establish a secure connection for the first time, log on to the Access Gateway using a Web browser. Contact your administrator for the Web address and logon credentials. The typical format of a Web address is https://companyname.com.

To install the Access Gateway Plugin

1. In a Web browser, type the Web address of the Access Gateway.
2. Type your user name and password and click **Logon**.
3. Click the link to install the plugin.

When the download is complete, the plugin connects and displays a message in the notification area on the taskbar. You can also log on using the Access Gateway icon in the notification area.

If you want to connect using the Access Gateway Plugin without using a Web browser, you can configure the plugin to display the logon dialog box when you click the icon in the notification area.

Note: To configure Access Gateway Plugin settings, you must be logged on.

To configure logon using the Access Gateway Plugin

1. In the notification area, right-click the Access Gateway icon and click **Configure Access Gateway**.
2. Click the **Profile** tab and then click **Change Profile**.
3. On the **Options** tab, click **Use the Access Gateway Plugin for logon**.

You can log on by double-clicking the Access Gateway icon on the desktop or by right-clicking the Access Gateway icon in the notification area on the taskbar and clicking **Logon**. For more information about configuring the Access Gateway Plugin, see “Changing Settings in the Advanced Options Dialog Box” on page 13.

Ending Access Gateway Plugin Sessions

There are two ways you can end your session with the Access Gateway Plugin:

- Logging off from the session
- Exiting the session

When you log off, the session ends and the Access Gateway icon remains in the notification area.

To logoff from the Access Gateway

There are two ways you can log off from the Access Gateway:

- Double-click the Access Gateway icon on your desktop.

- Right-click the Access Gateway icon in the notification area and click **Logoff**.

When you exit a session, the session ends and the Access Gateway icon is removed from the notification area.

To exit the session

Right-click the Access Gateway icon in the notification area and click **Exit**.

Cleaning Up Your Computer when Your Session Ends

During a session, temporary files are created on your computer. The Access Gateway has a cleanup feature to remove temporary files from your computer. This feature is enabled by your system or network administrator.

You can select the following items for cleanup, which removes them from your computer:

- Access Gateway Plugin
- Certificates used for authentication
- Applications used during the session
- Passwords and autocomplete data
- History and Web addresses typed in the address bar
- Cookies and temporary files

Finding Information on the Summary Tab

The **Summary** tab provides information about your session. These include:

- Total number of files viewed
- Total number of registry entries changed
- Total number of cookies installed
- Total number of applications used

Configuring the Cleanup Level

You can configure the Access Gateway to delete some or all of the data sets when you log off. You might want to retain some of the data such as autocomplete data, stored passwords, and history, especially if it is your personal computer. Data is categorized into three groups to help you selectively delete data. The groups are:

None. When this level is selected, none of the data sets are deleted.

Browser Only. When this level is selected, you can set the Access Gateway to delete one or more of the following data sets:

- Passwords and autocomplete data stored by the browser
- History and Web addresses typed in the address bar
- Browser cache cookies and temporary files

Everything. When this level is selected, you can set the Access Gateway to delete all temporary data that was generated by your computer.

Configuring the Cleanup Process

Your system administrator controls the cleanup process. The cleanup dialog box appears only if the administrator configured the Access Gateway to display the dialog box to you. In addition, the administrator can also configure the Access Gateway to delete specific data sets from your computer when you exit the session. The options corresponding to these data sets are disabled on the **List** tab of the **Citrix Windows Cleanup** dialog box. The remaining options are enabled or disabled based on the cleanup level that you choose.

To select data sets

1. In the **Citrix Windows Cleanup** dialog box, click **List**.
2. Select or clear the check box next to the data set.

Viewing the Cleanup Logs

The Access Gateway Plugin logs all the cleanup activity in a file that is stored on your hard drive. The file lists the action performed and the files that were deleted.

To view the log file

On the **Summary** tab, click **View Log**.

Changing Settings in the Access Gateway Plugin

Your system administrator configures most of the settings you need to successfully connect to the Access Gateway and gain access to network resources. Depending on how your administrator configured the Access Gateway, there are settings you can change in the Access Gateway Plugin.

This chapter explains logging on using the Access Gateway Plugin and configuring settings.

In This Chapter

Changing Settings in the Advanced Options Dialog Box

In the Access Gateway Plugin dialog box, you can change the following settings:

- Configuring the IP address or Web address for the Access Gateway
- Configuring proxy server settings
- Disabling or enabling security certificate warnings

Note: These settings can only be changed if you have configured the Access Gateway Plugin to log on using the Access Gateway dialog box instead of a Web browser. For more information, see “To configure logon using the Access Gateway Plugin” on page 9.

