

Secure Login Service

Log Messages

Version 5.20.0.5, January 7, 2026



Type: AUDIT

Message ID

ERR_CONCURRENT_REQUEST

Message text

Processing error caused by concurrent request from client! Request URI: "{0}", method: "{1}", requested page: "{2}". Possible, typical causes: non-public location for '/favicon.ico' or static resources (CSS, JS..), multiple JavaScripts in a page triggering multiple form-posts etc.

Log4j variables

uri, method, requested_page

Description

An incoming request had to be blocked because the SLS was already processing another one from the same client. Usually, the reason for this is a configuration issue in the HSP, most likely static resources used by the login page, such as CSS, JS or favicon, being in a non-public location.

Category: AUDIT**Severity:** ERROR**Message ID**

ERROR_HANDLED

Message text

Exception handled. User: "{0}", Exception message: "{1}"

Log4j variables

user, message

Description

Some error occurred and was handled. Usually, there should be additional, more specific log records in the debug and / or exception log. This log message makes sure that an error becomes visible in the audit log as well, even if it happens after an already logged successful authentication step, e.g. during the creation of the login ticket.

Category: AUDIT**Severity:** ERROR**Message ID**

FEDERATION_MESSAGE_RECEIVED

Message text

Federation protocol message received. Protocol: "{0}", role: "{1}", type: "{2}", status: "{3}", local entity ID: "{4}", sender entity ID: "{5}"

Log4j variables

protocol, role, type, status, entity_id

Description

A federation protocol message was received by this SLS from another Federation service (such as a SAML or OpenID connect message).

Category: AUDIT**Severity:** INFO**Message ID**

FEDERATION_MESSAGE_SENT

Message text

Federation protocol message sent. Protocol: "{0}", role: "{1}", type: "{2}", status: "{3}", local entity ID: "{4}", receiver entity ID: "{5}"

Log4j variables

protocol, role, type, status, entity_id

Description

A federation protocol message was sent from this SLS to another Federation service (such as a SAML or OpenID connect message).

Category: AUDIT

Severity: INFO

Message ID

IDP_SLO_FAILED

Message text

SAML Single Logout from all SAML SPs ({1}) completed with {2} failures. User: "{0}".

Log4j variables

user, number_of_sps, number_of_sps_logout_failed

Description

Single Logout failed for some SAML Service Providers (see logfiles for details).

Category: AUDIT

Severity: INFO

Message ID

IDP_SLO_SUCCESS

Message text

SAML Single Logout from all SPs ({1}) successfully completed. User: "{0}".

Log4j variables

user, number_of_sps

Description

A user was logged out successfully from all logged in SAML Service Providers.

Category: AUDIT

Severity: INFO

Message ID

IDP_SP_LOGIN_FAILED_SENT

Message text

SAML authentication failed Response sent to SP "{1}". User: "{0}".

Log4j variables

user, sp_entity_id

Description

Login at SLS has failed, error SAML Response sent to indicated Service Provider (see logfiles for details).

Category: AUDIT

Severity: INFO

Message ID

IDP_SP_LOGIN_SUCCESS_SENT

Message text

SAML authentication success Response sent to SP "{1}". User: "{0}".

Log4j variables

user, sp_entity_id

Description

Login at SLS was successful, success SAML Response sent to indicated Service Provider.

Category: AUDIT**Severity:** INFO**Message ID**

IDP_SP_LOGOUT_FAILED

Message text

SAML logout from SP "{1}" failed. User: "{0}".

Log4j variables

user, sp_entity_id

Description

A user could not be logged out from the indicated SAML Service Provider (see logfiles for details).

Category: AUDIT**Severity:** INFO**Message ID**

IDP_SP_LOGOUT_SUCCESS

Message text

SAML logout from SP "{1}" successfully completed. User: "{0}".

Log4j variables

user, sp_entity_id

Description

A user was logged out successfully from the indicated SAML Service Provider.

Category: AUDIT**Severity:** INFO**Message ID**

OP_RP_LOGIN_FAILED_SENT

Message text

OIDC failed response sent to RP "{2}". Type: "{1}". User: "{0}".

Log4j variables

user, type, rp_client_id

Description

Login at SLS has failed, error OIDC response of indicated type sent to indicated Relying Party (RP/client).

Category: AUDIT
Severity: INFO

Message ID

OP_RP_LOGIN_SUCCESS_SENT

Message text

OIDC success response sent to RP "{2}". Type: "{1}". User: "{0}".

Log4j variables

user, type, rp_client_id

Description

Login at SLS was successful, success OIDC response of indicated type sent to indicated Relying Party (RP/client).

Category: AUDIT
Severity: INFO

Message ID

REQUESTED_PAGE_CHANGED

Message text

Restarting the login process, because the 'requested page' suddenly changed. User: "{0}". Original URI: "{1}". New URI: "{2}"

Log4j variables

user, uri_original, uri_new

Description

During a login process, the 'requested page' value suddenly changed. This can mean that a user invoked a different application URI during an ongoing login process. Since that requested page may have different access area level and / or authorization requirements, the whole login process is started from scratch.

Category: AUDIT
Severity: INFO

Message ID

SESSION_STARTED

Message text

SLS session started. Session ID: "{0}", Reason: "{1}"

Log4j variables

id, reason

Description

A new SLS session had be started. See log message for exact reason.

Category: AUDIT
Severity: INFO

Message ID

SP_IDP_LOGOUT_FAILED

Message text

SAML logout initiated by IdP "{1}" failed. User: "{0}".

Log4j variables

user, idp_entity_id

Description

A user was not logged out in response to a LogoutRequest by the indicated SAML Identity Provider; an error LogoutResponse has been sent to the IdP (see logfiles for details).

Category: AUDIT**Severity:** INFO**Message ID**

SP_IDP_LOGOUT_SUCCESS

Message text

SAML logout initiated by IdP "{1}" successfully completed. User: "{0}".

Log4j variables

user, idp_entity_id

Description

A user was logged out successfully in response to a LogoutRequest by the indicated SAML Identity Provider; a success LogoutResponse has been sent to the IdP.

Category: AUDIT**Severity:** INFO**Message ID**

TRANSACTION_VERIFIED

Message text

Transaction verified. Msg: "{0}"

Log4j variables

message

Description

This message might appear only, if you are using the SLS to verify transactions.

Category: AUDIT**Severity:** INFO**Message ID**

USER_APP_LOGOUT

Message text

Logging out user from application. User: "{0}", Logout URI: "{1}"

Log4j variables

user, uri

Description

A user was logged out from the application and the SES session.

Category: AUDIT**Severity:** INFO**Message ID**USER_AUTH_FAILED

Message text

Authentication failed. User: "{0}", Reason: "{1}", Model: "{2}", Backends: "{3}"

Log4j variables

user, reason, model, backend_types

Description

The user authentication failed. This message appears only, if a callout to the backend system was performed. See log message for details.

Category: AUDIT

Severity: INFO

Message ID

USER_AUTH_FAILED_TECH

Message text

Authentication failed due to a technical problem. User: "{0}". Reason: "{1}"

Log4j variables

user, reason

Description

The user authentication failed due to a technical problem. This message appears only, if a callout to the backend system was performed. See log message for details.

Category: AUDIT

Severity: ERROR

Message ID

USER_AUTH_SUCCESS

Message text

Authentication successfully completed. User: "{0}", Model: "{1}", Backends: "{2}", Authentication strength: "{3}"

Log4j variables

user, model, backend_types, authentication_strength

Description

A user was successfully authenticated.

Category: AUDIT

Severity: INFO

Message ID

USER_ID_SWITCH

Message text

User attempted username change in session (logout required first!). Current user id: "{0}", new user id: "{1}"

Log4j variables

user_current, user_new

Description

An authenticated user performed a login on the SLS again and used a different loginname than during the initial login. This means that the user effectively tried to switch the user id within a session; one possible reason is that when an authenticated user was locked out due to the inactivity timeout, another user tried to gain access to the application session of that user, by

authenticating using valid (but different) credentials. So it could be a sign of an attempt to access data of another user.

