



Release Notes for Cisco Secure ACS 4.1.3

Revised: July 9, 2007, OL-12629-02
CDC Date: May 5, 2007

These release notes pertain to Cisco Secure Access Control Server, hereafter referred to as ACS version 4.1.3. These release notes contain information for the Windows and Solution Engine platforms. Where necessary, the appropriate platform is clearly identified.

Contents

These release notes contain:

- [Introduction, page 1](#)
- [New and Changed Information, page 2](#)
- [Product Documentation, page 16](#)
- [Known Caveats in ACS for Windows and the Solution Engine 4.1.3, page 18](#)
- [Resolved Caveats in ACS for Windows and the Solution Engine 4.1.3, page 23](#)
- [Installation Notes for ACS 4.1.3, page 25](#)

Introduction

ACS 4.1.3 is a maintenance release for ACS 4.1 that consolidates ACS 4.1 customer patches and resolves other customer and internally found defects. ACS 4.1.3 is available through the Cisco Technical Assistance Center (TAC) only for upgrading existing ACS software deployments.

This release includes:

- ACS 4.1.3 software image.
- Appliance upgrade CD for ACS Solution Engines 1111, 1112, 1113.



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

New and Changed Information

ACS 4.1.3 contains these new enhancements:

- [Support for Microsoft Windows Server 2003 R2, page 2](#)
- [Support for 3Com/USR VSAs, page 2](#)
- [MAC and MAB Functionality Issues, page 3](#)
- [Support for User-Defined Vendors Extended VSA ID, page 3](#)
- [Addition of the cisco-AVPair Attribute to the VOIP Accounting Report, page 5](#)
- [Configuring the ACS RADIUS Server to Reject or Discard Requests to an External ODBC Database, page 6](#)
- [Addition of Session IDs to the CSAuth Diagnostic Log, page 7](#)
- [Description of Error Codes in the CSAuth Diagnostic Log, page 7](#)
- [Improved EAP Code Debug Messages, page 16](#)

Support for Microsoft Windows Server 2003 R2

ACS is supported on Windows Server 2003 R2.

Support for 3Com/USR VSAs

ACS now supports 3Com/USR VSAs. The 3Com/USR VSA format differs from other VSAs in that 3Com/USR VSAs have a 32-bit Extended Vendor-Type field and no length field.

The Authenticate Using drop-down list in the Network Configuration section of the ACS web interface now includes a new network device, RADIUS (3COMUSR).

**Note**

3Com/USR VSAs should be used for any device that uses these VSAs, not just the HiperARC cards.

Once you add the RADIUS (3COMUSR) to the Network Configuration section, it becomes available to the User Setup and Group Setup sections of the ACS web interface. These VSAs will also be available to the RADIUS accounting log. Use the Interface Configuration section to configure RADIUS (3COMUSR). For information on adding a network device, refer to the *User Guide for Cisco Secure ACS 4.1*.

MAC and MAB Functionality Issues

Cisco recommends that you apply patch 4.1.3.12.1 to ensure:

- ACS 4.1 functionality for MAB.
- ACS 4.0 functionality for MAC authentication.

After you apply the patch, if

- Service-Type(6) = 10 and NAP is present, MAB is invoked.
- Service-Type(6) = 10 and NAP is non-existent, MAC authentication is invoked.

This specification retains ACS 4.1 functionality for MAB and ACS 4.0 functionality for MAC authentication.

Support for User-Defined Vendors Extended VSA ID

In previous versions of ACS the vendor-specific attribute (VSA) ID length was restricted to one byte, the default value, and the VSA ID value could not be greater than 255. ACS 4.1.3 supports VSA ID lengths of 1, 2 or 4 bytes. In addition, customers can specify whether the VSA has an internal length field or not.

You can use CSUtil or RDBMS synchronization to install dictionary components for vendors that require extended VSA ID length.

Use the CSUtil.ini file to Install User-Defined Vendor or VSA Data

Use the CSUtil **-addUDV** option with the vendor **.ini** file to install VSA data for vendors that require extended VSA ID length. [Table 1](#) contains two additional codes and definitions in the vendor **.ini** file used to modify the vendor configuration.

Table 1 CSUtil.ini file Options and Definitions for Vendor Configuration

Option	Value	Description
Need Internal Length	TRUE or FALSE	Sets the presence of Internal Length field in VSA. If not used, then the default is TRUE.
ID Length	1, 2 or 4 bytes.	Sets the Vendor-Specific Attribute (VSA) Type length in bytes. If not used, then the default is 1 byte.



Note

ACS 4.1.3 supports hex-numbering for the VSA ID feature. Values starting with **0x** are assumed to be hex values.

Use the following sample format of the vendor **.ini** file for setting the ID Length and VSA values. In this example,

- Need Internal Length value is TRUE.
- ID Length is two bytes
- vendor VSA ID values are 264 and 0x109.

```
[User Defined Vendor]
Name=vendor-name
IETF Code=vendor-IETF-code
```

```
Need Internal Length = TRUE
ID Length=2
VSA 264=Ascend-Max-RTP-Delay
VSA 0x109= Ascend-RTP-Port-Range
```

```
[Ascend-Max-RTP-Delay]
Type=INTEGER
Profile=OUT
[Ascend-RTP-Port-Range]
Type=STRING
Profile=OUT
```

Use the RDBMS Synchronization Action Codes to Install User-Defined Vendor or VSA Data

Use the RDBMS Synchronization action codes to install VSA data for vendors that require extended VSA ID length. [Table 2](#) contains two additional codes and definitions for modifying the vendor configuration.

Table 2 RDBMS Account Action Codes and Definition for Vendor Configuration

Action Code	Name	Required	Description
356	SET_VSA_ID_LEN	V1, V2	Sets the Vendor-Specific Attribute (VSA) Type length in bytes. <ul style="list-style-type: none"> V1 contains the vendor IETF code. V2 contains VSA-Type Length, which takes the values 1, 2 or 4.
357	SET_VSA_INTERNAL_LEN	V1, V2	Sets the presence of Internal Length field in VSA. <ul style="list-style-type: none"> V1 contains the vendor IETF code. V2 contains BOOL value. 1-(TRUE) if VSA requires the Internal Length field. 0-(FALSE) if the Internal Length field is not required.

Configuring the Workstation Name For Windows Authentications

You use ACS to define a custom workstation name when authenticating against Active Directory (AD). In previous versions of ACS, a workstation name of CISCO was used for authentications to AD. This enhancement allows multiple ACS deployments using a single AD tree.

