Pulse Secure

Pulse Policy Secure

Error Messages Reference Guide

Published Date April 2019
3.0

Pulse Secure, LLC
2700 Zanker Road, Suite 200 San
Jose, CA 95134

Pulse Secure assumes no responsibility for any inaccuracies in this document. Pulse Secure reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Products made or sold by Pulse Secure or components thereof might be covered by one or more of the following patents that are owned by or licensed to Pulse Secure: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899,

6,552,918, 6,567,902, 6,578,186, and 6,590,785.

The information in this document is current as of the date on the title page.

END USER LICENSE AGREEMENT

The Pulse Secure product that is the subject of this technical documentation consists of (or is intended for use with) Pulse Secure software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at **http://www.pulsesecure.net/support.** By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Contents

Table of Contents

Requesting Technical Support

Technical product support is available through the Pulse Secure Global Support Center (PSGSC). If you have a support contract, then file a ticket with PSGSC.

- Product warranties—For product warranty information, visit **https://www.pulsesecure.net**
- Find product documentation: **https://www.pulsesecure.net/techpubs/**
- Find solutions and answer questions using our Knowledge Base: **https://www.pulsesecure.net/support**

Opening a Case with PSGSC

You can open a case with PSGSC on the Web or by telephone.

- Use the Case Management tool in the PSGSC at **https://www.pulsesecure.net/support**.
- Call Phone: 1-844-751-7629 (Toll Free, US). For international or direct-dial options in countries without toll-free numbers, see **https://www.pulsesecure.net/support**

PART 1

Pulse Policy Secure Error Messages

About this Guide

This document describes system log messages for Pulse Policy Secure. Use the information to interpret the error messages and determine the appropriate corrective action.

Active Directory related Error Messages

The below table describes the error codes when issues occur with your Active Directory connection.

Table 1: Active Directory Error Messages

Error Code	Error Message	Description	Corrective Action
AUT30833	Authentication failure for AD realm <*realm-name*> due to large time drift. Please make sure the system time on this device and Active Directory server <*server-name*> are in sync.	This notification signifies that the PPS device time and the Active Directory server time are not in sync.	Ensure that the PPS device and AD server date and time are always in sync. Use Network Time Protocol (NTP) server to set the date and time for both appliances.
AUT30834	Authentication failure for AD server <*server-name*>: protocol disallowed by configuration	The configured authentication protocol is not supported on AD server.	The UPN format for user login is not supported for MS-CHAP v2. Check the configuration.
SYS30901	Active Directory authentication server <*server-name*>: Invalid AD credentials while attempting to join the domain. If not joined, user and machine authentication will fail.	The user credentials used to join the AD domain is invalid. Please use valid credentials to join the AD domain.	Please use valid credentials to join the AD domain.
SYS30912	Active Directory authentication server <*server-name*>: No logon servers are currently available. Device could not connect to any domain controller of the domain.	The current Active Directory domain controller is not reachable; the user or machine authentication requests fail for a few seconds (less than 2 minutes) before attempting to authenticate users with another domain controller in the Active Directory domain.	Ensure that the AD domain controller is reachable. For more details, see MICROSOFT AD QUICK-REFERENCE-TROUBLESHOOTING GUIDE.
AUT30899	Active Directory authentication server, <*server-name*>: Received access denied message from the server.	The access to the AD server is denied.	The access is denied due to invalid AD credentials, trust password mismatch and so on. For more information, see

Error Code	Error Message	Description	Corrective Action
			MICROSOFT TECHNET.
AUT24414	Authentication succeeded	The login succeeded for *<UserName>*/*<Realm Name>* from *<IP address/MAC Address> of the <User Agent>*.	Not Applicable
AGU30457	Starting dsagentd session	The login session is created successfully. The session is being monitored for logout, role changes, time-outs and so on.	Not Applicable
AUT24326	Authentication succeeded	The authentication is successful for *<username>*/*<auth server display name>* from *<IP address of endpoint from where user logins/ calling station MAC address for L2> <Custom source IP address>*	Not Applicable
AUT24327	Authentication failed	The authentication failed for the *<username>*/*<authentication server>* from the following *<IP Address/ MAC Address>*.	If the authentication server is AD then check the previous logs related to the authentication flow. Check the user login logs from admin console Maintenance > Troubleshooting page. Try restarting winbind services.
AUT22925	Host Checker failed	This message signifies the Host Checker failure. It displays the policy name and reasons for policy failure.	• Possible reasons could be incorrect ESAP package. See KB. • Incorrect rule configuration.

