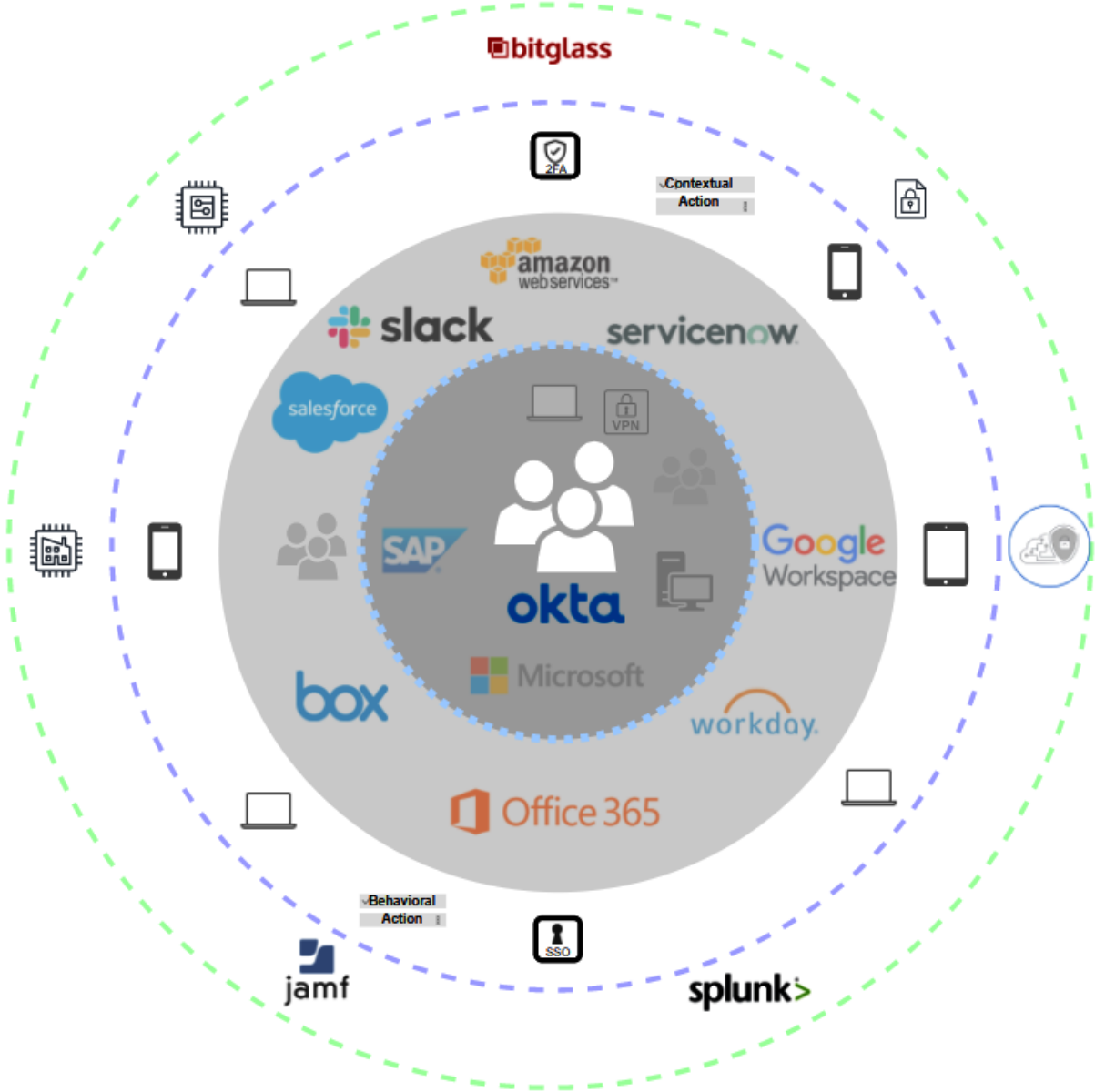
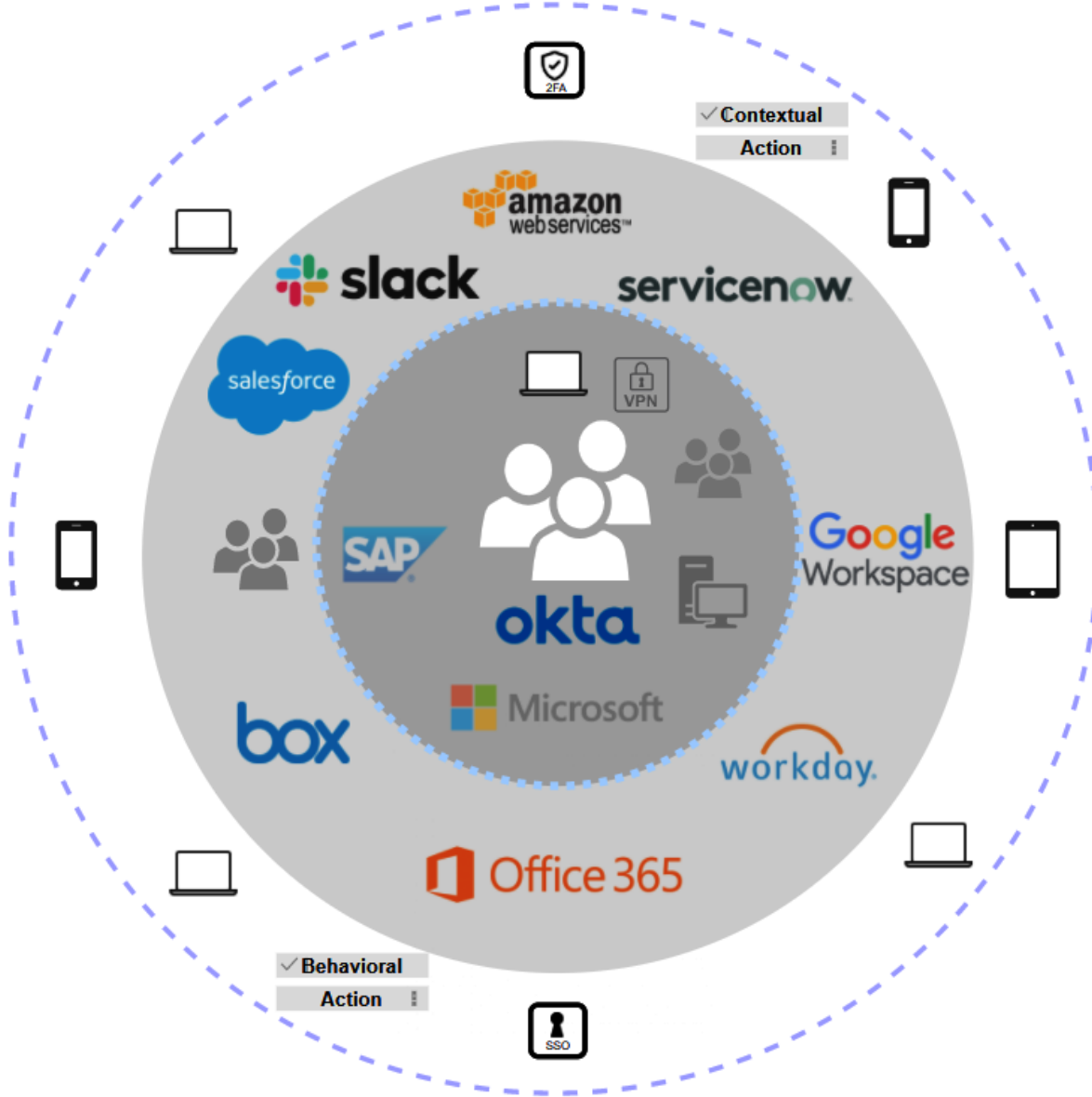