The Windows External Database section of the ACS web interface now contains a new configuration section. You use the new configuration section to customize the workstation name.

To configure a workstation name:

-
- Step 1** In the navigation bar, click **External User Databases**.
The External User Database page appears.
- Step 2** Click **Database Configuration**.
The External User Database Configuration page appears.
- Step 3** Click **Windows Database**.
The Windows Authentication Configuration page appears.
- Step 4** Click **Configure**.
- If you are running ACS for Windows, the Windows Authentication Configuration page appears.
 - If you are running the Solution Engine, click **Windows Authentication Configuration**. The Windows Authentication Configuration page appears
- Step 5** Choose one of the options to configure a workstation name:
- CISCO**—Configures CISCO as the workstation name. This is the default.
 - Local**—Configures the local machine name as the workstation name. By default, ACS displays the local host name.
 - User defined workstation name**—Specifies a name for the workstation. (Limit: 15 characters).



Note Ensure that all user accounts have login permission to the workstation.

Windows Authentication Configuration Error Messages

Table 3 lists the Windows Authentication Error Messages.

Table 3 Windows Authentication Configuration Errors

Error Number	Description
1	Workstation name contains invalid characters. alpha-numeric are the only valid characters,

Addition of the cisco-AVPair Attribute to the VOIP Accounting Report

ACS has added the **cisco-AVPair** attribute to the VoIP Accounting Report.

To configure the VoIP Accounting Report:

-
- Step 1** In the navigation bar, click **System Configuration**.
The System Configuration page appears.
- Step 2** Click **VoIP Accounting Configuration**.
The VoIP Accounting Configuration page appears.
- Step 3** Configure the log.
- Step 4** Click **Submit**.
- Step 5** Restart ACS in **System Configuration > Service Control** to adopt the new settings.

- Step 6** In the navigation bar, click **System Configuration > Logging**.
The Logging Configuration page appears.
- Step 7** Click **Configure** next to the **VoIP Accounting Column**.
- Step 8** Choose the **cisco-AVPair** attribute and move it to the Logged Attributes list.
- Step 9** Click Submit.
The Logging Configuration page reappears.
- Step 10** In the navigation bar, click **Reports and Activity**.
The Reports and Activity page appears.
- Step 11** Click **VoIP Accounting**.
The VoIP Accounting report appears and displays the **cisco-AVPair** attribute.



Note Multiple Cisco-AVPair attributes values are concatenated in the VOIP Accounting report with a semi-colon.

The screenshot shows a text box containing the text "Cisco-AVPair" in blue, with "val4; val3; val2" below it, illustrating how multiple values are concatenated.

Configuring the ACS RADIUS Server to Reject or Discard Requests to an External ODBC Database

You use ACS RADIUS server to send an access reject reply or discard the access-request. In some deployments, the ACS server might send an access reject or discards an access request. For example, in the event of an external ODBC database failure, ACS can deny the authentication (access reject), or not respond at all. Conversely, if ACS discards an access request the network access device that can fail over to another ACS server. A drawback to this approach is that discards can cause excessive network traffic and load on the network access devices as requests continue to travel from network access devices to the ACS servers.

To configure a RADIUS server:

- Step 1** In the navigation bar, click **External User Databases**.
The External User Databases page appears.
- Step 2** Click **Database Configuration**.
The External User Database Configuration page appears.
- Step 3** Click **External ODBC Database**.
The CiscoSecure ODBC Authentication Configuration page appears.
- Step 4** In the RADIUS behavior in the event of database failure section select one of the RADIUS server options, shown in [Table 4](#).
- Step 5** Click Submit.

Table 4 *RADIUS Server Reject and Discard Request Options*

Option	Description
Send an access reject (your devices will stay with this RADIUS server).	The network access devices will retry the same RADIUS server and not fail over to another RADIUS server.
Discard the access request (your devices may try a different RADIUS server).	The network access devices will use the available RADIUS servers.

Addition of Session IDs to the CSAuth Diagnostic Log

ACS supports a session ID parameter for the CSAuth diagnostic log. You can use a unique session ID to differentiate log threads in the CSAuth diagnostic logs.

[Example 1](#) shows the session ID **1000** is processed by two different threads (2560, 2548) in the network model thread. You can filter the logs by session ID to restrict the output for each session.

Example 1 *CSAuth Diagnostic Log with session ID*

```
AUTH 09/08/2006 18:29:57 I 5081 2560 1000 Start RQ1040, client 1 (127.0.0.1)
AUTH 09/08/2006 18:30:13 I 5094 2548 Worker 1 processing message 17.
AUTH 09/08/2006 18:30:14 I 0991 2368 0000 pvNASMonitorThreadMain: start NM
update ...
AUTH 09/08/2006 18:30:14 I 1006 2368 0000 pvNASMonitorThreadMain: commit NM
update ...
AUTH 09/08/2006 18:30:14 I 5081 2560 1000 Done RQ1040, client 1, status 0
AUTH 09/08/2006 18:30:14 I 1011 2368 0000 pvNASMonitorThreadMain: succeeded
to commit NM update
AUTH 09/08/2006 18:30:28 I 5081 2548 1000 Start RQ1012, client 2 (127.0.0.1)
AUTH 09/08/2006 18:30:28 I 5081 2548 1000 Done RQ1012, client 2, status 0
```



Note

The additional session ID field in the ACS diagnostic log involves minimal overhead: eight bytes per line for each authentication session.

Description of Error Codes in the CSAuth Diagnostic Log

The ACS 4.1.3 CSAuth diagnostic logs now display a description of client requests and responses. Previous versions of ACS used a numeric code for client requests and responses. The description is useful for locating client requests and responses in the CSAuth diagnostic logs.

[Figure 1](#) contains two CSAuth diagnostic log examples. The first example represents an entry from previous versions of the CSAuth diagnostic log. The second example represents how this entry appears in the CSAuth 4.1.3 diagnostic log.

Example 2 shows that in the CSAuth diagnostic log:

- `UDB_AUTHENTICATE_USER` replaces the RQ1026 request code shown in the first example.
- `UDB_CHALLENGE_REQUIRED` replaces the 2046 status code shown in the first example.

