Contents

1 Welcome...........................................................................................................5
   Documentation Conventions...........................................................................6

2 Getting Started with the Access Gateway Plug-in...........................................7
   How the Access Gateway Works......................................................................8
   Access Gateway Plug-in System Requirements.............................................8
   Creating Connections using the Access Gateway Plug-in .........................8
      Connecting Using a Web Address ............................................................9
   Downloading and Installing the Access Gateway Plug-in...........................9
   Connecting Using the Access Gateway Plug-in Dialog Box........................9
   Scanning Your Computer for Software......................................................10
   Logging On with a Client Certificate.........................................................10
      To import a client certificate to Firefox................................................11
   Ending Access Gateway Plug-in Sessions..................................................11
   To logoff from the Access Gateway............................................................11
   To exit the session.......................................................................................11
   Cleaning Up Your Computer when Your Session Ends..............................12
      Finding Information on the Summary Tab.............................................12
      Configuring the Cleanup Level..................................................................12
      Configuring the Cleanup Process.........................................................13
      Viewing the Cleanup Logs.....................................................................13
   Upgrading the Access Gateway Plug-in......................................................13

3 Changing Settings in the Access Gateway Plug-in........................................15
   Changing Settings in the Advanced Options Dialog Box............................16
      Setting the Access Gateway Web Address.............................................16
      Configuring Proxy Servers for the Access Gateway Plug-in....................16
      Logging on with a Secondary Password..............................................17
   Changing Settings from the Access Gateway Menu....................................17
      Opening the Access Interface..................................................................18
      Viewing and Changing Access Gateway Plug-in Information and Settings..18
Chapter 1

Welcome

Topics:

• Documentation Conventions

This chapter describes who should read the Citrix Access Gateway Plug-in for Windows User Guide.

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

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.
Documentation Conventions

Citrix product documentation uses the following typographic conventions.

<table>
<thead>
<tr>
<th>Presentation or Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User interface controls</strong></td>
<td>Names of buttons, boxes, options, or other controls in the user interface.</td>
</tr>
<tr>
<td><strong>Command names</strong></td>
<td>Names of commands, such as <code>ipconfig</code>.</td>
</tr>
<tr>
<td><strong>Variable names</strong></td>
<td>Variable placeholders for information you provide. For example, <code>filename</code> means you type the actual name of a file.</td>
</tr>
<tr>
<td><strong>Terms</strong></td>
<td>Terms newly introduced or otherwise emphasized.</td>
</tr>
<tr>
<td><strong>Code examples</strong></td>
<td>Text displayed in code or a text file.</td>
</tr>
<tr>
<td><strong>{braces}</strong></td>
<td>In a command, a series of items, one of which is required. For example, `{yes</td>
</tr>
<tr>
<td><strong>[brackets]</strong></td>
<td>In a command, optional items. For example, <code>[/ping]</code> means you can type <code>/ping</code> with the command. Do not type the brackets themselves.</td>
</tr>
<tr>
<td>**</td>
<td>(vertical bar)**</td>
</tr>
<tr>
<td><strong>... (ellipses)</strong></td>
<td>The previous item(s) in the command can be repeated. For example, <code>/route:devicename[,....]</code> means you can type additional <code>devicenames</code> separated by commas.</td>
</tr>
</tbody>
</table>
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 Plug-in. If you are trying to log on to your internal network, install the plug-in on your computer and then log on.

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

When the Access Gateway Plug-in 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 Plug-in to ensure that certain personal firewalls and antivirus applications are running on your computer.

Access Gateway Plug-in System Requirements

The Access Gateway Plug-in runs on the following operating systems:

- Windows XP (32-bit)
- Windows Vista (32-bit and 64-bit)
- Windows 7 (32-bit and 64-bit)

The following Web browsers are supported:

- Internet Explorer
- Firefox

Creating Connections using the Access Gateway Plug-in

To connect with and use the Access Gateway Plug-in, 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 plug-in 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 Plug-in, 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 plug-in, 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 Plug-in.

