Audit and Diagnostics logging

Tip: Also see details about how to enable debug logging and setting up logging runtime in Jira and Confluence.

Audit logging

To enable audit logging, you will have to turn it on in your logging configuration. Both successful and failed Kerberos and SAML logins will be logged. For failed logins, there will be an additional sentence explaining why it failed. By adding the two lines, you will get logging in a similar pattern as the security logging in Jira (as Jira has the most precise logging of logins). This feature was added in version 3.5.15.

Logging will look like this:

```
The user 'johndoe' has PASSED authentication using Kerberos
The user 'john.doe@mycompany.com' has PASSED authentication using SAML
```

Enabling in Confluence

This is done in Confluence by adding the following two lines below in the bottom of the file:
<confluence-binaries>/confluence/WEB-INF/classes/log4j.properties

```
log4j.logger.com.kantegasso.AuditLog = INFO, confluencelog
log4j.additivity.com.kantegasso.AuditLog = false
```

Log will be written to: atlassian-confluence.log

Enabing in Jira

This is done in Jira by adding the following two lines below in the "# Security logs" section in the file:
<jira-binaries>/atlassian-jira/WEB-INF/classes/log4j.properties

```
log4j.logger.com.kantegasso.AuditLog = INFO, securitylog
log4j.additivity.com.kantegasso.AuditLog = false
```

Log will be written to: atlassian-jira-security.log

Enabling in other Atlassian products

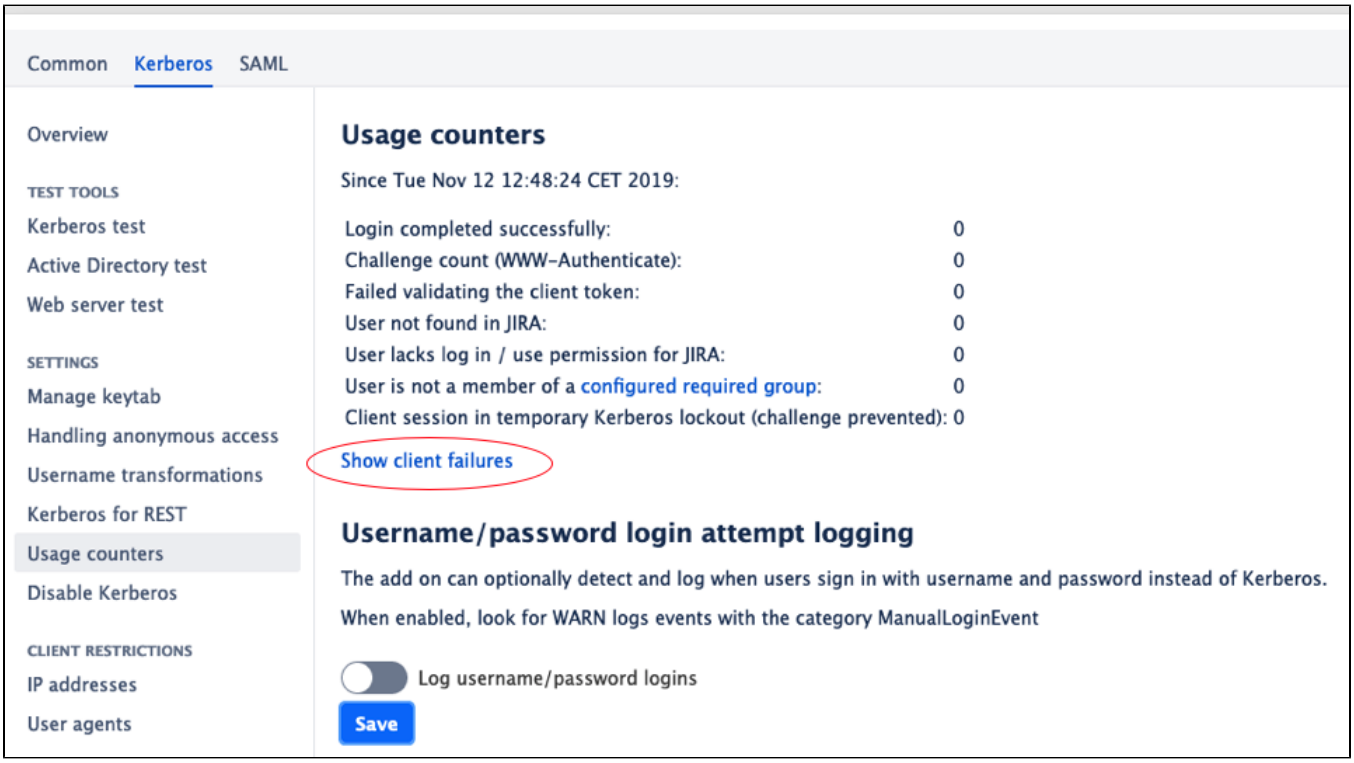
Similarly you may enable audit logging in other Atlassian products. Please contact us if you have problems setting this up and we will help you out.