Figure 1 *CSAuth Diagnostic Log Entry*

Example 1

```
AUTH 09/11/2006 09:55:27 I 5081 2512 Done RQ1026, client 50, status -2046
```

Example 2 (with Descriptive text)

```
AUTH 09/11/2006 09:55:27 I 5081 2512 Done UDB_AUTHENTICATE_USER, client 50, status
UDB_CHALLENGE_REQUIRED
```

Table 5 and Table 6 list the descriptive text for requests and status that appear in the 4.1.3 CSAuth diagnostic logs.

Descriptive Request Text in the CSAuth Diagnostic Logs

Table 5 lists the descriptive text in the CSAuth diagnostic logs and the corresponding request code.

Table 5 Descriptive Request Text and Request Code

Request Text	Request Code
UDB_BASE_CMD	1000
UDB_HAIL	1001
UDB_OPEN	1002
UDB_CLOSE	1003
UDB_GOODBYE	1004
UDB_PING	1005
UDB_REFRESH	1006
UDB_REFRESH_EX	1007
UDB_RESET_HOST_CACHE	1008
UDB_USER_ADD	1010
UDB_USER_REMOVE	1011
UDB_VALID_USER	1012
UDB_USER_ENUM_BY_GROUP	1013
UDB_CHANGE_PASSWORD	1014
UDB_SET_PASS_STATUS	1015
UDB_GET_PASS_STATUS	1016
UDB_USER_ENUM	1017
UDB_USER_GET_INFO	1018
UDB_USER_PAP_CHECK	1019
UDB_USER_PROF_ASSIGN	1020
UDB_USER_PROF_COUNT	1021
UDB_USER_PROF_GET	1022
UDB_USER_CHAP_CHECK	1023
UDB_USER_CHECK_EXPIRY	1024
UDB_USER_SET_INFO	1025
UDB_AUTHENTICATE_USER	1026
UDB_SEND_RESPONSE	1027
UDB_SET_PASSWORD	1028

Table 5 Descriptive Request Text and Request Code (continued)

Request Text	Request Code
UDB_USER_LOCN_CHECK	1029
UDB_SET_VALUE	1030
UDB_GET_VALUE	1031
UDB_GET_NEXT_VALUE	1032
UDB_DEL_VALUE	1033
UDB_FIND_VALUE	1034
UDB_GET_VALUE_BY_NAME	1035
UDB_LOG	1040
UDB_SET_APPDATA	1041
UDB_GET_APPDATA	1042
UDB_DEL_DB	1043
UDB_AVERT_LOG	1044
UDB_DIR_CREATE	1050
UDB_FILE_CREATE	1051
UDB_FILE_WRITE	1052
UDB_FILE_READ	1053
UDB_FILE_CLOSE	1054
UDB_FILE_EXISTS	1055
UDB_FILE_APPEND	1056
UDB_FILE_SET_PTR	1057
UDB_USER_LIST_ADD	1070
UDB_USER_LIST_DEL	1071
UDB_USER_LIST_GET	1072
UDB_USER_LIST_COUNT	1073
UDB_USER_LIST_UPDATE	1074
UDB_USER_ALIAS_SET	1080
UDB_USER_ALIAS_DEL	1081
UDB_USER_ALIAS_VALID	1082
UDB_START_TRANSACTION	1090
UDB_END_TRANSACTION	1091
UDB_KICK_SYNC_TX	1092
UDB_KICK_SYNC_RX	1093
UDB_EXCHANGE_SYNC_INFO	1094
UDB_AQUIRE_IP_ADDRESS	1095
UDB_VALIDATE_PASSWORD	1096
UDB_EXTRACT_AGING_DATA	1097

Table 5 *Descriptive Request Text and Request Code (continued)*

Request Text	Request Code
UDB_AUTH_FAILED	1098
UDB_RESET_USER_PASSWORD_AGING_DATA	1099
UDB_GET_AGING_INFO	1100
UDB_DO_BACKUP_NOW	1101
UDB_AQUIRE_CALLBACK	1102
UDB_GET_AGING_LIMIT	1103
UDB_PURGE_NAS	1104
UDB_SEND_FAKE_STOPS	1105
UDB_SERVICE_CONTROL	1106
UDB_RESET_GROUP	1107
UDB_SET_ENABLE_PASS_STATUS	1108
UDB_UPDATE_AGING_POLICY	1109
UDB_ADD_HOST	1110
UDB_DEL_HOST	1111
UDB_GET_HOST	1112
UDB_UPDATE_HOST	1113
UDB_ADD_PROXY	1114
UDB_DEL_PROXY	1115
UDB_ADD_PROXY_TARGET	1116
UDB_ADD_NDG	1117
UDB_DEL_NDG	1118
UDB_GET_NDG_ID	1119
UDB_SET_USER_FEATURE_FLAG	1120
UDB_GET_USER_COUNTER	1121
UDB_RESET_USER_COUNTER	1122
UDB_RESET_GROUP_USERS_COUNTER	1123
UDB_GET_FIRST_QUOTA_TYPE	1124
UDB_GET_NEXT_QUOTA_TYPE	1125
UDB_SET_QUOTA	1126
UDB_HAS_USER_QUOTA_EXHAUSTED	1127
UDB_SHARED_PROFILE	1128
UDB_ADD_UDV	1140
UDB_DEL_UDV	1141
UDB_GET_VID_FROM_IETF	1142
UDB_ADD_UDV_VSA	1143
UDB_ADD_UDV_VSA_ENUM	1144

Table 5 *Descriptive Request Text and Request Code (continued)*

Request Text	Request Code
UDB_ADD_UDV_VSA_PROFILE	1145
UDB_SET_REP_DIRTY_FLAG	1150
UDB_USER_COMMIT_NOW	1151
UDB_POLICY_CREATE_CONTEXT	1152
UDB_USER_REMOVE_DYNAMIC	1153

Table 6 lists the descriptive text in the CSAuth diagnostic logs and the corresponding status code.