# Chapter 1: IAM and Okta

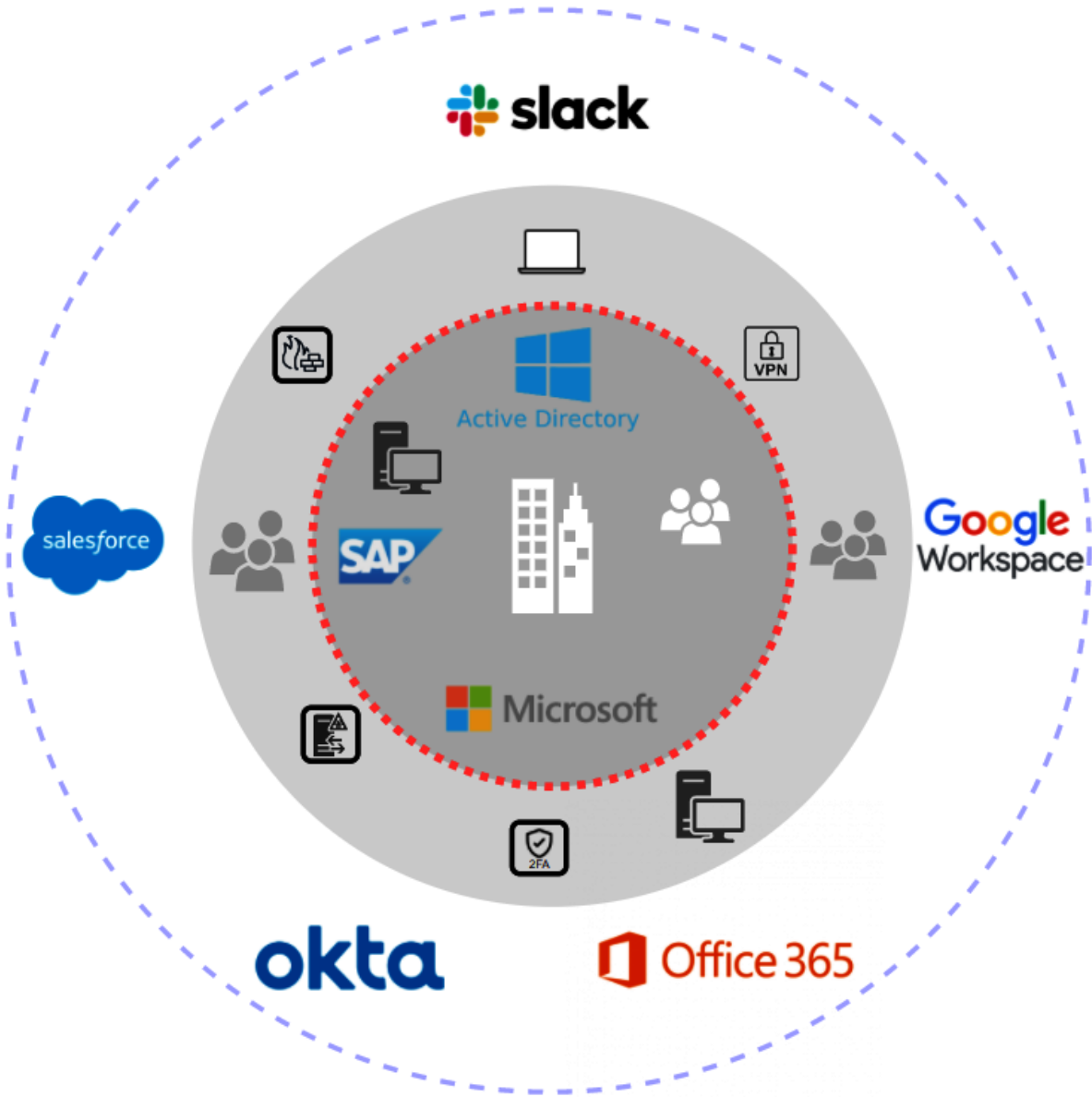
ZERO TRUST STAGE 3



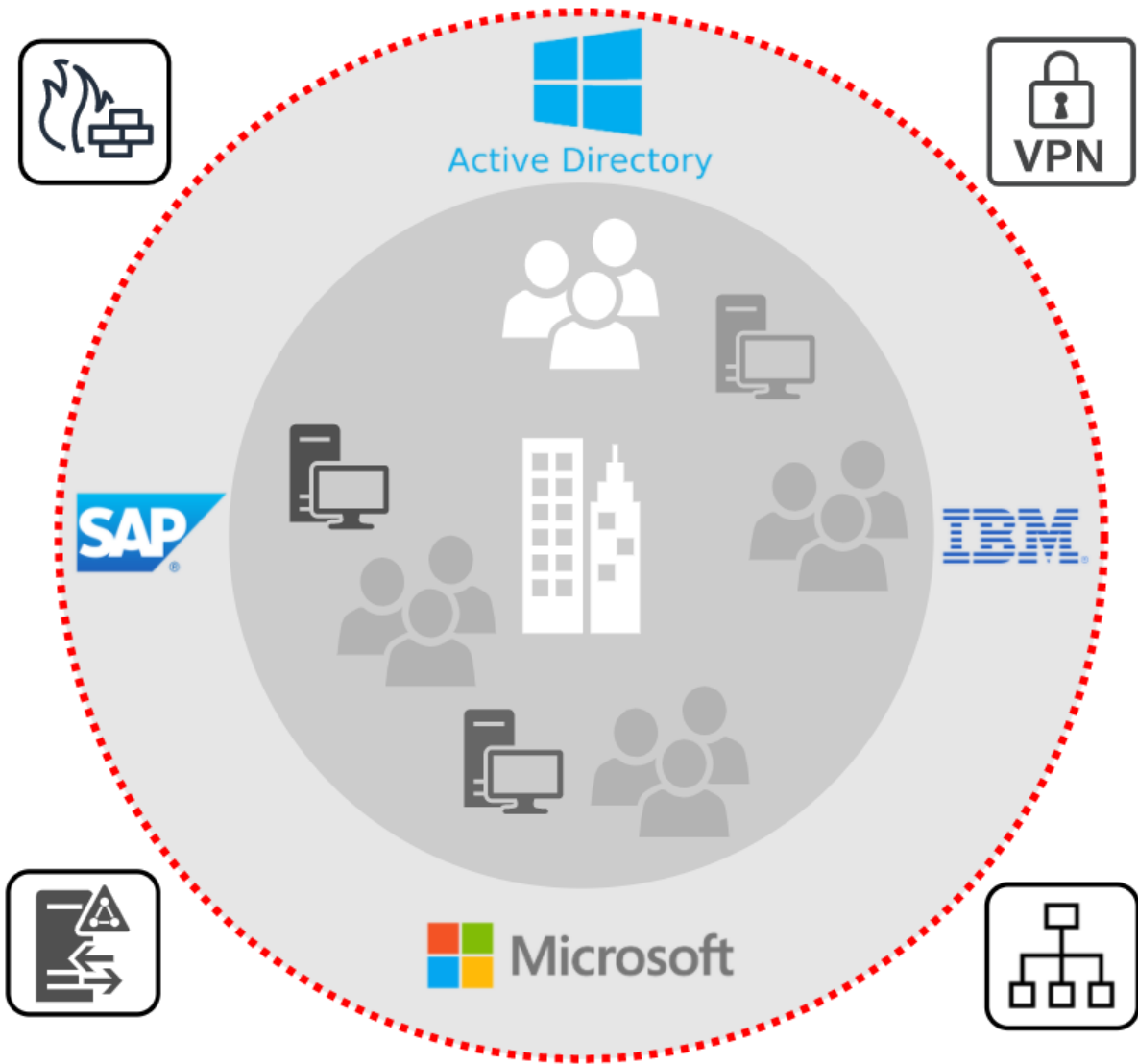
ZERO TRUST STAGE 2



ZERO TRUST STAGE 1



ZERO TRUST STAGE 0





## Chapter 2: Working with Universal Directory

SETTINGS

To App

To Okta

Integration

 → 

**General** Edit

Import users from G Suite to create new Okta users. If the Okta user already exists, the two accounts will automatically be linked. Imported users are assigned G Suite access when they are confirmed on the Import tab.

