



Installation File Parameters

This chapter describes the installation file parameters. The following topics are covered in this section:

- [Installation File Options](#)
- [Profile Parameters](#)
- [Installation File Examples](#)

Installation File Options

The installation file is organized into several sections used to define the installation options. Each section is identified by a heading enclosed in brackets []. Under each heading, you must add a parameter line to specify the desired options.

**Note**

The section headings can be placed in any order; for example: [Firmware Upgrade] can be listed before [Log file].

**Note**

The *yes* or *no* parameter options can also be specified using Yes or No, YES or NO, y or n, Y or N, or 1 or 0.

**Note**

A profile configured for LEAP is not supported by the auto profile switching feature until you manually configure the LEAP parameters using the ACU.

**Note**

The number of profiles supported by the ACU is limited to 16. The auto installer discards new or existing profiles to limit the number of profiles to 16.

The supported section headings are shown in [Table 2-1](#):

Table 2-1 Installation File Headings



Section Heading	Description
[Logfile]	This section specifies the name and location of the installation log file. Parameter line: File Name = drive:\directory\filename.log
[Install Apps]	This section specifies whether the ACU is installed by the auto installer. The ACU is used to configure the client adapter and security options.  Note For proper ACU functionality, your client adapter driver must be version 8.0x or later. For driver installation instructions, refer to the <i>Cisco Aironet Wireless LAN Adapters Installation and Configuration Guide</i> .  Note ACU version 5.0x is installed by the auto installer. Parameter line: ACU = yes or no

Table 2-1 Installation File Headings (continued)


Section Heading	Description
[Administrative Overrides]	<p>Specifies whether the ACU can be used to change the WEP keys and specifies administrative profile options. When a feature is not allowed, the ACU grays-out the option on the screen.</p> <p> Note These parameters apply to all profiles and override corresponding parameters that can be specified in an individual profile.</p>
Parameter Line	Description
Allow Edit Profile	<p>Specifies whether the profiles can be edited.</p> <p>Range: yes or no</p>
Allow Export Profile	<p>Specifies whether the profiles can be exported to a file.</p> <p>Range: yes or no</p>
Allow Import Profile	<p>Specifies whether new profiles can be imported from a file</p> <p>Range: yes or no.</p>
Allow Edit WEP	<p>Specifies whether the WEP keys can be changed</p> <p>Range: yes or no.</p>
Existing Profiles	<p>Specifies three options for handling existing profiles:</p> <p>Delete—causes all existing profiles to be deleted before the profiles in the installation file are added.</p> <p>Preserve—causes all existing profiles to be saved before the profiles in the installation file are added. Profiles in the installation file with the same name as existing profiles are not used. The existing default profile is used.</p> <p>Overwrite—causes all existing profiles to be saved before the profiles in the installation file are added. Existing profiles with the same name as those contained in the installation file are overwritten. The default profile specified in the installation file is used.</p> <p>Range: Preserve, Delete, or Overwrite</p>

Table 2-1 Installation File Headings (continued)

Section Heading	Description														
[App Parameters]	This section specifies global ACU settings that are applied to all profiles.														
	<table border="1"> <thead> <tr> <th>Parameter Line</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Folder Name</td> <td>Specifies the Window program folder name for the ACU. Default: Cisco Systems, Inc.</td> </tr> <tr> <td>Program Location</td> <td>Specifies the path for the ACU files on your hard disk. Default: C:\Program Files\Cisco Aironet</td> </tr> <tr> <td>Enable LEAP</td> <td>Enable or disable the LEAP security option. Range: yes or no Default: no</td> </tr> <tr> <td>Allow LEAP Data Save</td> <td>Specifies whether the ACU allows the storage and reuse of the LEAP username and password. When set to <i>no</i>, the ACU option to use the saved LEAP username and password is not visible on the ACU screen. See profile note above. Range: yes or no Default: no</td> </tr> <tr> <td>Create ACU icon on desktop</td> <td>Specifies whether the ACU icon is placed on the PC desktop. Range: yes or no Default: no</td> </tr> <tr> <td>Allow non-admin to modify profiles</td> <td>Specifies whether a user without administrator privileges can change the profiles. This option is supported only on the Windows NT, the Windows 2000, or the Windows XP operating systems. Range: yes or no Default: yes</td> </tr> </tbody> </table>	Parameter Line	Description	Folder Name	Specifies the Window program folder name for the ACU. Default: Cisco Systems, Inc.	Program Location	Specifies the path for the ACU files on your hard disk. Default: C:\Program Files\Cisco Aironet	Enable LEAP	Enable or disable the LEAP security option. Range: yes or no Default: no	Allow LEAP Data Save	Specifies whether the ACU allows the storage and reuse of the LEAP username and password. When set to <i>no</i> , the ACU option to use the saved LEAP username and password is not visible on the ACU screen. See profile note above. Range: yes or no Default: no	Create ACU icon on desktop	Specifies whether the ACU icon is placed on the PC desktop. Range: yes or no Default: no	Allow non-admin to modify profiles	Specifies whether a user without administrator privileges can change the profiles. This option is supported only on the Windows NT, the Windows 2000, or the Windows XP operating systems. Range: yes or no Default: yes
Parameter Line	Description														
Folder Name	Specifies the Window program folder name for the ACU. Default: Cisco Systems, Inc.														
Program Location	Specifies the path for the ACU files on your hard disk. Default: C:\Program Files\Cisco Aironet														
Enable LEAP	Enable or disable the LEAP security option. Range: yes or no Default: no														
Allow LEAP Data Save	Specifies whether the ACU allows the storage and reuse of the LEAP username and password. When set to <i>no</i> , the ACU option to use the saved LEAP username and password is not visible on the ACU screen. See profile note above. Range: yes or no Default: no														
Create ACU icon on desktop	Specifies whether the ACU icon is placed on the PC desktop. Range: yes or no Default: no														
Allow non-admin to modify profiles	Specifies whether a user without administrator privileges can change the profiles. This option is supported only on the Windows NT, the Windows 2000, or the Windows XP operating systems. Range: yes or no Default: yes														