Error Code	Error Message	Description	Corrective Action
AUT23458	Login failed	The user login failed due to following reasons: • Wrong Certificate • Admin Only • Admin Recovery • Feature Unlicensed • Max Sessions • Short Password • Account Disabled • Account Locked Out • Account Expired • No Roles • Too Many Sessions • Revoked Certificate • IP Denied • UA Denied • IP Blocked • No Certificate • Radius • Realm Remediate • Role Remediate • OCSP Failure • No Assertion • Connect Error • SignIn Notification Decline • Chassis SSO Failed • Login Cancel • Too Many EES • Too Many PRM • Token Or OTP • Invalid Assertion • Empty Assertion • SPNEGO_SSO • Max Session Per User • Empty User Name • Password Change required but Password Management disabled • FIPS Client Required • Needs SAML Authentication • No Realm • Maximum Onboard Devices • Login Failed on Reject	The corrective actions based on error message: • For Wrong certificate- Obtain a client certificate with the key usage of Digital Signature. • For Admin only- Only Admin Login is allowed. • For Account Locked Out- The account is locked out due to too many incorrect login attempts. • For FIPS client required- Use Pulse Client if you are using older clients like OAC. • For invalid/untrusted certificate message- Try reimporting the CA certificate. See KB. • For Maximum onboard devices- Check the license limit of your hardware. See KB. • For Token or OTP- This could be due to time synchronization issue between the client and the authenticator. Pulse Secure recommends to use a NTP server to avoid time drift issues. • For Certificate revoked- Disable the certificate revocation check on your browser security settings and try again. • Too many EES- The number of concurrent Enhanced Endpoint Defense (Malware Protection) users

Error Code	Error Message	Description	Corrective Action
			signed into the system has exceeded the system limit. • Too Many PRM- The number of concurrent Shavlik Remediation users signed into the system has exceeded the system limit. • For Realm remediate- The realm is defined as a remediation realm. • For Empty user name- The user name field is empty. • For RADIUS related messages- see KB.
AUT24803	Host Checker passed	The Host Checker policy passed on host address for the user.	NA

System Upgrade related Error Messages

The below table describes the error codes when issues occur during the Pulse Policy Secure (PPS) upgrade.

Table 2: System Upgrade Error Messages

Error Code	Error Message	Description	Corrective Action
ADM23396	System software upgrade failed. The service package uploaded is not valid.	The appliance upgrade failed due to invalid package. Please upload the correct package.	Verify the package version and upload the correct version to the system.
ADM24487	System software upgrade failed. Installation timed out.	This notification signifies that the installation can take more than 60 minutes to complete. Hence aborting the installation and rebooting.	Please check the network connectivity and retry.
ADM30480	System software upgrade failed. The service package uploaded is not supported on Virtual Appliances. Virtual Appliances are supported only from software version <*version-number*>.	The uploaded package is incompatible with the virtual server. The minimum version supported is <*version-number*>	Please check the software package version is above the minimum supported version before uploading.

Firewall Enforcement related Error Messages

The below table describes the error codes when issues occur with your L3 firewall enforcement.