Category: AUDIT

Severity: WARN

Message ID

USER_LOGGED_OUT

Message text

Logout successfully completed. User: "{0}". Redirected to: "{1}".

Log4j variables

user, destination

Description

A user logged out successfully and was redirected to the specified location (see logfile for details).

Category: AUDIT

Severity: INFO

Message ID

USER_MAPPED

Message text

Mapping successfully performed. User: "{0}". Mapped id: "{1}".

Log4j variables

user, id

Description

User was mapped to the mapped id.

Category: AUDIT

Severity: INFO

Message ID

USER_MISSING_TOKEN

Message text

Operation failed: "{0}", The user needs a "{1}" to perform this operation.

Log4j variables

reason, token

Description

This message indicates a wrong configured application or sls model. The user should not be able to request impossible operations.

Category: AUDIT

Severity: INFO

Message ID

USER_PASSWORD_CHANGED

Message text

Password change successfully completed. User: "{0}".

Log4j variables

user

Description

A user has successfully changed the password.

Category: AUDIT**Severity:** INFO**Message ID**

USER_PASSWORD_RESET

Message text

Password reset. User: "{0}". New password sent to: "{1}".

Log4j variables

user, email

Description

This message indicates that the password for a user was reset by the SLS. This procedure may occur, if a user forgot his password. A new password will be generated and sent to the user by email.

Category: AUDIT**Severity:** INFO**Message ID**

USER_REAUTH_FAILED

Message text

Re-authentication failed. User: "{0}" Reason: "{1}"

Log4j variables

user, reason

Description

A user failed to perform a re-authentication. See the log message for details.

Category: AUDIT**Severity:** INFO**Message ID**

USER_REAUTH_SUCESS

Message text

Re-authentication successfully completed. User: "{0}"

Log4j variables

user

Description

A user had successfully performed a re-authentication.

Category: AUDIT**Severity:** INFO**Message ID**

USER_SESSION_EXPIRED

Message text

A login service session expired. User: "{0}", State: "{1}", Session: "{2}", Errors: "{3}"

Log4j variables

user, state, session, errors

Description

A user either closed his browser, or the browser crashed before the current process was completed. See the log message for information about the current model state of the session, and if there had been any errors during that session.

Category: AUDIT

Severity: INFO

Message ID

USER_STEP1_OK

Message text

Username and password authentication successful. User: "{0}".

Log4j variables

user

Description

User successfully performed the first login step.

Category: AUDIT

Severity: INFO

Type: ERROR

Message ID

AAI_NTLM_LOGIN_DETECTED

Message text

Possible AAI NTLM Request detected! Please make sure that the SRM configuration does not use the NTLM AAI module for the SLS login location!

Log4j variables

-

Description

Possible AAI NTLM Request detected! The current request contained an NTLM 'Authorization' header, but was a POST request. NTLM login always uses GET requests only, so this indicates that accidentally NTLM AAI login was configured in the SRM for the SLS location. This leads to strange problems caused by the SRM sending two separate requests to the SLS for one single client request, which is why AAI on the SLS location MUST always be disabled.

Category: SYSTEM**Severity:** ERROR**Message ID**

BACKEND_INVALID

Message text

Invalid backend system / host specified. System: "{0}"

Log4j variables

backend_system

Description

The host name specified for the back-end system was invalid.

Category: SYSTEM**Severity:** ERROR**Message ID**

BACKEND_STATE_UNCLEAR

Message text

The state of a back-end system is unclear. Back-end system: "{0}"

Log4j variables

backend_system

Description

The state of a back-end system is unclear. This usually means that a request could be successfully sent to the back-end system, but no response was sent back. One typical cause can be extreme load on that system. Since it is unclear in that moment if the request was processed, and if any underlying kind of database had been changed, the same request should not be sent again to avoid accidental multiple data changes that could result in locking out a user under certain circumstances.

Category: SYSTEM**Severity:** ERROR**Message ID**

BACKEND_UNAVAILABLE

Message text

Backend service not available. Reason: "{0}", Back-end system: "{1}"

Log4j variables

reason, backend_system

Description

The back-end service was not available. See log message for details.

Category: SYSTEM

Severity: ERROR

Message ID

BAD_REQUEST

Message text

Bad request. Reason: "{0}"

Log4j variables

reason

Description

The client request was invalid. See SES/HSP error logs for details.

Category: USER

Severity: ERROR

Message ID

CUSTOM_JEXL_ERROR

Message text

A custom error was caused intentionally through JEXL. Reason: "{0}"

Log4j variables

reason

Description

A custom error was created through the JEXL function 'failWithCustomError'. See log message for details.

Category: USER

Severity: ERROR

Message ID

ERR_BLACKLIST_FAILED

Message text

Browser blacklist check failed. Reason: "{0}"

Log4j variables

reason

Description

There was a technical error while processing the blacklist file. Check if the file exists and / or if the user account used for running the SLS has the right to read the file.

Category: SYSTEM

Severity: ERROR

Message ID

ERR_CACHE_NOT_FOUND

Message text

The cache with name "{0}" could not be found.

Log4j variables

name

Description

A cache related JEXL function referred to a cache that does not exist (any more). See the log message for details and verify / correct the configuration accordingly.

Category: SYSTEM**Severity:** ERROR**Message ID**

ERR_CLASS_INVALID_JAVA_VERSION

Message text

Class (maybe referenced indirectly) compiled with incompatible Java version. Class: "{0}", current JVM version: "{1}"

Log4j variables

class, version

Description

A Java class could not be loaded because it was compiled with a (probably newer) Java version that is not compatible with the one used at runtime by this service. Please check the JVM requirements as defined in the documentation and verify your runtime environment / profile. Be aware that the class name logged in the error message is not always the actual cause of the problem; it might as well be a class reference by an import within that class. Therefore, you may also want to look for any additional JAR files referenced by the class named in the error message.

Category: SYSTEM**Severity:** ERROR**Message ID**

ERR_CONFIG

Message text

Configuration error. Reason: "{0}"

Log4j variables

reason

Description

There is a problem with the configuration. See the log message for details and verify / correct the configuration accordingly.

Category: SYSTEM**Severity:** ERROR**Message ID**

ERR_CONFIG_ADAPTER

Message text

Log4j variables	Adapter configuration error. Reason: "{0}"
Description	reason There is a problem with the adapter configuration. See the log message for details and verify / correct the configuration accordingly. Category: SYSTEM Severity: ERROR
Message ID	ERR_CONFIG_SLS
Message text	SLS configuration error. Reason: "{0}"
Log4j variables	reason
Description	There is a problem with the configuration. See the log message for details and verify / correct the configuration accordingly. Category: SYSTEM Severity: ERROR
Message ID	ERR_CONFIG_STRUTS
Message text	Struts configuration error. Reason: "{0}"
Log4j variables	reason
Description	There is a problem with the Struts configuration. See the log message for details and verify / correct the configuration accordingly. Category: SYSTEM Severity: ERROR
Message ID	ERR_ILLEGAL_PKI_TRUST_GROUP
Message text	Illegal PKI trust group alias "{0}"
Log4j variables	alias
Description	The indicated trust group alias is not configured in any PKI adapter properties. Category: SYSTEM Severity: ERROR

Message ID

ERR_INTERNAL_STATE

Message text

Invalid internal state! Reason: "{0}"

Log4j variables

reason

Description

Invalid internal process (model) state. This is a severe internal error that may be caused by configuration errors or JVM problems.

Category: SYSTEM**Severity:** ERROR**Message ID**

ERR_INV_ADAPTER

Message text

Invalid adapter class assigned. Class: "{0}" is not an instance of Type: "{1}".

Log4j variables

class, type

Description

An adapter implementation class is not inherited from the appropriate interface. Please verify the adapter configuration.

Category: SYSTEM**Severity:** ERROR**Message ID**

ERR_INV_FILENAME

Message text

Error reading file: "{0}", Reason: "{1}".