Setting the Access Gateway Web Address

When the Access Gateway Plugin is configured, you use the preconfigured IP address of the Access Gateway to connect. You can also configure the plugin to connect to a different appliance.

To configure the Access Gateway Plugin Web address

1. On the desktop, right-click the Access Gateway icon and click **Open**.
2. In the Access Gateway Plugin dialog box, right-click and then select **Advanced Options**.
3. Under **Citrix Access Gateway configuration**, in **Web address**, type the Web address and click **OK**.

   The Web address can be an IP address, such as 192.168.1.2, or Web address such as https://ag1.mycompany.com.

Configuring Proxy Servers for the Access Gateway Plugin

A proxy server is a computer that sits between your client device and servers in the internal network. Proxy servers intercept requests from your Web browser to the server in the internal network to see if it can fulfill the requested Web page. If the proxy server cannot fulfill the request, it sends the request to the server in the secure network.

When a proxy server is configured manually, automatic detection of proxy settings is disabled.

To configure proxy settings for the Access Gateway Plugin

1. On the desktop, right-click the Access Gateway icon and click **Open**.
2. In the dialog box, right-click and then select **Advanced Options**.
3. Under **Proxy settings**, select **Manually configure proxy server**.
4. In **IP Address** and **Port**, type the IP address and port number.

Note: To access the log on dialog box and Advanced Options to configure proxy settings, you must log off from the Access Gateway.

Logging on with a Secondary Password

Some Access Gateway appliances might require you to log on using two authentication types. This might include your user name and password and a personal identification number (PIN) followed by a number from a token, such as provided by RSA SecurID.

The Access Gateway dialog box default setting is to display logon fields for your user name and password. You can configure the Access Gateway Plugin to show the secondary password field.

To show the secondary password field

1. On the desktop, right-click the Access Gateway dialog box and click **Open**.
2. Right-click anywhere in the dialog box and select **Show Secondary Password**.

Note: If the secondary password field is not needed, in the Access Gateway dialog box, right-click anywhere in the dialog box and select **Hide Secondary Password**.

Changing Settings from the Access Gateway Menu

When you are logged on, you can change settings from Access Gateway icon in the notification area by right-clicking the icon and then selecting an item from the menu. From this menu, you can:

- Open the Access Interface or the home page configured by your system administrator
- Start the File Transfer utility
- Change configuration settings
- Open the connection log
- Display the current Access Gateway Plugin message
- Open the online help
- Logoff and exit the Access Gateway Plugin

Your administrator can configure the Access Gateway Plugin so you do not have access to the Access Interface, the File Transfer utility, or configuration settings. If your administrator configured the Access Gateway Plugin this way, these items do not appear on the menu.

Opening the Access Interface

The Access Interface, provided by Citrix, allows you to test connections to other computers, configure bookmarks, transfer files, and connect to Web-based email, such as Outlook Web Access. For more information about the home page, see “Working with the Access Interface” on page 21.

Your system administrator might disable the Access Interface and use a different Web page as your home page. This section describes working with the Access Interface.

To open the Access Interface

In the notification area, right-click the Access Gateway icon and click **Home**.

Viewing and Changing Access Gateway Plugin Information and Settings

Using the menu available from the Access Gateway icon in the notification area, you can open the **Citrix Access Gateway Configuration** dialog box. You can view information about the Access Gateway connection and configure settings for the connections.

To open the Configuration dialog box

Right-click the Access Gateway icon in the notification area and click **Configure Access Gateway**.

Viewing Connection Statistics

In the **Configuration** dialog box, you can view the following information:

- View connection statistics
- View your profile, such as the Access Gateway you are connected to, the networks that you can connect to, and other configuration settings
- Configure logging information for the Access Gateway connection
- View connection compression information

The **General** tab displays information about the connection. This information is helpful for technical support personnel if you are having problems with your connection.

Note: Your administrator might have the Access Gateway configured to prevent access to the connection statistics.

To view connection statistics

1. In the notification area, right-click the Access Gateway icon and click **Configure Access Gateway**.
2. Click the **General** tab.

The **Compression** tab shows information about connections that are compressed.

To view compression statistics

1. In the notification area, right-click the Access Gateway icon and click **Configure Access Gateway**.
2. Click the **Compression** tab.

For more information about the Compression tab, see “Viewing Compression Statistics” on page 28.

Changing Settings on the Profile Tab

Within the **Configuration** dialog box, on the **Profile** tab, you can change the following connection settings:

- Configuring split tunneling, split DNS, and local area network access
- Adding or removing domain and IP address settings to connect to specific resources in the internal network
- Enabling or disabling networks
- Configuring your computer to log on with the Access Gateway Plugin each time without using the Web browser
- Disabling or enabling security certificate warnings

Configuring Split Tunneling

When split tunneling is enabled, the Access Gateway filters traffic using the IP address of the destination network. Traffic meant for your organization’s network is sent through the Access Gateway and the rest of the traffic is sent to your local area network or the Internet.

