



APPENDIX A

Error Codes

Revised: November 11, 2009, OL-12555-02

Table A-1 provides an alphabetized list of the ACS error codes. For complete information on error codes, see the Microsoft website.

Table A-1 ACS 4.x Error Codes

Error Codes	Possible Root Cause	Resolution
ACS Failed Attempts:EAP type not configured Username = "anonymous"	The Allow Anonymous In-Band PAC Provisioning option is not enabled.	Check whether a valid certificate has been installed on the ACS server as the ACS server must have the correct certificate installed.
A valid EAP-FAST master key does not exist; make sure EAP-FAST replication is operational	Failed to get the master key for Protected Access Credentials (PAC) construction.	Check the EAP-FAST replication configuration.
Access denied because no profile matched	The authentication request does not match any NAP.	Check the NAP configuration.
Access denied to Voice-Over-IP group	If the user is present in the Voice-Over-IP (VOIP) group, the authentication fails.	Enable access to a VOIP group; or, assign a new group for the user.
Access denied: fast-reconnect was successful, but user was not found in cache	Fast-Reconnect is enabled and the dynamic user is removed from ACS.	Disable Fast-Reconnect and try authenticating. Re-enable Fast Reconnect.
Access rejected due to authorization policy in the network access profiles	The request for NAP authorization policy failed.	Check the NAP configuration policy.
ACS account disabled	The administrator has disabled the account.	The administrator must enable the account.
ACS ARAP password invalid	Incorrect ARAP password.	Provide the correct ARAP password.
ACS CHAP password invalid	The password provided for CHAP is invalid.	Provide a valid password.
ACS login time restriction	The user is denied access at a specific time.	Change the login time restriction or ensure that the authentication occurs only during the specified time.

Table A-1 ACS 4.x Error Codes

Error Codes	Possible Root Cause	Resolution
ACS MSCHAP password is invalid	The password provided for MS-CHAP is invalid.	Provide a valid password.
ACS password invalid	Invalid password.	Use a valid password.
ACS User Account Expired	The user account has expired.	Create a new user account.
ACS User exceeded max sessions	The ACS user has exceeded the maximum session.	Wait for the current session to end and try again.
ACS user unknown	The user is not present in the ACS internal DB.	Create the user in the ACS internal DB.
ACS user's password has expired	Configure a new password.	Configure a new password.
ACS account disabled	The administrator has disabled the account.	The administrator must enable the account.
Audit Server returned an error	The audit server returned an error.	Check the audit server configuration.
Authentication protocol is not allowed for this network access profile	Protocol is not allowed for the current NAP.	Check the NAP configuration and modify it, if required.
Authentication session invalidated	The session does not exist.	Check the NAS configuration and open a new session.
Authentication type not supported by ExternalDB	The external DB does not support the specified authentication type.	Use an authentication that the external DB supports.
Badly formed Downloadable ACL request from device	The download request for ACL contains a missing Message-Authenticator or AAA: event VSA.	Use the correct ACL format.
Cached token rejected/expired	The cached token has expired or is rejected.	Use a new token.
Certificate name or binary comparison failed	Machine certificates do not match or the name in the certificate and the user account do not match.	Use correct certificates.
CLI user unknown	The given CLI user is unknown.	Use a valid user name.
Could not access password aging state in ACS internal DB	Unable to access the password state after age check.	Restart ACS and try again.
Could not check password aging state in ACS internal DB	Unable to check the password-aging state in the ACS internal DB.	Check the ACS configuration for password aging.
Could not communicate with external policy server - authentication failure	Unable to reach the external policy server; or, the server is down.	Check the connection to the external policy server.
Could not communicate with external policy server - wrong HCAP version	Unable to communicate with the external policy server; wrong Host Credentials Authorization Protocol (HCAP) version.	The HCAP version of ACS and the external policy server are different.
Could not communicate with the Audit Server	The audit server cannot be reached or is down.	Check the connection to the external audit server.
Could not connect to external policy server - timeout error	Unable to communicate with the external policy server.	Check the external policy server configuration.