Table 2-1 Installation File Headings (continued)






Section Heading	Description																										
[Device Resident Wep Keys]	Specifies up to four WEP keys, the key size, the transmit key, the home WEP key, and whether to save the WEP key information in the client adapter Flash memory.																										
	<table border="1"> <thead> <tr> <th>Parameter Line</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Save Keys to Flash</td> <td>Specifies whether the WEP key information is saved in the client adapter Flash memory. Range: yes or no Default: no</td> </tr> <tr> <td>WepKey1</td> <td>Specifies the WEP 1 key. A 40-bit WEP key can contain 5 ASCII characters or 10 hexadecimal characters. A 128-bit WEP key can contain 13 ASCII characters or 26 hexadecimal characters. See Note below. Range: ASCII entry—5 or 13 ASCII characters Hex entry—10 or 26 characters using 0 to 9, a to f, or A to F.</td> </tr> <tr> <td>WepKey1size</td> <td>Specifies the size of the WEP 1 key. The size must be specified as either 40 bits or 128 bits. Range: 40 or 128</td> </tr> <tr> <td>WepKey1IsTransmit</td> <td>Specifies the WEP 1 key is used to transmit data. Only one WEP key can be specified as the transmit key. Range: yes or no</td> </tr> <tr> <td>WepKey2</td> <td rowspan="3">Specifies the WEP 2 key values. See WEP 1 key descriptions.</td> </tr> <tr> <td>WepKey2size</td> </tr> <tr> <td>WepKey2IsTransmit</td> </tr> <tr> <td>WepKey3</td> <td rowspan="3">Specifies the WEP 3 key values. See WEP 1 key descriptions.</td> </tr> <tr> <td>WepKey3size</td> </tr> <tr> <td>WepKey3IsTransmit</td> </tr> <tr> <td>WepKey4</td> <td rowspan="3">Specifies the WEP 4 key values. See WEP 1 key descriptions.</td> </tr> <tr> <td>WepKey4size</td> </tr> <tr> <td>WepKey4IsTransmit</td> </tr> <tr> <td>WepKey5</td> <td>Specifies the home network WEP key.</td> </tr> <tr> <td> Note</td> <td>The auto installer does not pad the keys with 0s; for example: an ASCII key of 123 must be entered as 1 2 3 0 0 for 40-bit WEP or 1 2 3 0 0 0 0 0 0 0 0 0 0 0 0 for 128-bit WEP (spaces added for clarity).</td> </tr> </tbody> </table>	Parameter Line	Description	Save Keys to Flash	Specifies whether the WEP key information is saved in the client adapter Flash memory. Range: yes or no Default: no	WepKey1	Specifies the WEP 1 key. A 40-bit WEP key can contain 5 ASCII characters or 10 hexadecimal characters. A 128-bit WEP key can contain 13 ASCII characters or 26 hexadecimal characters. See Note below. Range: ASCII entry—5 or 13 ASCII characters Hex entry—10 or 26 characters using 0 to 9, a to f, or A to F.	WepKey1size	Specifies the size of the WEP 1 key. The size must be specified as either 40 bits or 128 bits. Range: 40 or 128	WepKey1IsTransmit	Specifies the WEP 1 key is used to transmit data. Only one WEP key can be specified as the transmit key. Range: yes or no	WepKey2	Specifies the WEP 2 key values. See WEP 1 key descriptions.	WepKey2size	WepKey2IsTransmit	WepKey3	Specifies the WEP 3 key values. See WEP 1 key descriptions.	WepKey3size	WepKey3IsTransmit	WepKey4	Specifies the WEP 4 key values. See WEP 1 key descriptions.	WepKey4size	WepKey4IsTransmit	WepKey5	Specifies the home network WEP key.	 Note	The auto installer does not pad the keys with 0s; for example: an ASCII key of 123 must be entered as 1 2 3 0 0 for 40-bit WEP or 1 2 3 0 0 0 0 0 0 0 0 0 0 0 0 for 128-bit WEP (spaces added for clarity).
Parameter Line	Description																										
Save Keys to Flash	Specifies whether the WEP key information is saved in the client adapter Flash memory. Range: yes or no Default: no																										
WepKey1	Specifies the WEP 1 key. A 40-bit WEP key can contain 5 ASCII characters or 10 hexadecimal characters. A 128-bit WEP key can contain 13 ASCII characters or 26 hexadecimal characters. See Note below. Range: ASCII entry—5 or 13 ASCII characters Hex entry—10 or 26 characters using 0 to 9, a to f, or A to F.																										
WepKey1size	Specifies the size of the WEP 1 key. The size must be specified as either 40 bits or 128 bits. Range: 40 or 128																										
WepKey1IsTransmit	Specifies the WEP 1 key is used to transmit data. Only one WEP key can be specified as the transmit key. Range: yes or no																										
WepKey2	Specifies the WEP 2 key values. See WEP 1 key descriptions.																										
WepKey2size																											
WepKey2IsTransmit																											
WepKey3	Specifies the WEP 3 key values. See WEP 1 key descriptions.																										
WepKey3size																											
WepKey3IsTransmit																											
WepKey4	Specifies the WEP 4 key values. See WEP 1 key descriptions.																										
WepKey4size																											
WepKey4IsTransmit																											
WepKey5	Specifies the home network WEP key.																										
 Note	The auto installer does not pad the keys with 0s; for example: an ASCII key of 123 must be entered as 1 2 3 0 0 for 40-bit WEP or 1 2 3 0 0 0 0 0 0 0 0 0 0 0 0 for 128-bit WEP (spaces added for clarity).																										