Log4j variables

filename, reason

Description

An error occurred while reading a file. Check if the file exists and / or if the user account used for running the service has the right to read the file.

Category: SYSTEM**Severity:** ERROR**Message ID**

ERR_INV_PROPERTY

Message text

Failed reading a property from a '*.properties' file. Property: "{0}", Value: "{1}", Reason: "{2}"

Log4j variables

property, value, reason

Description

This message appears, if a specified configuration property hasn't the proper format or value.

Category: SYSTEM
Severity: ERROR

Message ID

ERR_LDAP_EXCEPTION

Message text

LDAP exception occurred. LDAP bind principal was: "{0}". Reason: "{1}"

Log4j variables

ldap_principal, reason

Description

Exception thrown in underlying LDAP implementation. If an LDAP error code could be obtained from the inner exception, it is appended to the message name, e.g. ERR_LDAP_EXCEPTION_32. For more details check the inner exception.

Category: SYSTEM
Severity: ERROR

Message ID

ERR_MISCONFIGURED_XPATH_VARIABLE_RULE

Message text

Misconfigured rule for JEXL/Groovy variable creation via XPath: Reason: "{0}"

Log4j variables

reason

Description

A Rule for creating a JEXL/Groovy variable by parsing an XML response is misconfigured. Check the corresponding XML response template (if present) and rules configured directly via properties (if present). See the log message for details and verify / correct the configuration accordingly.

Category: SYSTEM
Severity: ERROR

Message ID

ERR_SEND_EMAIL

Message text

Failed to send email. Reason: "{0}"

Log4j variables

reason

Description

Failed to send email due to a configuration or connection issue.

Category: USER
Severity: ERROR

Message ID

ERR_SLS_COMPRESSION

Message text

	Compression-related error. Operation: "{0}", Reason: "{1}"
Log4j variables	operation, reason
Description	Data compression or de-compression failed for some reason (usually a technical issue). See the log message for details. Category: SYSTEM Severity: ERROR
Message ID	ERR_SLS_CRYPT
Message text	SSL / Crypto related error. Reason: "{0}"
Log4j variables	reason
Description	Cryptography-related error (algorithm was not available etc.). One likely cause is that the JVM used to run the login service does not contain the unrestricted security policies that must be downloaded separately from Sun's website. Category: SYSTEM Severity: ERROR
Message ID	ERR_UNKNOWN_HOST
Message text	Unable to communicate with host, hostname unknown! Reason: "{0}"
Log4j variables	reason
Description	Unable to communicate with host. The hostname could not be resolved, so there may be a DNS configuration issue, or an invalid hostname in the SLS configuration. Category: SYSTEM Severity: ERROR
Message ID	ERR_WS_SOAP_FAULT
Message text	The received HTTP SOAP response contains a fault with value "{0}", which is configured for a {1}. Config property: "{2}"
Log4j variables	fault_value, exception_type, property
Description	The received HTTP SOAP response contains a SOAP Fault. For details check the response body. Category: SYSTEM Severity: ERROR

Message ID

ERR_XPATH_JEXL_VARIABLE_CREATION_FAILED

Message text

Failed to extract JEXL variable "{0}" from an XML document by XPath expression. Reason: "{1}"

Log4j variables

name, reason

Description

A rule for creating a JEXL variable by parsing an XML document failed, either because the XPath expression has been misconfigured or or possibly due to illegal data in the parsed XML document. See the log message for details and verify / correct the configuration accordingly.

Category: SYSTEM**Severity:** ERROR**Message ID**

EXPR_EMPTY

Message text

Empty expression in configuration. Expression: "{0}"

Log4j variables

expression

Description

An expression in the configuration was empty. A likely cause is there is a mistake with the brackets or a typo in the configuration string.

Category: SYSTEM**Severity:** ERROR**Message ID**

EXPR_MISSING_CLOSING_BRACKET

Message text

Bracket missing in expression in configuration. Expression: "{0}"

Log4j variables

expression

Description

A (probably closing) bracket was missing in an expression in the configuration.

Category: SYSTEM**Severity:** ERROR**Message ID**

GROOVY_SCRIPTDIRS_RECOMPILE_FAILURE

Message text

Updated Groovy script files failed to compile (staying at last good state). Reason: "{0}"

Log4j variables

reason

Description

A change of script files in the configured Groovy script directories had been detected and the updated Groovy script files failed to compile successfully.

Category: SYSTEM
Severity: ERROR

Message ID

INVALID_EXPR

Message text

Invalid expression in configuration. Expression: "{0}"

Log4j variables

expression

Description

An expression in the configuration could not be evaluated. Check for errors (like missing parenthesis characters).

Category: SYSTEM
Severity: ERROR

Message ID

JEXL_DATAPROTECTOR_ERROR

Message text

A DataProtector operation failed. Operation: "{0}". Reason: "{1}"

Log4j variables

operation, reason

Description

An encryption or decryption operation with the DataProtector failed. See the log message for details. However, a typical source for this problem would be an invalid keystore. So make sure that the keystore used for the operation contains the correct key (which depends on the passphrase that was entered when the keystore was created).

Category: SYSTEM
Severity: ERROR

Message ID

JEXL_FORBIDDEN_VARIABLENAME

Message text

Attempt to create JEXL variable with a reserved name. Forbidden name: "{0}"

Log4j variables

name

Description

A JEXL expression tried to create / set a variable with a name that is reserved by the framework for a function class. Please just use a different name for the variable. See the log message for the name in question.

Category: SYSTEM
Severity: ERROR

Message ID

JEXL_FUNCTION_OVERWRITTEN

Message text

JEXL function object lost; probably overwritten by buggy JEXL script. Check scripts for '=' assignment operators in conditions, where '==' should be used. Object: "{0}"

Log4j variables

object

Description

An instance of a JEXL function object such as 'session', 'function' or 'response' has disappeared from the current JEXL context (or wasn't of the correct Java class type anymore). The most common reason is an accidental assignment of some String or other value to such a variable in a buggy condition: In conditions, the '==' operator must be used to compare two values; a simple typo like '=' will instead assign the right-hand value to the left-hand variable, thereby overwriting it. Fix it by replacing the buggy '=' operator with the correct '==' or 'eq' operator.

Category: SYSTEM

Severity: ERROR

Message ID

JEXL_ILLEGAL_ARGUMENTS

Message text

Required arguments missing in JEXL function for creating a failure. Expression: "{0}"

Log4j variables

expression

Description

The JEXL functions which allow to cause an authentication failure required the correct number of arguments for the given message ID. Please read the 'log-messages.pdf' file for a complete list of all IDs and the number of arguments they take.

Category: SYSTEM

Severity: ERROR

Message ID

JEXL_INVALID_MESSAGE_ID

Message text

Invalid message ID used in JEXL function for creating a failure. See 'log-messages.pdf' for valid IDs. Invalid ID: "{0}"

Log4j variables

id

Description

The JEXL functions which allow to cause an authentication failure required a message ID (which is then used through the error mapping to display a message to the end-user). In this case, an illegal (non-existent) ID was used. Please read the 'log-messages.pdf' file for a complete list of all error IDs.

Category: SYSTEM

Severity: ERROR

Message ID

JVM_ERROR_OCCURRED

Message text

A Java VM Error occurred. An SLS restart is advised. Error: "{0}"

Log4j variables

jvm_error

Description

A Java error occurred. This is a kind of throwable (not an exception) which indicates a serious technical problem, like an OutOfMemoryError. Since errors usually indicate issues within the JVM itself, the state of the SLS must be considered invalid at that point, and the login service should be restarted.

Category: SYSTEM
Severity: ERROR

Message ID

JWT_ERROR

Message text

A JWT (JSON Web Token) error occurred. User: "{0}". Reason: "{1}".

Log4j variables

user, reason

Description

A JWT (JSON Web Token) related error occurred during processing of JWTs, see reason for details.