Split tunneling has three options:

- **On.** When split tunneling is enabled, the Access Gateway Plugin compares the destination IP address and port against the values configured by the system administrator on the Access Gateway. If one of the values match, the packets are sent to the remote network through the Access Gateway. Otherwise, they are diverted to your network.

- **Off.** When you choose this option, split tunneling is disabled and the Access Gateway Plugin sends all traffic to the remote network through the Access Gateway.
- **Reverse On.** When Reverse On is enabled, Internet connections and requests to your LAN are sent through the Access Gateway. Connections to internal network resources are not sent through the Access Gateway. This is typically used when the Access Gateway resides in the internal network and you are connecting from your office.

Important: If split tunneling is disabled on the Access Gateway, the corresponding controls for split tunneling and split DNS are disabled in the Access Gateway Plugin and you cannot change the settings. All network traffic is sent through the Access Gateway.

To change split tunneling settings

1. Right-click the Access Gateway Plugin icon in the notification area and click **Configure Access Gateway**.
2. Click the **Profile** tab and then click **Change Profile**.
3. Under **Split tunneling**, select the option you want and click **OK**.

Uninstalling the Access Gateway Plugin

You can uninstall the Access Gateway Plugin using Add or Remove Programs in Control Panel. To uninstall the plugin, you must be logged on as an administrator.

To uninstall the Access Gateway Plugin

1. Click **Start > Control Panel**.
2. Under **Programs**, click **Uninstall a program**.
3. Select **Citrix Access Gateway Plugin** and click **Remove**.

After the plugin is removed, you must restart your computer.

CHAPTER 4

Using the Citrix Access Gateway Plugin for ActiveX

The Access Gateway allows you to access authorized resources on a remote network over a secure connection. To establish the secure connection, you must first log on to the Access Gateway using the logon page. Contact your administrator for the Web address and the logon credentials. The typical format of a Web address is as follows: https://ag1.companyname.com. The following procedure lists the steps to start an Access Gateway session using the Access Gateway Plugin for ActiveX.

You can use the Access Gateway Plugin for ActiveX only if your system administrator configured its use on the Access Gateway.

Note: The Access Gateway Plugin for ActiveX is supported only on Windows XP with Internet Explorer 6.0 or earlier. Citrix recommends using the Access Gateway Plugin for Windows for user connections instead of the Access Gateway Plugin for ActiveX.

To install the Access Gateway Plugin for ActiveX, you must be logged on as an administrator or be able to provide administrator credentials, such as a user name and password.

To connect using the Access Gateway Plugin for ActiveX

1. In a Web browser, type the Web address of the Access Gateway.

   The logon page appears.

   Enter your user name and password and click **Login**.

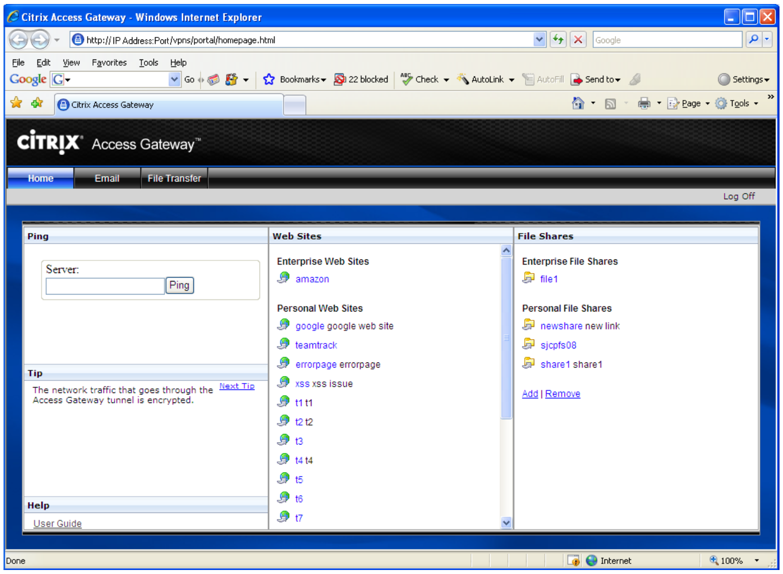
   When you log on to the Access Gateway for the first time, in the Secure Remote Access dialog box, you are asked to install the Access Gateway Plugin for ActiveX. Double-click the dialog box to install the plugin.

When the download is complete, the Secure Remote Access Session window displays the following message: “Closing this window exits the Access Gateway session.” This indicates that the Access Gateway session is now active. The Access Interface or home page configured by the administrator appears in the main browser window.

