APPENDIX C

Windows Client Registry Settings

This appendix describes how to configure and enable various Clean Access Agent features using Windows client machine registry settings. Topics include:

- Access to Authentication VLAN Change Detection on Clients with Multiple Active NICs
- Disable Exit on Clean Access Agent Taskbar Menu
- Require WSUS Update/Installation Dialog to Be On Top of Other Desktop Windows
- Additional SWISS Response Packet Delay Timeout Value
- Client-side MAC Address Exceptions for Agent-to-Clean Access Server Advertisement
- Change the Clean Access Agent Discovery Host Address
- Clean Access Agent Stub Verifying Launch Program Executable for Trusted Digital Signature

In order to configure a Windows client machine to use any of the following additional features for the Clean Access Agent, you must define the appropriate registry keys on the client.

Table C-1 Access to Authentication VLAN Change Detection on Clients with Multiple Active NICs

Registry Key (DWORD)	Default Value (Decimal)	Valid Range	Behavior
Location: HKEY_LOCAL_MACHINE\Software\Cisco\Clean Access Agent\ [1]			
RetryDetection	5	0 and above	If ICMP or ARP polling fails, this setting configures the Agent to retry <*x*> times before refreshing the client IP address.
PingArp	0	0-2	• If this value is set to **0**, poll using ICMP. • If this value is set to **1**, poll using ARP. • If this value is set to **2**, poll using ICMP first, then (if ICMP fails) use ARP.
PingMaxTimeout	1	1-10	Poll using ICMP and if no response in <*x*> seconds, then declare ICMP polling failure.
DHCPServiceStartStop	0	Any	• If this setting is 0, do not perform DHCP services (**net dhcp stop/start**) when IP refresh fails with API. • If any value other than 0, perform DHCP services.

Table C-1 Access to Authentication VLAN Change Detection on Clients with Multiple Active NICs

Registry Key (DWORD)	Default Value (Decimal)	Valid Range	Behavior
VlanDetectInterval	0	0, 5-60	• If this setting is **0**, the Access to Authentication VLAN change feature is disabled. • If this setting is **1-5**, the Agent sends ICMP/ARP queries every 5 seconds. • If this setting is **6-60**, ICMP/ARP every <*x*> seconds. (Any value greater than 60 seconds automatically reverts to 60.)

[1] These five registry key settings are designed to support version 4.1.3.2 and later of the Windows Clean Access Agent. If using version 4.1.3.0 or 4.1.3.1 of the Windows Agent, you only need to specify the "VlanDetectInterval" registry setting to configure a Windows Agent machine to operate using the Access to Authentication VLAN change detection feature. If you configure any of the additional version 4.1.3.2 and later registry settings using version 4.1.3.0 or 4.1.3.1, Cisco NAC Appliance does not identify or use the settings for the Access to Authentication VLAN change detection feature.

Refer to Configure Access to Authentication VLAN Change Detection, page 4-61 for additional details.

Table C-2 Disable Exit on Clean Access Agent Taskbar Menu

Registry Key (DWORD)	Default Value (Decimal)	Valid Range	Behavior
Location: HKEY_LOCAL_MACHINE\Software\Cisco\Clean Access Agent\			
DisableExit	0	0,1	Exit is disabled on the Agent taskbar menu when the Registry DWORD key DisableExit = 1 is created at HKLM\SOFTWARE\Cisco\Clean Access Agent\\

Table C-3 Require WSUS Update/Installation Dialog to Be On Top of Other Desktop Windows

Registry Key (DWORD)	Default Value (Decimal)	Valid Range	Behavior
Location: HKEY_LOCAL_MACHINE\Software\Cisco\Clean Access Agent\			
KeepWSUSOnTop	0	0,1	• If this setting is **0**, the Agent behaves as designed and WSUS update/installation dialogs are *not* forced to the top of the Windows desktop. • If this setting is **1**, the WSUS update/installation dialog always appears on top of other Windows on the client desktop.

Refer to Create Windows Server Update Service Requirement, page 12-18 for additional details.