Table A-1 ACS 4.x Error Codes

Error Codes	Possible Root Cause	Resolution
Could not open a connection to external policy server	Unable to reach the external policy server or the sever is down.	Check the connection to the external policy server.
Could not open a connection to external policy server - Could not validate server certificate	Unable to open a connection with the external policy server.	Unable to validate server certificate. Check the validity of the server certificate.
DB object lock not granted	Unable to access the DB.	Try accessing the DB again.
EAP-FAST anonymous in-band provisioning is disabled	The Allow Anonymous In-Band PAC Provisioning option is disabled in the EAP-FAST configuration settings.	Enable the option.
EAP-FAST authenticated in-band provisioning is not disabled	The EAP-FAST Authenticated In-Band Provisioning option is not disabled.	Check the ACS EAP-FAST configuration.
EAP-FAST Type not configured	The supplicant requesting for EAP-FAST authentication, is not configured in ACS.	Enable EAP-FAST at the global level; or, at the matched profile (NAP) level.
EAP-FAST user ID does not match to initiators ID presented inside the PAC	The client sends a PAC with an initiator ID that does not match the user ID.	Check the configuration of the supplicant.
EAP-FAST users PAC is invalid	The client sends an expired PAC.	The client sends an expired PAC.
EAP_LEAP Type not configured	The supplicant requesting for EAP-LEAP authentication, is not configured in ACS.	Enable LEAP at global level.
EAP_MSCHAP Type not configured	The supplicant requesting for authentication from EAP-PEAP or EAP-FAST with EAP-MSCHAP as the inner method, is not configured in ACS.	Enable EAP-MSCHAP as the inner method for PEAP; or EAP-FAST, at the global level or matched profile (NAP) level.
EAP_PEAP Type not configured	The supplicant requesting for EAP-PEAP authentication is not configured in ACS.	Enable EAP-PEAP at the Global level; or, at matched profile (NAP) level.
EAP-TLS or PEAP authentication failed during SSL handshake	This failure occurs when: <ul style="list-style-type: none"> The server validation is not configured correctly on the client. The machine certificate is not provisioned on the machine (when used with EAP-TLS). Unable to provide a user certificate for authentication. The AAA server certificate has expired. The Root CA certificate is not installed or is not installed correctly on the client. The same CA certificate is used for intermediate CA or Root CA certificate: Root CA duplication. 	If the Certification Authority (CA) or ACS certificates have expired or are missing, distribute, renew, or update the certificates to the clients trusted root certificate store. Check if NTP is enabled on the client and ACS. Install the appropriate CA certificate on your system as Authenticated in-band PAC Provisioning requires a valid Trusted Root CA certificate. We do not recommend self-signed certificates. Use a CA instead.

Table A-1 ACS 4.x Error Codes

Error Codes	Possible Root Cause	Resolution
EAP_TLS Type not configured	The supplicant requesting for EAP-TLS authentication is not configured in ACS.	Enable EAP-TLS at global level; or, at NAP.
EAP-TLS or PEAP authentication failed due to unknown CA certificate during SSL handshake	The supplicant used an invalid certificate.	Install the correct certificate in ACS; or, in the supplicant.
EAP-TLS or PEAP authentication failed due to different protocol version during SSL handshake	This error occurs when there is a difference in the TLS version.	No configuration required for ACS.
EAP-TLS or PEAP authentication failed due to invalid certificate during SSL handshake	The supplicant used an expired, or revoked, or invalid certificate.	Install the correct certificate in the supplicant.
Enabling TACACS+ is not allowed for this Access Server	The Enable Privilege option is set in the TACACS+ Advanced options.	Check the access server configuration.
Error assigning RADIUS Authorization Components to a user	Unable to locate RADIUS Authorization Components (RAC) for the user.	Check the RAC configuration.
Error communicating with the audit server, or invalid response was returned	Unable to reach the audit server; or, the server is down.	Check the audit server connectivity and configuration.
Error parsing Audit Server Response	The audit server displayed an error while parsing the request.	Check the version of the audit server and ACS supports it.
External DB account disabled	The External User Account is disabled.	The windows administrator must reset this option.
External DB account expired	The External User Account has expired.	The windows administrator must reset this option.
External DB account locked out	The External User Account is locked.	The windows administrator must reset this option.
External DB account restriction	The Windows User Account is restricted.	The windows administrator must reset this option.
External DB ARAP password is invalid	The ARAP password is invalid.	Provide the correct password.
External DB CHAP password is invalid	The CHAP password is invalid.	Use the correct password.
External DB did not return MPPE key material	If the remote RADIUS server does not return the MSCHAP-MPPE-Keys attribute, the MPPE key material cannot be extracted and returned to CSAuth. This is required for an Aironet LEAP authentication.	If the remote RADIUS server does not return the MSCHAP-MPPE-Keys attribute, the MPPE key material cannot be extracted and returned to CSAuth. This is required for an Aironet LEAP authentication.
External DB EAP authentication failed	When an invalid EAP password is used, authentication fails.	Check the configuration of the supplicant.
External DB is not configured	The supplier key is not present in the registry; or, the external DB does not exist for the user.	The supplier key is not present in the registry or the external DB does not exist for the user.
External DB is not configured for this network access profile	An external DB is not configured for the unknown user policy.	Configure the external DB.