You can now access resources within the internal network. For example, if you are logged on to your office network, you can start your email client and access your messages.

Working with the Access Interface

The Access Gateway has the Access Interface, which is the home page as shown in the following figure. This page lists the most commonly accessed internal Web sites and file shares for your organization. The administrator configures the links visible under **Enterprise Web Sites**. You can create your own bookmarks to appear under **Personal Web Sites**. This chapter covers the configuration tasks that you can perform in the Access Interface.



Enterprise Web Sites
- amazon

Personal Web Sites
- google google web site
- teamtrack
- errorpage errorpage
- xss xss issue
- t1 t1
- t2 t2
- t3
- t4 t4
- t5
- t6
- t7

Enterprise File Shares
- file1

Personal File Shares
- newshare new link
- sjcpfs08
- share1 share1

Add | Remove

The network traffic that goes through the Access Gateway tunnel is encrypted.

The Access Gateway default home page, called the Access Interface

Note: The Access Interface is the default home page that ships with the Access Gateway. Your system administrator can use a different home page, so you might not see the Access Interface when you log on.

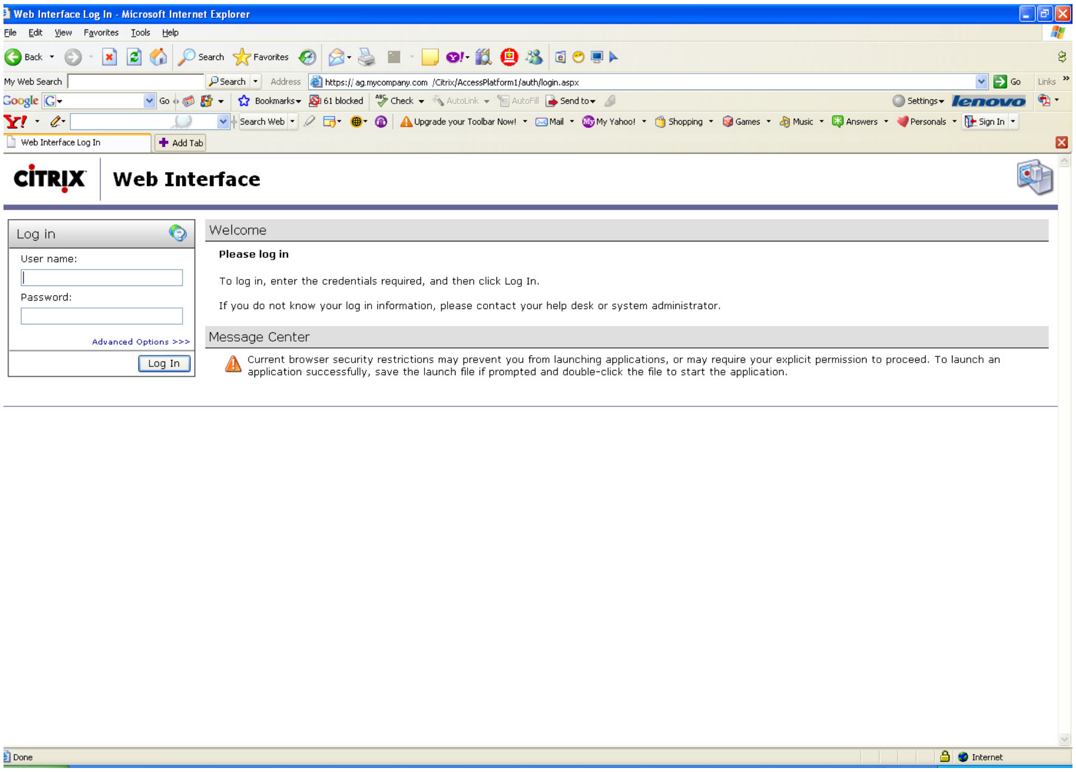
Logging on to the Access Interface

There are several options for logging on to the home page, depending on how your system administrator configured the Access Gateway appliance. You might receive the Access Interface or a custom home page installed by your system administrator. If you type in a Web address after logging on, you might see three choices. The options are:

- Citrix Access Gateway
- Citrix XenApp
- Clientless access

Citrix XenApp provides access to applications that reside in your organization’s network. Your system administrator can publish any type of application, such as Microsoft Word or Outlook.