Table 2-1 Installation File Headings (continued)

Section Heading	Description								
[Firmware Upgrade]	<p>Specifies client adapter radio firmware upgrade parameters.</p> <p> Note The firmware file must be an image file as denoted by the <i>img</i> in the filename extension.</p> <table border="1"> <thead> <tr> <th>Parameter Line</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Upgrade</td> <td> <p>Specifies whether the firmware is upgraded.</p> <p>Range: yes, no, or newer</p> </td> </tr> <tr> <td>Display Flash Progress</td> <td> <p>Specifies whether the progress of the firmware upgrade is displayed.</p> <p>Range: yes or no</p> </td> </tr> <tr> <td>Firmware Path</td> <td> <p>Specifies the location of the firmware file.</p> <p>Range: Drive:\Directory\filename.img</p> </td> </tr> </tbody> </table>	Parameter Line	Description	Upgrade	<p>Specifies whether the firmware is upgraded.</p> <p>Range: yes, no, or newer</p>	Display Flash Progress	<p>Specifies whether the progress of the firmware upgrade is displayed.</p> <p>Range: yes or no</p>	Firmware Path	<p>Specifies the location of the firmware file.</p> <p>Range: Drive:\Directory\filename.img</p>
Parameter Line	Description								
Upgrade	<p>Specifies whether the firmware is upgraded.</p> <p>Range: yes, no, or newer</p>								
Display Flash Progress	<p>Specifies whether the progress of the firmware upgrade is displayed.</p> <p>Range: yes or no</p>								
Firmware Path	<p>Specifies the location of the firmware file.</p> <p>Range: Drive:\Directory\filename.img</p>								
[Profile Names]	<p>Specifies the names of individual parameter profiles to be configured into the client PC. You can configure up to 16 individual profile names, such as Work, Home, Factory, Building A, or Airport.</p> <p>Parameter line: (Up to 16 names can be listed, each on an individual line) (See the “Profile Parameters” section on page 2-7 for additional information.)</p> <p> Note To prevent overwriting older ACU profiles, you should avoid using a profile name of <i>Enterprise</i> or <i>Home</i>.</p>								


Profile Parameters

The ACU enables you to specify up to 16 individual configuration profiles. In these profiles you can specify the desired parameter values used to configure the client adapter and network security for operation in a specific area, such as the home, office, or airport. The auto loader supports only the ACU parameters defined in [Table 2-2](#).


Note

To use the parameters in [Table 2-2](#), you must add a parameter line under the profile name headings to specify the desired values of the profile parameter options; for example: IsDefault = yes. See the “[Installation File Examples](#)” section on [page 2-14](#) for sample installation files.