**Schedule import** never  
Select never if you prefer to import manually

**Okta username format** Email Address  
Select the username users should enter to log into Okta.

**Update application username on** Create only

---

**User Creation & Matching** Edit

Imported user is an exact match to Okta user if

- Okta username format matches
- Email matches
- The following attribute matches:

## Add Attribute

Data type

string ▼

Display name ?

Variable name ?

Description

Enum

Define enumerated list of values

Attribute Length

Between ▼

min

and

max

Attribute required

Yes

Cancel

Save

Save and Add Another

## Add Person

User type ?

User ▼

First name

Last name

Username

Must be an email

Primary email

Secondary email (optional)

Groups (optional)

Password ?

Set by user ▼

Send user activation email now ?

Save

Save and Add Another

Cancel

**Allow partial matches**

Partial match on first and last name

**Confirm matched users**

Auto-confirm exact matches

Auto-confirm partial matches

**Confirm new users**

Auto-confirm new users

Auto-activate new users

Save

Cancel

Okta username format

SAM Account Name ▲

Email Address

Okta.

Update application username on









SAM Account Name

User Principal Name (UPN)

JIT provisioning

Custom



JIT provisioning requires [delegated authentication](#) to be enabled.




Source	Name	People	Apps	Directories
	<b>00. Organization</b> All apps for the whole org	104	7	0
	<b>00. organization - managed devices</b> No description	1	2	1
	<b>00.1 Stockholm HQ</b> Everyone @ HQ	33	0	0
	<b>00.2 New York office</b> No description	36	0	0
	<b>00.3 All remote</b> Remote workers across the globe	30	0	0
	<b>01. Sales</b> No description	42	3	0
	<b>02. Marketing</b> No description	27	1	0
	<b>03. Finance</b> No description	24	1	0



Q Search...

Last Push	Push Status
-----------	-------------

Jun 7, 2020 12:49:54 PM	 Active ▼	
----------------------------	--	---

-  **Deactivate group push**  
Stop pushing group memberships. Existing memberships are unaffected.
-  **Unlink pushed group**  
Stop pushing group memberships and optionally delete the pushed group.
-  **Push now**  
Push this group's memberships to Zendesk

- 
- 

PUSHED GROUPS				
---------------	---	--	---	---

PUSHED GROUPS				
---------------	---	--	---	---

## Unlink Pushed Group

### What do you want to do with this group?

No user accounts are deleted with either option

- Delete the group in the target app (recommended)**  
Delete the group in the target app. User accounts will not be deleted.
- Leave the group in the target app**  
Okta stops pushing memberships and the group remains in the target.

Unlink

Cancel

PUSHED GROUPS

+ Push Groups ▾

Refresh App Groups

✎ Bulk Edit



## Push Groups to G Suite

PUSHED GROUPS
Close

**PUSH GROUPS BY NAME**

To sync group memberships from Okta to G Suite, choose a group in Okta and a group in the app.

01. Regional sales

 Push group memberships immediately

Group	Match result & push action
01. Regional sales	No Match found <div style="margin-bottom: 5px;"> <span style="color: green; font-weight: bold;">+</span> Create Group ▾ <span style="margin-left: 10px;">G 01. Regional sales</span> </div> <div style="margin-bottom: 5px;"> <span style="color: green; font-weight: bold;">+</span> Create Group           </div> <div> <span style="color: blue; font-weight: bold;">🔗</span> Link Group           </div>

PUSHED GROUPS

+ Push Groups ▾

Refresh App Groups

Bulk Edit

← Back to Applications



G Suite

Active ▾



[View Logs](#)

General

Sign On

Mobile

Provisioning

Import

Assignments

Push Groups

## Push Groups to G Suite




PUSHED GROUPS


+ Push Groups ▾


Refresh App Groups

Bulk Edit

Group In Okta	Group In G Suite	Last Push	Push Status
00. Organization All apps for the whole org	00. Organization All users of the org	May 8, 2020 4:33:12 AM	<span style="color: green; font-weight: bold;">👤 Active</span> ▾ <span style="border: 1px solid #ccc; border-radius: 50%; padding: 2px 5px;">i</span>

	<b>All Users</b> No description	0	0	0
	<b>Domain Admins</b> devoteamlabs.site/Users/Domain Admins	0	0	0
	<b>Everyone</b> All users in your organization	191	0	0
	<b>Finance</b> No description	4	0	0
	<b>Domain Users</b> devoteamlabs.site/Users/Domain Users	1	0	0

 Add Group Q Search...

Source	Name	People	Apps	Directories
	<b>00. organization</b> No description	1	2	1



Master priority 

- Inherit from profile master ▲
- Inherit from profile master
- Inherit from Okta
- Override profile master

Save Attribute

Cancel

# Profile Masters

Profile Master	Priority
Active Directory devoteamlabs.site	1 
SAML Identity Provider DT inbound SAML	2 

## Profile & Lifecycle Mastering

[Edit](#)

Allow G Suite to master Okta users

Enabling this setting allows G Suite to control the profiles of assigned users and makes these profiles read only in Okta. Profiles are managed based on [profile master priority](#).

## Chapter 3: Single Sign-On for a Great End User Experience

Rule Name

TIP: Describe what this rule does

IF User's IP is

Manage configuration for [Networks](#)

AND User's device platform is  Any device  
 Any of these devices:

AND User is accessing  Any application  
 Any of following applications:

AND User matches

THEN Use this identity provider

Manage configuration for [Identity Providers](#)  
Manage configuration for [IWA](#)

[Create Rule](#) [Cancel](#)

+ Add Identity Provider						Search...
Name	Type	Account Mode	Profile Master	Actions		
DT inbound SAML	Saml2	JIT	✓	Active	Configure	
IdP ID	0					
SAML metadata	<a href="#">Download metadata</a>					
Assertion Consumer Service URL	https://...okta.com/sso/saml2/...					
Audience URI	https://www.okta.com/saml2/service-provider/...					

## Add Identity Provider

### GENERAL SETTINGS

**Name**

**Protocol** SAML2

### AUTHENTICATION SETTINGS

**IdP Username**  ?

[Expression Language Reference](#)

**Filter** ?  Only allow usernames that match defined RegEx Pattern


**Match against** ?

Choose the user attribute to match against the IdP username.

**If no match is found** ?  Create new user (JIT)  
 Redirect to Okta sign-in page

Name	Type	Account Mode	Profile Master	Actions
DT inbound SAML	Saml2	JIT	✓	Active ▾    Configure ▾
Okta hub	Saml2	JIT	✓	Active ▾    Configure ▾

[Show More](#)

 Login with Facebook

 Login with Twitter

 Login with Google+

OR

### Sign in manually

Username or email

Password

Remember me    **LOGIN**

[Register now](#) | [Forgot password?](#)

ATTRIBUTE STATEMENTS (OPTIONAL)

[LEARN MORE](#)

Name	Name format (optional)	Value
<input type="text"/>	Unspecified ▲	<input type="text"/>
<input type="button" value="Add Another"/>	Unspecified	
	URI Reference	
	Basic	

GROUP ATTRIBUTE STATEMENTS (OPTIONAL)

Name	Name format (optional)	Filter
<input type="text"/>	Unspecified ▼	Starts with ▼ <input type="text"/>
<input type="button" value="Add Another"/>		