If you selected Citrix XenApp, you might see the following home page:



Web Interface Log In - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address https://ag.mycompany.com/Citrix/AccessPlatform1/auth/login.aspx
Go
Web Interface Log In
Add Tab
CiTRIX
Web Interface
Log in
User name:
Password:
Advanced Options >>>
Log In
Welcome
Message Center
Done
Internet

Please log in

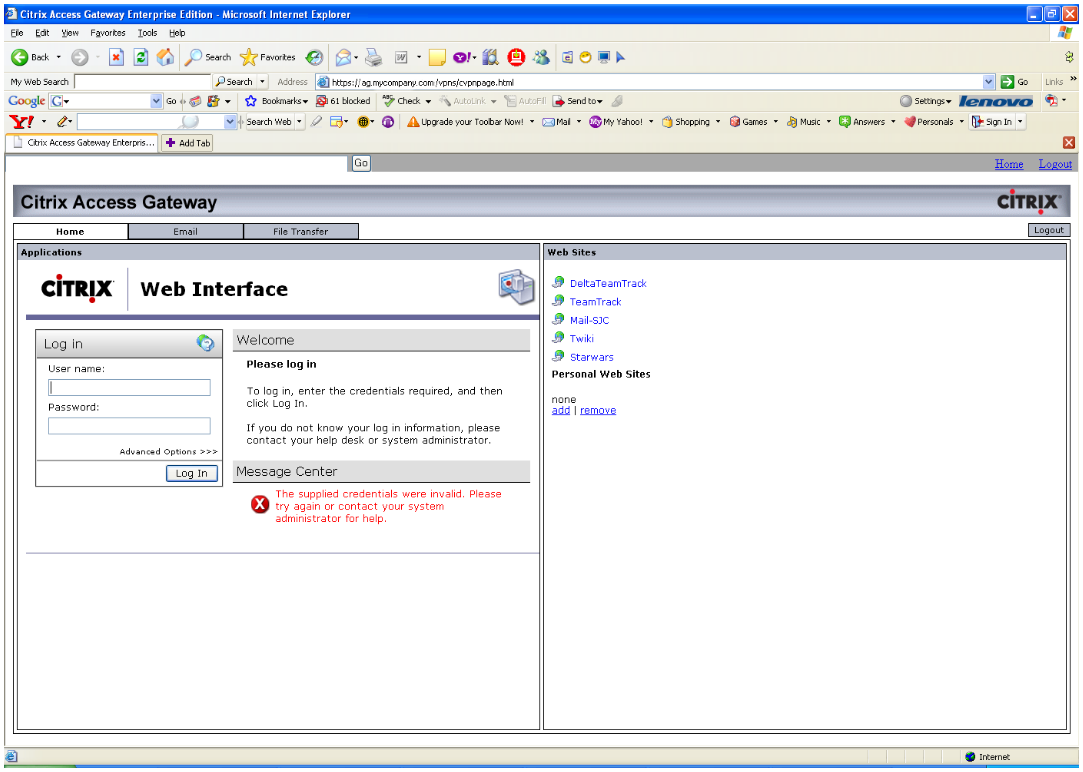
To log in, enter the credentials required, and then click Log In.

If you do not know your log in information, please contact your help desk or system administrator.

Current browser security restrictions may prevent you from launching applications, or may require your explicit permission to proceed. To launch an application successfully, save the launch file if prompted and double-click the file to start the application.

The Web Interface

If you log on using clientless access, the Access Interface home page appears with the Web Interface logon in the left pane, as shown in the following illustration:



Please log in

To log in, enter the credentials required, and then click Log In.

If you do not know your log in information, please contact your help desk or system administrator.

The supplied credentials were invalid. Please try again or contact your system administrator for help.

Access Interface with Web Interface logon in the left pane

When you log on to the Web Interface, you then receive the home page and have access to the provided tools.

Adding Bookmarks on the Home Tab

Your system administrator can add bookmarks to the Access Interface. These appear as links under **Web Sites**.You can also create your own links to commonly accessed network resources, such as a SharePoint site in the intranet. These appear as links under **Personal Web Sites**.

These bookmarks can be links to either intranet or Internet Web sites or file shares in the internal network.

To add a bookmark

1. Click **Add**.
2. In **Name**, type the name for the link.
3. In **Address**, type the Web address of the Web site or the network path to the internal Web server.
4. In **Description**, type a description for the link and click **Add**.

Note: The Access Gateway differentiates automatically between Web addresses and network file paths based on the format in which they are entered, such as *http://www.mycompany.com* or *\\server\sharename*. When creating a link, you do not need to specify the resource type.

To remove a bookmark

1. Click **Remove**.
2. Select the bookmark and click **Remove**.

Note: You can remove bookmarks that are listed under **Personal Web Sites** but not those under **Web Sites**.

Using the Email Tab

The email tab provides you with access to your email using Microsoft Outlook Web Access. When you click the tab, your email appears just as if you were using a local version of Microsoft Outlook.

To use Outlook Web Access, it must be configured by your system administrator.

Connecting to File Shares Using the File Transfer Tab

This page allows you to log on to the internal network and access shared resources.

To open the File Transfer tab

In the Access Interface, click the **File Transfer** tab.