Category: SYSTEM
Severity: ERROR

Message ID

LDAP_ADD_ATTRIBUTE_FAILED

Message text

Failed to add an LDAP attribute. Attribute: "{0}", DN: "{1}", Operation: "{2}", Reason: "{3}".

Log4j variables

attribute, dn, operation, reason

Description

An attribute value could not be added in the LDAP directory. Check the log message for details.

Category: SYSTEM
Severity: ERROR

Message ID

LDAP_MODIFY_ATTRIBUTE_FAILED

Message text

Failed to modify (or search) LDAP attribute. Attribute: "{0}", DN: "{1}", Operation: "{2}", Reason: "{3}".

Log4j variables

attribute, dn, operation, reason

Description

An attribute value could not be modified (or searched) in the LDAP directory. Check the log message for details.

Category: SYSTEM
Severity: ERROR

Message ID

LDAP_PASSWORD_CHANGE_FAILED

Message text

Failed to perform LDAP password change. DN: "{0}", Reason: "{1}".

Log4j variables

dn, reason

Description

An LDAP password change could not be performed for some reason. Check the log message for details.

Category: SYSTEM

Severity: ERROR

Message ID

MODEL_CONFIG_ERROR

Message text

Invalid model/state configuration. Error during model initialisation. Model: "{0}".

Log4j variables

model

Description

This error appears, if a requested model/state could not be found. Please verify the states in all SLS model configurations.

Category: SYSTEM

Severity: ERROR

Message ID

MODEL_EMPTY

Message text

Invalid model configuration, model has no states. Model: "{0}".

Log4j variables

model

Description

This error appears, if a requested model had no states configured. Please verify the states in all SLS model configurations.

Category: SYSTEM

Severity: ERROR

Message ID

MULTIPLE_MODELS_FOR_URI

Message text

More than one model for uri defined. Uri: "{0}", Model1: "{1}", Model2: "{2}"

Log4j variables

uri, model1, model2

Description

This error appears, if the same uri has been configured for more than one model. Please verify the model configuration.

Category: SYSTEM

Severity: ERROR

Message ID

NO_MODEL_FOR_URI

Message text

No model for uri defined. Uri: "{0}"

Log4j variables

uri

Description

This error appears, if a required model could not be found. Please verify the model configuration.

Category: SYSTEM

Severity: ERROR

Message ID

OIDC_ERROR

Message text

An OpenID Connect error occurred. User: "{0}". Reason: "{1}".

Log4j variables

user, reason

Description

An OpenID Connect (OIDC) related error occurred during processing of OIDC messages/objects, see reason for details.

Category: SYSTEM

Severity: ERROR

Message ID

PATH_PREFIX_NAMESPACE_MISSING

Message text

An XPath expression used a prefix for which no namespace was found in the XML data: "{0}" (use 'ws.adapter.ignore.namespaces=true' to avoid namespace issues)

Log4j variables

data

Description

An XPath expression was applied to XML data, and the XPath expression contained prefixes which had no corresponding namespace definition in the XML data. Either adapt the XML data or the XPath expression (in case of the Webservice adapter, the response templates may contain the invalid prefixes) or disable namespace handling for the WS adapter, by setting the property 'ws.adapter.ignore.namespaces=true'

Category: SYSTEM

Severity: ERROR

Message ID

SAML_ERROR

Message text

A SAML error occurred. User: "{0}". Reason: "{1}".

Log4j variables

user, reason

Description

A SAML (Security Assertion Markup Language) related error occurred during processing of SAML messages/objects, see reason for details.

Category: SYSTEM**Severity:** ERROR**Message ID**

SPNEGO_EXCEPTION

Message text

Spnego/Kerberos exception occurred. Process: "{0}". Problem guess: "{1}"

Log4j variables

reason, guess

Description

Exception thrown in underlying spnego/kerberos implementation. For details check the inner exception.

Category: SYSTEM**Severity:** ERROR**Message ID**

STARTUP_ERROR

Message text

There were startup errors. Reason: "{0}"

Log4j variables

reason

Description

The service failed to start due to some technical or configuration error. See log file for details.

Category: SYSTEM**Severity:** ERROR**Message ID**

WEBAUTHN_ERROR

Message text

A WebAuthn error occurred. User: "{0}". Reason: "{1}".

Log4j variables

user, reason

Description

A WebAuthn (Web Authentication / FIDO2) related error occurred during processing of WebAuthn messages/objects, see reason for details.

Category: SYSTEM**Severity:** ERROR

Type: INFO

Message ID

BACKEND_AVAILABLE_AGAIN

Message text

Backend service has become available again. Back-end system: "{0}"

Log4j variables

backend_system

Description

The previously unavailable back-end service has become available again.

Category: SYSTEM**Severity:** INFO**Message ID**

BACKEND_SYSTEM

Message text

Back-end selected. Adapter: "{0}", System: "{1}"

Log4j variables

type, backend_system

Description

The adapter of the defined type (like 'ldap') uses the named back-end authentication system.

Category: SYSTEM**Severity:** INFO**Message ID**

BACKEND_SYSTEM_TOP

Message text

Back-end system with shortest response time: Type: "{0}", Time/ms: "{1}", System: "{2}"

Log4j variables

type, time_ms, backend_system

Description

Informational log which simply tells which of the available back-end systems of a certain type performs best.

Category: SYSTEM**Severity:** INFO**Message ID**

CONFIG_UPDATED

Message text

Configuration updated successfully. Detail: "{0}",

Log4j variables

detail

Description

If a configuration change was performed and the configuration was updated with the new configuration properties.

Category: SYSTEM
Severity: INFO

Message ID

FAILOVER_ENDS

Message text

Backendsystem "{0}" state is back to normal for the next call. Skip Counter decreased to 0 now.

Log4j variables

type

Description

This info will appear when the skip-counter of a back end system is back to 0.

Category: SYSTEM
Severity: INFO

Message ID

GENERAL_INFO

Message text

Information: "{0}"

Log4j variables

info

Description

Informational log, see message for details.

Category: SYSTEM
Severity: INFO

Message ID

GROOVY_SCRIPTDIRS_RECOMPILE_SUCCESS

Message text

Updated Groovy script files compiled successfully.

Log4j variables

-

Description

A change of script files in the configured Groovy script directories had been detected and the updated Groovy script files have been compiled successfully.

Category: SYSTEM
Severity: INFO

Message ID

GROOVY_STATIC_VARIABLE_INTENTIONALLY_SHARED

Message textStatic non-final field (marked as shared intentionally between login sessions) found in Groovy script.
Reason: "{0}"

Log4j variables

reason

Description

A static non-final field has been found in a Groovy script. This means that different login sessions can read from and write to this field, which is potentially a security risk (sessions not fully separated). However, the variable has been marked as safe to share between login sessions because its name contains the string 'SlsIntentionallyShared'.

Category: SYSTEM**Severity:** INFO**Message ID**

INVALID_REQ_PARAM

Message text

The SLS ignores the invalid REQ parameter. Parameter: "{0}"

Log4j variables

parameter

Description

There was a REQ parameter in the request, but the SLS had a problem during decryption. The invalid REQ parameter is ignored. Details of the failure are logged before, when the decryption exception was thrown.

Category: USER**Severity:** INFO**Message ID**

JWT_INFO

Message text

A JWT (JSON Web Token) info message. User: "{0}". Reason: "{1}".

Log4j variables

user, reason

Description

JWT (JSON Web Token) related information is given, see reason for details.

Category: SYSTEM**Severity:** INFO**Message ID**

MEMORY_USAGE

Message text

Currently used memory: {0}, Total Java VM memory: {1}.

Log4j variables

memory_used, memory_total

Description

Informational log, informs about memory usage.

Category: SYSTEM**Severity:** INFO

Message ID

MISSING_REQ_PARAM

Message text

The SLS expected a request with a REQ parameter, Details "{0}".