Response ?	Signed ▼
Assertion Signature ?	Signed ▼
Signature Algorithm ?	RSA-SHA256 ▼
Digest Algorithm ?	SHA256 ▼
Assertion Encryption ?	Unencrypted ▼
Enable Single Logout ?	<input type="checkbox"/> Allow application to initiate Single Logout
Assertion Inline Hook	None (disabled) ▼
Authentication context class ?	PasswordProtectedTransport ▼
Honor Force Authentication ?	Yes ▼
SAML Issuer ID ?	<input type="text" value="http://www.okta.com/\${org.externalKey}"/>

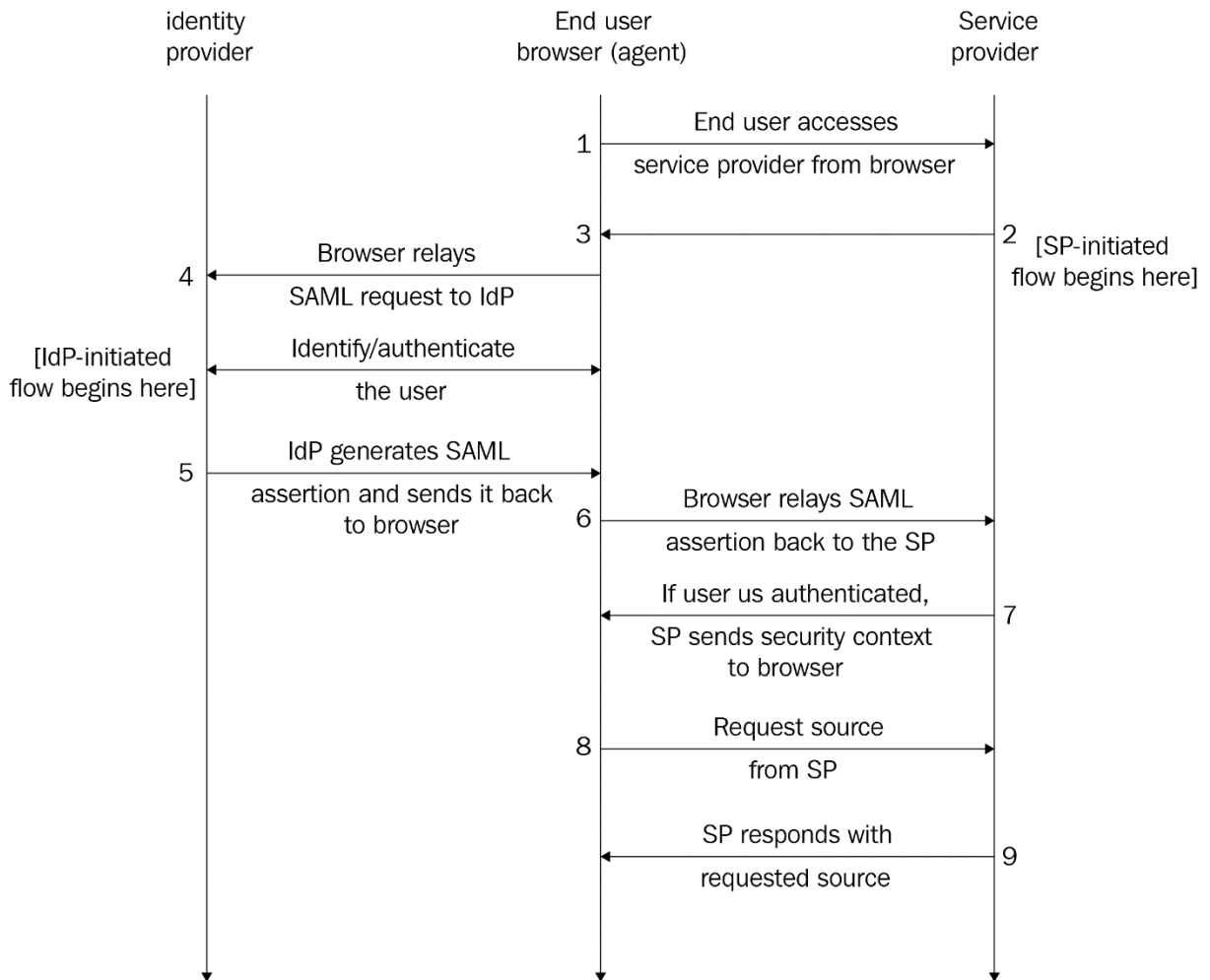


Name ID format ?

Application username ?

Update application username on

- Unspecified ▲
- Unspecified
- EmailAddress
- x509SubjectName
- Persistent
- Transient



Welcome to the Replicon Customer Zone

User Name

Password

[Forgot your Password or User Name?](#)



Remember Me

```



    <dt>_</dt>
    <dd>
      <input name="ctl00ContentPlaceHolder1$LoginNameTextBox"
        type="text" maxlength="128" id="LoginNameTextBox" style="
        display:block;" => $0
      </dd>
    <dt>_</dt>
    <dd>_</dd>
    </dl>
    <div id="PwdForgot" class="forgotPassword" style="margin-
    bottom: 5px;">_</div>
    <div id="ButtonRow" class="buttonRow">_</div>
    <div class="loginAreaChild">_</div>
    <input type="hidden" name="
    ctl00ContentPlaceHolder1$hdnAlternateLoginProviders" id=
  
```

... #loginPanel #pnlInternalLogin div #LoginFields dd input#LoginNameTextBox

Styles	Event Listeners	DOM Breakpoints	Properties	Accessibility
Filter			:hov .cls +,	

Your Apps   Admin Web Version

Search for an app Alt O

	<b>Salesforce.com</b> Salesforce.com	Quick Access
	<b>monday.com</b> monday.com	

Work  
Private



# Atlassian Jira Server

SAML, SWA, Provisioning

## CATEGORIES

### Featured

API Management	6
Apps	6116
Apps for Good	9
CASB	3
Directories and HR Systems	13
Security Applications	662
Okta Applications	11
Okta Test Applications	14
VPN	22



Enter your organization name to sign in:  
<https://yoursitename.okta.com>

Site Name

Username

Password

Sign In





Search your apps

[Back to the old dashboard](#)

My Apps

Recently Used

Work

personal

Unused

[Add Section](#)

Notifications

Add Apps

HenkJan

Admin

Settings

Recent Activity

Sign out

Last sign in: 6 minutes ago

© 2020 Okta, Inc. | Privacy

Recently Used

 LinkedIn	 Atlassian Cloud Confluence SAML	 Hootsuite	 Zendesk	 Okta Advanced Server Access
--------------	--	---------------	-------------	------------------------------------

Work

 Slack	 G Suite (admin) Google Account	 BambooHR	 Workplace by Facebook	 Microsoft Office 365 (admin demo) Office...
-----------	---------------------------------------	--------------	---------------------------	--

 Salesforce.com	 NetSuite	 Azure Portal Login	 Okta Advanced Server Access	 ServiceNow UD
--------------------	--------------	------------------------	------------------------------------	-------------------

 Google Cloud Platform	 Atlassian Cloud Jira SAML	 Bitglass Admin portal	 Atlassian Cloud Confluence SAML	 LinkedIn
---------------------------	----------------------------------	---------------------------	--	--------------

## Add Rule

### Rule Name

TIP: Describe what this rule does

### Exclude Users

Exclude Users

IF User's IP is

Anywhere

Manage configuration for [Networks](#)

AND Authenticates via

Any

AND Behavior is

Select behavior

AND Risk is

Any

THEN Access is

Allowed

Prompt for Factor

Manage configurations for [Multifactor Authentication](#)

Per Device

Every Time

Per Session

Factor Lifetime

15

Minut... ▾

Session expires after

2

Hours ▾

Create Rule

Cancel

## Add Policy

### Policy Name

TIP: Describe what this policy does

### Policy Description

Description

### Assign to Groups

Assign to groups

Create Policy and Add Rule

Cancel

## Authentication

Password

Sign On

Add New Okta Sign-on Policy

# Authentication

Password

Sign On

Add New Okta Sign-on Policy



1 Office sign in policy



2 MFA Hard token sign on



3 MFA normal



4 MFA SMS



5 Default Policy



## Add Rule

### Rule Name

TIP: Describe what this rule does

### Exclude Users

Exclude Users

IF

User's IP is

Anywhere

Manage configuration for [Networks](#)