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

**Downloading and Installing the Access Gateway Plug-in**

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://ag.companyname.com`.

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 **Network Access** to install the plug-in.

When the download is complete, the plug-in 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.

**Connecting Using the Access Gateway Plug-in Dialog Box**

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

**Note:** To configure Access Gateway Plug-in settings, you must be logged on.

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 Plug-in 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 Plug-in, see **Changing Settings in the Advanced Options Dialog Box** on page 16.

---

### Scanning Your Computer for Software

Your system or network administrator might configure the Access Gateway to scan your computer for software, files, processes and other items. This is called **endpoint analysis**. When you log on, the Endpoint Analysis Plug-in installs automatically and scans your device to make sure the required software or processes are present. If it is not present, you might not be able to log on.

The Endpoint Analysis Plug-in can also scan your device after you log on to make sure that the required software continues to be present and the latest version required by your network. If the device is found to be out of compliance, your session might end.

When you log on, you can choose to scan your device or to skip the scan. You want to allow the scan to occur. If you skip the scan, you might not be able to log on to the Access Gateway and be unable to connect to resources in the internal network.

### Logging On with a Client Certificate

You might log on to the Access Gateway using a client certificate. When you log on to the Access Gateway, your details in the certificate are matched against information configured on the Access Gateway. If the details match, you can log on. If the details do not match, log on might be denied.

The Access Gateway can authenticate a client certificate that is stored in one of these locations:

- In the certificate store of the Windows operating system on your device. In this case, the client certificate is installed separately in the certificate store using the Microsoft Management Console.
- In a smart card or a hardware token. In this case, the certificate is embedded within the smart card and read from a smart card reader attached to the network.
- Common access cards that are used by the United States Department of Defense for identification and authentication.

To install the client certificate on your device, follow the instructions provided by your system administrator or help desk personnel.

If you have multiple client certificates installed on your device, the Access Gateway Plug-in prompts you to select the correct certificate to log on.

If you log on using Internet Explorer or the Access Gateway Plug-in dialog box, the client certificate is used from the Windows certificate store. If you log on using the Firefox Web browser, you need to import the certificate to Firefox.
To import a client certificate to Firefox

1. Open the Firefox Web browser.
2. On the menu, click Tools and then click Options.
3. Click Advanced.
4. In the Certificate Manager dialog box, click Your Certificates, and then click Import.
5. Navigate to the certificate stored on your computer and click Open.
   You might be asked for a password for the certificate. Contact your system administrator or help desk personnel for the password.
6. Click OK.

For more information about importing certificates to Firefox, see the Firefox Help.

Ending Access Gateway Plug-in Sessions

There are two ways you can end your session with the Access Gateway Plug-in:

- Logging off from the session
- Exiting the session

To logoff from the Access Gateway

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

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

- Click Log Off in the Access Interface.
- Right-click the Access Gateway icon in the notification area and click Logoff.

To exit the session

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

- 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 Plug-in
- 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 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 you choose.

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 Plug-in 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.

On the Summary tab, click View Log.

Upgrading the Access Gateway Plug-in

The Access Gateway Plug-in for Windows upgrades automatically when a new version of the software is available. When you log on to the Access Gateway, it detects the plug-in version installed on your device. If it does not match the version on the Access Gateway, the software is upgraded on your computer without any further action required. When the upgrade is complete, you can then log on to the Access Gateway and connect to network resources in the internal network.

If your system administrator configures the Access Gateway to scan your computer for software, files, processes and other items, the Endpoint Analysis Plug-in installs automatically and scans your computer for the required software. The Endpoint Analysis Plug-in also upgrades automatically when a new version becomes available.