Table 3: Firewall Enforcement Error Messages

Error Code	Error Message	Description	Corrective Action
GWE23592	Enforcer message from <*enforcer-name*> has unknown serial number <*enforcer-serial-number*>	This notification signifies that an invalid enforcer, which has an unrecognized serial number is being added to the system.	Ensure that a valid enforcer with correct serial number is added on PPS.
GWE24666	Platform mismatch for gateway with serial number <*serial-number*>. Connecting gateway has platform <*platform-name*> but is configured as <*platform-name*> with platform <*platform-name*>.	This notification signifies that the connection profile is misconfigured with an incorrect enforcer type.	Configure the enforcer with a valid gateway type. For example, SRX is configured as ScreenOS, ensure that the gateway type is correct.
GWE24024	Error configuring IPsec routing for Enforcer %1(%2): source and destination zones "%3" are the same	The IPsec routing policy is not configured correctly.	The policy should have different source and destination zone for IPsec configuration.
GWE30827	IC is not configured as RADIUS Auth Server on Ex enforcer <EX Switch Name>	PPS is not configured as a RADIUS server on Juniper EX switch.	Configure PPS as a RADIUS server on EX switch.
GWT31292	Enforcer:<*Gateway Name*> (<*Gateway IP address*>) Enforcer failed to execute <*command-name*> command for <*Source IP*>	The enforcer failed to execute the command for source IP address.	Check the network connectivity between PPS and Screen OS.
GWT31383	Gateway (Gateway IP address) request error: <*Curl Error code*>	A communication error has been encountered between PPS and PAN firewall.	Check the curl error code for corrective action. For more information, see CURL ERROR CODES.
GWT31291	Enforcer: <Enforcer Name> (<Enforcer IP address>) is unreachable	Indicates that the enforcer is offline and unreachable	PPS retries to connect automatically. If the problem persists, check the network connectivity with Firewall.
GWT31316	API Key retrieval for gateway IP address <Enforcer IP Address> has <Error code>	Logs the API key retrieval status.	Check the network connectivity and retry to retrieve the API key.

RADIUS related Error Messages

The below table describes the error codes when issues occur with your RADIUS connection.

Table 4: RADIUS Error Messages

Error Code	Error Message	Description	Corrective Action
SBR24600	<SBR Error>	RADIUS non informal message such as a RADIUS Reject message.	Check the RADIUS reject message from the protocol specification for resolution.
AUT23314	Radius Accounting: Failed to send radius accounting <*session-type*> session <*Status*> request for <*username*>	Unable to send RADIUS (start, stop) accounting messages to RADIUS server.	Check the network connectivity between PPS and external RADIUS server.
EAM30455	License key restriction: number of concurrent Enhanced Endpoint Security (Malware Protection) users (Number of concurrent users) exceeded the system limit (Max user limit). <*username*>/<*realm-name*> is not allowed to login.	The maximum number of concurrent users are connected. No new users are allowed to connect.	You can purchase new user licenses.
SBR24461	RADIUS: <Error message>	The error message describes protocol failure in any of the following cases: • PEAP configuration • TLS configuration • TTLS configuration	The authentication protocol set must be configured on the PPS based on the client configuration.
BR24574	RADIUS: <Error message>	The server certificate is not found for interface.	Install the server certificate.
EAM30585	Detected both OAC and Pulse connections from <Endpoint IP Address>	The user is connecting both OAC and Pulse client simultaneously.	You must connect one client at a time.
SBR24575	RADIUS: Received RADIUS message with Message-Authentication-Code from client <client name> (client IP>) but Key Wrap is not enabled for this client.	This error message describes that the Cisco Key wrap is not enabled but RADIUS messages are received with Message Authenticator Code (RFC 6218).	Enable the key wrap option in the RADIUS Client page.
SBR24575	RADIUS: Invalid Message-Authentication-Code from RADIUS client <client name> (<client IP>), discarding. Incorrect Message Authenticator Code Key(MACK)	This error message is displayed when Mac-authentication-code mismatch occurs. This mismatch can occur if MACK keys does not match.	Check if MACK is correctly configured for the client in the RADIUS Client page.

Error Code	Error Message	Description	Corrective Action
SBR24575	RADIUS: Received RADIUS message with Message-Authentication-Code from client <client name> (client IP>) but Key Wrap is not enabled for this client.	When Cisco Key wrap is not enabled but RADIUS messages are received with Message Authenticator Code (RFC 6218).	Check if key wrap is disabled for the Client in 'Radius Client' page
SBR24575	RADIUS: Invalid Message-Authentication-Code from RADIUS client <client name>(<client IP>), discarding. Incorrect Message Authenticator Code Key(MACK)?	When Mac-authentication-code mismatch occurs. This mismatch can occur if MACK keys does not match.	Check if MACK is correctly configured for the Client in 'Radius Client' page.

