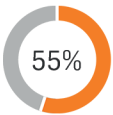
syracom
business efficiency engineering

Secure Login

Two-factor authentication (2FA) for Atlassian Tools

Part of Consileon Group

Are you afraid your valuable and secret business information in your Atlassian tools are secured enough? Well, you should change your password — regularly! But do not mind, by sheer brute force or simple phishing, passwords are a pretty ridiculous way of authentication. Two-factor authentication, also called multiple-factor or multiple-step verification, is an authentication mechanism to double check that your identity is legitimate: you can be sure, that the individuum in front of the screen is the human you think it is!



Spear-Phishing campaigns targeting employees of companies increased 2015 by 55%. Over 60% of this attacks were against small und mid-size companies.

(Source: 2016 Internet Security Threat Report)

According to Symantec, 80% of identity attacks could have been prevented by the usage of two-factor authentication.

(Source: Symantec Inforgraphic - Strong Authentication...No passwords)

86% of the people using 2FA feel, that their accounts are more secure. So the result of a study by TeleSign from 2015.

(Source: The June 2015 TeleSign Consumer Account Security report)

A series of recent password hacks at well-known brands like Twitter and LinkedIn flashes the focus on problems of passwords and how vulnerable we are. Two-factor authentication is a possible solution, and many companies are racing to deploy it. You can also secure your Atlassian tools on-premise and behind the firewall, easily! Don't wait...

Security: what is two-factor authentication?

Two-factor authentication (2FA) puts another level of authentication on top of an account log-in. When you have to enter just your username and password, that's only a single-factor authentication. 2FA requires the user to have two types of credentials before being able to access an account:

Something you know

like your username and password

Something you have

such as a smartphone or a hardware token, like a Yubikey

User convenience: Is it hard to use?

It adds an extra step to the login process: you have to enter an additional PIN from your authenticator to get access to the system. So, the two-factor authentication makes it a bit harder to log in, but it's effortless like using a key to unlock your house.

Integration: How does ist work with Atlassian Tools like JIRA and Confluence?

After logging in for the first time, you have to go through a simple onboarding process. You simply have to scan a QR code with your authenticator app and enter the generated PIN for validation. After that, the plugin will ask you for the PIN, every time you log into your system.

Meet Maike. Maike leads our HR department. As she has a small child at home, she works in the office half the week. The other half she works from home. Beside JIRA and Confluence, she uses some additional HR systems and cares a lot about the personal data of our employees. That way she always works with the secure internal network or using a secure VPN connection from home.

With Marc and Alex, this is an entirely different story. They are always on the move, visiting customers and working from different places. Today Marc worked from the client's side, accessing some relevant documentation in Confluence. This evening he and Alex are sitting in the lobby of their hotel, working together on some user stories in JIRA. Moreover, tomorrow, as a coffee addict, Alex will work the first two hours from his favorite coffee house, reviewing some concepts.

Ensure proper usage of your data by the right person: working from within your company you do not want to force colleagues entering a PIN using the second factor like a mobile authenticator. However, if somebody works remotely, a second factor is needed to identify that person and avoid misuse. Such scenarios can be configured using the IP-based white-/blacklist of **Secure Login** to detect internal IP ranges.

Speaking of Marc and Alex: Even if they work together for years now, they always had different opinions about mobile devices and the proper operating systems. Marc loves his Android phone as much as Alex insists on his iOS devices, mainly as he fell in love with his smartwatch. Everyone has a different taste, and so **Secure Login** supports a lot of the various mobile authenticators for different types and brands of devices, as much as operating systems:

	Apple iPhone/iPad	Apple Watch	Google Android	Windows Phone	Black Berry
Authy	✓	✓	✓		
Duo Mobile	✓		✓	✓	✓
Free OTP	✓		✓		
Google Authenticator	✓		✓		✓
Toopher	✓		✓		
Authenticator				✓	
Symantec VIP Access	✓		✓		

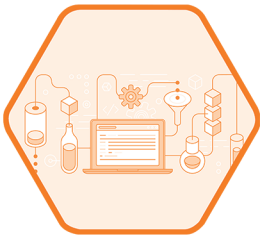
Often a smartphone is not provided to all employees or externals by your company. At the same time, you do not want to use a mobile authenticator on a private asset or labor unions are against that: use a hardware authenticator like a Yubikey together with **Secure Login**[1], instead.

[1] *Read more about the usage of Secure Login with Yubikey in our blog at http://www.syracom.de/news/blog/atlassian-solution-partner/using-secure-login-with-yubikey.html*

Do you remember the news coverage about Bob, the developer, a few years ago? Bob was smart and outsourced his job to a Chinese company, without his employer knowing anything about it. He quietly passed his user credentials to some Chinese developers, paying them a small percentage of his salary and spent the working day surfing on the Internet.