If you can connect to more than one Access Gateway appliance, the software version that runs on each appliance might be different. For example, ag1 might have a newer version of the Access Gateway software than the ag2 appliance. If you originally connect to ag1, end the session and then connect to ag2, the Access Gateway Plug-in and Endpoint Analysis Plug-in downgrade automatically to the version on ag2.
Chapter 3

Changing Settings in the Access Gateway Plug-in

Topics:

• Changing Settings in the Advanced Options Dialog Box
• Changing Settings from the Access Gateway Menu
• Configuring Split Tunneling
• Uninstalling the Access Gateway Plug-in

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 Plug-in.

This chapter explains logging on using the Access Gateway Plug-in and configuring settings.
Changing Settings in the Advanced Options Dialog Box

In the Access Gateway Plug-in 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 Plug-in to log on using the Access Gateway dialog box instead of a Web browser. For more information, see Creating Connections using the Access Gateway Plug-in on page 8.

Setting the Access Gateway Web Address

When the Access Gateway Plug-in is configured, you use the preconfigured IP address of the Access Gateway to connect. You can also configure the plug-in to connect to a different appliance.

1. In the notification area, right-click the Access Gateway Plug-in icon and click Logon.
2. In the Citrix Access Gateway dialog box, right-click anywhere in the dialog box 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 Plug-in

A proxy server is a computer that sits between your 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.

1. In the notification area, right-click the Access Gateway icon and click Logon.
2. In the **Citrix Access Gateway** dialog box, right-click anywhere in the dialog box 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, 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 Plug-in to show the secondary password field.

1. In the notification area, right-click the Access Gateway icon and click **Open**.
2. Right-click anywhere in the dialog box and click **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 Plug-in message
- Open the online help
- Logoff and exit the Access Gateway Plug-in

Your administrator can configure the Access Gateway Plug-in so you do not have access to the Access Interface, the File Transfer utility, or configuration settings. If your
administrator configured the Access Gateway Plug-in 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.

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

### Viewing and Changing Access Gateway Plug-in 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.

**Note:** You must be logged on to open the 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.
1. In the notification area, right-click the Access Gateway icon and click **Configure Access Gateway**.

2. Click the **General** tab.

**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 Plug-in 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 Plug-in 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 Plug-in 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 Plug-in and you cannot change the settings. All network traffic is sent through the Access Gateway.
1. Right-click the Access Gateway Plug-in icon in the notification area and click Configure Access Gateway.

2. Click the Profile tab and then click Change Profile.

3. On the Connections tab, under Split tunneling, select the option you want and click OK.

Uninstalling the Access Gateway Plug-in

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

1. Click Start-Control Panel.

2. Click Add or Remove Programs.

Chapter 4

Working with the Access Interface

Topics:

• Logging on to the Access Interface
• Adding Bookmarks on the Home Tab

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.

Figure 4-1. 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 are logged on and a list of your published applications appears.

If you log on using clientless access or with the Access Gateway Plug-in and your administrator configured published applications on the Access Gateway, the Access Interface home page appears with your published applications in the left pane, as shown in the following illustration:

**Figure 4-2. Access Interface with published applications in the left pane**
Adding Bookmarks on the Home Tab

Your system administrator can add bookmarks to the Access Interface. These appear as links under Enterprise 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.

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.

Removing a Bookmark

You can remove bookmarks that are listed under Personal Web Sites but not those under Enterprise Web Sites.

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

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.

In the Access Interface, click the File Transfer tab.
Opening the File Transfer tab using the Access Gateway icon

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

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.
- **New Folder.** 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, type the address of the file share. You can also enter your user name, password, and domain name if required. If you have access to the file share after logging on to the Access Gateway, you might not need to enter your user name and password or the domain name.

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. If your user credentials are required, click **Enter Credentials** and complete Steps 4 through 7. Otherwise, click **Log On**.