THEN

User can

change password




perform self-service password reset

perform self-service account unlock

Create Rule

Cancel

Add Rule

Priority	Rule Name	Access	Status	Actions
1	No selfservice		Active	  

## Edit Policy

### Common password check ?

Restrict use of common passwords

### Password age

Enforce password history for last  passwords

Minimum password age is

Password expires after  days

Prompt user  days before password expires

### Lock out

Lock out user after  unsuccessful attempts

Account is automatically unlocked after  minutes

Show lock out failures

Send lockout email to user

## ACCOUNT RECOVERY

### Self-service recovery options

SMS

Voice Call

Email

Reset/Unlock recovery emails are valid for

### Password recovery question complexity

characters

Update Policy

Cancel

## Edit Policy


### Policy name

Finance passwords

### Policy description

a stricter pwd policy

### Add group

 03. Finance ×

## AUTHENTICATION PROVIDERS

### Applies to

Okta

## PASSWORD SETTINGS

### Minimum length

10 characters

### Complexity requirements

- Lower case letter
- Upper case letter
- Number (0-9)
- Symbol (e.g., !@#\$\$%^&\*)
- Does not contain part of username
- Does not contain first name
- Does not contain last name

# Authentication

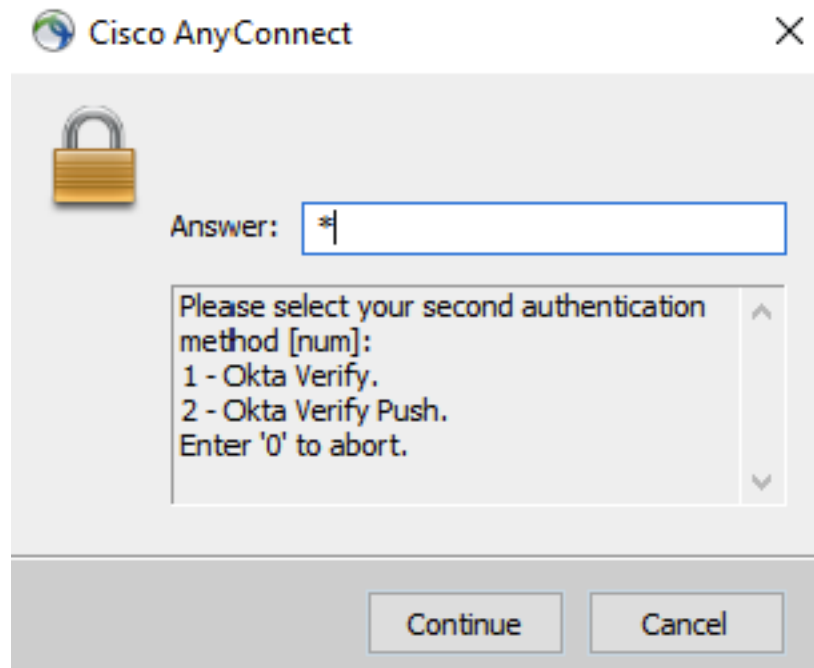
Password

Sign On

Add New Password Policy

- 1 Administrators passwords
- 2 Finance passwords
- 3 Office passwords
- 4 Standard organisation passw...
- 5 Active Directory Policy**
- 6 Default Policy


## Chapter 4, Increasing Security with Adaptive Multi-Factor Authentication



✓ Extra Verification

Extra verification increases your account security when signing in to Okta and other applications you use






Okta Verify	Remove
Security Key or Biometric Authenticator	Set up another
YubiKey 5 Last used 2 months ago	Remove
Google Authenticator	Set up

 + Add Rule

Priority	Rule name	Status	Actions
----------	-----------	--------	---------






1  MFA denied access Active  

CONDITIONS	ACTIONS
------------	---------

- |  |   |
|--|---|
|  In group: 98.4 MFA security question |  Deny access |
|  Anywhere                             |   |
|  Any client                           |   |
|  Any                                  |   |

2 Default sign on rule Active Not editable


CONDITIONS	ACTIONS
------------	---------

- |  |  |
|--|--|
|  User assigned this app |  Allow access |
|  Anywhere               |  |
|  Any client            |  |
|  Any                  |  |

# Enable macOS Device Trust


Device Trust

Enable macOS Device Trust

Learn more link (optional) 

Trust is established by

Jamf Pro ▼

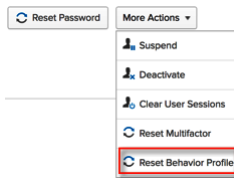
Enter the information below for a user with API privileges to connect to Jamf Pro API. We recommend you create separate credential for API Access. [View more information](#) 

Jamf URL










API Username

API Password

Test API Credentials



**Add Rule**

Priority	Rule Name	Access	Status	Actions
1	Sales team High risk	Allowed	Active ▾	  
2	Sales team Medium risk	Allowed	Active ▾	  
3	Sales team Low risk	Allowed	Active ▾	  

**IF** User's IP is

Manage configuration for [Networks](#)

**AND** Authenticates via















**AND** Behavior is

**AND** Risk is

**THEN** Access is



# Behavior Detection

Add Behavior ▾				
Name	Behavior Type	Details		Actions
New City	Location	Location granularity Evaluate against past	City 10 authentications	Active ▾  
New Country	Location	Location granularity Evaluate against past	Country 10 authentications	Active ▾  
New Device	Device	Evaluate against past	20 authentications	Active ▾  
New Geo-Location	Location	Location granularity Evaluate against past Radius from location	Latitude - Longitude 20 authentications 20 kilometers	Active ▾  
New IP	IP	Evaluate against past	50 authentications	Active ▾  
New State	Location	Location granularity Evaluate against past	State or Region 15 authentications	Active ▾  
Velocity	Velocity	Velocity	805 Km/h	Active ▾  

## Add Dynamic Zone

Zone Name

**Blacklist access from IPs matching conditions listed in this zone**

WARNING: Selecting this option will prevent matching IPs from accessing Okta.

IP Type

Locations

+ Add Another

Save

Cancel

Add Zone ▾



IP Zone

Create ranges of gateway IPs and proxy IPs



Dynamic Zone

Conditions for IP Type and location

## Add IP Zone

Zone Name

**Blacklist access from IPs matching conditions listed in this zone**

WARNING: Selecting this option will prevent matching IPs from accessing Okta.

Gateway IPs ?

Add your current IP address 82.197.207.175 Max 150

Proxy IPs ?