Clustering related Error Messages

The below table describes the error codes when issues occur with your cluster setup.

Table 5: Cluster Error Messages

Error Code	Error Message	Description	Corrective Action
NET24470	VIPs failed over to node <node-name>, reason: <node-name>	This event occurs in an Active/Passive cluster environment during the node transition.	This occurs when an active node in the cluster is inactive due to a hardware failure or due to an admin triggered fail over.
NET24571	<*node-name*> cannot yield vips, reason <*node-name*> Logged when admin initiated yield cannot happen since the other node(s) are in a bad state	This event occurs when the VIP cannot be owned by other nodes as the other node is in bad state (not reachable, unresponsive).	Check the state of the other node.

System related Error Messages

The below table describes the error codes when issues occur with your system.

Table 6: System Related Error Messages

Error Code	Error Message	Description	Corrective Action
ERR31093 /ERR24632	Program <*process-name*> recently failed.	This notification is generated when a process fails. A core dump is generated for debugging purpose.	If the process is continuously crashing, collect the process snapshot and contact support team.
ERR30440	<*process-name*> (pid <PID>) terminated due to high memory usage (actual memory in MB > hard limit maximum memory in MB).	The process is terminated due to high memory usage.	The issue could be because of heavy load on PPS. You can reduce the concurrent load on PPS. If the issues persist, upgrade the Hardware.
ADM20931	You did not check the 'Import Device Certificate(s)' check box	The device certificate is exported from a different configuration. The device certificate could not be imported.	Check the option to import device certificate while importing the configuration.

Licensing related Error Messages

The below table describes the error codes when issues occur with your license server.

Table 7: Licensing Related Error Messages

Error Code	Error Message	Description	Corrective Action
LIC30496	Failed to register with license server <*server-name*> - <*client-name*>.	The license server failed to register the client. The possible reasons are: • Another client is registered with same ID • Client is already registered • Client is configured as Server • ID mismatch	Verify the machine ID getting registered with the license server and ensure that it has a valid ID.
LIC30566	Client configuration for client <*server-name*> has expired, any licenses leased to this client are being revoked.	The leased license is expired on Pulse Policy Secure.	Since the license is expired add a new license for the client.
LIC30828	Auto-leasing penalty has been activated due to excess auto-lease activity by client <*client-name*>	This message signifies that the Auto leasing penalty option is turned ON after license expiry.	You can activate the license key to avoid penalty.
ADM10310	License key <*key*> expired.	License Key is expired and requires license renewal.	You can renew the license key.

Samba related Error Messages

The below table describes the error codes related to Samba server on your PPS appliance.

Table 8: Samba Related Error Messages

Error Code	Error Message	Samba Error Code- Description	Corrective Action
AUT30833	Authentication failure for AD realm <Realm Name> due to large time drift. Please make sure the system time on this device and Active Directory server <*server name*> are in sync.	STATUS_TIME_DIFFERENCE_AT_DC - Our PCS/PPS box and the AD server which was attempted to contact were out of sync.	The PPS appliance and the AD server are out of sync. Use NTP server for time synchronization. Ensure that the time difference is not more than 5 minutes.
AUT30835	Authentication failure for AD server <server name>: bad username or authentication information.	STATUS_LOGON_FAILURE -The attempted logon is invalid. This is either due to a bad username or authentication information.	The following are some of the possible causes: - An invalid username and/or password was used - LM Compatibility mismatch between the source and target For more information and corrective action, see Microsoft TechNet
AUT30836	Authentication failure for AD server <*server name*>: specified account does not exist	STATUS_NO_SUCH_USER - The username you typed does not exist!.	The most common causes are: - Incorrect username - AD replication to/from target server may not be completed. For more information and corrective action, see Microsoft TechNet
AUT30837	Authentication failure for AD server <*server name*>: AD Server does not have a computer account for this trust relationship	STATUS_NO_TRUST_SAM_ACCOUNT – - Domain trust is broken - When a trusted domain user is authenticated, the trust between the user domain and trusted domain is not accurate.	If the trust relationship between these two domains is downlevel type. To resolve this issue, recreate the trust between the Active Directory domains to eliminate the downlevel trust type. For more information, see Microsoft TechNet.
AUT30899	Active Directory authentication server <*server name*>: Received access denied message from the server.	STATUS_ACCESS_DENIED - A process has requested access to an object, but has not been granted those access rights.	The most common causes are: - Attempting to join a machine who's name already exists in Active Directory

