Electronic Signatures

Title 21 CFR 11 Validation Report

www.anovaapps.com | products@anovapps.com

Electronic Signatures

The Electronic Signatures app provides a mechanism for confirming user credentials in order to protect your Jira records. The app is compliant with Title 21 CFR Part 11 which enables you to prevent unauthorized actions on the tickets using electronic signatures.

A perfect way to ensure workflow security in Jira, to keep things under control, and save you from needless trouble. The add-on provides more digital reliability and fewer paper records in your daily routine, eliminates continuous manual checks and reminders.

Common Use Cases:

- Prevent unauthorized actions on Jira issues
- Get your Jira records compliant with the FDA regulation CFR 21 part 11
- Avoid undesirable transitions within unsigned Jira tickets
- Confirm actions by certifying it with a signature in the form of a personal PIN or password
- Request several signatures at one time
- Notify the users about the need to provide signatures on the Issues
- View information on all issue signatures in a separate tab

Hosting Options:

- Cloud
- Server
- Data Center

Title 21 CFR Part 11

Title 21 CFR Part 11 is the FDA's regulations for electronic documentation and electronic signatures. It outlines the administration of electronic records in FDA-regulated industries and defines the criteria under which electronic records and electronic signatures are considered trustworthy, reliable, and equivalent to paper records.

Title 21 CFR 11 is important for those FDA-regulated companies that want to use electronic records and electronic signatures instead of their paper signatures to comply with FDA regulations more quickly and effectively.

This document describes how Electronic Signatures add-on helps to comply with FDA 21 CFR Part 11. Here you can find a detailed match of sections 21 CFR 11 to the characteristics of the Electronic Signatures app.

Subpart A - General Provisions

Sec. 11.1 Scope.

Electronic Signatures add-on enables you to check user credentials and meets the requirements of technical elements of Title 21 CFR Part 11 that define the criteria under which electronic records and electronic signatures are considered trustworthy, reliable, and equivalent to paper records. According to this part, electronic signatures can be equivalent to full handwritten signatures.

> *(a) The regulations in this part set forth the criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.*
>
> *(b) This part applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted, under any records requirements set forth in agency regulations. This part also applies to electronic records submitted to the agency under requirements of the Federal Food, Drug, and Cosmetic Act and the Public Health Service Act, even if such records are not specifically identified in agency regulations. However, this part does not apply to paper records that are, or have been, transmitted by electronic means.*
>
> *(c) Where electronic signatures and their associated electronic records meet the requirements of this part, the agency will consider the electronic signatures to be equivalent to full handwritten signatures, initials, and other general signings as required by agency regulations, unless specifically excepted by regulation(s) effective on or after August 20, 1997.*
>
> *(d) Electronic records that meet the requirements of this part may be used in lieu of paper records, in accordance with 11.2, unless paper records are specifically required.*
>
> *....*

Sec. 11.2 Implementation.

In accordance with Subpart A, section 11.2, persons may use Electronic Signatures add-on for both submitted and non-submitted records.

(a) For records required to be maintained but not submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that the requirements of this part are met.

(b) For records submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that:

(1) The requirements of this part are met; and

(2) The document or parts of a document to be submitted have been identified in public docket .

...

Sec. 11.3 Definitions.

According to definition of electronic signature, User Validator Field and Logged User Validator Field which use username and password, as well as PIN in case of using Jira cloud, can be considered electronic signatures because their data is a compilation of series of symbols executed, adopted, or authorized by an individual.

...

(5) Digital signature means an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.

(6) Electronic record means any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.

(7) Electronic signature means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.

(8) Handwritten signature means the scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate a writing in a permanent form. The act of signing with a writing or marking instrument such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark.

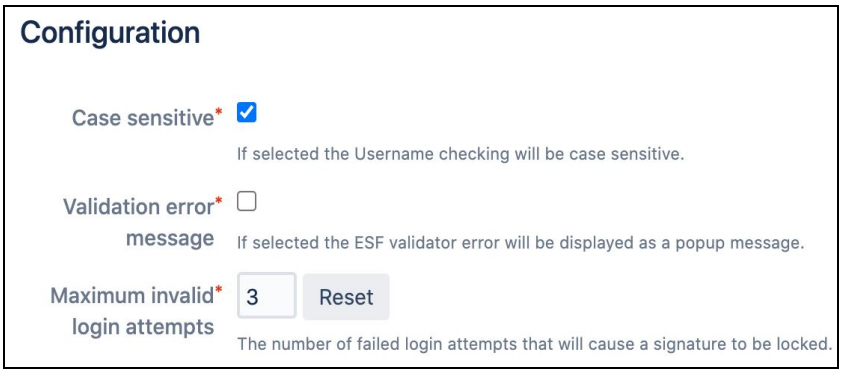
...

Subpart B - Electronic Records

Sec. 11.10 Controls for closed systems.

Electronic Signatures app prevents unauthorised actions on Jira tickets. The add-on contains custom fields for checking user credentials or a PIN in case of Jira cloud. To execute transition or edit issues the users have to type valid credentials to proceed. In compliance with 21 CFR 11.10, only a Jira Administrator, a person with appropriate knowledge, authority and permission is able to install and configure Electronic Signatures plugin.

In addition to this, we are continually working to ensure more security with Electronic Signatures . On the configuration page you are able to set up count of invalid login attempts and 'Username check' sensitivity.



Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:

(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.

(d) Limiting system access to authorized individuals.

(e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information.