Table A-1 ACS 4.x Error Codes

Error Codes	Possible Root Cause	Resolution
External DB is not operational	An external server such as the RSA token server is not operational or does not respond.	Check if the external server is working or is correctly configured.
External DB MSCHAP password is invalid	The MSCHAP password is invalid.	Use a valid password.
External DB password expired	The user password has expired.	Reset the user's windows password.
External DB password invalid	If an invalid or empty password is provided during RSA token authentication, the PIN is rejected.	Provide the correct PIN.
External DB reports about an error condition	<p>This error occurs when:</p> <ul style="list-style-type: none"> • The DSN fails to open. • The ODBC authentication occurs again and CSAuth tries a reload or initialize. • The LDAP interface initialization fails; or, winsock initialization fails for RADIUS authentication. • The external ODBC DB is not available while checking for an unknown user policy. • Any error occurs during authentication. <p>When these conditions occur, ACS discards or rejects the configuration.</p>	Configure the external DB in ACS correctly. Check the connectivity and functioning of the external DB by using another tool.
External DB user invalid or bad password	An authentication failure has occurred in NTAauthn.	Check the configuration of the supplicant.
External DB user unknown	Invalid user.	Enter a valid user.
External user not found	User is not present.	Check for the user in the DB.
Failed to allocate IP address for a user	Check the configuration of the IP address pool.	Check the configuration of the IP address pool.
Internal error	An unknown error code is generated when the auth failure code is not found.	Check the logs.
Internal error assigning RADIUS Authorization Components attributes	Iterator for RAC is not created.	Check the RAC configuration.
Internal error during Downloadable ACL exchange	Internal error.	Check the logs in full mode.
Internal error while assigning Downloadable ACL to a user	The ACL is not present in the Shared Profile Component (SPC) database.	Check the ACL configuration.

Table A-1 ACS 4.x Error Codes

Error Codes	Possible Root Cause	Resolution
Internal Error due to Invalid Password Type	This error occurs due to an: <ul style="list-style-type: none"> Invalid external DB Corrupted DB Un-supported upgrade path or restore 	Reconfigure the external DB, remove the dynamic user and re-authenticate it.
Internal Error due to Invalid Service control data	This error occurs when services crash or hang.	Restart the services.
Internal Error due to NDG Creation Error	This error occurs when the internal data or memory handling is invalid.	Restart the services.
Internal Error due to Invalid State	This error occurs when the internal data or memory handling is invalid.	Restart the services.
Internal Error due to initialization failure	This error occurs when the DLL is not found; or, is not loaded.	Check for the correct DLL.
Internal Error due to Invalid Authentication Type	This error occurs due to an invalid authentication type.	Check the authentication type and external DB.
Internal Error due to Failure of Replication	This error occurs due to an exception in the replication.	Restart the services.
Internal Error due to raise of exception	This error occurs due to high stress.	Restart the services.
Internal Error due to logging activity	This error occurs when there is a failure in logging.	Restart the services.
Internal Error due to invalid context handle	This error occurs when there is a delay in receiving the challenge.	The supplicant must send the challenge at the appropriate time.
Internal Error due to Authentication failure	This error occurs when invalid credentials are used.	Use valid credentials.
Internal Error due to Crypto Failure	This error occurs when the service does not have the required privileges.	The user must change the local policies related to crypt32.
Internal Error due to packet fragment handling error	This error occurs when the supplicant sends an invalid mail-packet.	The supplicant must send a valid packet.
Internal Error due to Registry Access Failure	This failure is caused by external APIs.	The supplicant must run the service with valid privileges.
Internal Error due to invalid user-id	This error occurs if the user-profile is not present in ACS.	Use a valid username.
Invalid API Data received	CSAuth uses an error code while processing a request from CSTACACS or CSRADIUS.	
Invalid CHAP Data received	The supplicant used invalid data for the CHAP protocol.	Check the supplicant configuration.
Invalid EAP Data received	The supplicant used invalid data for the ARAP protocol.	Check the supplicant configuration.
Invalid message authenticator in EAP request	Invalid authentication code in keywrap message.	Check the NAS or supplicant configuration.