Error Code	Error Message	Samba Error Code- Description	Corrective Action
			• Secure channel is broken • Trust password mismatch • Incorrect credentials • NTLM blocking is enabled For corrective action, see Microsoft TechNet
AUT30914	Active Directory authentication server <server name>: No logon servers are currently available. Device could not connect to any domain controller of the domain.	STATUS_NO_LOGON_SERVERS - The domain controller was not reachable/resolvable. The winbindd failed to connect to Domain Controller.	Possible failure reason are DNS forwarder configurations issues, Invalid entries in HOST file, Network issues etc. For more information and corrective action, see Microsoft TechNet
AUT30924	Active Directory authentication server <server name>: Account name either does not exist or is not properly formed.	STATUS_INVALID_ACCOUNT_NAME - The name provided is not a properly formed account name.	Enter the correct username and password.
SYS30948	IO timeout happened on Active Directory authentication server <server name>.	STATUS_IO_TIMEOUT – The operations such as authentication, join, password change and so on attempted by Winbindd process has timed out. DC not resolved from DNS server DC and AD servers are slow and overloaded.	Check the DNS server configuration and domain name resolution from the DNS server. Check if the Kerberos realm is reachable from System > Troubleshooting tools > Prob Kerberos DNS setup.
AUT30949	Active Directory authentication server <server name>: Trust relationship failed with the trusted domain.	STATUS_TRUSTED_DOMAIN_FAILURE - The logon request failed because the trust relationship between the primary domain and the trusted domain failed.	Check if the Kerberos realm is reachable from System > Troubleshooting tools > Prob Kerberos DNS setup.
AUT30950	authentication server <server name>: Transport connection has been reset	STATUS_CONNECTION_RESET - The transport connection has been reset.	Fix network issues
AUT30951	Active Directory authentication server <server name> is unreachable	STATUS_HOST_UNREACHABLE - The remote system is not reachable by the transport.	Fix network issues
AUT30923	Active Directory authentication server <server name>: Received NTSTATUS code <error code>	STATUS_NO_TRUST_LSA_SECRET-Your connection to the domain is broken from this machine!	The possible causes are: • Secure channel corruption with the host • The computer object has been deleted from Active Directory • Blocked ports on a firewall Try reset domain join.

Error Code	Error Message	Samba Error Code- Description	Corrective Action
AUT30923	Active Directory authentication server <server name> : Received NTSTATUS code <error code>	STATUS_INSUFFICIENT_RESOURCES- You have resource issues on your system that is preventing Netlogon from connecting or operating properly.	The possible causes are: - Available physical memory exhaustion - Paged pool or non-paged pool memory exhaustion - Free System PTE (Page Table Entries) exhaustion To troubleshoot this issue, use Performance Monitor, Resource Monitor, Xperf, or other performance diagnostics tool.
AUT30923	Active Directory authentication server <server name> : Received NTSTATUS code <error code>	RPC_NT_CALL_CANCELLED- RPC communications are having problems that need to be resolved!	For corrective action, see Microsoft TechNet
AUT30923	Active Directory authentication server <server name> : Received NTSTATUS code <error code>	STATUS_NO_MEMORY- You have an out of memory condition on the system or in RPC	Domain controller, client, or target server may have exhausted virtual memory/page file or physical memory The possible fixes are: - Check your page file usage with Performance Monitor - Look for handle leaks with Performance Monitor, Resource Monitor, or Task Manage - User ports may be exhausted
AUT30923	Active Directory authentication server <server name> : Received NTSTATUS code <error code>	STATUS_NETLOGON_NOT_STARTED- The Netlogon service is not started or the Domain Controller is not advertising!	The possible causes are: - The Netlogon service is not started on the application server or domain controller - Sysvol and/or Netlogon is not shared on the Domain Controller
AUT30923	Active Directory authentication server <server name> : Received NTSTATUS code <error code>	STATUS_ACCOUNT_RESTRICTION- Indicates a referenced user name and authentication information are valid, but some user account restriction has prevented successful authentication (such as time-of-day restrictions).	The possible causes are: - The username and password are correct, but there is an account restriction on the user account (such as valid workstation, valid logon hours, etc.). The value