4. In **User name**, type your user name.

5. In **Password**, type your password.

6. In **Domain**, type a valid domain name.

7. Click **Log On**.

If the remote server is not assigned a specific domain, leave the **Domain** 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.
Chapter 5

Troubleshooting the Access Gateway Plug-in

Topics:

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

The Access Gateway Plug-in 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.
Opening the Connection Log

The connection log for the Access Gateway Plug-in 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.

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 Plug-in

You can configure the Access Gateway Plug-in to log all errors to a text file. The Access Gateway Plug-in 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.

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

In Windows Vista and Windows 7, the log files are located in the directory %systemdrive%\ProgramData\Citrix\AGEE and at %systemdrive%\Users\%username%\AppData\Local\Citrix\AGEE. You can use these log files to troubleshoot the Access Gateway Plug-in.

You can set the level of logging for the Access Gateway Plug-in. The logging levels are:

- Do not record debugging messages
- Record event messages
- Record Access Gateway Plug-in statistics
- Record all errors, event messages, and statistics

1. Right-click the Access Gateway Plug-in 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 Plug-in might encounter. This information is helpful when you encounter a problem and are working with your technical support staff.

1. Right-click the Access Gateway Plug-in icon in the notification area and click Configure Access Gateway.
2. Click the **Trace** tab.
3. Under **Client trace log**, click **View Log File**.

### 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.

1. In the notification area, right-click the Access Gateway icon and click **Configure Access Gateway**.
2. Click the **Compression** tab.
Chapter 6

Access Gateway Session Error Codes

Topics:

• Access Gateway Session Error Codes

During your Access Gateway session, information is logged regarding the session. These are error codes you can provide to your help desk personnel or system administrator if you are experiencing difficulties with your session or connection.
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.