Table C-4 Additional SWISS Response Packet Delay Timeout Value

Registry Key (DWORD)	Default Value (Decimal)	Valid Range	Behavior
Location: HKEY_CURRENT_USER\Software\Cisco\Clean Access Agent\			
SwissTimeout	1	> 1	• If this setting is **1**, the Agent performs SWISS discovery as designed and no additional response packet delay timeout value is introduced. • If the setting is an integer **greater than 1**, the Clean Access Agent waits the additional number of seconds for a SWISS discovery response packet from the Clean Access server before sending another discovery packet to be sure network latency is not delaying the response packet en route.

Refer to the "Configuring the CAS Managed Network" chapter of the *Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide* for details.

Table C-5 Client-side MAC Address Exceptions for Agent-to-Clean Access Server Advertisement

Registry Key (String)	Default Value (Decimal)	Valid Range	Behavior
Location: HKEY_LOCAL_MACHINE\Software\Cisco\Clean Access Agent\			
ExceptionMACList	—	Valid MAC address	If you specify one or more MAC addresses in this setting, the Clean Access Agent does not advertise those MAC addresses to the CAS during login and authentication to help prevent sending unnecessary MAC addresses over the network. The text string you specify must be a comma-separated list of MAC addresses including colons. For example: `AA:BB:CC:DD:EE:FF,11:22:33:44:55:66`

Refer to Agent Sends IP/MAC for All Available Adapters, page 11-10 for additional details.

Table C-6 Change the Clean Access Agent Discovery Host Address

Registry Key (String)	Default Value (Decimal)	Valid Range	Behavior
Location: HKEY_LOCAL_MACHINE\Software\Cisco\Clean Access Agent\			
ServerUrl	—	—	Search for this registry setting to determine the Discovery Host address the Clean Access Agent uses to connect to the Cisco NAC Appliance system in a Layer 3 deployment. You can also use this function to specify a new Discovery Host address for the Agent to use when authenticating with Cisco NAC Appliance.

Refer to Clean Access Agent MSI Installers, page 11-23 for additional details.

Table C-7 Clean Access Agent Stub Verifying Launch Program Executable for Trusted Digital Signature

Registry Key	Default Value (Decimal)	Valid Range	Supported Value Names
Location: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\CCAAgentStub\			
Trust<*N*>	—	0 and above	The Trust<*N*> chain is a digital signature for the executable that the Clean Access Agent Stub uses to determine whether or not Windows can trust the executable before launching.
Certificate	—	—	• 2.5.4.3 - COMMON_NAME or • 2.5.4.3 - SUBJECT_NAME • 2.5.4.4 - SUR_NAME • 2.5.4.5 - DEVICE_SERIAL_NUMBER • 2.5.4.6 - COUNTRY_NAME • 2.5.4.7 - LOCALITY_NAME • 2.5.4.8 - STATE_OR_PROVINCE_NAME • 2.5.4.9 - STREET_ADDRESS • 2.5.4.10 - ORGANIZATION_NAME • 2.5.4.11 - ORGANIZATIONAL_UNIT_NAME • 2.5.4.12 - TITLE • 2.5.4.13 - DESCRIPTION • 2.5.4.14 - SEARCH_GUIDE • 2.5.4.15 - BUSINESS_CATEGORY • 2.5.4.16 - POSTAL_ADDRESS • 2.5.4.17 - POSTAL_CODE • 2.5.4.18 - POST_OFFICE_BOX • 2.5.4.19 - PHYSICAL_DELIVERY_OFFICE_NAME • 2.5.4.20 - TELEPHONE_NUMBER

Table C-7 Clean Access Agent Stub Verifying Launch Program Executable for Trusted Digital Signature (continued)

Registry Key	Default Value (Decimal)	Valid Range	Supported Value Names
FileVersionInfo	—	—	• ProductName • CompanyName • FileDescription • FileVersion • InternalName • LegalCopyright • OriginalFileName • ProductVersion • Comments • LegalTrademarks • PrivateBuild • SpecialBuild

Refer to Configuring a Launch Programs Requirement, page 12-43 for additional details.