Error Code	Error Message	Samba Error Code- Description	Corrective Action
			under SubStatus should provide the restriction details. • Active Directory Replication may not be complete
AUT30923	Active Directory authentication server <server name> : Received NTSTATUS code <error code>	STATUS_PASSWORD_RESTRICTION- When trying to update a password, this status indicates that some password update rule has been violated. For example, the password may not meet length criteria	User is attempting to reset password and it does not meet requirements specified by policy (length, history, complexity)
AUT30923	Active Directory authentication server <server name> : Received NTSTATUS code <error code>	STATUS_INVALID_WORKSTATION- The user account is restricted such that it may not be used to log on from the source workstation.	The possible causes are: • The user is trying to logon from a machine they aren't assigned to. • Active Directory replication may not be complete
AUT30923	Active Directory authentication server <server name> : Received NTSTATUS code <error code>	STATUS_WRONG_PASSWORD- When trying to update a password, this return status indicates that the value provided as the current password is not correct.	The possible causes are: • Your password is expired • Your password is incorrect • Active Directory Replication may not be complete
AUT30923	Active Directory authentication server <server name> : Received NTSTATUS code <error code>	STATUS_ACCOUNT_EXPIRED-The user's account has expired	The possible causes are: • Your account is expired • Active Directory Replication may not be complete
AUT30923	Active Directory authentication server <server name> : Received NTSTATUS code <error code>	STATUS_PASSWORD_EXPIRED- The user account's password has expired.	The possible causes are: • Your password is expired • Active Directory Replication may not be complete
AUT30923	Active Directory authentication server <server name> : Received NTSTATUS code <error code>	STATUS_INVALID_LOGON_HOURS- The user account has time restrictions and may not be logged onto at this time.	The possible causes are: • You are set with logon hours restrictions and have attempted to logon outside of those time restrictions • Active Directory Replication may not be complete

Error Code	Error Message	Samba Error Code- Description	Corrective Action
AUT30923	Active Directory authentication server <server name> : Received NTSTATUS code <error code>	STATUS_ACCOUNT_LOCKED_OUT-The user account has been automatically locked because too many invalid logon attempts or password change attempts have been requested.	The possible causes are: • Your user/machine account is locked out. For joined machine account, delete the account and rejoin from PPS. For user account, unlock the user account from the AD server. • Active Directory Replication may not be complete.
AUT30923	Active Directory authentication server <server name> : Received NTSTATUS code *<error code>*	STATUS_ACCOUNT_DISABLED- The referenced account is currently disabled and may not be logged on to.	The possible causes are: • Your user account is disabled. Enable the user account from the AD server. • Active Directory Replication may not be complete
AUT30923	Active Directory authentication server <server name> : Received NTSTATUS code *<error code>*	STATUS_INVALID_SERVER_STATE-Indicates the Sam Server was in the wrong state to perform the desired operation.	Domain controller may be shutting down or restarting. For corrective action, see Microsoft KB 942636 or KB 973667
AUT30923	Active Directory authentication server <server name> : Received NTSTATUS code *<error code>*	STATUS_TRUST_FAILURE- The network logon failed. This may be because the validation authority can't be reached.	• Check the Domain join status • Check the network connection
AUT30923	Active Directory authentication server <server name> : Received NTSTATUS code *<error code>*	STATUS_PASSWORD_MUST_CHANGE-The user's password must be changed before signing in.	The possible causes are: • User has the "user must change password at next logon" flag set. Time to change your password! • Active Directory Replication may not be complete
AUT30923	Active Directory authentication server <server name> : Received NTSTATUS code *<error code>*	STATUS_NO_SUCH_GROUP- The specified group does not exist.	Check the user group membership.