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0001-1000</td>
<td>Normal operation</td>
</tr>
<tr>
<td>1001-2000</td>
<td>Internal error</td>
</tr>
<tr>
<td>2001-3000</td>
<td>Access Gateway Plug-in errors</td>
</tr>
<tr>
<td>3001-4000</td>
<td>Browser errors</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Codes</th>
<th>Message</th>
<th>Explanation</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>0001</td>
<td>Loading...</td>
<td>This message indicates that Access Gateway Plug-in is loading the configuration and the interception software before the Access Gateway session is established.</td>
<td>None</td>
</tr>
<tr>
<td>0002</td>
<td>Connection established. To end this session, right-click the Access Gateway icon and click Logoff</td>
<td>This message appears when the Access Gateway Plug-in successfully connects.</td>
<td>None</td>
</tr>
<tr>
<td>0003</td>
<td>Exiting...</td>
<td>This appears when the user clicks Logoff from the Access Gateway menu.</td>
<td>None</td>
</tr>
<tr>
<td>0004</td>
<td>Your session timed-out, you are not connected.</td>
<td>This error message appears when the client session times out.</td>
<td>None</td>
</tr>
<tr>
<td>0004</td>
<td>You are not logged on.</td>
<td>This error message appears when the Access Gateway Plug-in is not connected.</td>
<td>None</td>
</tr>
<tr>
<td>Codes</td>
<td>Message</td>
<td>Explanation</td>
<td>Action</td>
</tr>
<tr>
<td>-------</td>
<td>-------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>0005</td>
<td>Your session is going to time-out in <code>&lt;number&gt;</code> of seconds.</td>
<td>This error message appears when a session is configured for a forced time-out.</td>
<td>None</td>
</tr>
<tr>
<td>0006</td>
<td>Downgrading the Access Gateway Plug-in from <code>&lt;versionNumber&gt;</code> to <code>&lt;versionNumber&gt;</code>.</td>
<td>The Access Gateway is installing an earlier version of the software.</td>
<td>None</td>
</tr>
<tr>
<td>0006</td>
<td>Upgrading the Access Gateway Plug-in from <code>&lt;versionNumber&gt;</code> to <code>&lt;versionNumber&gt;</code>.</td>
<td>The Access Gateway Plug-in is upgrading to a new version of the software.</td>
<td>None</td>
</tr>
<tr>
<td>1001</td>
<td>There is an internal error. For more information, please contact your help desk or system administrator.</td>
<td>This message indicates that Access Gateway Plug-in failed to open the interception file.</td>
<td>Restart the client device and logon using a Windows account that has administrative privileges.</td>
</tr>
<tr>
<td>1002</td>
<td>There is an internal error. For more information, contact your help desk or system administrator.</td>
<td>This message indicates that the version of the Access Gateway Plug-in and the version of the interception software do not match.</td>
<td>Reinstall the Access Gateway Plug-in.</td>
</tr>
<tr>
<td>1003</td>
<td>Failed to allocate memory.</td>
<td>The Access Gateway Plug-in ran out of memory.</td>
<td>When this error appears, users should logoff, restart the Access Gateway Plug-in, and logon again. Report this error to your help desk or system administrator.</td>
</tr>
<tr>
<td>1004</td>
<td>There is an internal error. For more information, please contact your administrator.</td>
<td>The Access Gateway Plug-in cannot call the Windows API successfully.</td>
<td>None</td>
</tr>
<tr>
<td>Codes</td>
<td>Message</td>
<td>Explanation</td>
<td>Action</td>
</tr>
<tr>
<td>-------</td>
<td>---------</td>
<td>-------------</td>
<td>--------</td>
</tr>
<tr>
<td>1005</td>
<td>There is an internal error. For more information, please contact your administrator.</td>
<td>The Access Gateway Plug-in failed to create the temporary interception file.</td>
<td>Users need to log on using an administrator's account.</td>
</tr>
<tr>
<td>1006</td>
<td>There is an internal error. For more information, please contact your administrator.</td>
<td>The client security check failed when scanning the Windows process list.</td>
<td>Users need to log on using an administrator's account.</td>
</tr>
<tr>
<td>1007</td>
<td>There is an internal error. For more information, please contact your administrator.</td>
<td>The client security check failed when opening a Windows system service.</td>
<td>Users need to log on using an administrator's account.</td>
</tr>
<tr>
<td>1008</td>
<td>There is an internal error. For more information, please contact your administrator.</td>
<td>The Access Gateway Plug-in failed.</td>
<td>Restart the Access Gateway Plug-in and send the debug trace file to your help desk or system administrator.</td>
