SURF | okta

Authenticate User Identity

While Maintaining Zero-Trust

Authentication, identity and control over the browser is a vital part of securing the company, and reducing the threat landscape among distributed workforces. By combining Okta's identity platform and SURF's Zero-Trust browser, organizations receive full control, visibility and security over the access to company data and intellectual property - without affecting productivity or agility.

Together, Okta and SURF help enterprises streamline their operations without risking security - regardless the device – BYOD or corporate owned.

About the integration:

Users of SURF and Okta enjoy easy-to-manage authentication through the IDP directly to the Zero-Trust browser providing increased control and visibility into employee corporate actions, and device health.

Enterprises can seamlessly apply policies from SURF's browser to their pre-defined Okta users and groups from a single dashboard. All Okta users and groups are easily imported and synced into SURF, giving complete access control to critical assets and applications via the enterprise browser.

Okta's Integration with SURF allows Okta users to:

Isolate work environment from device and web threats.

Ensure that only authorized users have access to sensitive data and applications.

Protect the company on unmanaged devices.

Integration Benefits

Conditional Access & Session Protection

Okta and SURF combine to enforce conditional access controls, allowing access to sensitive data solely through the SURF browser. This thwarts session hijacking attempts, ensuring attackers can't access data outside SURF. Authentication policies can restrict access to specific user groups, enhancing security.

Secure Session Data Encryption

SURF enhances session data security with unique browser-based encryption. Even if attackers access session data, it remains unreadable outside of SURF. This encryption layer protects sensitive information in the browser session manager.

Collapse the Stack

Okta users will be able to easily collapse their cybersecurity stack and ensure quick validation of all users and devices. This will increase agility and improve business efficiency while maintaining security through safe browsing, phishing protection, DLP controls, web filtering and more.

Password Hijacking Defense

Keylogger Protection: SURF using a virtual keyboard for authentication and therefore can prevent from passwords being spoofed. SURF + Okta collaborate to encrypt Okta passwords as they are typed, enhancing security against keyloggers.
Phishing Protection: SURF allows credential entry only on approved domains, proactively defending against phishing attacks.

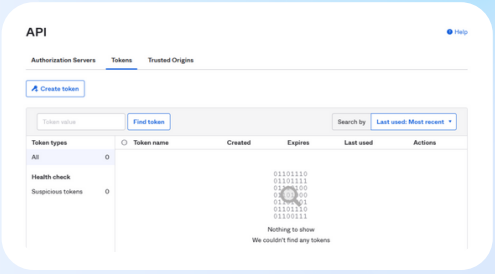
SURF + okta

info@surf.security
www.surf.security

Simple Steps to Set Up

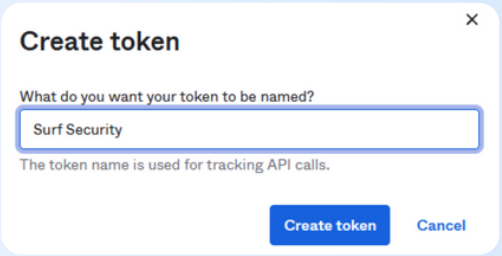
1

Starting from your Okta dashboard. Click “**Security**”, “**API**”, and then “**Tokens**”.



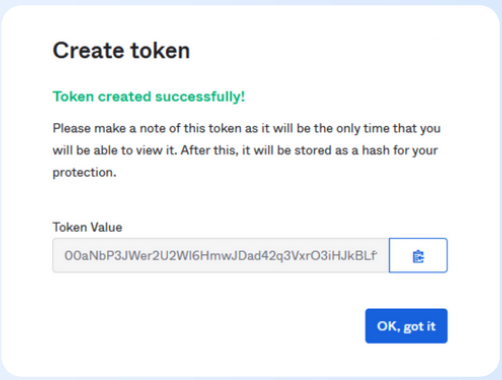
2

Click “**Create token**”, and enter **SURF Security**.



3

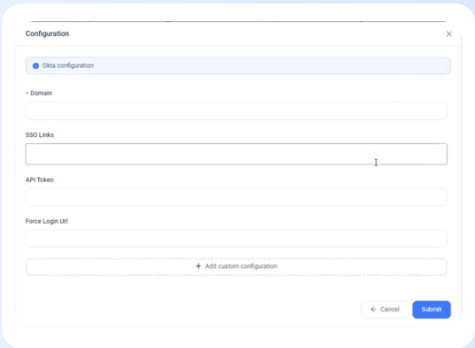
Copy the token value, and paste it into the **SURF dashboard.**



4

On your SURF admin dashboard, click “**Settings**”, “**Integration**”, “**Add New Integration**”, and then “**Okta**”.

Enter your Okta domain into the domain field, paste all applications you’ve set up with Okta in the SSO field, and then paste your previously copied token value into the API token field.



SURF + okta

info@surf.security
www.surf.security