Table 6 *Descriptive Status Text and Request Code*

Status Description	Status Code
UDB_BASE_ERR	1000
UDB_DB_NOT_OPEN	1001
UDB_INVALID_ENTRY	1002
UDB_CANT_CREATE_MAP	1003
UDB_CANT_CREATE_VIEW	1004
UDB_CANT_OPEN_INDEX	1005
UDB_DB_IS_OPEN	1006
UDB_SIZE_MISMATCH	1007
UDB_CANT_OPEN_FILE	1008
UDB_CRC_FAILED	1009
UDB_CANT_INIT_INDEX	1010
UDB_INVALID_DATA	2011
UDB_CANT_GROW_FILE	1012
UDB_USER_INVALID	2013
UDB_DUPLICATE_NAME	1014
UDB_INVALID_PASSWORD	2015
UDB_IPC_DATA_INVALID	1016
UDB_FEATURE_NOT_READY	1017
UDB_SERVER_BUSY	1018
UDB_REGISTRY_READ_FAIL	1019
UDB_UNKNOWN_VARIABLE	2020
UDB_NO_FILE_HANDLES	1021
UDB_DIR_CREATE_FAILED	1022
UDB_FILE_WRITE_FAILED	1023
UDB_FILE_READ_FAILED	1024
UDB_INVALID_DIR_NAME	1025
UDB_INVALID_FILE_NAME	1026

Table 6 *Descriptive Status Text and Request Code (continued)*

Status Description	Status Code
UDB_MALLOC_FAIL	1027
UDB_INVALID_HANDLE	1028
UDB_USER_NOT_OWNER	1029
UDB_CANT_REBUILD_INDEX	1030
UDB_CANT_REMOVE_OLD_DB	1031
UDB_USER_REMOVED	2032
UDB_NO_VARIABLE	1033
UDB_PASSWORD_DISABLED	2034
UDB_FILE_SET_PTR_FAILED	1035
UDB_USER_LICENCE_LIMIT	1036
UDB_APP_NOT_LICENSED	1037
UDB_BAD_SECRET	1038
UDB_DB_VERSION_MISMATCH	1039
UDB_DIR_REMOVE_FAILED	1040
UDB_CANT_ASSIGN_PROFILE	1041
UDB_LOGGER_OFFLINE	1042
UDB_CANT_ACCESS_USERLIST	1043
UDB_SESSION_COUNT_EXCEEDED	2044
UDB_PASSWORD_REQUIRED	2045
UDB_CHALLENGE_REQUIRED	2046
UDB_NO_SESSION	1047
UDB_INTERNAL_ERROR	1048
UDB_BAD_TODDOW	2049
UDB_CANT_LOCK_RECORD	1050
UDB_NT_DIALIN_REQUIRED	2051
UDB_NT_PW_WRONG	2052
UDB_NT_AC_RESTRICTED	2053
UDB_NT_TOD_DOW	2054
UDB_NT_PW_EXPIRED	2055
UDB_NT_AC_DISABLED	2056
UDB_NT_BAD_WORKSTATION	2057
UDB_NT_UNKNOWN_ERR	1058
UDB_NT_PASS_CHANGE	2059
UDB_NT_NO_DOMAIN	2060
UDB_NT_AC_LOCKED	2061
UDB_NT_NO_BROWSER	2062

Table 6 Descriptive Status Text and Request Code (continued)

Status Description	Status Code
UDB_INVALID_CHAP_PW	2063
UDB_INVALID_ARAP_PW	2064
UDB_INVALID_TOKEN_PW	2065
UDB_INVALID_UNIX_PW	2066
UDB_TOKEN_SERVER_DOWN	1067
UDB_USER_CLI_FILTERED	2068
UDB_NO_SENDAUTH_PW	1069
UDB_NO_TOKENSRV	1070
UDB_NT_NO_LOGON_NOT_GRANTED	2071
UDB_CANT_START_TRANSACTION	1072
UDB_VARDB_NOT_OPEN	1073
UDB_NOT_IN_CACHE	1074
UDB_CANT_OPEN_ODBC_DB	1075
UDB_DLL_MISMATCH	1076
UDB_NOT_INSTALLED	1077
UDB_CHAP_ENFORCED	2078
UDB_ACCESS_DENIED	2079
UDB_REPLICATION_DENIED	1080
UDB_FAILED_TO_AQUIRE_IP_ADDR	1081
UDB_PASSWORD_DEAD	2082
UDB_PASSWORD_STATE_NOT_ACCESSIBLE	1083
UDB_PASSWORD_AGE_CHECK_FAILED	1084
UDB_NEW_PASSWORD_NOT_GOOD	2085
UDB_FAILED_TO_EXTRACT_DATA	1086
UDB_EXTERN_DB_ERROR	2087
UDB_BACKUP_FAILED_TO_START	1088
UDB_FAILED_TO_AQUIRE_CALLBACK	1089
UDB_FAILED_TO_PERFORM_SERVICE_OP	1090
UDB_TIME_OUT_WAITING_TO_START_AUTH	1091
UDB_AUTH_NOT_SUPPORTED_BY_EXT_DB	2092
UDB_CACHED_TOKEN_REJECTED	2093
UDB_TOKEN_PIN_CHANGED	2094
UDB_INVALID_MSCHAP_PW	2095
UDB_INVALID_EXT_CHAP_PW	2096
UDB_INVALID_EXT_ARAP_PW	2097
UDB_INVALID_EXT_MSCHAP_PW	2098

Table 6 Descriptive Status Text and Request Code (continued)

Status Description	Status Code
UDB_INVALID_EXT_USER	2099
UDB_NT_AC_EXPIRED	2100
UDB_AUTH_DENIED_DUE_TO_VOIP	2101
UDB_MALFORMED_USERNAME	2102
UDB_CANT_OPEN_HOST_DB	1103
UDB_CANT_OPEN_PROXY_DB	1104
UDB_CANT_OPEN_NDG_DB	1105
UDB_HOST_DB_FAILURE	1106
UDB_PROXY_DB_FAILURE	1107
UDB_NDG_DB_FAILURE	1108
UDB_INVALID_COUNTER_TYPE	1109
UDB_EXTERN_DB_TRANSIENT_ERROR	1110
UDB_INVALID_QUOTA_INDEX	1111
UDB_USAGE_QUOTA_EXCEEDED	2112
UDB_NT_CHANGE_PASS_FAILED	2113
UDB_CANT_LOAD_DLL	1114
UDB_EXTN_DLL_REJECTED	2115
UDB_INVALID_EXT_EAP_PW	2116
UDB_EAP_METHOD_NOT_SUPPORTED	2117
UDB_EAP_TLS_PASS_HS_USER_NOT_FOUND	2118
UDB_EAP_NO_MATCH_NAME_IN_CERT	2119
UDB_EAP_TLS_HANDSHAKE_FAILED	2120
UDB_EAP_IGNORE	2121
UDB_SUPPLIER_NOT_CONFIGURED	2122
UDB_UDV_CONFIG_ERROR	1123
UDB_USER_FOUND	2124
UDB_USER_NOT_FOUND	2125
UDB_EAP_FAILED	1126
UDB_MISSING_MPPE_DATA	2127
UDB_EAP_MACHINE_AUTH_DISABLED	2128
UDB_NT_NO_REMOTE_AGENT	2129
UDB_EAP_FAST_PAC_PROVISIONING	2130
UDB_EAP_FAST_USER_AND_IID_NOT_MATCH	2131
UDB_EAP_FAST_PAC_INVALID	2132
UDB_EAP_FAST_INBAND_NOT_ALLOWED	2133
UDB_EAP_FAST_INVALID_MASTER_KEY	2134