Log4j variables

detail

Description

There was no REQ parameter in the request, but the SLS expected a REQ parameter. This can i.e. happen, when a user is on a page of a 3rd party application, which should respond the SLS a status in the REQ parameter, but the user navigates with the browser back button to SLS. See the error message for details.

Category: USER**Severity:** INFO**Message ID**

MODULE_ACTUALLY_USED

Message text

Module used: "{0}" - "{1}"

Log4j variables

module_title, module_description

Description

Lists a module used in the current SLS instance. All such modules must be licensed appropriately.

Category: SYSTEM**Severity:** INFO**Message ID**

MODULE_USAGE_REASON

Message text

why: "{0}"

Log4j variables

detail

Description

Lists details about why the SLS determined a certain module to be actually in use.

Category: SYSTEM**Severity:** INFO**Message ID**

OIDC_INFO

Message text

An OpenID Connect info message. User: "{0}". Reason: "{1}".

Log4j variables

user, reason

Description

OpenID Connect (OIDC) related information is given, see reason for details.

Category: SYSTEM
Severity: INFO

Message ID

SAML_INFO

Message text

A SAML info message. User: "{0}". Reason: "{1}".

Log4j variables

user, reason

Description

SAML (Security Assertion Markup Language) related information is given, see reason for details.

Category: SYSTEM
Severity: INFO

Message ID

SLS_GOT_TGT

Message text

The SLS logged in successfully to the KDC. KDC user: "{0}".

Log4j variables

kdc_user

Description

Informational log, telling the kerberos user account name of the sls. And the successful log in to KDC.

Category: SYSTEM
Severity: INFO

Message ID

SLS_INFO

Message text

Information: "{0}"

Log4j variables

info

Description

Informational log, see message for details.

Category: SYSTEM
Severity: INFO

Message ID

SLS_MISSING_AUTH

Message text

Missing authorization "{0}" for path "{1}"

Log4j variables

	authorization, path
Description	<p>Informational log, about missing authorization. Helps to spot config error, which forced a redirect to the SLS.</p> <p>Category: SYSTEM Severity: INFO</p>
Message ID	SLS_SESSION_INFO
Message text	Number of open sessions: before cleanup {0}, after cleanup {1}.
Log4j variables	sessions_before_cleanup, sessions_after_cleanup
Description	<p>Informational log, informs about number of currently open sessions.</p> <p>Category: SYSTEM Severity: INFO</p>
Message ID	SLS_START
Message text	USP Secure Login Service successfully started. Version: "{0}", Instance: "{1}", JVM: "{2}"
Log4j variables	version, instance, jvm_info
Description	<p>The SLS startup message. This message appears when the login service startup procedure has completed.</p> <p>Category: SYSTEM Severity: INFO</p>
Message ID	SLS_STEPUP
Message text	Missing authentication level "{0}" current level is "{1}"
Log4j variables	authentication_level_missing, authentication_level_current
Description	<p>The SLS was requested to perform a step up. This is just Informational log to spot a config error, which forced a redirect to the SLS.</p> <p>Category: SYSTEM Severity: INFO</p>
Message ID	SLS_STOP

Message text

USP Secure Login Service shutdown performed. Version: "{0}"

Log4j variables

version

Description

The SLS shutdown message. This message appears when the login service was stopped.

Category: SYSTEM

Severity: INFO

Message ID

TENANT_FOUND

Message text

Tenant successfully resolved and set. Tenant: "{0}".

Log4j variables

tenant

Description

Informational log, informs about successful tenant resolving.

Category: USER

Severity: INFO

Message ID

TENANT_NOT_FOUND

Message text

Tenant could not be resolved. Value: "{0}"

Log4j variables

tenant

Description

Informational log, informs about an unsuccessful tenant resolving.

Category: USER

Severity: INFO

Message ID

TENANT_SWITCHING

Message text

The request contains another tenant than the one previously selected in this session. Old tenant: "{0}", New tenant: "{1}".

Log4j variables

tenant_old, tenant_new

Description

Informational log, in productive environment the user's SlsSession will be invalidated, then can restart with the requested new tenant.

Category: USER

Severity: INFO

Message ID

USER_CANCEL

Message text

The user cancelled the execution of this model.

Log4j variables

-

Description

Informational log, informs about an unsuccessful tenant resolving.

Category: USER**Severity:** INFO**Message ID**

WEBAUTHN_INFO

Message text

A WebAuthn info message. User: "{0}". Reason: "{1}".

Log4j variables

user, reason

Description

WebAuthn (Web Authentication / FIDO2) related information is given, see reason for details.

Category: SYSTEM**Severity:** INFO

Type: WARN

Message ID

ACCESS_AREA_HEADER_FORBIDDEN

Message text

The header 'AccessArea' was set for allowing access without actual authentication.

Log4j variables

-

Description

The header 'AccessArea' was set to a value other than 'Invalidate' or 'InvalidateAll', meaning that the SES session should have been set to authenticated mode. However, a cross-check revealed that no actual authentication had been performed yet, so this was either an SLS internal error, or a malicious try to set the header, for instance from within a manipulated (or customized) SLS JSP.

Category: SYSTEM**Severity:** WARN**Message ID**

ACTION_NOT_ALLOWED_BY_GET

Message text

GET for current model state ignored! Use JEXL function 'session.processNextGETasPOST()' to enforce GET request processing.

Log4j variables

-

Description

An action was requested with a GET request, but was only allowed with a POST request. At this point, only a POST request will advance the model state. Certain actions in the SLS will only actually perform anything with a POST request. GET requests will not advance the model in the session - usually. If, for whatever reason, a GET request should be processed like a POST request, the JEXL function 'session.processNextGETasPOST()' must be used.

Category: USER**Severity:** WARN**Message ID**

ADAPTER_CLASS_MISSING

Message text

Configured adapter class not available. Class: "{0}"

Log4j variables

class

Description

An adapter class specified somewhere in a configuration file was not found in the classpath. This may be a severe problem or not, depending on if that adapter should actually be used by the SLS instance (or if the configuration error is just some kind of copy-paste-leftover etc.).

Category: SYSTEM**Severity:** WARN**Message ID**

Message text	AUTH_REQUIRED
Log4j variables	Authentication required. Reason: "{0}"
Description	reason User must authenticate first before the requested function (like a password change) can be performed. Category: USER Severity: WARN
Message ID	AUTH_VERIFICATION
Message text	Authentication verification required. Reason: "{0}"
Log4j variables	reason
Description	User must submit credentials again (re-authentication is required). Category: USER Severity: WARN
Message ID	CA_CERTIFICATE_EXPIRED
Message text	The CA certificate with Subject "{0}" is expired.
Log4j variables	subject
Description	The CA certificate used to verify a client certificate during authentication is expired. This CA certificate should be renewed. Note that removal of this CA certificate will lead to authentication failure for users still using the same client certificates. Category: SYSTEM Severity: WARN
Message ID	CA_CERTIFICATE_NOT_YET_VALID
Message text	The CA certificate with Subject "{0}" is not yet valid.
Log4j variables	subject
Description	The CA certificate used to verify a client certificate during authentication is not yet within the validity period. Note that removal of this CA certificate will lead to authentication failure for users still using the same client certificates.

Category: SYSTEM
Severity: WARN

Message ID

CACHE_ELEMENTS_EVICTED

Message text

{1} element(s) had to be evicted from cache "{0}".

Log4j variables

name, count

Description

If this is a cache that has been created with the cache.createCache() JEXL/Groovy function, consider increasing the maximal number of elements in the cache.

Category: SYSTEM
Severity: WARN

Message ID

CACHE_FIRST_ELEMENT_EVICTED

Message text

The first element had to be evicted from cache "{0}"; additional warnings will be logged each time after {1} more element(s) have been evicted.

Log4j variables

name, warn_step_size

Description

If this is a cache that has been created with the cache.createCache() JEXL/Groovy function, consider increasing the maximal number of elements in the cache.

Category: SYSTEM
Severity: WARN

Message ID

CERTIFICATE_EXPIRED

Message text

The client certificate is expired.