Table 2-2 Profile Parameters

Parameter	Description
Client Name	<p>Specifies the client’s logon name.</p> <p>Parameter line: Client Name = (Up to 16 alphanumeric characters)</p>  <p>Note Each user on the network should have a unique client name.</p>
Use Logon Name	<p>Specifies whether the Window’s logon name is used as the client’s logon name.</p> <p>Parameter line: Use Logon Name = yes or no</p>
Use Computer Name	<p>Specifies whether your computer’s name is used as the client’s logon name.</p> <p>Parameter line: Use Computer Name = yes or no</p>
SSID1	<p>Service set identifier (SSID) identifies the specific wireless network that you want to access. See the notes below.</p> <p>Parameter line: SSID1 = Up to 32 ASCII characters (case sensitive)</p>
SSID2	<p>Identifies an optional SSID for a second wireless network that enables you to roam to the network without having to reconfigure your client adapter. See the notes below.</p> <p>Parameter line: SSID2 = Up to 32 ASCII characters (case sensitive)</p>
SSID3	<p>Identifies an optional SSID for a third wireless network that enables you to roam to the network without having to reconfigure your client adapter. See the notes below.</p> <p>Parameter line: SSID3 = Up to 32 ASCII characters (case sensitive)</p>


Note

If you do not specify an SSID parameter, your client adapter can associate to any access point on the network that is configured to allow broadcast SSIDs (see the AP Radio Hardware page in the *Cisco Aironet Access Point Software Configuration Guide*). If the access points with which you wish to communicate are not configured to allow broadcast SSIDs, the value of this parameter must match the SSID of the access points. Otherwise, you cannot access the wireless network.


Note

If you include an SSID parameter line but do not specify a parameter value, the existing SSID value is cleared.

Table 2-2 Profile Parameters (continued)

Parameter	Description								
Power Save Mode	<p>Sets your client adapter to its optimum power consumption setting.</p> <p>Parameter line: Power Save Mode = cam, max psp, or fast psp</p> <p>Default: CAM</p>								
	<table border="1"> <thead> <tr> <th>Power Save Mode</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>CAM (Constantly Awake Mode)</td> <td> <p>Keeps the client adapter powered up continuously so there is little lag in message response time.</p> <p>Consumes the most power but offers the highest throughput. Is recommended for desktop computers and devices that use AC power.</p> </td> </tr> <tr> <td>Max PSP (Max Power Savings)</td> <td> <p>Causes the access point to buffer incoming messages for the client adapter, which wakes up periodically and polls the access point to see if any buffered messages are waiting for it. The adapter can request each message and then go back to sleep.</p> <p>Conserves the most power but offers the lowest throughput. Is recommended for devices for which power consumption is the ultimate concern (such as small battery-powered devices).</p> </td> </tr> <tr> <td>Fast PSP (Power Save Mode)</td> <td> <p>Switches between a PSP mode and CAM, depending on network traffic. This mode switches to CAM when retrieving a large number of packets and switches back to PSP after the packets have been retrieved.</p> <p>Is recommended when power consumption is a concern but you need greater throughput than that allowed by Max PSP</p> </td> </tr> </tbody> </table>	Power Save Mode	Description	CAM (Constantly Awake Mode)	<p>Keeps the client adapter powered up continuously so there is little lag in message response time.</p> <p>Consumes the most power but offers the highest throughput. Is recommended for desktop computers and devices that use AC power.</p>	Max PSP (Max Power Savings)	<p>Causes the access point to buffer incoming messages for the client adapter, which wakes up periodically and polls the access point to see if any buffered messages are waiting for it. The adapter can request each message and then go back to sleep.</p> <p>Conserves the most power but offers the lowest throughput. Is recommended for devices for which power consumption is the ultimate concern (such as small battery-powered devices).</p>	Fast PSP (Power Save Mode)	<p>Switches between a PSP mode and CAM, depending on network traffic. This mode switches to CAM when retrieving a large number of packets and switches back to PSP after the packets have been retrieved.</p> <p>Is recommended when power consumption is a concern but you need greater throughput than that allowed by Max PSP</p>
Power Save Mode	Description								
CAM (Constantly Awake Mode)	<p>Keeps the client adapter powered up continuously so there is little lag in message response time.</p> <p>Consumes the most power but offers the highest throughput. Is recommended for desktop computers and devices that use AC power.</p>								
Max PSP (Max Power Savings)	<p>Causes the access point to buffer incoming messages for the client adapter, which wakes up periodically and polls the access point to see if any buffered messages are waiting for it. The adapter can request each message and then go back to sleep.</p> <p>Conserves the most power but offers the lowest throughput. Is recommended for devices for which power consumption is the ultimate concern (such as small battery-powered devices).</p>								
Fast PSP (Power Save Mode)	<p>Switches between a PSP mode and CAM, depending on network traffic. This mode switches to CAM when retrieving a large number of packets and switches back to PSP after the packets have been retrieved.</p> <p>Is recommended when power consumption is a concern but you need greater throughput than that allowed by Max PSP</p>								
Network Type	<p>Specifies the type of network in which your client adapter is installed.</p> <p>Parameter line: Network Type = Ad Hoc or Infrastructure</p> <p>Default: Infrastructure</p>								
	<table border="1"> <thead> <tr> <th>Network Type</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Ad Hoc</td> <td>Often referred to as <i>peer to peer</i> and used to set up a small network between two or more wireless devices.</td> </tr> <tr> <td>Infrastructure</td> <td>Used to set up a connection to a wired Ethernet network (through an access point).</td> </tr> </tbody> </table>	Network Type	Description	Ad Hoc	Often referred to as <i>peer to peer</i> and used to set up a small network between two or more wireless devices.	Infrastructure	Used to set up a connection to a wired Ethernet network (through an access point).		
Network Type	Description								
Ad Hoc	Often referred to as <i>peer to peer</i> and used to set up a small network between two or more wireless devices.								
Infrastructure	Used to set up a connection to a wired Ethernet network (through an access point).								