Table 6 Descriptive Status Text and Request Code (continued)

Status Description	Status Code
UDB_GROUP_DISABLED	2135
UDB_AVERT_NO_MAPPING	2136
UDB_EAP_PASSWORD_CHANGE_DISABLED	2137
UDB_AVERT_PROCEED_TO_UUP	2138
UDB_AVERT_LOCAL_POLICY_FAILED	2139
UDB_AVERT_EX_POLICY_FAILED	2140
UDB_AVERT_GENERAL_FAILURE	2141
UDB_ACCESS_DENIED_FAST_REC_NO_USER	2142
UDB_ACCESS_DENIED_MAR_RESTRICTION	2143
UDB_AVERT_UNKNOWN_ATTRIBUTE	2144
UDB_AUTH_PROTOCOL_NOT_ALLOWED	2145
UDB_EAP_FAST_ANON_INBAND_NOT_ALLOWED	2146
UDB_AUDIT_BAD_RESPONSE	2147
UDB_AUDIT_TOO_MANY_ROUND_TRIPS	2148
UDB_POSTURE_VALIDATION_FAILED	2149
UDB_MAC_AUTH_BYPASS_NOT_ALLOWED	2150
UDB_ACCESS_DENIED_NO_SERVICE	2151
UDB_AUTHORIZATION_REJECT	2152
UDB_PV_FAILED_NO_SERVICE	2153
UDB_LOCAL_USER_HAS_EXT_DB_AUTH	2154
UDB_SERVICE_EXT_DB_NOT_ALLOWED	2155
UDB_NT_LOGON_FAILURE	2156
UDB_MAC_AUTH_BYPASS_GROUP_DISABLE	2157
UDB_BADLY_FORMED_DACL_RQ	2158
UDB_INTERNAL_DACL_ERROR	2159
UDB_DACL_ASSIGN_ERROR	2160
UDB_INTERNAL_RAC_ERROR	2161
UDB_RAC_MISSING_ERROR	2162
UDB_AUDIT_RECIEVED_ERROR	2163
UDB_AUDIT_SERVER_UNREACHEABLE	2164
UDB_AUDIT_PARSE_ERROR	2165
UDB_EXT_POLICY_VER_ERROR	2166
UDB_EXT_POLICY_CONN_ERROR	2167
UDB_EXT_POLICY_AUTH_ERROR	2168
UDB_EXT_POLICY_TIMEOUT_ERROR	2169
UDB_ERR_PROFILE_TOO_BIG	1170

Table 6 Descriptive Status Text and Request Code (continued)

Status Description	Status Code
UDB_EXT_POLICY_CONN_ERROR_CA_UNKNOWN	2171
UDB_BASE_WARN	1000
UDB_ALREADY_OPEN	1001
UDB_PASSWORD_EXPIRED	1002
UDB_UNKNOWN_PASS_STATUS	1003
UDB_UDB_VALUE_OVERWRITE	1004
UDB_BUFFER_TOO_SMALL	1005
UDB_SIZE_SMALLER	1006
UDB_USER_NOT_ALIAS	1007
UDB_NO_MORE_QUOTA_TYPES	1008

Line Numbers in Diagnostic Logs

All ACS diagnostic log files now contain the correct line number of the source code that generated the error. In previous versions of ACS, the dzlog function contained the hard-coded source code line number which was populated to the ACS diagnostic log.

Improved EAP Code Debug Messages

All EAP debug messages are now reported to the CSAuth diagnostic log.

Product Documentation

Table 7 lists the product documentation for ACS 4.1.3.

Table 7 Product Documentation

Document Title	Description
<i>Documentation Guide for Cisco Secure ACS 4.1</i>	<ul style="list-style-type: none"> Printed document with the product. PDF on the product CD-ROM. On Cisco.com: http://www.cisco.com/en/US/products/sw/secursw/ps5338/prod_release_notes_list.html
<i>Release Notes for Cisco Secure ACS 4.1</i>	New features, documentation updates, and resolved problems. Available on Cisco.com: http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_release_notes_list.html
Product online help	Help topics for all pages in the ACS web interface. Choose an option from the ACS menu; the help appears in the right pane.

Table 7 Product Documentation (continued)

Document Title	Description
<i>User Guide for Cisco Secure ACS 4.1</i>	<p>ACS functionality and procedures for using the ACS features. Available in the following formats:</p> <ul style="list-style-type: none"> • By clicking Online Documentation in the ACS navigation menu. The user guide PDF is available on this page by clicking View PDF. • PDF on the ACS Recovery CD-ROM. • On Cisco.com: http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_user_guide_list.html
<i>Supported and Interoperable Devices and Software Tables for Cisco Secure ACS 4.1</i>	<p>Supported devices and firmware versions for all ACS features. Available on Cisco.com:</p> <p>http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_device_support_tables_list.html</p>
<i>Installation and User Guide for User Changeable Passwords 4.1</i>	<p>Installation and user guide for the user-changeable password add-on. Available on Cisco.com:</p> <p>http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_installation_guides_list.html</p>
<i>Configuration Guide for Cisco Secure ACS 4.1.</i>	<p>Provides provide step-by-step instructions on how to configure and deploy ACS. Available on Cisco.com:</p> <p>http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_installation_and_configuration_guides_list.html</p>
<i>Installation Guide for Cisco Secure ACS 4.1 Windows</i>	<p>Details on installation and upgrade of ACS software and post-installation tasks. Available in the following formats:</p> <ul style="list-style-type: none"> • PDF on the ACS Recovery CD-ROM. • On Cisco.com: http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_installation_guides_list.html
<i>Installation Guide for Cisco Secure ACS Solution Engine 4.1</i>	<p>Details on ACS SE 1112 and ACS SE 1113 hardware and hardware installation, and initial software configuration.</p> <ul style="list-style-type: none"> • PDF on the ACS Recovery CD-ROM. • Available on Cisco.com: http://www.cisco.com/en/US/products/sw/secursw/ps5338/prod_installation_guides_list.html