</tr>
<tr>
<td>1010</td>
<td>Your logon failed.</td>
<td>The user could not log on.</td>
<td>None</td>
</tr>
<tr>
<td>1011</td>
<td>The Access Gateway Plug-in failed to download the correct configuration.</td>
<td>The Access Gateway Plug-in cannot download the Access Gateway configuration successfully.</td>
<td>Check the network status and then contact your system administrator.</td>
</tr>
<tr>
<td>1012</td>
<td>The Access Gateway Plug-in could not start. For more information, see the connection log.</td>
<td>The Access Gateway Plug-in failed to establish a connection. For more information, check the connection log and make any necessary changes.</td>
<td>Locate the error in the connection log and then report to your help desk or system administrator.</td>
</tr>
<tr>
<td>1013</td>
<td>Failed to parse configuration. Check the connection log for more information.</td>
<td>There is a configuration error on the Access Gateway.</td>
<td>Contact your help desk or system administrator.</td>
</tr>
<tr>
<td>1014</td>
<td>The client device could not resolve the Access</td>
<td>The Access Gateway Plug-in failed to resolve the domain name.</td>
<td>Modify the HOSTS file or ask your system administrator.</td>
</tr>
<tr>
<td>Codes</td>
<td>Message</td>
<td>Explanation</td>
<td>Action</td>
</tr>
<tr>
<td>-------</td>
<td>---------</td>
<td>-------------</td>
<td>--------</td>
</tr>
<tr>
<td>Gateway Web address.</td>
<td>The secure connection cannot be established.</td>
<td>The Access Gateway Plug-in could not establish a secure connection.</td>
<td>administrator to change or fix the configuration.</td>
</tr>
<tr>
<td>1015</td>
<td>Failed to downgrade the Access Gateway Plug-in from <code>&lt;versionNumber&gt;</code> to <code>&lt;versionNumber&gt;</code>.</td>
<td>The installation of an earlier version of the Access Gateway Plug-in failed.</td>
<td>Contact your help desk or system administrator.</td>
</tr>
<tr>
<td>1016</td>
<td>Failed to upgrade the Access Gateway Plug-in from <code>&lt;versionNumber&gt;</code> to <code>&lt;versionNumber&gt;</code>.</td>
<td>The Access Gateway Plug-in failed to upgrade to the latest version.</td>
<td>Contact your help desk or system administrator.</td>
</tr>
<tr>
<td>2001</td>
<td>Your Access Gateway session timed-out and you are not connected.</td>
<td>This message indicates that your Access Gateway session timed out.</td>
<td>Log off of from the Access Gateway Plug-in and then log on again.</td>
</tr>
<tr>
<td>2003</td>
<td>There is a configuration issue on the Access Gateway.</td>
<td>This message indicates that the configuration on the Access Gateway is not correct.</td>
<td>Contact your system administrator to configure the Access Gateway correctly.</td>
</tr>
<tr>
<td>2004</td>
<td>You need to install endpoint security software.</td>
<td>This message indicates that at least one of the required endpoint security applications is not installed.</td>
<td>Contact your system administrator to install the required security software.</td>
</tr>
<tr>
<td>2005</td>
<td>You need to upgrade the endpoint security software.</td>
<td>This message indicates that the endpoint security software is not the correct version.</td>
<td>Contact your system administrator to upgrade the security software.</td>
</tr>
<tr>
<td>Codes</td>
<td>Message</td>
<td>Explanation</td>
<td>Action</td>
</tr>
<tr>
<td>-------</td>
<td>---------</td>
<td>-------------</td>
<td>--------</td>
</tr>
<tr>
<td>2006</td>
<td>The required security software is not activated.</td>
<td>This message indicates that the endpoint security software is not activated.</td>
<td>Start the security software.</td>
</tr>
<tr>
<td>2007</td>
<td>This version of the Access Gateway Plug-in is updated. Please logon again.</td>
<td>This message indicates that the interception code does not match the version of the Access Gateway Plug-in.</td>
<td>Log off and log on again.</td>
</tr>
<tr>
<td>2008</td>
<td>This version of the Access Gateway Plug-in is updated. Please logon again.</td>
<td>The Access Gateway Plug-in upgrade is successful, but did not activate automatically.</td>
<td>Log off and log on again.</td>
</tr>
<tr>
<td>2009</td>
<td>The proxy server requires unsupported authentication.</td>
<td>There is a local forward proxy setting that requires authentication. Not all proxy-supported authentication types are supported by the Access Gateway Plug-in.</td>
<td>None</td>
</tr>
<tr>
<td>2010</td>
<td>Proxy server authentication failed, please logon again.</td>