ZScaler proxy addresses can be found [here](#) Max 150

**Dynamic Zones** and **Behaviors** use the configured proxies to identify where requests originated.

**ThreatInsight** automatically whitelists the configured proxies for your org.

Save

Cancel

Add Zone ▾
















IP Zone

Create ranges of gateway IPs and proxy IPs



Dynamic Zone

Conditions for IP Type and location

Add Zone ▾					
Name	Zone Type	Details		Actions	
AWS VM's	IP	Gateway IPs	198.51.100.2/24		Active ▾  
Blacklist	Dynamic	IP Type	Any		Active ▾  
		Locations	Afghanistan China <a href="#">See All</a>		
BlockedIpZone	 IP Blacklist				
HQ	Dynamic	IP Type	Any		Active ▾  
		Locations	United States, California		
LegacyIpZone	IP				
New York	Dynamic	IP Type	Any		Active ▾  
		Locations	United States, New York		
Singapore	Dynamic	IP Type	Any		Active ▾  
		Locations	Singapore		

# Multifactor

Factor Types

Factor Enrollment

Add Multifactor Policy



1

MFA EfficientOffice



2

MFA security Question



3

MFA Google Auth



4

MFA SMS



5

MFA Okta verify



6

MFA Default







7

Default Policy

# Multifactor

Factor Types

Factor Enrollment

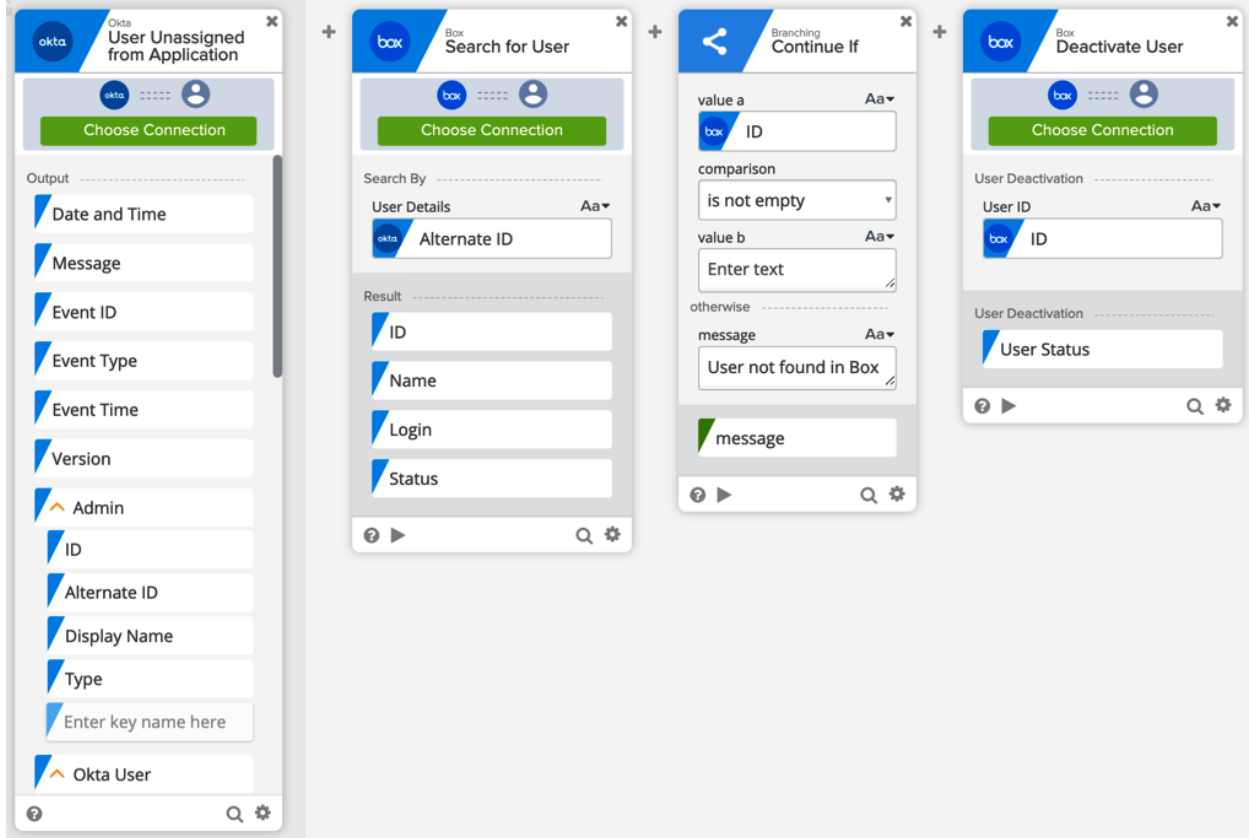
Okta Verify	
SMS Authentication	
Voice Call Authentication	
Google Authenticator	
FIDO2 (WebAuthn)	
YubiKey	
Duo Security	
Symantec VIP	
On-Prem MFA	
RSA SecurID	
Security Question	
Email Authentication	

## Chapter 5, Automating Using Life Cycle Management

The image displays three sequential steps in a workflow automation tool:

- Step 1: Search for User**
  - Provider: Box
  - Options: Search By, User Details, Alternate ID (Okta)
  - Result: User ID, Role, Name, Login, Status
- Step 2: Branching Continue If**
  - value a: User ID (from Step 1)
  - comparison: is not empty
  - value b: Enter text
  - otherwise message: User not found in Box
- Step 3: Deactivate User**
  - User Deactivation: User ID (from Step 2)
  - User Deactivation: User Status

Arrows indicate the data flow: 'User ID' from the search results is passed to 'value a' in the branching step, and 'User ID' from the branching step is passed to the 'User ID' field in the deactivation step.




[Workflow](#) [Reports](#) [Settings](#)

[Automations](#)

[Inline Hooks](#)

[Event Hooks](#)

[Workflows console](#) 



← Back to all Automations

Active ▾

Delete

### deactivate users

#### When the following conditions are all true

+ Add Condition	
Name	
🕒	Every day at 11:59 PM CEST <span>✎</span>
👤	For the groups: 00. Organization <span>✎</span>
👤	User inactive in Okta for 30 day(s) <span>✎</span>

#### Perform the following actions

+ Add Action	
Name	
💬	Send email to the user <span>✎</span>
👤	Change user lifecycle state in Okta to "Deactivated" <span>✎</span>

#### If request is approved

Assign the app and provision an account according to your provisioning options.

- Send email to requester
- Send email to approvers
- Send email to others...

#### If request is denied

- Send email to requester
- Send email to approvers
- Send email to others...

#### Approver must respond within

1 Week ▾

#### If request expires

- Send email to requester
- Send email to approvers
- Send email to others...

Save

Cancel

## REQUESTS

Allow users to request app  No

Yes

Note for requester (optional)

Add a description of the app or instructions for the requester

500 characters remaining

## APPROVAL

Approval  Not Required

Required

Save

Cancel

# Self Service

Settings

Usage

## User App Requests

Edit

### App Catalog Settings

- Allow users to add org-managed apps
- Allow users to add personal apps
- Allow users to email "Technical Contact" to request an app

### ▼ 02. Marketing

IF user.department equals "Marketing"

THEN Assign to 02. Marketing

EXCEPT Richard Allen

## Groups

Group
<b>Everyone</b> All users in your organization
<b>00.1 Stockholm HQ</b> Everyone @ HQ • Managed by <b>00.1 HQ</b>
<b>00. Organization</b> All apps for the whole org • Managed by <b>00. Organization</b>
<b>04. devops</b> Managed by <b>04. Devops</b>

**Name**

**IF**  Use basic condition  Use Okta Expression Language (advanced)

**THEN** Assign to  **80.1 Office business essentials**

This rule will not add users to a group they've been manually removed from.

**Name**

**IF**  Use basic condition  Use Okta Expression Language (advanced)

includes any of the following

**90. Offboarding - grace period**

**THEN** Assign to  **98.2 MFA SMS**

This rule will not add users to a group they've been manually removed from.

**Name**

**IF**  Use basic condition  Use Okta Expression Language (advanced)

[Expression Language Reference](#)

**THEN** Assign to  05. Customer Support

This rule will not add users to a group they've been manually removed from.

**Name**

**IF**  Use basic condition  Use Okta Expression Language (advanced)

includes any of the following

**THEN** Assign to  00. RDS domain access

This rule will not add users to a group they've been manually removed from.

**Name**

**IF**  Use basic condition  Use Okta Expression Language (advanced)

includes any of the following

**THEN** Assign to  01. Sales

This rule will not add users to a group they've been manually removed from.

**Name**

**IF**  Use basic condition  Use Okta Expression Language (advanced)

**THEN** Assign to

This rule will not add users to a group they've been manually removed from.