Table 7 Product Documentation (continued)

Document Title	Description
<i>Regulatory Compliance and Safety Information for Cisco Secure ACS Solution Engine 4.1</i>	Translated safety warnings and compliance information. <ul style="list-style-type: none"> Printed document with the product. PDF on the ACS Recovery CD-ROM. Available on Cisco.com: http://www.cisco.com/en/US/products/sw/secursw/ps5338/prod_installation_guides_list.html.
<i>Installation and Configuration Guide for Cisco Secure ACS Remote Agents</i>	Installation and configuration guide for ACS remote agents for remote logging. <ul style="list-style-type: none"> PDF on the ACS Recovery CD-ROM. Available on Cisco.com: http://www.cisco.com/en/US/products/sw/secursw/ps5338/products_installation_and_configuration_guides_list.html

Known Caveats in ACS for Windows and the Solution Engine 4.1.3

Table 8 contains known caveats in ACS for Windows and the Solution Engine 4.1. 3.

Table 8 Known Caveats in ACS Windows and the Solution Engine 4.1.3

Bug ID	Summary	Explanation
CSCdv86708	DEL/HTTP Port Allocation is not replicated.	<p>Symptom Changes to HTTP Port Allocation settings do not appear to replicate. After the HTTP Port Allocation settings are changed on the Access Policy Setup page in the Administration Control section on the primary Cisco Secure ACS server and replication succeeds, the secondary Cisco Secure ACS server does not display the changes to the HTTP Port Allocation settings in the HTML interface.</p> <p>Workaround .The changes to the HTTP Port Allocation settings do replicate successfully; however, to see the changes on the secondary Cisco Secure ACS server, restart the CSAdmin service.</p>
CSCeg52536	Failed PEAP authentication not shown up in ACS logs.	<p>Symptom PEAP-MS-CHAPv2 with Machine authentication. ACS does not show any failure in the logs nor sending a radius reject if a client machines which does not belong to the AD domain at all tries to authenticate. Looking in the auth.log, it shows correctly that windows authentication fails.</p> <p>Workaround None.</p>

Table 8 Known Caveats in ACS Windows and the Solution Engine 4.1.3

Bug ID	Summary	Explanation
CSCeh52700	AD expired-user passed EAP-TLS authentication; should be rejected.	<p>Symptom EAP-TLS authentication will still pass for users in Active Directory even if their account has expired - no error is given from ACS.</p> <p>Conditions EAP-TLS authentication of users in Active Directory running in Windows 2000 environment.</p> <p>Workaround None.</p>
CSCeh86479	CSUtil import -85 errors to be changed to info msg-not error.	<p>Symptom The CSutil utility with the options -n, -g, and -u may print an ODBC error message similar to the following:</p> <pre>ODBC Error. Message=[Sybase][ODBC Driver][Adaptive Server Anywhere]Communication error, SqlState=08S01, NativeError=-85</pre> <p>Workaround None. This would only happen when running csutil from Remote Services. This is really an informational message, and can be ignored.</p>
CSCse25423	Bypass Info & extBDinfo fields in the passed\failed reports are empty.	<p>Symptom Bypass Info & extBDinfo fields in the passed authentication \failed attempts page in reports and activity are</p> <p>Conditions</p> <ol style="list-style-type: none"> 1. Select the Bypass Info & extBDinfo attributes in logging page under system configuration page for both passed authentication \failed attempts. 2. Submit 3. Perform MAB request. <p>Workaround None.</p>
CSCsf11087	Cisco:PA: attributes not showing in Passed Auth rpt for Linux client.	<p>Symptom Cisco:PA attributes are not showing up in the Passed Authentication Report for a Linux client with CTA 2.1.0.10 installed. The attributes are showing up in the AUTH.log file and are showing up for a Win XP client on the same network.</p> <p>Conditions</p> <ol style="list-style-type: none"> 1. In System Configuration > Logging > Passed Authentication select Cisco:PA attributes. 2. Click Submit. 3. Perform authentication using Linux client with CTA. 2.1.0.10 4. Check pass authentication log in reports and activity page. <p>Workaround None.</p>

Table 8 Known Caveats in ACS Windows and the Solution Engine 4.1.3

Bug ID	Summary	Explanation
CSCsf16737	CSAuth, CSAdmin, CSRADIUS, CSTacacs are not started up after reboot.	<p>Symptom After a system reboot, the following Services are not started up when Windows service, Windows Firewall/Internet Connection Sharing (ICS) is started:</p> <ul style="list-style-type: none"> • CSAuth • CSRADIUS • CSTacacs • CSAdmin <p>Workaround Disable Windows Service Windows Firewall/Internet Connection Sharing (ICS). To do so, Start > Run. Enter <i>services.msc</i> and press OK. In the Services dialog box, scroll to Windows Service Windows Firewall/Internet Connection Sharing (ICS). Right click, and select Properties. In the Startup type: box change Automatic to Disabled.</p> <p>Note You can also manually start each service.</p>
CSCsg02005	CSMon utilizes 100% CPU - while trying to communicate with SMTP Server.	<p>Symptom ACS hits 100% CPU load on CSMon.</p> <p>Conditions ACS or ACS-SE running 3.3.3.11 with e-mail notification on.</p> <p>Workaround Turn off e-mail notification.</p>
CSCsg26367	Replication error on ACS 4.0. Slave does not apply changes.	<p>Symptom ACS 4.0.1(27) master is sending the changed files on the slave, only the skipped files are shown.</p> <p>Logs confirm the reception of the files (RQ1051, RQ1052, RQ1054). CSMon kicks in after the configured replication timeout value (5 minute default), as configured, restarting the CSAuth service. So Slave is not showing the files that master says it has sent, then more or less hangs until restarted by CSMON. Master is not recovering from the loss of communication with slave:</p> <pre>AUTH 09/14/2006 00:22:48 E 1017 4268 Comms lib:Tcp_Connect: Failed to connect to 172.29.128.133, sock error 10061 AUTH 09/14/2006 00:22:48 E 1017 4268 Comms lib:Transport connect failed AUTH 09/14/2006 00:22:48 E 1017 4268 Comms lib:Bad endpoint address (0x00000000) trapped at V:\ismg_israel_acs\Acs\EndPoint\Core\endpoint.c:1788</pre> <p>Conditions Replications over a WAN connection.</p> <p>Workaround None. Logs show that when the replication is retried, it is usually successful.</p>