<td>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.</td>
<td>None</td>
</tr>
<tr>
<td>2011</td>
<td>The Access Gateway failed to validate the secure certificate.</td>
<td>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 Plug-in cannot detect the required certificate.</td>
<td>Contact your help desk or system administrator to provide the correct client certificate.</td>
</tr>
<tr>
<td>Codes</td>
<td>Message</td>
<td>Explanation</td>
<td>Action</td>
</tr>
<tr>
<td>-------</td>
<td>---------</td>
<td>-------------</td>
<td>--------</td>
</tr>
<tr>
<td>2012</td>
<td>The Access Gateway Plug-in failed to start the interception driver.</td>
<td>The Access Gateway Plug-in did not start the interception driver. To do so requires the user to be logged on as an administrator.</td>
<td>Log on with the Access Gateway Plug-in using an administrator’s account.</td>
</tr>
<tr>
<td>2013</td>
<td>Failed to read the proxy settings in the Web browser.</td>
<td>The Access Gateway Plug-in did not read the proxy settings in the browser.</td>
<td>None</td>
</tr>
<tr>
<td>2014</td>
<td>The Access Gateway Plug-in is not supported on this version of your operating system. For more information, contact your help desk or system administrator.</td>
<td>The user is attempting to install the Access Gateway Plug-in on an unsupported version of the operating system.</td>
<td>None</td>
</tr>
<tr>
<td>2014</td>
<td>You need to stop <code>&lt;applicationName&gt;</code> application.</td>
<td>The Access Gateway is configured to prevent the client device from running the specified application.</td>
<td>Stop the application.</td>
</tr>
<tr>
<td>2015</td>
<td>This logon exceeds the maximum number of allowed users.</td>
<td>All of the licenses on the Access Gateway are in use.</td>
<td>Contact your help desk or system administrator.</td>
</tr>
<tr>
<td>2016</td>
<td>The Access Gateway is not available.</td>
<td>The connection to the Access Gateway cannot be established.</td>
<td>None</td>
</tr>
<tr>
<td>2017</td>
<td>Configured custom error message.</td>
<td>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.</td>
<td>Contact your help desk or system administrator.</td>
</tr>
<tr>
<td>2017</td>
<td>Your computer does not have the necessary security software to connect to the</td>
<td>If the client security check fails and the system administrator does not use the customized error</td>
<td>Contact your help desk or system administrator.</td>
</tr>
<tr>
<td>Codes</td>
<td>Message</td>
<td>Explanation</td>
<td>Action</td>
</tr>
<tr>
<td>-------</td>
<td>---------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Access Gateway. Please contact your help desk or system administrator.</td>
<td>message, this default error message appears.</td>
<td></td>
</tr>
<tr>
<td>2018</td>
<td>The Access Gateway did not detect keyboard or mouse activity. The session has timed out.</td>
<td>The session timed out because activity from the client device is not detected for a specified amount of time.</td>
<td>Log off and then log on again.</td>
</tr>
<tr>
<td>2019</td>
<td>The connection to the Access Gateway cannot be established due to a failed endpoint analysis.</td>
<td>The Access Gateway is configured to deny access to this application.</td>
<td>Stop the application.</td>
</tr>
<tr>
<td>2020</td>
<td>The Web Interface is used for user connections. To logon, use Internet Explorer.</td>
<td>The Web Interface is supported on Internet Explorer only.</td>
<td>Use Internet Explorer to connect to the Web Interface.</td>
</tr>
<tr>
<td>3001</td>
<td>You are already logged on to the Access Gateway.</td>
<td>You are logged on to the Access Gateway using the Access Gateway Plug-in.</td>
<td>None</td>
</tr>
<tr>
<td>3002</td>
<td>You are not logged on to the Access Gateway.</td>
<td>The Access Gateway session cookie cannot be found. Check to see if the user is logged on.</td>
<td>Log on using the Access Gateway Plug-in.</td>
</tr>
<tr>
<td>3003</td>
<td>The Access Gateway Plug-in supports Internet Explorer Version 4 and later.</td>
<td>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.</td>
<td>Upgrade Internet Explorer and log on again.</td>
</tr>
<tr>
<td>Codes</td>
<td>Message</td>
<td>Explanation</td>
<td>Action</td>
</tr>
<tr>
<td>-------</td>
<td>---------</td>
<td>-------------</td>
<td>--------</td>
</tr>
<tr>
<td>3006</td>
<td>The Endpoint Analysis Plug-in did not start. Contact your help desk or system administrator.</td>
<td>The plug-in failed to start.</td>
<td>Contact your help desk or system administrator.</td>
</tr>
</tbody>
</table>