TACACS+ related Error Messages

The below table describes the error codes related to TACACS+ server on your PPS appliance.

Table 9: TACACS+ Related Error Messages

Error Code	Error Message	Description	Corrective Action
TAC31628	Limit of <*max count*> TACACS+ concurrent users reached.	TACACS+ concurrent user connections have reached the configured system limit.	Check the configuration file for the user limit.
TAC31629	TACACS+ request received from unknown TACACS+ client <*switch IP*>.	The incoming TACACS+ connection is dropped since it is received from an unknown host.	Check if the client IP address is configured in TACACS+ clients page.
TAC31628	Invalid TACACS+ packet from <switch IP>, discarding. Incorrect shared secret	The incoming TACACS+ connection is dropped due to shared-secret mismatch.	Check if the shared secret configured for the client is same when compared with the client request.
TAC31612	TACACS+ Shell authorization rejected for <*user*> on switch-<*switch ip*>. Reason- No session found	Exec authorization failure due to no session found.	Check if session is created in 'Active users' page.
TAC31612	TACACS+ authorization rejected for command-<cmd> from <user> on switch-<switch ip>. Reason- No session found	Command authorization failure due to no session found.	Check if session is created in 'active users' page.
TAC31612	TACACS+ authorization rejected for command-<*cmd*> from <*user*> on switch-<*switch ip*>. Reason- No Shell policy found for the assigned roles	Command authorization failure due to no shell policy assigned to roles.	Check if shell policy is configured and is correctly mapped to device group and roles.
TAC31612	TACACS+ authorization rejected for command-<*cmd*> from <*user*> on switch-<switch ip>. Reason- Matched with the rule – [command = <*command*> Arguments = <*argument*> action = deny] in shell policy-<*policy name*>	Command authorization failure due to action 'deny' set in command set.	Check the action configured in matched command set in shell policy page.
TAC31612	TACACS+ authorization rejected for command-<*cmd*> from <*user*> on switch-<*switch ip*>. Reason- No match found. Default action is 'deny' in shell policy-<*policy name*>	Command authorization failure due to action 'deny' set in default action.	Check if none of the configured command set matched with the request. If yes, the check the default action configured.

Error Code	Error Message	Description	Corrective Action
AUT23458	Login failed using auth server System Local (Local Authentication). Reason: Failed	Login failure due to authentication failure.	Check if the role mapping is based on username or group name. If using groupname, ensure all groups are listed when you click on groups under role mapping.
AUT23458	Login failed. Reason: No Roles	Login failure due to no role available.	Check if the user is configured with an appropriate role and role mapping rules.
AUT31627	Received a TACACS+ Accounting stop request. Terminated Session	Session deletion due to accounting stop received.	Check if accounting stop request is sent by client.
ADM20664	Session timed out for *<user>*/*<realm>* due to inactivity (last access at *<time>*). Idle session identified during routine system scan.	Session deletion due to session timeout.	Login again as previous session is expired.

Behavioral Analytics related Error Messages

The below table describes the error codes related to behavioral analytics on your PPS appliance.

Table 10: Behavioral Analytics Related Error Messages

Error Code	Error Message	Description	Corrective Action
UBA31663	Failed to update profile for user *<user_name>*	This indicates updating of user profile with the new details failed for Behavioral Analytics.	This error condition gets auto corrected on the server. No need of any explicit corrective action by Administrator.
SYS31750	Export of behavioral analytics package failed. Please upload the package manually from System > Behavioral Analytics > Configuration.	This indicates Behavioral Analytics package is not retained properly post system upgrade or config import.	Administrator need to manually upload the Behavioral Analytics package on Behavioral Analytics configuration page on server.
SYS31751	Import of behavioral analytics package failed. Please upload the package manually from System > Behavioral Analytics > Configuration.	This indicates Behavioral Analytics package is not retained properly post system upgrade or config import.	Administrator need to manually upload the Behavioral Analytics package on Behavioral Analytics configuration page on server.

