



## Authenticate User Identity To A Secured Endpoint Environment On Any Device

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.






### 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:

-  Ensure that only authorized users have access to sensitive data and applications.
-  Isolate work environment from device and web threats.
-  Protect the company from the threats of unmanaged devices.

## Integration Benefits

### Manage Access

Companies can enforce their users' log-in through SURF's Zero-Trust browser, making it **simpler to implement conditional access**, and **easily define which users have access to data**.

### Tools Consolidation

Okta's customers **Ensure quick validation of all users and devices**. This will **increase agility and improve business efficiency** while maintaining security via safe browsing, phishing protection, DLP controls, web filtering and more, by consolidating the security tool stack

### Enable BYOD

By integrating SURF's isolated and secured enterprise browser, Okta administrators can **easily manage permissions on any device**.

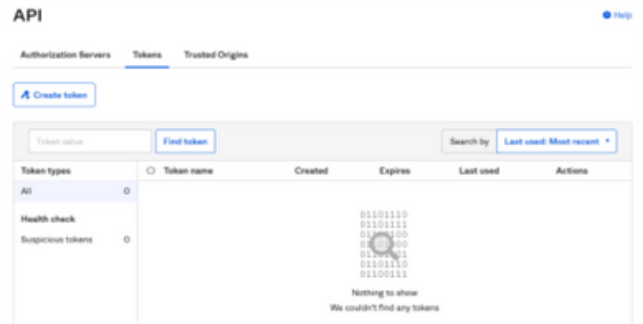
### Transactional MFA

Enabling a higher level of user validation process by enforcing **transactional MFA on any selected application and URL's**.

# 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**.

## Create token

What do you want your token to be named?

Surf Security

The token name is used for tracking API calls.

Create token

Cancel

3

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

## Create token

Token created successfully!

Please make a note of this token as it will be the only time that you will be able to view it. After this, it will be stored as a hash for your protection.

Token Value

00aNbP3JWer2U2WI6HmwJDad42q3VxrO3iHJkBLF

OK, got it

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.