Log4j variables

-

Description

The certificate sent by the client during the SSL handshake is expired.

Category: USER
Severity: WARN

Message ID

CERTIFICATE_INVALID

Message text

The client certificate is invalid. Reason: "{0}"

Log4j variables

reason

Description

The certificate sent by the client during the SSL handshake is invalid. See the log message for details.

Category: USER

Severity: WARN

Message ID

CERTIFICATE_NOT_TRUSTED

Message text

The client certificate was not signed by a trusted issuer.

Log4j variables

-

Description

The certificate sent by the client during the SSL handshake is not signed by a trusted Certification Authority (CA). One likely cause for this problem may be a configuration error in the PKI adapter. Check the configuration for trusted CAs as described in the Admin Guide.

Category: USER

Severity: WARN

Message ID

CERTIFICATE_NOT_YET_VALID

Message text

The client certificate is not yet valid.

Log4j variables

-

Description

The certificate sent by the client during the SSL handshake is not yet valid, which means that the current Date or the specified Date is before the notBefore date/time in the Certificate validity period.

Category: USER

Severity: WARN

Message ID

CERTIFICATE_REVOKED

Message text

The client certificate has been revoked. Reason: "{0}"

Log4j variables

reason

Description

The certificate sent by the client during the SSL handshake has been revoked. See the log message for details.

Category: USER

Severity: WARN

Message ID

CONFIG_PROPERTY_EXISTS_TWICE

Message text

Configuration property has been set twice (in two property files). Property: "{0}"

Log4j variables

property

Description

A configuration property was set twice (or more), in different property files. Check the configuration property files for occurrences of the property (the name is printed to the log record). This is only a warning because in this case both property definitions had the same value. If the same property had been defined twice with different values, the service would have failed startup with an error message.

Category: SYSTEM

Severity: WARN

Message ID

ERR_INV_REGEX

Message text

Error while parsing Expression: {0} key: {1}. Entry will be ignored

Log4j variables

regex, key

Description

An invalid regular expression was added to the browser blacklist configuration. The login service continues execution. Nevertheless, the regular expressions in the browser blacklist properties file should be checked.

Category: SYSTEM

Severity: WARN

Message ID

ERR_JSP_TAGUSAGE

Message text

Error while execution of tag: {0} Details: {1}

Log4j variables

tag, detail

Description

Probably the jsp is using the tag in a wrong way.

Category: SYSTEM

Severity: WARN

Message ID

ERR_REGEX_FUNCTION

Message text

Parameters of JEXL function 'regex' may be invalid: REGEX: "{0}", Input: "{1}", Detail: "{2}"

Log4j variables

regex, input, detail

Description

The arguments for the JEXL 'regex' function may have been mixed up in the configuration property. Check the parameters and make sure that the first one is the regular expression, and the second the input string that should be parsed.

Category: SYSTEM
Severity: WARN

Message ID

ERR_RELOADING_BLACKLIST

Message text

Error while reloading the browser blacklist configuration. Reason: "{0}"

Log4j variables

reason

Description

Browser blacklist configuration reload error. See the log message for details. The most common cause is that the blacklist file specified in the SLS configuration does not exist (for instance if it was moved or renamed).

Category: SYSTEM
Severity: WARN

Message ID

FAILOVER_PERFORM

Message text

Adapter failover performing. Info: "{0}", Causing backend-exception: "{1}".

Log4j variables

info, cause

Description

This warning will appear if a failover to another back-end system will be performed. Usage of the causing backend system is not possible until the failover procedure is done. The end of the failover procedure is indicated by a log of the message 'FAILOVER_PERFORMED'. Unsuccessful usage of the backend system during the failover process is indicated with the log message 'BACKEND_FAILOVER_PENDING'

Category: SYSTEM
Severity: WARN

Message ID

FAILOVER_PERFORMED

Message text

Adapter failover has been performed.

Log4j variables

-

Description

This warning will appear if a failover of the back-end system has been performed. The failover procedure has only been performed if the adapter supports it.

Category: SYSTEM
Severity: WARN

Message ID

FORMATTER_POOL_EXCEEDED

Message text

The pool for JEXL date formatting objects has reached it's size limit and is being cleaned up! Size: "{0}"

Log4j variables

size

Description

The pool for date formatter objects should actually remain stable after having grown to the number of threads pooled by the app server. If it still grows larger and larger, there might be a problem with the server threads; but it might also be that for some reasons, the server just occasionally creates new threads, so this cleanup is just a necessary precaution.

Category: SYSTEM**Severity:** WARN**Message ID**

GENERAL_WARNING

Message text

Reason: "{0}"

Log4j variables

reason

Description

A general warn message. Check the log files for further details.

Category: SYSTEM**Severity:** WARN**Message ID**

GROOVY_STATIC_VARIABLE

Message text

Static non-final field in Groovy script. Reason: "{0}"

Log4j variables

reason

Description

A static non-final field has been found in a Groovy script. This means that different login sessions can read from and write to this field, which is potentially a security risk (sessions not fully separated). It is recommended to refactor to an instance field or a static final field. If really needed and safe to use, change the variable name so that it contains the string 'IsIntentionallyShared' (comparison not case sensitive).

Category: SYSTEM**Severity:** WARN**Message ID**

ILLEGAL_CHARS_IN_URL

Message text

A redirect URL with illegal characters was used. URL: "{0}"

Log4j variables

url

Description

A redirect URL, either from the 'requestedPage' header or the 'target' parameter, contained illegal characters such as line breaks. This could indicate some kind of attack. Check the log files for details.

Category: USER**Severity:** WARN**Message ID**

INVALID_CHALLENGE_RESPONSE

Message text

Invalid challenge. Reason: "{0}"

Log4j variables

reason

Description

The challenge code is invalid. See log message for details.

Category: USER**Severity:** WARN**Message ID**

INVALID_CRED

Message text

Invalid credential(s). Reason: "{0}"

Log4j variables

reason

Description

A user credential is invalid. See log message for details.

Category: USER**Severity:** WARN**Message ID**

INVALID_NEW_PWD_SAME_AS_OLD

Message text

Password change failed because the new password is the same as the old one.

Log4j variables

-

Description

Password change failed because the new password is the same as the old one.

Category: USER**Severity:** WARN**Message ID**

INVALID_PARAM_PASSING

Message text

Value(s) for parameter passing are invalid or incomplete. Parameter: "{0}"

Log4j variables

parameter

Description

Value(s) for parameter passing are invalid or incomplete. See log message for details.

Category: USER

Severity: WARN

Message ID

INVALID_PARM_FULLREGEX

Message text

Invalid request parameter. Parameter: "{0}", Reason: "{1}"

Log4j variables

parameter, reason

Description

A request parameter is invalid according to the full regular expression configured for the parameter checker. See log message for details.

Category: USER

Severity: WARN

Message ID

INVALID_PARM_LENGTH

Message text

Invalid request parameter length. Parameter: "{0}", Reason: "{1}"

Log4j variables

parameter, reason

Description

A request parameter length is invalid according to the rules configured for the parameter checker. See log message for details.

Category: USER

Severity: WARN

Message ID

INVALID_PARM_REGEX

Message text

Invalid request parameter. Parameter: "{0}", Reason: "{1}"

Log4j variables

parameter, reason

Description

A request parameter contains invalid characters. See log message for details.

Category: USER

Severity: WARN

Message ID

JEXL_ERROR_FUNC_IN_JSP_STATE

Message text

JEXL error throwing function found in JSP state action; note that this function will only be executed once the model advances to the next state, not while the JSP is displayed. Also, it will result in a 500 error response instead of switching to the 'failedState', due to different internal processing of JSP states compared to other states like 'do.auth'. State: "{0}". Function: "{1}"

Log4j variables

operation, reason

Description

A JEXL function was found in JSP state action; note that this function will only be executed once the model advances to the next state, not while the JSP is displayed. Also, it will result in a 500 error response instead of switching to the 'failedState', due to different internal processing of JSP states compared to other states like 'do.auth'. It is recommended to move the JEXL function to a different state before or after the JSP, depending on the use-case at hand.