Table 8 Known Caveats in ACS Windows and the Solution Engine 4.1.3

Bug ID	Summary	Explanation
CSCsg71852	ACS ignoring RADIUS request, may not be fixed.	<p>Symptom 3750 Switch with NAC-802.1x authentications re-uses the same Radius ID for different users when ACS takes more time to reply for the original radius request.</p> <p>Conditions This behavior was observed in 12.2(25)SEE2.</p> <p>Workaround None.</p>
CSCsg99626	CSDBSync crashes - faulting module odbcs32.dll.	<p>Symptom CSDBSync crashes when enter CSDBSync.exe -run, and RDBMS sync doesn't occur. drwtsn32.log and user.dmp are generated.</p> <p>Conditions The customer executed the batch file like below: It seemed CSDBSync didn't stop because there was no Service stop event in CSDBSync.log like below.</p> <pre> CSDbSync 12/02/2006 23:30:41 A 0000 4460 Transaction processing invoked manually CSDbSync 12/02/2006 23:30:47 A 0000 4828 ===== Service started ===== </pre> <p>Normally, the log is like below;</p> <pre> CSDbSync 12/01/2006 23:30:40 A 0000 4700 Service stop requested <<<HERE! CSDbSync 12/01/2006 23:30:43 A 0000 4164 Transaction processing invoked manually CSDbSync 12/01/2006 23:30:51 A 0000 2160 ===== Service started ===== </pre> <p>Workaround None.</p>
CSCsh12148	Cannot reinstall CSA after removing it.	<p>Symptom This problem occurs only on the Quanta S27 appliance (1113) when trying to reinstall the CSA after removing it using the rollback function. The CSA rollback succeeds; but before the appliance reboots the following error appears: "The process cannot access the file because it is being used by another process." Then, after the appliance reboots, an error message appears when trying to reinstall CSA.</p> <p>Workaround None.</p>
CSCsh29345	ACS 4.0 - Unable to delete server under Network Configuration.	<p>Symptom Unable to delete a ACS Server(s) from the Network Configuration > AAA Servers. After selecting the server to delete and then clicking on Delete > Apply, the ACS will respond with, "Are you sure you wish to delete this AAA Server?" If you select Yes, nothing happens.</p> <p>Conditions Saw this issue on a ACS Windows server running 4.0(1) Build 27. This issue was duplicated easily in the lab by restoring the customer database to an existing ACS server.</p> <p>Workaround Backup the customer database and send to DE. Delete the server manually with an external tool.</p>

Table 8 Known Caveats in ACS Windows and the Solution Engine 4.1.3

Bug ID	Summary	Explanation
CSCsh48625	ACS radius error 2162 - switch isn't sent RAC/DACL client recvs token.	<p>Symptom ACS 4.0.1(27) was upgraded to 4.1.1.23 and none of the NAC features were imported. The network access profiles and posture validation rules missing from the previous version.</p> <p>Conditions Upgrade to 4.1.1.23 when NAP and Posture validation configured</p> <p>Workaround None.</p>
CSCsh77806	EAP-TLS will fail authentication if name contains forward slash /.	<p>Symptom EAP-TLS users authenticating to ACS (and in turn to Active Directory) fail authentication if the Distinguished Name returned from the LDAP server contains a forward slash. Logs from the ACS will cite this as a permissions issue and do not make it clear that it's the format of the username at fault.</p> <p>Conditions Distinguished Name: CN=Lastname\, Firstname Department1/Department2,OU=... but presumably will be seen in any instance in which the Distinguished Name contains a forward slash. Windows Domain controllers will allow the forward slash as a part of the username and do not appear to use an escape character prior to the forward slash (the above example does include an escape character prior to the comma). The issue is possibly a bug in Microsoft's handling of the forward slash character. Since this character is used as a separator in LDAP, the LDAP replies back should be padded with a backslash prior to the forward slash.</p> <p>Workaround Avoid use of forward slashes in user names authentication via EAP-TLS.</p>
CSCsi42199	ACS 4.1 can fail to restore configuration on Windows 2003 R2.	<p>Symptom ACS may fail to shut down the csadmin service during a restore of an ACS database. Subsequent reboots of the ACS server will result in all ACS services failing to start.</p> <p>Conditions Issue has only been reproducible with:</p> <ul style="list-style-type: none"> • Specific configurations • Windows 2003 R2 • ACS 4.1.1.23 and subsequent codes <p>Workaround Use Windows 2003 or Windows 2000 server rather than Windows 2003 R2. ACS Solution Engines are not affected by this issue.</p>

Table 8 Known Caveats in ACS Windows and the Solution Engine 4.1.3

Bug ID	Summary	Explanation
CSCsi50359	Enable authentications are rejected with Internal Error message.	<p>Symptom Users on CatOS switches are denied enable authentication, even though they're entering the correct password. Login authentications work correctly.</p> <p>Conditions This has been observed on ACS 4.1.1(23). Other versions may be affected as well. The problem occurs when the users have TACACS+ Enable Control set to Use Group Level Setting.</p> <p>Workaround Configure the user to have a max privilege level setting under Max Privilege for any AAA Client.</p>
CSCsi57134	QoS values incorrect for WLC	<p>Symptom QoS values incorrect on WLC after pushing override from ACS.</p> <p>Workaround .Obtain patch to update the values in ACS database.</p>

Resolved Caveats in ACS for Windows and the Solution Engine 4.1.3

Table 9 contains the resolved caveats for the ACS 4.1.3 release. Check the Bug Navigator on Cisco.com for any resolved bugs that might not appear here.