You can also open the **File Transfer** tab from the Access Gateway icon in the notification area.

To open the File Transfer tab using the Access Gateway icon

In the notification area, right-click the Access Gateway icon and click **File Transfer**.

The following sections cover the various components of the **File Transfer** tab.

Configuring Settings in the Top Panel

There are several buttons on the top panel of the browser window that allow you to perform various tasks for storing and transferring files.

- **Log On**. Click this button to log on to the internal network or a specific computer on the network.
- **Up**. Click this button to navigate to the previous folder.
- **Refresh**. Click this button to refresh the contents of the active folder.
- **Mkdir**. Click this button to create a new folder.
- **Download**. Click this button to download the selected file from the remote server.
- **Upload**. Click this button to upload the selected file from the client device to a folder on the remote server.
- **Delete**. Click this button to delete the selected file from the remote computer.
- **Rename**. Click this button to change the name of a file or folder.
- **Log Off**. Click this button to disconnect from the remote server.

Viewing Folders and Files in the Left Panel

The servers, their directories, and the directory structure appears in a tree format in the left panel. Click the plus (+) icon to view folders.

Connecting to Network Resources in the Right Panel

The right panel displays the **File Server** window. Use this window to log on to a file server in the internal network. To access the file server, leave the **Address** field blank or click **Network Neighborhood** in the left panel.

To log on to a file server from the Access Gateway Plugin

1. In the notification area, right-click the Access Gateway icon and click **Transfer Files**.
2. In **Address**, type the name of the file share.

3. In **Login**, type your user name.
4. In **Password**, type your password.
5. In **Domain**, type a valid domain name.

   If the remote server is not assigned a specific domain, leave the field blank.

   Note: If you leave this field blank, you are logged on to the internal network and not to a specific server.

The right panel now displays the subfolders and files. The location of the active folder appears in the **Address** field.

Troubleshooting

The Access Gateway Plugin provides tools to help you troubleshoot your connections and sessions. You can use a variety of statistics and logs to report problems to your help desk or system administrator.

In This Chapter

- Opening the Connection Log
- Reporting Errors with the Access Gateway Plugin
- Viewing Compression Statistics

Opening the Connection Log

The connection log for the Access Gateway Plugin provides details of your connection to the Access Gateway and network resources. This log is useful for troubleshooting problems with your connection. You can provide the log to your Help desk support personnel or to your system administrator.

To open the connection log

1. In the notification area, right-click the Access Gateway icon.
2. On the menu, click **Show Connection Log**.

Reporting Errors with the Access Gateway Plugin

You can configure the Access Gateway Plugin to log all errors to a text file. The Access Gateway Plugin logs all of its major activities into a log file. These are stored on your device. You can send these files to your help desk or system administrator.

On Windows XP, log files are located in the directory %systemdrive%\Documents and Settings\All Users\Application Data\Citrix\AGEE.

On Windows Vista, the log files are located in the directory %systemdrive%\ProgramData\Citrix\AGEE. You can use these log files to troubleshoot the Access Gateway Plugin.

You can set the level of logging for the Access Gateway Plugin. The logging levels are:

- Record error messages
- Record event messages
- Record Access Gateway Plugin statistics
- Record all errors, event messages, and statistics

To enable logging

1. Right-click the Access Gateway Plugin icon in the notification area and click **Configure Access Gateway**.
2. Click the **Trace** tab, select the log level, and click **OK**.

Viewing the Log Files

The log files provide information about problems the Access Gateway Plugin might encounter. This information is helpful when you encounter a problem and are working with your technical support staff.

To view the log files

1. Right-click the Access Gateway Plugin icon in the notification area and click **Configure Access Gateway**.
2. On the **Trace** tab, click **View Log File**.

You can also view the connection log, which shows the connection information between the Access Gateway Plugin and the internal network.

To view the connection log files

Right-click the Access Gateway Plugin icon in the notification area and click **Show Connection Log**.

Viewing Compression Statistics

The compression tab displays statistics about the current Access Gateway session’s TCP traffic compression rates, broken down by individual connections. The columns on this tab include the following statistics.

- **Port**. The port number on which the connection is communicating.

- **Uncompressed Data**. Size of the data before compression is applied.
- **Compressed Data**. The data size after compression is applied.
- **Bandwidth Saving**. The approximate bandwidth savings when compression is used, expressed as a percentage. This is calculated by the compressed data size subtracted from the actual size, divided by the actual data size.
- **Compression Ratio**. The compression ratio based on actual data size versus the compressed data size.

Note: Bandwidth savings could occasionally show as a negative value. This happens with applications where transmitted data is sent in very small pieces and other applications where data is compressed before it is sent.