G Suite User Profile Mappings

G Suite to Okta User | Okta User to G Suite

G Suite	G Suite User Profile	Okta	Okta User User Profile
	appuser		user
Username is set by G Suite		login	string
<input type="text" value="appuser.nameGivenName"/>	<input type="button" value="→"/>	firstName	string
<input type="text" value="appuser.nameFamilyName"/>	<input type="button" value="→"/>	lastName	string
<input type="text" value="Choose an attribute or enter an expression..."/>	<input type="button" value="→"/>	middleName	string
<input type="text" value="Choose an attribute or enter an expression..."/>	<input type="button" value="→"/>	honorificPrefix	string

Enter an Okta user to preview their mappings...

Okta Attribute	Value	Apply on
Username	Configured in <a href="#">Sign On settings</a>	
login		
First name	appuser.nameGivenName	Create <input type="button" value="✎"/> <input type="button" value="✕"/>
firstName		

**Profile & Lifecycle Mastering**

Allow BambooHR to master Okta users

Enabling this setting allows BambooHR to control the profiles of assigned users and makes these profiles read only in Okta. Profiles are managed based on [profile master priority](#).

When a user is deactivated in the app

When a user is reactivated in the app  Reactivate suspended Okta users  Reactivate deactivated Okta users

When enabled, existing users will be reactivated automatically

## Integration

Edit

### AGENT

Connect to these agents  csv-okta-agent

To connect more agents, download the agents.

### CSV FIELD SETTINGS

#### Unique identifier field

Once set, this field cannot be changed

#### Deactivation field

This field provides an explicit way for an admin to designate that a user should be deactivated

#### Deactivation value

If a user's deactivation field contains this value, the user will be deactivated

### CSV IMPORT FILEPATHS

#### Full import filepath

#### Incremental import filepath

If provided, this must be different from the full import filepath



# CSV Directory

Active ▼



[View Logs](#)

General

Provisioning

Import

People



## Confirm Imported User Assignments



Click Confirm to complete the following assignments:

- 1 new Okta users will be created from Zendesk users
- 1 existing Okta users will be assigned to Zendesk users
- 0 Zendesk users will be ignored


Auto-activate users after confirmation

Confirm

Cancel

 **EXACT** Okta user match 

Name:	Kay Berg
Username:	Kay.Berg@avalondemo.com
Email:	Kay.Berg@avalondemo.com

 **NEW** Okta user

Name:	Kay Berg
Username:	kay.berg@avalondemo.com
Email:	kay.berg@avalondemo.com

 **EXISTING** Okta user I specify

 **IGNORE** this user for now

# Import Results

Import Now Clear Unconfirmed Users **6** imported users need review · **0** imported users confirmed

ALL	NO	EXACT	PARTIAL	IGNORED	Search	Confirm Assignments 0	
Show 10	Showing 1 - 6 of 6		First	Previous	1	Next	Last
zendesk	Imported User	Okta	Okta User Assignment				
<b>1 EXACT</b>	Okta user match found Name: Kay Berg Username: kay.berg@avalondemo.com Email: kay.berg@avalondemo.com	ASSIGN TO →	<b>EXACT</b> Okta user match Name: Kay Berg Username: Kay.Berg@avalondemo.com Email: Kay.Berg@avalondemo.com	<input type="checkbox"/>			
<b>NO</b>	Okta user matches found Name: Sample customer Username: customer@example.com Email: customer@example.com	ASSIGN TO →	<b>NEW</b> Okta user Name: Sample customer Username: customer@example.com Email: customer@example.com	<input type="checkbox"/>			
<b>1 EXACT</b>	Okta user match found Name: HenkJan de Username: henkjan.devries@devoteam.com Email: henkjan.devries@devoteam.com	ASSIGN TO →	<b>EXACT</b> Okta user match Name: HenkJan de Vries Username: henkjan.devries@devoteam.com Email: henkjan.devries@devoteam.com	<input type="checkbox"/>			
<b>1 EXACT</b>	Okta user match found Name: Reagan Hancock Username: reagan.hancock@avalondemo.com Email: reagan.hancock@avalondemo.com	ASSIGN TO →	<b>EXACT</b> Okta user match Name: Reagan Hancock Username: Reagan.Hancock@avalondemo.com Email: Reagan.Hancock@avalondemo.com	<input type="checkbox"/>			
<b>1 EXACT</b>	Okta user match found Name: Hilda Herring Username: hilda.herring@avalondemo.com Email: hilda.herring@avalondemo.com	ASSIGN TO →	<b>EXACT</b> Okta user match Name: Hilda Herring Username: Hilda.Herring@avalondemo.com Email: Hilda.Herring@avalondemo.com	<input type="checkbox"/>			
<b>1 EXACT</b>	Okta user match found Name: Ali Stuart Username: ali.stuart@avalondemo.com Email: ali.stuart@avalondemo.com	ASSIGN TO →	<b>EXACT</b> Okta user match Name: Ali Stuart Username: Ali.Stuart@avalondemo.com Email: Ali.Stuart@avalondemo.com	<input type="checkbox"/>			
Show 10	Showing 1 - 6 of 6		First	Previous	1	Next	Last



← Back to Applications



G Suite

Active ▾



View Logs

General

Sign On

Mobile

Provisioning

**Import**

Assignments

Push Groups

## Import Results

Import Now

Clear Unconfirmed Users

0 imported users need review · 2 imported users confirmed

ALL	NO	EXACT	<b>PARTIAL</b>	IGNORED	Q Search	Confirm Assignments 0			
Show 10						First	Previous	Next	Last
	Imported User		Okta User Assignment						<input checked="" type="checkbox"/>
No records found									
Show 10						First	Previous	Next	Last
						Confirm Assignments 0			

## User Creation & Matching

Cancel

Imported user is an exact match to Okta user if

Okta username format matches

Email matches

The following attribute matches:

firstName

The following combination of attributes matches:

Okta username format or Email

Allow partial matches

Partial match on first and last name

Confirm matched users

Auto-confirm exact matches

Auto-confirm partial matches

Confirm new users

Auto-confirm new users

Auto-activate new users

Save

Cancel

Okta username format

Custom

Select the username users should enter to log into Okta.

Enter an expression

[Expression Language Reference](#)

Enter an Okta user to preview this mapping





### General

Cancel

Import users from G Suite to create new Okta users. If the Okta user already exists, the two accounts will automatically be linked. Imported users are assigned G Suite access when they are confirmed on the Import tab.

#### Schedule import

never ▼

Select never if you prefer to import manually

#### Okta username format

Email Address ▼

Select the username users should enter to log into Okta.

#### Update application username on

Create only

Save

Cancel



### Deactivate Users

Enable

Deactivates a user's Box account when it is unassigned in Okta or their Okta account is deactivated. Accounts can be reactivated if the app is reassigned to a user in Okta.

#### Box user status on deactivation

Deleted ▼

#### File management upon user deletion

Transfer user's files to service account user ▼

#### Box email address of service account user



### Provisioning to App

Cancel

#### Create Users

Enable

Creates or links a user in G Suite when assigning the app to a user in Okta.

The [default username](#) used to create accounts is set to **Okta username**.

#### Update User Attributes

Enable

Okta updates a user's attributes in G Suite when the app is assigned. Future attribute changes made to the Okta user profile will automatically overwrite the corresponding attribute value in G Suite.

#### Deactivate Users

Enable

Deactivates a user's G Suite account when it is unassigned in Okta or their Okta account is deactivated. Accounts can be reactivated if the app is reassigned to a user in Okta.

#### Sync Password

Enable

Creates a G Suite password for each assigned user and pushes it to G Suite.

#### Password type ?

- Sync a randomly generated password
- Sync Okta Password

Save

SETTINGS

To App

To Okta

Integration

# Capabilities

## Access

---

✓ SAML  
.....

OIDC  
.....

WS-Federation  
.....

✓ SWA  
.....

## Provisioning

---

✓ Create  
.....

✓ Update  
.....

✓ Deactivate  
.....

Sync Password  
.....

✓ Group Linking  
.....

✓ Group Push  
.....