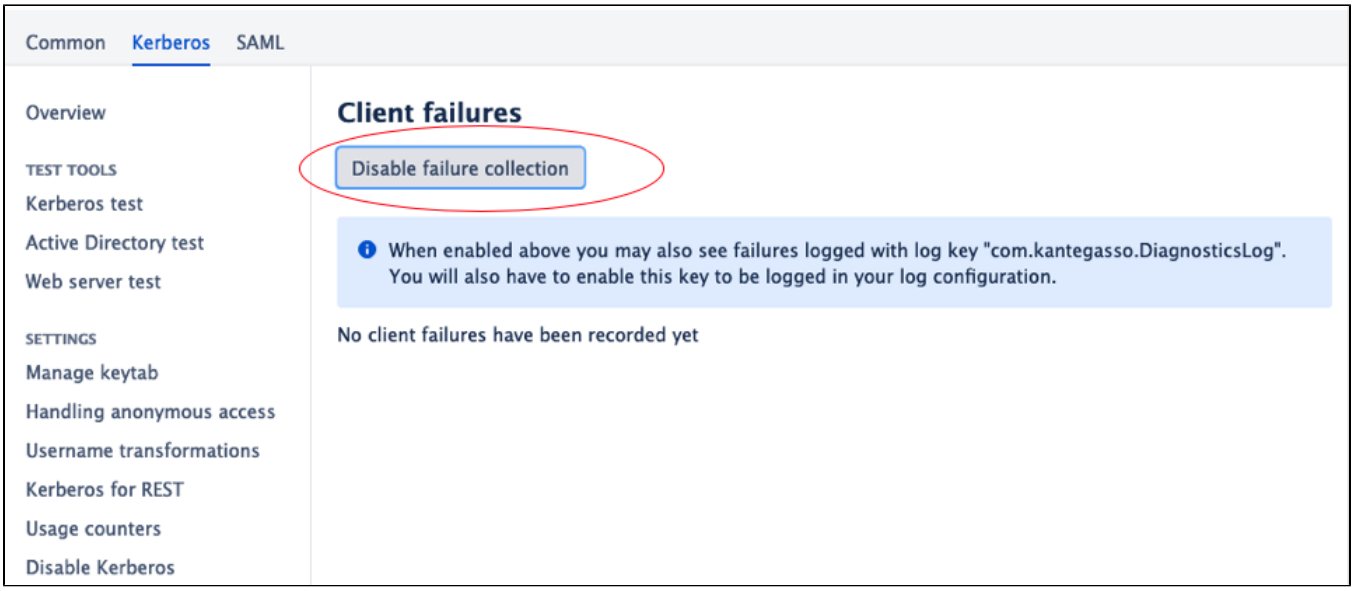
Diagnostics logging

Similarly you may enable diagnostics logging. Currently we only log detailed failures of Kerberos logins to this log. Log statements are written in standardized JSON format with keys "timestamp", "context" and "message" (the last containing several comma separated details form the fail) for easy analysis in log monitoring tools and look like this:

```
2019-11-11 15:23:07,231 https-jsse-nio-8443-exec-7 WARN anonymous 923x9201x1 bm4kxx 127.0.0.1 /rest/analytics/1.
0/publish/bulk
[com.kantegasso.DiagnosticsLog] {"timestamp":"2019-11-11 15:23:07,230","context":"Kerberos","message":"
Authentication has FAILED,
KerberosTicket: HTTP/kerberos-dev-local.example.com@EXAMPLE.LOCAL, EncType: 18, RequestUri: /jira/login.jsp,
RemoteIP: 127.0.0.1,
Reason: Failed to validate client token, Exception: GSSException: Failure unspecified at GSS-API level
(Mechanism level:
Invalid argument (400) - Cannot find key of appropriate type to decrypt AP REP - AES256 CTS mode with HMAC SHA1-
96)"}
```

Diagnostics log must be enabled similarly to audit logging. Follow same way of setting up just replace 'com.kantegasso.AuditLog' with 'com.kantegasso.DiagnosticsLog' in the examples above. In addition to enable the Kerberos failures to be collected and sent to this log, you must press the 'Enable failure collection' button on Client failures found from the 'Usage counters' page:





This feature was added in version 3.6.13.