Table 2-2 Profile Parameters (continued)


Parameter	Description												
Data Rate	<p>Specifies the rate at which you want your client adapter to transmit or receive packets to or from access points (in infrastructure mode) or other client devices (in ad hoc mode).</p> <p>Parameter line: Data Rate = Auto, 1, 2, 5.5, or 11</p> <p>Default: Auto</p> <table border="1"> <thead> <tr> <th>Data Rate (Mbps)</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Auto</td> <td>Uses the 11-Mbps data rate when possible but drops to lower rates when necessary.</td> </tr> <tr> <td>1</td> <td>Offers the greatest range but the lowest throughput.</td> </tr> <tr> <td>2</td> <td>Offers less range but greater throughput than the 1-Mbps option.</td> </tr> <tr> <td>5.5</td> <td>Offers less range but greater throughput than the 2-Mbps option.</td> </tr> <tr> <td>11</td> <td>Offers the greatest throughput but the lowest range.</td> </tr> </tbody> </table>	Data Rate (Mbps)	Description	Auto	Uses the 11-Mbps data rate when possible but drops to lower rates when necessary.	1	Offers the greatest range but the lowest throughput.	2	Offers less range but greater throughput than the 1-Mbps option.	5.5	Offers less range but greater throughput than the 2-Mbps option.	11	Offers the greatest throughput but the lowest range.
Data Rate (Mbps)	Description												
Auto	Uses the 11-Mbps data rate when possible but drops to lower rates when necessary.												
1	Offers the greatest range but the lowest throughput.												
2	Offers less range but greater throughput than the 1-Mbps option.												
5.5	Offers less range but greater throughput than the 2-Mbps option.												
11	Offers the greatest throughput but the lowest range.												
Data Retries	<p>Defines the number of times a packet is resent if the initial transmission is unsuccessful.</p> <p>Parameter line: Data Retries = 1 to 128</p> <p>Default: 16</p> <p> Note If your network protocol performs its own retries, set this parameter to a smaller value than the default. This way notification of a “bad” packet is sent up the protocol stack quickly so the application can retransmit the packet if necessary.</p>												
Fragment Threshold	<p>Defines the threshold size above which an RF data packet is split up or fragmented. If one of those fragmented packets experiences interference during transmission, only that specific packet needs to be resent.</p> <p>Throughput is generally lower for fragmented packets because the fixed packet overhead consumes a higher portion of the RF bandwidth.</p> <p>Parameter line: Fragment Threshold = (256 to 2312)</p> <p>Default: 2312</p>												

Table 2-2 Profile Parameters (continued)



Parameter	Description
Antenna Mode Receive	<p>Specifies the type of antenna that your client adapter uses to receive data.</p> <p>Parameter line: Antenna Mode Receive = Both, Right, or Left</p> <ul style="list-style-type: none"> PC card – The PC card’s integrated, permanently attached antenna operates best when used in diversity mode. Diversity mode enables the card to use the better signal from its two antenna ports. <p>Default: Both (Diversity)</p> LM card – The LM card is shipped without an antenna; however, an antenna can be connected through the card’s external connector. If a snap-on antenna is used, diversity mode is recommended. Otherwise, select the mode that corresponds to the antenna port to which the antenna is connected. <p>Default: Both (Diversity)</p> PCI client adapter – The PCI client adapter must use the Right Antenna Only option. <p>Default: Right</p>
Antenna Mode Transmit	<p>Specifies the antenna that your client adapter uses to transmit data. See the Antenna Mode (Receive) parameter above for information on the options available for your client adapter.</p> <p>Parameter line: Antenna Mode Receive = Both, Right, or Left</p>
RTS Threshold	<p>Specifies the size of the data packet that the low-level RF protocol issues to a request-to-send (RTS) packet.</p> <p>Setting this parameter to a small value causes RTS packets to be sent more often. When this occurs, more of the available bandwidth is consumed and the throughput of other network packets is reduced, but the system is able to recover faster from interference or collisions, which may be caused from a high multipath environment characterized by obstructions or metallic surfaces.</p> <p>Parameter line: RTS Threshold = 0 to 2312</p> <p>Default: 2312</p> <p> Note Refer to the IEEE 802.11 Standard for more information on the RTS/CTS mechanism.</p>
RTS Retry Limit	<p>Specifies the number of times the client adapter resends a request-to-send (RTS) packet if it does not receive a clear-to-send (CTS) packet from the previously sent RTS packet.</p> <p>Setting this parameter to a large value decreases the available bandwidth whenever interference is encountered but makes the system more immune to interference and collisions, which may be caused from a high multipath environment characterized by obstructions or metallic surfaces.</p> <p>Parameter line: RTS Retry Limit = 1 to 128</p> <p>Default: 16</p> <p> Note Refer to the IEEE 802.11 Standard for more information on the RTS/CTS mechanism.</p>
IsDefault	<p>Specifies whether this is the default profile that is used when the PC is powered up.</p> <p>Parameter line: IsDefault = yes or no</p>