To view compression statistics

1. In the notification area, right-click the Access Gateway icon and then click **Configure Access Gateway**.
2. Click the **Compression** tab.

Access Gateway Session Error Codes

The following error codes appear in the Access Gateway session window. These codes can be used for troubleshooting problems with the Access Gateway.

Error Code	Description
0001-1000	Normal operation
1001-2000	Internal error
2001-3000	Access Gateway Plugin errors
3001-4000	Browser errors

The following table lists the specific error codes displayed by the Access Gateway session. It also provides a description of these error codes.

Codes	Message	Explanation	Action
0001	Loading...	This message indicates that Access Gateway Plugin is loading the configuration and the interception software before the Access Gateway session is established.	None
0002	Connection established. To end this session, right-click the Access Gateway icon and click Logoff	This message appears when the Access Gateway Plugin successfully connects.	None
0002	Closing this window ends the Access Gateway session	This message appears when the user closes the Web browser and is connected using the Access Gateway Plugin for ActiveX.	

Codes	Message	Explanation	Action
0003	Exiting...	This appears when the user clicks Logoff from the Access Gateway menu.	None
0004	Your session timed-out, you are not connected.	This error message appears when the client session times out.	None
0004	You are not logged on.	This error message appears when the Access Gateway Plugin is not connected.	None
0005	Your session is going to time-out in <*number*> of seconds.	This error message appears when a session is configured for a forced time-out.	None
0006	Downgrading the Access Gateway Plugin from <*versionNumber*> to <*versionNumber*>.	The Access Gateway is installing an earlier version of the software.	None
0006	Upgrading the Access Gateway Plugin from <*versionNumber*> to <*versionNumber*>.	The Access Gateway Plugin is upgrading to a new version of the software.	None
1001	There is an internal error. For more information, please contact your help desk or system administrator.	This message indicates that Access Gateway Plugin failed to open the interception file.	Restart the client device and logon using a Windows account that has administrative privileges.
1002	There is an internal error. For more information, contact your help desk or system administrator.	This message indicates that the version of the Access Gateway Plugin and the version of the interception software do not match.	Reinstall the Access Gateway Plugin.

Codes	Message	Explanation	Action
1003	Failed to allocate memory.	The Access Gateway Plugin ran out of memory.	When this error appears, users should logoff, restart the Access Gateway Plugin, and logon again. Report this error to your help desk or system administrator.
1004	There is an internal error. For more information, please contact your administrator.	The Access Gateway Plugin cannot call the Windows API successfully.	None
1005	There is an internal error. For more information, please contact your administrator.	The Access Gateway Plugin failed to create the temporary interception file.	Users need to log on using an administrator's account.
1006	There is an internal error. For more information, please contact your administrator.	The client security check failed when scanning the Windows process list.	Users need to log on using an administrator's account.
1007	There is an internal error. For more information, please contact your administrator.	The client security check failed when opening a Windows system service.	Users need to log on using an administrator's account.
1008	There is an internal error. For more information, please contact your administrator.	The Access Gateway Plugin failed.	Restart the Access Gateway Plugin and send the debug trace file to your help desk or system administrator.
1010	Your logon failed.	The user could not log on.	None

Codes	Message	Explanation	Action
1011	The Access Gateway Plugin failed to download the correct configuration.	The Access Gateway Plugin cannot download the Access Gateway configuration successfully.	Check the network status and then contact your system administrator.
1012	The Access Gateway Plugin could not start. For more information, see the connection log.	The Access Gateway Plugin failed to establish a connection. For more information, check the connection log and make any necessary changes.	Locate the error in the connection log and then report to your help desk or system administrator.
1013	Failed to parse configuration. Check the connection log for more information.	There is a configuration error on the Access Gateway.	Contact your help desk or system administrator.
1014	The client device could not resolve the Access Gateway Web address.	The Access Gateway Plugin failed to resolve the domain name.	Modify the HOSTS file or ask your system administrator to change or fix the configuration.
1015	The secure connection cannot be established.	The Access Gateway Plugin could not establish a secure connection.	Contact your help desk or system administrator.
1016	Failed to downgrade the Access Gateway Plugin from <*versionNumber*> to <*versionNumber*>.	The installation of an earlier version of the Access Gateway Plugin failed.	Contact your help desk or system administrator.
1016	Failed to upgrade the Access Gateway Plugin from <*versionNumber*> to <*versionNumber*>.	The Access Gateway Plugin failed to upgrade to the latest version.	Contact your help desk or system administrator.
2001	Your Access Gateway session timed-out and you are not connected.	This message indicates that your Access Gateway session timed out.	Log off of from the Access Gateway Plugin and then log on again.