Table A-1 ACS 4.x Error Codes

Error Codes	Possible Root Cause	Resolution
Invalid MS-CHAP Data received	The supplicant used invalid data for the MS-CHAP protocol.	Check the supplicant configuration.
Invalid Protocol Data	This error occurs when: <ul style="list-style-type: none"> ACS receives invalid data. CHAP challenge of less than 1 byte is received. An empty EAP message occurs in a conversation between NAS and ACS. 	Check the NAS configuration.
Invalid PDE Data received	The supplicant used invalid posture data.	Check the supplicant configuration.
Invalid RDBMS Sync Data received	Invalid data for RDBMS Sync.	Check the configuration.
Invalid TEAP Data received	The supplicant used invalid data for the TEAP protocol.	Check the supplicant configuration.
Invalid TLV Data received	The supplicant used invalid data for the TLV protocol.	Check the supplicant configuration.
Invalid VARSDB Data received	The supplicant used invalid data for the EAP protocol.	Check the supplicant configuration.
MAC auth bypass is not allowed	The Radius MAC authentication is not enabled. (Allow agentless request processing.)	Enable the Allow Agentless Request Processing option.
MAC-Authentication-Bypass group is disabled	This is a configuration issue.	Enable the respective group for MAC bypass.
Machine authentication is not permitted	This is a configuration issue.	In the windows external DB section, enable the Machine Authentication for the specific inner method.
Missing message authenticator in EAP request	This is a client related issue.	The client must send a message authenticator.
Number of audit round trips has exceeded limit	This is a configuration issue.	Increase the limit.
PEAP or EAP-FAST password change against Windows DB is disabled	This is a configuration issue.	Enable the Password Change option in the windows external DB.
Posture Validation failed because no profile matched	This is a configuration issue.	The profile must be configured.
Posture Validation Failure (general)	This is a general error.	Configure the posture server correctly.
Posture Validation Failure on External Policy	This is a general error.	Configure the posture server correctly.
Posture Validation Failure on Internal Policy	This is a general error.	Configure the posture server correctly.
TACACS+ enable password invalid	The password verification failed.	Use a valid password.

Table A-1 ACS 4.x Error Codes

Error Codes	Possible Root Cause	Resolution
TACACS+ enable privilege too low	This is a configuration issue.	Increase the Enable Privilege Level.
Token PIN changed	This is a configuration issue.	Use the changed PIN.
Unknown attributes were detected in the posture validation request	This is a client related issue.	The client must send valid attributes.
User requires a TACACS+ Enable Password	This is a configuration issue.	The client must use an enabled password.
User requires TACACS+ outbound password	This is a configuration issue.	The client must use an outbound password.
Users Access Filtered	This is a configuration issue.	Configure NAR correctly.
Users of this group are disabled	This is a configuration issue.	Enable the group.
Users Radius request rejected (by Radius extension DLL)	This is a general error.	The client must use valid credentials.
Users Usage Quota has been exhausted	This is a configuration issue.	The client must use valid accounting requests.
Windows dialin permission required	This is a configuration issue.	Enable Dialin Permissions.
Windows domain controller not found	This is a configuration issue.	Configure AD and DNS correctly.
Windows External DB user access was denied due to a Machine Access Restriction	This is a configuration issue.	Configure NAR correctly.
Windows login server unavailable	This is a configuration issue.	Configure AD and DNS correctly.
Windows login time restriction	This is a configuration issue.	Configure AD and DNS correctly.
Windows login type not granted	This is a configuration issue.	Configure AD correctly.
Windows password change failed	This is a configuration issue.	The client must use a valid password.
Windows user must change password	This is a configuration issue.	The client must change the password.
Windows workstation not allowed	This is a configuration issue.	Configure AD correctly.