Table 2-2 Profile Parameters (continued)



Parameter	Description
IsFactoryDefault	<p>Specifies a special factory default profile. This profile is not editable from the ACU and is only used if all other profiles are removed.</p> <p>Parameter line: IsFactoryDefault = yes or no</p> <p>Default: no</p>
NotAllowEdit	<p>Specifies whether the profile can be edited. If activated, the ACU displays the profile in read-only mode.</p> <p>Parameter line: NotAllowEdit = yes or no</p> <p>Default: no</p>
NotAllowExport	<p>Specifies whether the profile can be exported to a file.</p> <p>Parameter line: NotAllowExport = yes or no</p> <p>Default: no</p>
NotAllowEditWepKey	<p>Specifies whether the WEP keys can be changed.</p> <p>Parameter line: NotAllowEditWepKey = yes or no</p> <p>Default: no</p>
DeviceResidentKeys	<p>Specifies whether the WEP keys stored in the client adapter Flash memory are to be used. If activated, the WEP keys defined in the profile are stored with the profile but given a length of zero (ignored by the system).</p> <p>Parameter line: DeviceResidentKeys = yes or no</p> <p>Default: no</p>
AutoSelect	<p>Specifies whether the ACU automatically scans for the first valid profile if the default profile is not valid for the current client radio location. The scan order is the order the profiles are listed under the [Profile Names] parameter.</p> <p>Parameter line: AutoSelect = yes or no</p> <p> Note If a profile is configured for LEAP, that profile is not supported by the auto profile switching feature until you manually configure the LEAP username and password parameters using the ACU.</p> <p> Note Two or more profiles must contain <i>AutoSelect = yes</i> before the ACU auto profile selection feature is enabled.</p>

Table 2-2 Profile Parameters (continued)



Parameter	Description																						
Network Security	<p>Specifies the security option used by the client adapter.</p> <p>Parameter line: Network Security = (desired security setting)</p> <p>Default: None_Open</p> <p> Note The auto installer defaults to None_Open if you specify an invalid security setting.</p> <p> Note The EAP security settings are valid only on computers running Windows XP.</p>																						
	<table border="1"> <thead> <tr> <th>Security Setting</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>None_Open</td> <td>No server based authentication and open key access point authentication.</td> </tr> <tr> <td>None_Open_Mixed</td> <td>No server based authentication, open access point authentication, and allow association to mixed cells.</td> </tr> <tr> <td>None_Open_Mixed_Wep</td> <td>No server based authentication, open key access point authentication, allow association to mixed cells, and WEP enabled.</td> </tr> <tr> <td>None_Open_Wep</td> <td>No server based authentication, open key access point authentication, and WEP enabled.</td> </tr> <tr> <td>None_Shared_Wep</td> <td>No server based authentication, shared key access point authentication, and WEP enabled.</td> </tr> <tr> <td>None_Shared_Mixed_Wep</td> <td>No server based authentication, shared key access point authentication, allow association to mixed cells, and WEP enabled.</td> </tr> <tr> <td>Leap_Open_Wep</td> <td>Leap server based authentication, open key access point authentication, and WEP enabled.</td> </tr> <tr> <td>Leap_Open_Disassociate_Wep</td> <td>Leap server based authentication, open key access point authentication, disassociate after logoff, and WEP enabled.</td> </tr> <tr> <td>Leap_Open_Disassociate_Wep_Mixed</td> <td>Leap server based authentication, open key access point authentication, disassociate after logoff, WEP enabled, and allow association to mixed cells.</td> </tr> <tr> <td>Leap_Open_Wep_Mixed</td> <td>Leap server based authentication, open key access point authentication, WEP enabled, and allow association to mixed cells.</td> </tr> </tbody> </table>	Security Setting	Description	None_Open	No server based authentication and open key access point authentication.	None_Open_Mixed	No server based authentication, open access point authentication, and allow association to mixed cells.	None_Open_Mixed_Wep	No server based authentication, open key access point authentication, allow association to mixed cells, and WEP enabled.	None_Open_Wep	No server based authentication, open key access point authentication, and WEP enabled.	None_Shared_Wep	No server based authentication, shared key access point authentication, and WEP enabled.	None_Shared_Mixed_Wep	No server based authentication, shared key access point authentication, allow association to mixed cells, and WEP enabled.	Leap_Open_Wep	Leap server based authentication, open key access point authentication, and WEP enabled.	Leap_Open_Disassociate_Wep	Leap server based authentication, open key access point authentication, disassociate after logoff, and WEP enabled.	Leap_Open_Disassociate_Wep_Mixed	Leap server based authentication, open key access point authentication, disassociate after logoff, WEP enabled, and allow association to mixed cells.	Leap_Open_Wep_Mixed	Leap server based authentication, open key access point authentication, WEP enabled, and allow association to mixed cells.
Security Setting	Description																						
None_Open	No server based authentication and open key access point authentication.																						
None_Open_Mixed	No server based authentication, open access point authentication, and allow association to mixed cells.																						
None_Open_Mixed_Wep	No server based authentication, open key access point authentication, allow association to mixed cells, and WEP enabled.																						
None_Open_Wep	No server based authentication, open key access point authentication, and WEP enabled.																						
None_Shared_Wep	No server based authentication, shared key access point authentication, and WEP enabled.																						
None_Shared_Mixed_Wep	No server based authentication, shared key access point authentication, allow association to mixed cells, and WEP enabled.																						
Leap_Open_Wep	Leap server based authentication, open key access point authentication, and WEP enabled.																						
Leap_Open_Disassociate_Wep	Leap server based authentication, open key access point authentication, disassociate after logoff, and WEP enabled.																						
Leap_Open_Disassociate_Wep_Mixed	Leap server based authentication, open key access point authentication, disassociate after logoff, WEP enabled, and allow association to mixed cells.																						
Leap_Open_Wep_Mixed	Leap server based authentication, open key access point authentication, WEP enabled, and allow association to mixed cells.																						