Table 9 Resolved Caveats in ACS Windows and the Solution Engine 4.1.3

Bug ID	Summary
CSCeb43948	Could not generate valid Password with password length => 9.
CSCed45731	ACS logs should indicate level of logging.
CSCee65661	Need the NoCacheUser feature for unknown user policy.
CSCeh42116	EAP-TLS Machine Authentication fails when AD PDC emulator down.
CSCsd12551	IP pools disappear occasionally from Group Setup/Edit Settings.
CSCsd20149	After initial config from Recovery CD, no GUI access.
CSCsd63894	ACS does not respond with the same ip address for RADIUS.
CSCsd95346	VSA definition for Total Control HiperARC card accounting attributes.
CSCsd97599	After Replication the Dynamic user still added as user in Group-Setup.
CSCsd98589	Authentications fail when NIC reconnected after reboot.
CSCse49827	ACS Remote Agent fails users with too many groups.
CSCsf28775	Expired accounts are incorrectly reported.
CSCsf30675	Monitoring audit log messages contain empty value for the AAA-server attributes.
CSCsf98129	Client host name in ACS cannot be deleted.

Table 9 **Resolved Caveats in ACS Windows and the Solution Engine 4.1.3 (continued)**

Bug ID	Summary
CSCsg13994	Upgrade from 4.0.1.27 to 4.1.1.23, no feedback from NAC.
CSCsg14329	ACS 4.0 and semi-colon separator in cisco-av-pair RADIUS attributes.
CSCsg19044	ACS Syslog and ODBC configurations cannot display Trend Micro, McAfee, and Qualys in Reports and Activities.
CSCsg24465	Update OS to support Daylight Saving Time for the 2007 energy bill.
CSCsg32883	Feature: Authentications from ACS not hardcoded to workstation CISCO.
CSCsg37381	ACS authentication stops intermittently with - Unknown error code: -1018.
CSCsg62393	Wrong shared key, if device is added as tacacs and radius in same NDG.
CSCsg62438	ACS can not handle more than 4 EAP-Message attributes in radius request.
CSCsg62459	Unable to delete CA Cert from CA list.
CSCsg87232	Enhancement: Add Cisco-AvPair to VOIP accounting records.
CSCsg89656	CSAuth does not shutdown cleanly in some ACS 4.0 installs.
CSCsg96534	ACS support for Windows 2003 R2 needs clarification.
CSCsg97429	TACACS+ Command Accounting does not work in ACS 4.1(1) Build 23.
CSCsg99542	Line number in ACS log files should be corrected.
CSCsh02206	Textual Commands and Error Codes enhancement.
CSCsh02215	Session Id to Diagnostic Logs.
CSCsh05964	ACS 4.1: Separate enable password fails when unix password type used.
CSCsh13994	ACS 4.1: Separate enable password fails when unix password type used.
CSCsh18732	Generic EAP code - debug messages should appear in release mode.
CSCsh18742	ACS should silently discard packet when external ODBC DB not available.
CSCsh21987	Feature: ACS should have ability to send access-reject to unknown EAP.
CSCsh24710	Shell Commands Authorization Set part of commands are effective.
CSCsh32888	Separate enable password does not work after ACS upgrade to 4.1.
CSCsh39305	Administrative access policy does not take effect after replication.
CSCsh43814	No users at IP x.x.x.x.
CSCsh48625	ACS radius error 2162 - switch isn't sent RAC/DACL client recvs token.
CSCsh62641	MAC authentication causes internal errors (radius-authentication).
CSCsh65197	CSAuth crashes when username has a comma.
CSCsh69160	EAP FAST1: ACS does not provide the supplicant with reason of rejection.
CSCsh74140	Loss of external database breaks NAD AAA redundancy concept.
CSCsh75933	EAP FAST configuration changes is not logged to Administrators report.
CSCsh77651	Anti-Virus is locking DB file.
CSCsh84447	Limited administrator sees first page empty if trying to list all users.
CSCsh87466	Authentication failure on first login after remote agent restart.
CSCsh89335	ACS EAP-FAST Replication fails generating server not responding error.

Table 9 **Resolved Caveats in ACS Windows and the Solution Engine 4.1.3 (continued)**

Bug ID	Summary
CSCsh91761	ACS: XSS vulnerability via search facility in online help.
CSCsi13371	Deleting the CRLs downloaded from the CDP in CRL folder - via ACS GUI.
CSCsi18979	ACS Windows and SE missing Juniper VSA.

Installation Notes for ACS 4.1.3

This section contains installation information for ACS 4.1.3.

- [Installing ACS 4.1.3 for Windows, page 25](#)
- [System Requirements ACS 4.1.3 for Windows, page 25](#)
- [Installing ACS 4.1.3 for Windows, page 25](#)
- [Upgrade Path for ACS Solution Engine 4.1.3, page 25](#)
- [Installing the ACS Solution Engine 4.1.3, page 26](#)

Upgrade Path ACS 4.1.3 for Windows

Cisco tested the upgrade to ACS for Windows Server 4.1.3 from release 4.1.1.23. For ACS 4.1 upgrade paths, refer to the *Installation Guide for Cisco Secure ACS 4.1 Windows*.



Note

ACS 4.1.3 is available only as an upgrade from ACS 4.1.1. You do not use a boot or installation CD to install ACS 4.1.3.



Note

Cisco does not support the upgrade from ACS 4.1.2 to ACS 4.1.3.

System Requirements ACS 4.1.3 for Windows

The system requirements for ACS 4.1.3 are the same as for ACS 4.1. For information on supported operating systems and web browsers, refer to the *Installation Guide for Cisco Secure ACS 4.1 Windows*.

Installing ACS 4.1.3 for Windows

You must have ACS 4.1 installed before you install ACS 4.1.3. ACS 4.1.3 is available through the Cisco TAC only for upgrading existing ACS software deployments. The installation instructions for ACS 4.1.3 are the same as for ACS 4.1. For information about installing ACS, refer to the *Installation Guide for Cisco Secure ACS 4.1 Windows*.

Upgrade Path for ACS Solution Engine 4.1.3

Cisco tested the upgrade to ACS Solution Engine 4.1.3 from release 4.1. For ACS 4.1 upgrade paths, refer to the *Installation Guide for Cisco Secure ACS Solution Engine 4.1*.

**Note**

You do not use a boot CD to install ACS 4.1.3. You must upgrade from ACS 4.1.1.23.

Installing the ACS Solution Engine 4.1.3

The 1113 Solution Engine has ACS 4.1 pre-installed. The ACS 4.1.3 Solution Engine upgrade package is available through the TAC only for upgrading existing ACS software deployments. The installation instructions for ACS 4.1.3 Solution Engine are the same as ACS 4.1. For information about installing ACS, refer to the *Installation Guide for Cisco Secure ACS Solution Engine 4.1*.

CCVP, the Cisco Logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0704R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.

Printed in the USA on recycled paper containing 10% postconsumer waste.