For sure, Bob is an extreme example, and **Secure Login** would not have prevented him from doing that, as he even sent his RSA token to China, to enable his contractors to work, while he didn't work at all. However, we see something comparable a lot in large projects having many externals involved: the typical situation: "hire one, get four." After a while, there are sitting four consultants from one company in your project, even if you only hired one. They are doing it with good intent, because the project is late, but do not want to bother you. So, they share the credentials of the one consultant you hired...

This scenario can be easily maintained with **Secure Login** having configured a blacklist of user group like "externals.". So, every external must log in via username and password but also by PIN.



Our concern as a vendor is to give our customers a seamless experience with our plugins. Security-related topics often pose a unique challenge in this context. So, with **Secure Login,** we do not only want to provide customers just with features, which address the different usage scenarios. Instead, we also want to give you with an easy to manage and cost-effective tool without unnecessery hurdles, like a modification of you Atlassian Tool itself or the underlying infrastructure. To archive this, **Secure Login** provides a lot of additional features:

- **Secure Login** is specially designed for the on-premise, behind the firewall usage, through to complete offline installations. There is no communication involved with any external service or system. The only communication taking place is within the onboarding process between **Secure Login** and the authenticator. However, even this only takes place through the camera of your smartphone.

- The plugin integrates itself into your Atlassian Tools as a request filter. This way you can combine Secure Login with custom authenticators and SSO solutions, like **EasySSO** by TechTime.

- If a user pairs a mobile device the first time or login via PIN, this actions can be logged within a separate audit log. Administrators are able to filter by users or time ranges as well as actions and will retrieve the related information for transparency or to detect misuse.

syracom is an independent business and IT consulting firm with expertise in various industries. We help our partners to design efficient and lasting business processes on the base of Atlassian Tools or other approaches. Our consulting services are based on your needs, and our solutions are individually tailored to your requirements. That enhances the added value our company can offer and gives you a decisive competitive edge. Quick, efficient and sustainable. **syracom** follows a comprehensive approach to consulting – based on an ideal combination of many years of professional and technological expertise. We identify your company goals, analyze existing business processes along the value-added chain, and deliver modern IT solutions.

Since 2012, **syracom** is officially an Atlassian Solution Partner. Having more than ten years experience in using, customizing and extending Atlassian tools, major German companies and large, international enterprises are trusting **syracom** to build individual solutions for them. Such solutions are compositions of tool setup, configurations as well as the development of add-ons for specific demands not covered by Atlassian natively. In opposite to this, **syracom**'s product family "**Secure-Login**" is published on the Atlassian Marketplace for the public, available for Atlassian JIRA and Confluence but planned to support Bitbucket and Bamboo shortly also.

Atlassian Solution Partner

SecurITy made in Germany
Trust Seal www.teletrust.de/itsmig

To show our customers how serious we are about their security, we joined the IT-Security Association Germany (TeleTrusT) at the end of 2016. Since then we are also a holder of the „IT Security made in Germany“ trust seal, which had been established initially 2005 by the German Federal Ministries of the Interior and Economics and Technology and representatives of the German IT security industry.

Status Sync

Reduce manual efforts and enhance transparency by keeping the status of issues on different hierarchy levels automatically in sync for epic/stories, parent/subtasks or linked issues.

Unused Avatar Remover

The "Unused Avater Remover" allows administrators to configure a recurring Jira service to automatically delete all avatar images from disk of deactivated or deleted users without manual efforts.

Personal Activity Stream Hide

Protect your user's privacy by disabling the personal activity stream to prevent misuse of personal working schedule or performance: other JIRA functions refer to the stream data will still be working.

Issue History Item Remover

Be able to remove individual history items of an issue as administrator to prevent "hate speech" or other information being logged within the history, which must be deleted due to e.g. regulatory requirements (GDPR) etc.

vCard for Confluence

Easily download the contact data of your team members in Confluence as vCard and import them into your favorite address book application, on any device.

syracom

Otto-von-Guericke-Ring 15
65205 Wiesbaden
Germany
Fon: +49 6122 9176 0
info@syracom.de
www.syracom.de

Munich
Germany

Cologne
Germany

Karlsruhe
Germany

Zurich
Switzerland

syracom at Atlassian Marketplace
https://marketplace.atlassian.com/vendors/1211842

Secure Login for JIRA
https://marketplace.atlassian.com/1213472

Secure Login for Confluence
https://marketplace.atlassian.com/1214491

Secure Login for Bitbucket
https://marketplace.atlassian.com/1218045

Secure Login for Bamboo
https://marketplace.atlassian.com/1218273

Support e-mail address
support@syracom-bee.atlassian.net

Support Service Desk
https://syracom-bee.atlassian.net/servicedesk

Documentation
https://syracom-bee.atlassian.net/wiki/spaces/SL

business efficiency engineering - the bee company