Table 2-2 Profile Parameters (continued)




Parameter	Description										
Network Security (continued)	<table border="1"> <thead> <tr> <th>Security Setting</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Eap_Open_Wep_Dynamic</td> <td>EAP server based authentication, open key access point authentication, WEP enabled, and dynamic WEP key assignments.</td> </tr> <tr> <td>Eap_Open_Wep_Mixed_Dynamic</td> <td>EAP server based authentication, open key access point authentication, WEP enabled, allow association to mixed cells, and dynamic WEP key assignments.</td> </tr> <tr> <td>Eap_Open_Wep_Static</td> <td>EAP server based authentication, open key access point authentication, WEP enabled, and static WEP key assignments. See the note below.)</td> </tr> <tr> <td>Eap_Open_Wep_Mixed_Static</td> <td>EAP server based authentication, open key access point authentication, WEP enabled, allow association to mixed cells, and static WEP key assignments. See the note below.</td> </tr> </tbody> </table>	Security Setting	Description	Eap_Open_Wep_Dynamic	EAP server based authentication, open key access point authentication, WEP enabled, and dynamic WEP key assignments.	Eap_Open_Wep_Mixed_Dynamic	EAP server based authentication, open key access point authentication, WEP enabled, allow association to mixed cells, and dynamic WEP key assignments.	Eap_Open_Wep_Static	EAP server based authentication, open key access point authentication, WEP enabled, and static WEP key assignments. See the note below.)	Eap_Open_Wep_Mixed_Static	EAP server based authentication, open key access point authentication, WEP enabled, allow association to mixed cells, and static WEP key assignments. See the note below.
	Security Setting	Description									
	Eap_Open_Wep_Dynamic	EAP server based authentication, open key access point authentication, WEP enabled, and dynamic WEP key assignments.									
	Eap_Open_Wep_Mixed_Dynamic	EAP server based authentication, open key access point authentication, WEP enabled, allow association to mixed cells, and dynamic WEP key assignments.									
	Eap_Open_Wep_Static	EAP server based authentication, open key access point authentication, WEP enabled, and static WEP key assignments. See the note below.)									
Eap_Open_Wep_Mixed_Static	EAP server based authentication, open key access point authentication, WEP enabled, allow association to mixed cells, and static WEP key assignments. See the note below.										
 <p>Note If the <i>Eap_Open_Wep_Static</i> or the <i>Eap_Open_Wep_Mixed_Static</i> options are selected, there must be a WEP key specified in the profile. If a WEP key is not specified, the Network Security option defaults to the corresponding EAP option that uses dynamic WEP key assignments.</p>											
WepKey1	<p>Specifies the WEP 1 key. A 40-bit WEP key can contain 5 ASCII characters or 10 hexadecimal characters. A 128-bit WEP key can contain 13 ASCII characters or 26 hexadecimal characters.</p>  <p>Note The auto installer does not pad the keys with 0s or nulls (00); for example: an ASCII key of 123 must be entered as 1 2 3 0 0 for 40-bit WEP or 1 2 3 0 0 0 0 0 0 0 0 0 0 0 for 128-bit WEP.</p>  <p>Note Your client adapter's WEP key must match the WEP key used by the access point or wireless clients with which you are planning to communicate. When you are setting more than one WEP key, the WEP keys must be assigned to the same WEP key numbers for all devices.</p> <p>Range: ASCII entry—5 or 13 ASCII characters Hex entry—10 or 26 characters using 0 to 9, a to f, or A to F.</p>										
WepKey1size	<p>Specifies the number of bits in the WEP key.</p> <p>Parameter line: WepKey1size = 40, 128, or 0 (0 specifies the WEP key is not used)</p>										
WepKey1IsTransmit	<p>Specifies the key you want to use to transmit packets. Only one WEP key can be set as the transmit key.</p> <p>Parameter line: WepKey1IsTransmit = yes or no</p>										
WepKey2	Specifies the second WEP key for your client adapter. See the corresponding description for WepKey1 parameters.										
WepKey2size											
WepKey2IsTransmit											

Table 2-2 Profile Parameters (continued)

Parameter	Description
WepKey3	Specifies the third WEP key for your client adapter. See the corresponding description for WepKey1 parameters.
WepKey3size	
WepKey3IsTransmit	
WepKey4	Specifies the fourth WEP key for your client adapter. See the corresponding description for WepKey1 parameters.
WepKey4size	
WepKey4IsTransmit	

Installation File Examples

Tabs and blank lines can be used in the installation file for reading clarity.