Category: SYSTEM**Severity:** WARN**Message ID**

JEXL_INVALID_EXPRESSION

Message text

A JEXL expression is invalid. Reason: "{0}"

Log4j variables

reason

Description

A JEXL expression seemed to use either an unknown prefix or invoked a non-existent method on that object. The cause is most likely a typo in an expression, like 'function.getXurrentYear()' instead of 'function.getCurrentYear()'.

Category: SYSTEM**Severity:** WARN**Message ID**

JEXL_INVALID_PREFIX

Message text

A JEXL function prefix or method name is unknown, could be a typo. Details: "{0}"

Log4j variables

detail

Description

A prefix in a JEXL expression (such as 'function.' in 'function.setVariable()') is invalid. Or the method name (such as 'setVariable' in 'function.setVariable()') This may be caused by a typo; consult the JEXL Guide PDF for the correct prefix for the function in question or check if the method has been added in a newer release.

Category: SYSTEM**Severity:** WARN**Message ID**

JWT_WARN

Message text

A JWT (JSON Web Token) warning occurred. User: "{0}". Reason: "{1}".

Log4j variables

user, reason

Description

A JWT (JSON Web Token) related warning occurred during processing of JWTs, see reason for details.

Category: SYSTEM

Severity: WARN

Message ID

MAX_COOKIE_SIZE_EXCEEDED

Message text

A cookie created by the SLS exceed the standard limit of 4k! Cookie: "{0}"

Log4j variables

name

Description

The SLS created a cookie which has a value larger than the limit of 4k defined by the HTTP standard. See the log message for the name of the cookie.

Category: SYSTEM

Severity: WARN

Message ID

MAX_LOCALES_EXCEEDED

Message text

The maximum number of locales to be cached has been exceeded! Potential DOS attack!

Log4j variables

-

Description

The SLS caches Java 'Locale' objects in order to re-use them internally, and this happens every time a new locale must be created because the client browser sent the language parameter with a new value. If this warning message appears, it indicates that the SLS received thousands of different locales, which is not really feasible, and indicates an attempt to fill the Java VM memory. Check the access logs if there are lots of requests with the 'language'-parameter, but with changing values.

Category: SYSTEM

Severity: WARN

Message ID

MISSING_AUTHORIZED_PATH

Message text

Invalid 'authorized path' (empty)! Check if SRM login location config contains 'HGW_RequestHeaders %SRM_ls_std' directive.

Log4j variables

-

Description

The value for the 'authorized path' used to create an SES session attribute was empty. Probably, the reason is that in the SLS configuration, a JEXL variable was used ('special.authorized.path'), but resolved to an empty string, because it had no value. And the reason for that is usually a config error in the SRM (header 'SessionInfo' not sent to SLS).

Category: SYSTEM

Severity: WARN

Message ID

MISSING_CERTIFICATE

Message text

The client certificate is missing. Reason: "{0}"

Log4j variables

reason

Description

No client certificate was available for authentication. Either the actual client certificate itself was missing, or it did not contain a valid certificate chain. See the log message for details.

Category: USER

Severity: WARN

Message ID

MISSING_CHALLENGE

Message text

The challenge is missing in the session.

Log4j variables

-

Description

The challenge is missing in the session. Maybe none has been created which could indicated an error in the login model. See log message for details.

Category: USER

Severity: WARN

Message ID

MISSING_CHALLENGE_RESPONSE

Message text

The response is missing.

Log4j variables

-

Description

The response / secret code is missing. See log message for details.

Category: USER

Severity: WARN

Message ID

MISSING_CRED

Message text

A credential is missing. Reason: "{0}"

Log4j variables

reason

Description

A credential is missing. See log message for details.

Category: USER

Severity: WARN

Message ID

MISSING_PARM

Message text

A required request parameter is missing. Parameter: "{0}"

Log4j variables

parameter

Description

A required request parameter is missing. See log message for details.

Category: USER

Severity: WARN

Message ID

MISSING_PARMGW_VALUES

Message text

Some parameter gateway value is missing. Details: {0}

Log4j variables

detail

Description

A parameter gateway value is missing. See log message for details.

Category: USER

Severity: WARN

Message ID

MISSING_PWD

Message text

The password is missing.

Log4j variables

-

Description

The login password is missing. See log message for details.

Category: USER

Severity: WARN

Message ID

MISSING_USERNAME

Message text

The username is missing.

Log4j variables

-

Description

The user login ID / username is missing. See log message for details.

Category: USER

Severity: WARN

Message ID

MOCK_CLASS_ACTIVE

Message text

Mock class activated in configuration property. Property: "{0}"

Log4j variables

property

Description

A mock-up class was activated in the configuration. See log message for the name of the configuration property.

Category: SYSTEM

Severity: WARN

Message ID

MOCK_CLASS_AVAILABLE

Message text

Mock class found in classpath. Class: "{0}"

Log4j variables

class

Description

A mock-up class was found in the classpath. To fix this, the test .jar file must be removed.

Category: SYSTEM

Severity: WARN

Message ID

NEW_PW_INVALID_CHARS

Message text

New password contains invalid characters. Regular Expression: "{0}"

Log4j variables

regex

Description

The new password contains invalid characters. Check the configuration to see the requirements (see administrator's guide for configuration details).

Category: USER

Severity: WARN

Message ID

NEW_PW_INVALID_LENGTH

Message text

Length of new password invalid. Minimum length: "{0}", maximum length: "{1}"

Log4j variables

minimum_length, maximum_length

Description

The new supplied passwords has an invalid length. Check the configuration to see the requirements (see administrator's guide for configuration details).

Category: USER**Severity:** WARN**Message ID**

NEW_PW_INVALID_REGEX

Message text

New password does not comply with the regular expression. Regular Expression: "{0}"

Log4j variables

regex

Description

The new password does not comply with the regular expression. Check the configuration to see the requirements (see administrator's guide for configuration details).

Category: USER**Severity:** WARN**Message ID**

NEW_PW_MISSING_CHARACTER_GROUP

Message text

New password does not contain characters of all the mandatory character categories

Log4j variables

-

Description

The new password does not contain characters of the mandatory character categories like 'upper case', 'lower case', 'numeric', 'special characters'. Check the entries in the password-policy.xml file

Category: USER**Severity:** WARN**Message ID**

NEW_PW_MUST_CONTAIN

Message text

New password has invalid content. Must contain: "{0}"

Log4j variables

character_type

Description

The new password does not contain some required content(s). Check the configuration to see the requirements (see administrator's guide for configuration details).

Category: USER
Severity: WARN

Message ID

NEW_PW_MUSTNT_CONTAIN

Message text

New password has invalid content. Must not contain: "{0}"

Log4j variables

character_type

Description

The new password has certain unallowed content (like 'numbers', or 'letters'). Check the configuration to see the requirements (see administrator's guide for configuration details).

Category: USER
Severity: WARN

Message ID

NEW_PW_NOT_MATCH

Message text

New passwords do not match.

Log4j variables

-

Description

The new supplied passwords do not match.

Category: USER
Severity: WARN

Message ID

OCSP_CERTIFICATE_EXPIRED

Message text

The OCSP signer certificate with Subject "{0}" is expired.

Log4j variables

subject

Description

The OCSP signer certificate used to verify certificate validity is expired. This OCSP certificate should be renewed.

Category: SYSTEM
Severity: WARN

Message ID

OCSP_CERTIFICATE_NOT_YET_VALID

Message text

The OCSP signer certificate with Subject "{0}" is not yet valid.

Log4j variables

subject

Description

The OCSP signer certificate used to verify certificate validity is not yet within the validity period.

Category: SYSTEM**Severity:** WARN**Message ID**

OCSP_VALIDATION_FAILED

Message text

Validation of an OCSP response with a certificate attributed to "{0}" failed.