IIoT Auto Provisioning with Palo Alto Networks Next Gen Firewall

The below table describes the error codes related to IIoT auto provisioning on your PPS appliance.

Table 11: IIoT Auto Provisioning Related Error Messages

Error Code	Error Message	Description	Corrective Action
GWT31690	Exception occurred during operation (PAN firewall policy operations such as Add, Delete, Modify).	This indicates that the either PAN firewall is not reachable or could be because of connection issues between PAN firewall and PPS.	Ensure that the PAN firewall is reachable. The status should turn green in Overview page upon successful addition. Ensure there are no connectivity issues.
GWT31692	Failed to execute the policy operation (Add, delete, modify policy)	This indicates that either the provided policy parameters are wrong or there is an issue on the PAN firewall to execute the policy operation.	Ensure that the policy input parameters are configured properly.
GWT31693	HTTP request failed	This indicates that the PAN firewall failed to fulfill HTTP request for policy operation. It could be because of PAN firewall server error.	Ensure that the PAN firewall responds to REST API requests.

Admission Control related Error Messages

The below table describes the error codes related to PPS and Juniper SDSN integration.

Table 12: PPS and Juniper SDSN Related Error Messages

Error Code	Error Message	Description	Corrective Action
INT31729	Request received from disabled Admission Control Client <*IP-Address*>	Indicates that client has been added for the Admission Control. However, it is not enabled.	Enable the configured client under Admission Control.
INT31729	Request received from unknown Admission Control Client <*IP-Address*>	Indicates that client has not been added for the Admission Control.	Add the client under Admission Control.

SNMP related Error Messages

The below table describes the error codes related to SNMP ACL based enforcement.

Table 13: SNMP ACL Enforcement Related Error Messages

Error Code	Error Message	Description	Corrective Action
INT31729	Request received from disabled Admission Control Client *<IP-Address>*	Indicates that client has been added for the Admission Control. However, it is not enabled.	Enable the configured client under Admission Control.

TOTP Server

The below table describes the error codes related to TOTP server.

Table 14: TOTP Server Related Error Messages

Error Code	Error Message	Description	Corrective Action
AUT23457	Login failed using auth server <Auth server name>. Reason: <Reason String>	When using TOTP (Time based One-Time Password) server as secondary authentication server, user login may fail. Common reasons are: 1. Login failure due to incorrect TOTP token. 2. Login failure because of time difference between Pulse Policy Secure and user's device	1. Make sure user inputs correct TOTP token. 2. Configure same time on Pulse Policy Secure and user's device.
USR31401	TOTP User <Username> account from Realm <Realm name> has been locked due to maximum number of invalid attempts.	TOTP user account can get locked if TOTP authentication fails consecutively for "Number of attempts allowed" configured on TOTP Auth Server page.	Follow below steps to avoid TOTP user account lock-out. 1. Make sure user inputs correct TOTP token. 2. Configure same time on Pulse Policy Secure and user's device 3. If TOTP user account is locked due to maximum number of invalid attempts, it can be unlocked from PPS Admin UI under TOTP Auth Server->Users's tab.
AUT31742	REST access failed to remote <TOTP server URL>: <Failure reason >	During TOTP authentication, REST access to remote TOTP server failed.	This could happen because of configuration issue while using remote TOTP server for authentication. Check below configurations 1. On remote TOTP server, properly configure REST API credentials and Realm. 2. On local TOTP server, enable an option to "Accept TOTP authentication from remote Pulse Secure devices".

Error Code	Error Message	Description	Corrective Action
			3. On local TOTP server, enable REST API access for admin user whose details are configured in remote TOTP server.

SAML Server

The below table describes the error codes related to SAML server.

Table 15: SAML Server Related Error Messages

Error Code	Error Message	Description	Corrective Action
ERR31066	SAML Consumer received and processed <SAML SSO Method>, Status: < FAILURE: Reason string> DetailedLogs: <Failure Detailed Message>	SAML Consumer received SAML response and failed to process it.	One of the common reasons for this message is the time synchronization issue between SAML IdP and SAML SP. Make sure both SAML IdP and SP are using the same time. If any time difference is there, it should be within the configured “Allowed Clock Skew” on SAML Server.