Codes	Message	Explanation	Action
2003	There is a configuration issue on the Access Gateway.	This message indicates that the configuration on the Access Gateway is not correct.	Contact your system administrator to configure the Access Gateway correctly.
2004	You need to install endpoint security software.	This message indicates that at least one of the required endpoint security applications is not installed.	Contact your system administrator to install the required security software.
2005	You need to upgrade the endpoint security software.	This message indicates that the endpoint security software is not the correct version.	Contact your system administrator to upgrade the security software.
2006	The required security software is not activated.	This message indicates that the endpoint security software is not activated.	Start the security software.
2007	This version of the Access Gateway Plugin is updated. Please logon again.	This message indicates that the interception code does not match the version of the Access Gateway Plugin.	Log off and log on again.
2008	The versions between the Access Gateway Plugin and the Access Gateway do not match. To upgrade, log on using the Web browser.	The Access Gateway Plugin does not match the Access Gateway version. Users can upgrade automatically by logging on to the Web browser.	Uninstall the Access Gateway Plugin, restart the client device, and log on again to install the plugin.
2008	This version of the Access Gateway Plugin is updated. Please logon again.	The Access Gateway Plugin upgrade is successful, but did not activate automatically.	Log off and log on again.
2009	The proxy server requires unsupported authentication.	There is a local forward proxy setting that requires authentication. Not all proxy-supported authentication types are supported by the Access Gateway Plugin.	None
2010	Proxy server authentication failed, please logon again.	There is a local forward proxy setting that requires authentication. This error message appears when the user failed to provide a valid user name or password.	None

Codes	Message	Explanation	Action
2011	The Access Gateway failed to validate the secure certificate.	The client certificate is not the correct certificate. The certificate can be stored in a Web browser or on a smart card. The Access Gateway Plugin cannot detect the required certificate.	Contact your help desk or system administrator to provide the correct client certificate.
2012	The Access Gateway Plugin failed to start the interception driver.	The Access Gateway Plugin did not start the interception driver. To do so requires the user to be logged on as an administrator.	Log on with the Access Gateway Plugin using an administrator's account.
2013	Failed to read the proxy settings in the Web browser.	The Access Gateway Plugin did not read the proxy settings in the browser.	None
2014	The Access Gateway Plugin is not supported on this version of your operating system. For more information, contact your help desk or system administrator.	The user is attempting to install the Access Gateway Plugin on an unsupported version of the operating system.	None
2014	You need to stop <*applicationName*> application.	The Access Gateway is configured to prevent the client device from running the specified application.	Stop the application.
2015	This logon exceeds the maximum number of allowed users.	All of the licenses on the Access Gateway are in use.	Contact your help desk or system administrator.
2016	The Access Gateway is not available.	The connection to the Access Gateway cannot be established.	None
2017	Configured custom error message.	This error message is configured by your system administrator and can be no more than 100 characters. This error message appears when the endpoint analysis fails.	Contact your help desk or system administrator.

Codes	Message	Explanation	Action
2017	Your computer does not have the necessary security software to connect to the Access Gateway. Please contact your help desk or system administrator.	If the client security check fails and the system administrator does not use the customized error message, this default error message appears.	Contact your help desk or system administrator.
2018	The Access Gateway did not detect keyboard or mouse activity. The session has timed out.	The session timed out because activity from the client device is not detected for a specified amount of time.	Log off and then log on again.
2019	The connection to the Access Gateway cannot be established due to a failed endpoint analysis.	The Access Gateway is configured to deny access to this application.	Stop the application.
2020	The Web Interface is used for user connections. To logon, use Internet Explorer.	The Web Interface is supported on Internet Explorer only.	Use Internet Explorer to connect to the Web Interface.
3001	You are already logged on to the Access Gateway.	You are logged on to the Access Gateway using the Access Gateway Plugin.	None
3002	You are not logged on to the Access Gateway.	The Access Gateway session cookie cannot be found. Check to see if the user is logged on.	Log on using the Access Gateway Plugin.
3003	The Access Gateway Plugin supports Internet Explorer Version 4 and later.	This message indicates that the Access Gateway is not able to detect the presence of Internet Explorer on the client device. It could also mean that the client device has an older, unsupported version of Internet Explorer installed. If you are using Windows Vista, Internet Explorer 7 is the only supported version for this operating system.	Upgrade Internet Explorer and log on again.

Codes	Message	Explanation	Action
3004	The ActiveX Plugin failed to start. Contact your help desk or system administrator.	The ActiveX Plugin failed to start.	Contact your help desk or system administrator.
3005	The ActiveX Plugin failed to activate.	The ETA ActiveX Plugin failed to start.	Contact your help desk or system administrator.
3006	The Endpoint Analysis Plugin did not start. Contact your help desk or system administrator.	The ActiveX plugin failed to start.	Contact your help desk or system administrator.