Log4j variables

subject

Description

OCSP response validation failures may be due to any problem with a trusted OCSP signer, such as invalid signature, key, or algorithm.

Category: USER**Severity:** WARN**Message ID**

OIDC_WARN

Message text

An OpenID Connect warning occurred. User: "{0}". Reason: "{1}".

Log4j variables

user, reason

Description

An OpenID Connect (OIDC) related warning occurred during processing of OIDC messages/objects, see reason for details.

Category: SYSTEM**Severity:** WARN**Message ID**

PARAMETER_PASSING_AVAILABLE

Message text

HSP parm passing classes found in classpath! Remove test .jar file!

Log4j variables

-

Description

The HSP parameter passing functionality is available (the code was found in the classpath), although it was not enabled in the configuration. To fix this, the test .jar file must be removed from the 'WEB-INF/lib' directory of the SLS web application.

Category: SYSTEM**Severity:** WARN

Message ID

PARAMETER_PASSING_ENABLED

Message text

HSP parm passing function enabled in the configuration. Property: "{0}"

Log4j variables

property

Description

The HSP parameter passing functionality was enabled in the configuration. See log message for the name of the configuration property.

Category: SYSTEM**Severity:** WARN**Message ID**

PARAMETER_PASSING_MISSING

Message text

HSP parm passing function enabled, property: "{0}", but class not found! Install test .jar file!

Log4j variables

property

Description

The HSP parameter passing functionality is enabled, but the implementation class was not found in the classpath. To fix this, the test .jar file must be installed in the 'WEB-INF/lib' directory of the SLS web application.

Category: SYSTEM**Severity:** WARN**Message ID**

REQ_PARAM_NOT_WRAPPED

Message text

The potential req-parameter is not treated as req-parameter because "{0}". Marker "{1}", potential req-parameter "{2}"

Log4j variables

reason, marker, parameter

Description

The requested page contains the marker with indicates a potential 'req' parameter. Valid req-parameters contain base64 encoded encrypted data for exchange between the SLS and another service (or the application). If this message is logged often, it is recommended to set a custom marker for wrapping req-parameters into the requested page. This can be done by setting in sls.properties 'req.wrapped.marker=myCustomMarkerABC' .

Category: USER**Severity:** WARN**Message ID**

REQ_PARAM_REUSED

Message text

'req' parameter data was re-used (potential replay-attack). Parameter: "{0}"

Log4j variables

parameter

Description

A 'req' parameter which contains encrypted data exchanged between the SLS and another service (or the application) was re-used. This could indicate a replay-attack. Check the log files for details.

Category: USER**Severity:** WARN**Message ID**

SAML_WARN

Message text

A SAML warning occurred. User: "{0}". Reason: "{1}".

Log4j variables

user, reason

Description

A SAML (Security Assertion Markup Language) related warning occurred during processing of SAML messages/objects, see reason for details.

Category: SYSTEM**Severity:** WARN**Message ID**

SESSION_EXPIRED

Message text

Session has expired.

Log4j variables

-

Description

The user's session has expired, usually due to inactivity for an extended period of time. Check the HSP (Http(s)Listener and SRManager) configuration to verify the timeout settings.

Category: USER**Severity:** WARN**Message ID**

SLOWDOWN

Message text

Login slowdown required. Waiting time: {0}, failed attempts: {1}

Log4j variables

waiting_time, failed_attempts

Description

A user performed several failed logins in a row. This could be an of some kind of brute-force attack. To make such attacks more difficult and inefficient, new authentication requests from this user will not be processed for a certain time (depends on the slowdown configuration, see administrator's guide).

Category: USER**Severity:** WARN

Message ID

SLS_LDAPS_REQUIRED

Message text

NOTE: This LDAP server requires LDAPS (TLS) connections. Please change your LDAP adapter configuration accordingly!

Log4j variables

-

Description

This LDAP server requires LDAPS (TLS/SSL) connections, but plain LDAP connections have been configured. Please configure LDAPS instead.

Category: SYSTEM**Severity:** WARN**Message ID**

SLS_SESSION_MISSING_VALUE

Message text

Expected value was not in sls session. key: {0}.

Log4j variables

key

Description

At this point it is expected, that the key is associated with any value.

Category: SYSTEM**Severity:** WARN**Message ID**

SLS_WARNING

Message text

Reason: "{0}"

Log4j variables

reason

Description

A general warn message. Check the log files for further details.

Category: SYSTEM**Severity:** WARN**Message ID**

STRONG_CIPHERS_NOT_AVAILABLE

Message text

Some strong crypto ciphers are not available. Unlimited jurisdiction strength policy files are probably not installed in SLS JVM!

Log4j variables

-

Description

Apparently, some strong cryptography ciphers are not available. The typical cause of this problem is that the unlimited jurisdiction strength policy files are not installed in the SLS JVM.

Category: SYSTEM
Severity: WARN

Message ID

TENANT_INVALID_HOSTNAME

Message text

Required hostname for tenant resolution is missing or invalid. Value: "{0}". Set 'HGW_ForceHost hostname' in SRM login location!

Log4j variables

hostname

Description

If the tenant resolution should be done through the hostname prefix, the SLS must receive an actual, valid hostname. However, by default, the value of the 'host' header sent to the SLS by the SRM is with the localhost IP. To change this, set the 'HGW_ForceHost' directive in the login location of the SRM configuration, with the actual hostname value.

Category: SYSTEM
Severity: WARN

Message ID

TRANSACTION_VERIFICATION_FAILED

Message text

Transaction verification has failed. Msg: "{0}"

Log4j variables

message

Description

This message may appear only, if you are using the SLS to verify transactions. The verification of a transaction has failed for the current user. An error page will be sent to the user and the user will be logged out from all applications.

Category: USER
Severity: WARN

Message ID

UNSUPPORTED_BROWSER

Message text

Blacklisted browser match. Rule: "{0}", User agent: "{1}"

Log4j variables

rule, user_agent

Description

A client's user-agent header matched with an entry in the blacklist. The client was forwarded to the information page and a log record was created.

Category: USER
Severity: WARN

Message ID

USER_INFO_COOKIE_INVALID

Message text

Failed to process the userinfo cookie, discarding it now. Reason: "{0}", Seed: "{1}", Cookie value: "{2}"

Log4j variables

reason, seed, cookie

Description

An existing SLS user info cookie could not be processed. This should not happen at all, but when it does, it's usually after an SLS restart, when the SES session remained alive. If the SLS session ID changed for any reason (for example due to a configuration change), the cookie cannot be decrypted anymore. In this case, the cookie is ignored and discarded.

Category: SYSTEM

Severity: WARN

Message ID

USER_NOT_ON_FILTER_LIST

Message text

User not allowed by active user filter. User: "{0}"

Log4j variables

user

Description

A user tried to authenticate, but her/his user id was not found in an active user filter whitelist file. The purpose of a whitelist filter file is to authenticate only user listed on the user filter file. The message is also logged if the user is on a blacklist file.

Category: USER

Severity: WARN

Message ID

WEBAUTHN_WARN

Message text

A WebAuthn warning occurred. User: "{0}". Reason: "{1}".

Log4j variables

user, reason

Description

A WebAuthn (Web Authentication / FIDO2) related warning occurred during processing of WebAuthn messages/objects, see reason for details.

Category: SYSTEM

Severity: WARN

Message ID

WS_SOAP_FAULT

Message text

The received HTTP SOAP response contains a fault with value "{0}", which is configured for logging a warning. Config property: "{1}"

Log4j variables

fault_value, property

Description

The received HTTP SOAP response contains a SOAP Fault. For details check the response body.

Category: SYSTEM

Severity: WARN

Message ID

XSS_IN_URL

Message text

A redirect URL contained potential XSS keywords. URL: "{0}"

Log4j variables

url

Description

A redirect URL, either from the 'requestedPage' header or the 'target' parameter, contained illegal keywords which indicate a possible cross-site-scripting attack. Check the log files for details.

Category: USER

Severity: WARN