Example 1

```
[LogFile]
    File Name                = C:\Program Files\Cisco Aironet\Log\CWUA.log

[Install Apps]
    ACU                      = yes

[Administrative Overrides]
    Allow Edit Profile       = yes
    Allow Export Profile     = no
    Allow Import Profile     = no
    Allow Edit WEP          = no
    Existing Profiles        = Delete

[App Parameters]
    Folder Name              = Cisco Systems, Inc
    Program Location         = C:\Program Files\Cisco Aironet
    Enable Leap              = no
    Allow Leap Data save    = no
    Create ACU icon on desk = no
    Allow Non Admin to modify profiles = no

[Device Resident Wep Keys]
    Save Keys to Flash       = no
    WepKey1                  = be9102034560afcb234b67aa10
    WepKey1size              = 128
    WepKey1IsTransmit        = yes
```

```

[Firmware Upgrade]
    Upgrade = yes
    Display Flash Progress = no
    Firmware Path = D:\Client\Firmware\client09.img

[Profile Names]
    Work

[Work]
    IsDefault = no
    IsFactoryDefault = no
    AutoSelect = no
    NotAllowEdit = no
    Not Allow Export = no
    NotAllowEditWepKey = no
    Client Name = joesmith
    Use Logon Name = no
    Use Computer Name = no
    SSID1 = YellowRose1
    SSID2 = Second Floor 1a
    SSID3 = factory location 21
    Power Save Mode = cam
    Network Type = Infrastructure
    Data Rate = auto
    Data Retries = 16
    Fragment Threshold = 2312
    Antenna Mode Receive = Both
    Antenna Mode Transmit = Both
    RTS Threshold = 2312
    Network Security = None_Open_Wep
    WepKey2 = 123Charlie
    WepKey2size = 40
    WepKey2IsTransmit = no
    WepKey3 = Happy Days
    WepKey3size = 40
    WepKey3IsTransmit = no
    WepKey4 = Special!Key+9
    WepKey4size = 0
    WepKey4IsTransmit = no

```

Example 2

```

[Firmware Upgrade]
    Upgrade = yes
    Display Flash Progress = no
    Firmware Path = c:\temp\firmware\client123c.img
[LogFile]
    File Name = D:\Cisco Aironet\Log\CWUA.log
[Administrative Overrides]
    Allow Export Profile = no
    Allow Import Profile = no
    Allow Edit WEP = no
    Existing Profiles = Preserve
[Install Apps]
    ACU = yes
[App Parameters]
    Folder Name = Cisco Systems, Inc
    Program Location = C:\Program Files\Cisco Aironet
    Enable Leap = yes
    Allow Leap Data save = no
    Create ACU icon on desk = no
    Allow Non Admin to modify profiles = no
[Profile Names]
    Profile 1
[Profile 1]
    Use Logon Name = yes
    SSID1 = CharlieBrown
    SSID2 = Apollo 11
    Network Security = Leap_Open_Disassociate_Wep
    WepKey1 = 09876543210987654321123456
    WepKey1size = 128
    WepKey1IsTransmit = yes

```

Example 3

```
[Install Apps]
    ACU                                = yes

[App Parameters]
    Folder Name                        = Wireless
    Program Location                   = C:\Program Files\Cisco Aironet Wireless

[LogFile]
    File Name                          = E:\Wireless\Log\CWUA.log

[Profile Names]
    Office
    Factory

[Office]
    AutoSelect                         = yes
    Use Logon Name                     = yes
    SSID1                              = CharlieBrown
    SSID2                              = zorro+MaskMan 2
    SSID3                              = Superman2101
    Network Security                   = None_Open_Wep
    WepKey1                            = 19cb38bd68ffade24910adfeba
    WepKey1size                        = 128
    WepKey1IsTransmit                  = yes
    WepKey2                            = 12345678901234567890123456
    WepKey2size                        = 128
    WepKey2IsTransmit                  = no
    WepKey3                            = {%1a!D$5h*+j}
    WepKey3size                        = 128
    WepKey3IsTransmit                  = no
```

[Factory]

Use Logon Name	= yes
SSID1	= HotDog2
Network Security	= None_Open_Wep
WepKey1	= a01d2cf9b87a3b2f1d021fde8a
WepKey1size	= 128
WepKey1IsTransmit	= yes

[Administrative Override]

Allow Export Profile	= no
Allow Import Profile	= no
Existing Profiles	= Overwrite