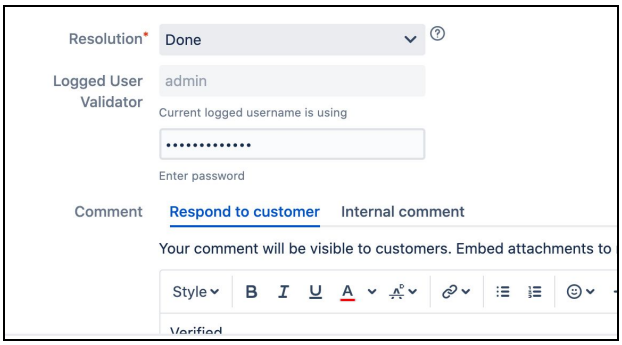
(g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.

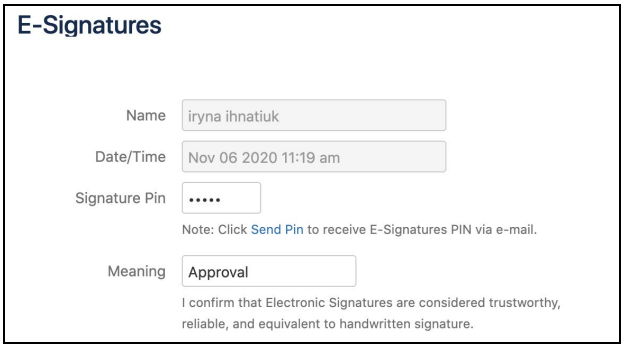
(i) Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.

...

Sec. 11.30 Controls for open systems.

Using either the User Validator Field or the Logged User Validator or a Signature Pin field within Electronic Signatures add-on, the user password is invisible and is not disclosed for security reasons and to ensure the authenticity, integrity, and the confidentiality.





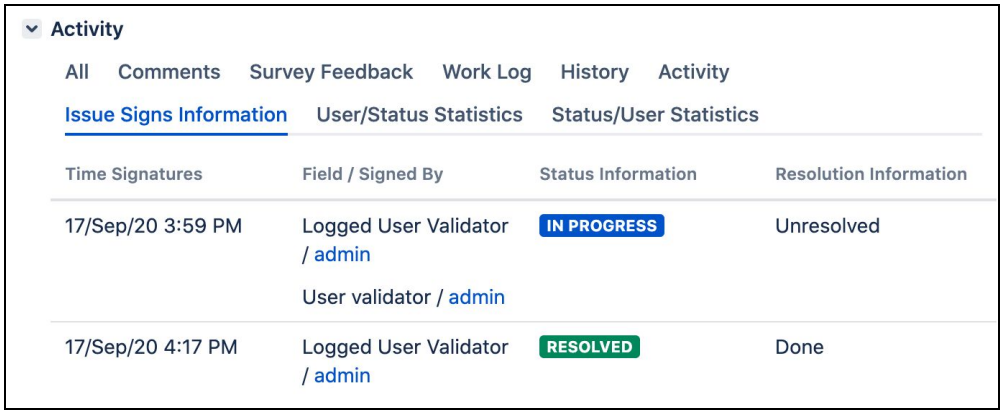
> *Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.*

Sec. 11.50 Signature manifestations.

Information about the username of the signee, date, time and meaning of the signature can be found within the ticket. To do this, go to the Issue Sign Information tab in Jira server platform and to E-Signatures tab if you use Jira cloud platform.

> *(a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:*
>
> *(1) The printed name of the signer;*
>
> *(2) The date and time when the signature was executed; and*
>
> *(3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.*

How it looks in Jira Server / Data Center:



See example of Jira Cloud ticket:

Sec. 11.70 Signature/record linking.

Electronic Signatures add-on automatically links signatures to issues and does not allow further modification to be tampered to ensure 21 CFR Part 11 compliance.

> *Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.*

Subpart C - Electronic Signatures

Sec. 11.100 General requirements.

Both the User/Logged User Validator Field use the username and password of the Jira user profile. Their reconciliation is unique to each Jira account and cannot be reused by, or reassigned to, anyone else. In case of using Electronic Signatures for Jira cloud, apart from login and password, a special PIN is verified, which is personal for each Jira user and cannot be transferred or disclosed to third parties, as well.

> *(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.*
>
> *(b) Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.*
>
> *(c) Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.*
>
> *...*

Sec. 11.200 Electronic signature components and controls.

Because the Electronic Signatures add-on is not based upon biometric data, identification always involves the use of mandatory authentication components, such as a username and password. If you use Electronic Signatures for Jira cloud, identification components include verification of username and password when logging in and checking your personal PIN when signing.

(a) Electronic signatures that are not based upon biometrics shall:

(1) Employ at least two distinct identification components such as an identification code and password.

(i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.

(ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.

(2) Be used only by their genuine owners; and

(3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.

...

Sec. 11.300 Controls for identification codes/passwords.

Existence of two or more users with the same combination of login and password is impossible and contradicts the Atlassian Password policies. As an organization admin, you can use a password policy to require all of your managed users to meet a minimum password strength or set a password expiration period. Apart from this, you can set up count of invalid login attempts during signing the issue and sensitivity check on Electronic Signatures configuration page.

Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:

(a) Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.

(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).

(c) Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.

(d) Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.

ABOUT Anova Apps

Here at Anova Apps, we are dedicated to innovating your Atlassian experience by consolidating many single-purpose apps with one powerful ecosystem. Our products provide solutions relating to automation, governance, integrations, migrations, and much more.

Visit us at anovaapps.com

Contact

107 S B St Ste 200,
San Mateo, CA
94401

products@anovaapps.com

(877) 753-2760