✓ Schema Discovery  
.....

Attribute Mastering  
.....

Attribute Writeback  
.....

# Chapter 6, Customizing Your Okta GUI

ACTIVATION

User Activation

These emails are sent to your new users who must follow the provided link to complete the Okta sign up process.

**i** You have edited the default email template which disables automatic translations. All users will receive the default language selected unless you add translations manually. To revert back to the default, click reset template(s) button.

Active Directory User Activation

LDAP User Activation

Send Push Verify Activation Link


Custom Email Reset to Default

PASSWORD

Forgot Password Denied

Add Translation

Default Language English (en) ▾

English (en) 

## Edit Default Email

**!** The default email template is provided automatically in all Okta-supported languages. If you edit the default template, Okta will not send the default email to end users automatically and you will need to add templates in multiple languages manually.

Language

English (en) ▾

Please select a language from the dropdown menu above

Subject

Welcome to Okta!

Message

```
<div id="welcome-ad" style="background-color:#fafafa;margin:0">
<table style="font-family:'proxima nova', 'century gothic', 'arial', 'verdana', sans-serif;font-size:14px;color:#5e5e5e;width:98%;max-width:600px;float:none;margin:0 auto" border="0" cellpadding="0" cellspacing="0" valign="top" align="left">
<tbody>
<tr align="middle">
<td style="padding-top:30px;padding-bottom:32px"></td>
</tr>
<tr bgcolor="#ffffff">
<td>
```

Save Cancel

## Customize Error Pages

Reset to Default Save and Publish Preview

```
1 <html>
2 <head>
3   <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
4   <meta name="viewport" content="width=device-width, initial-scale=1.0" />
5   <meta name="robots" content="none" />
```

Warning: Changing these settings can sometimes cause unexpected behavior or compromise the security of your system.



### Enable Okta plugin logs

Displays Okta plugin activity on the developer console. You can also record a log of plugin activity. This setting is intended for troubleshooting.



### Use local JavaScript

Configures the plugin to always use the local version of the content script instead of the latest version.

### Reset Plugin

This button will clear your Okta plugin cache.

[Reset Plugin](#)

## Advanced ▼

Warning: Changing these settings can sometimes cause unexpected behavior or compromise the security of your system.

### Enable Okta plugin logs

Displays Okta plugin activity on the developer console. You can also record a log of plugin activity. This setting is intended for troubleshooting.

### Use local JavaScript

Configures the plugin to always use the local version of the content script instead of the latest version.

## Reset Plugin

This button will clear your Okta plugin cache.

Reset Plugin



## Okta Plugin Settings



### Recommend strong passwords for apps

The Okta plugin will recommend strong random passwords when you reset app passwords.



### Prompt to save apps to your Okta dashboard

The Okta plugin will offer to save your app credentials and create the app on your Okta dashboard upon a successful sign in.



### Disable browser password prompts

This feature is not available because your privacy related settings are managed by your organization or another extension.

**Advanced** >

🔍 Search for an app



Recently Used

Work



ServiceNow UD



Workplace by Facebook



Microsoft Office 365 (admin demo) Office Portal



BambooHR



Salesforce.com

Web version

 Search for an app



## Recently Used

### Work

 servicenow

ServiceNow UD

 workplace  
by facebook

Workplace by Facebook

 Office 365

Microsoft Office 365 (admin demo) Office Portal

 bambooHR

BambooHR

 salesforce

Salesforce.com

Web version

Work +

 ServiceNow UD	 NetSuite	 Atlassian Cloud Jira SA...	 Atlassian Cloud Conflu...	 Google Cloud Platform
--	---	---	---	--

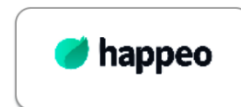
## Recently Used



Salesforce.com



LinkedIn



Happeo

## Sign-Out Page

Cancel

You can change the page your users are taken to when they sign out of Okta.

- Use the default sign-out page
- Use a custom sign-out page

**Sign-out page URL**

Save

## PERSONAL INFORMATION

- Personal Information is managed in Okta
- Personal Information is managed by a different application

Enter a message and redirect link to display on your users' Account tab above their Personal Information form. The form will be read-only.

### Custom Message

### Custom link label

### Custom link URL

Preview Message

## Customization

General

End-user dashboard

Custom Sign In

Custom Error Pages



**Sign-In Page** Cancel

You can change the heading, labels, and customize help links on your users' sign-in page. Values changed on the user's sign-in page will not be localized.

**HEADING**

**Sign In**

**USERNAME & PASSWORD FIELDS**

**Username label**

**Username info tip**


**Password label**

**Password info tip**

**Sign-In Configuration** Cancel

Upload an image to customize your organization's Sign-In Page.

**Sign-In Background Image**

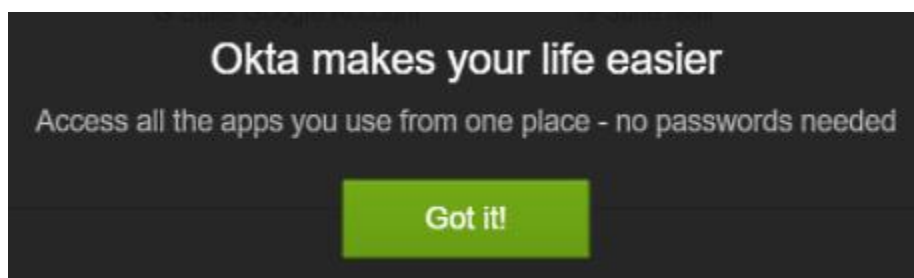


The image must be a png, jpg, or gif file, and be less than 2MB in size.

Browse..

Upload Image Use Default

Save



### Display Options Cancel

Link your organization's logo to a website by configuring a logo URL. Enable or disable the footer features and the onboarding screen for new end-users.

Logo URL	<input type="text" value="https://acme.com"/>
Okta Home footer	<input type="text" value="Enable"/>
Onboarding screen	<input type="text" value="Enable"/>

Save

### Organization Logo

Cancel

Upload your logo file


Välj fil packt.png

- File type must be .jpg, .png or .gif
- Maximum logo dimensions are 3,000x500px. Tip: Use a logo less than 300x50px to prevent scaling.
- Maximum file size is 100kB

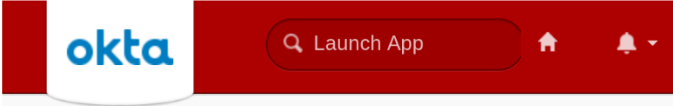
Upload Logo

**Application Theme**

Choose an application theme to customize the look-and-feel for your end users. Click on a thumbnail to choose a theme.




Change Theme Cancel



 **Forgot Password Text Message**

Okta can send you a text message with a recovery code. This feature is useful when you don't have access to your email.

<b>Country</b>	NL
<b>Phone number</b>	<input type="text"/>

 Edit  Delete



## Forgotten Password Question

Cancel

Select a forgotten password question so you can reset your password in case you have trouble signing in to your Okta account.

### Tips for choosing a good security question:

- Don't pick a question that someone could easily guess or find out the answer to by looking at your resume or social networking profile.
- Pick a question with an answer that is easy for you to remember.
- Don't write your security question down on a piece of paper where someone could find it.

### Question

What is the food you least liked as a child? ▼

### Answer

Save

## Change Password

Password requirements: at least 12 characters, a lowercase letter, an uppercase letter, a number, no parts of your username, does not include your first name, does not include your last name. Your password cannot be any of your last 4 passwords. At least 2 hour(s) must have elapsed since you last changed your password.

### Current password

### New password

### Confirm new password

Change Password

## Display Language

Cancel

Language

English ▲

Čeština

Dansk

Deutsch

Save

## ✓ Extra Verification

Extra verification increases your account security when signing in to Okta and other applications you use

Okta Verify

Remove

Security Key or Biometric Authenticator

Set up another

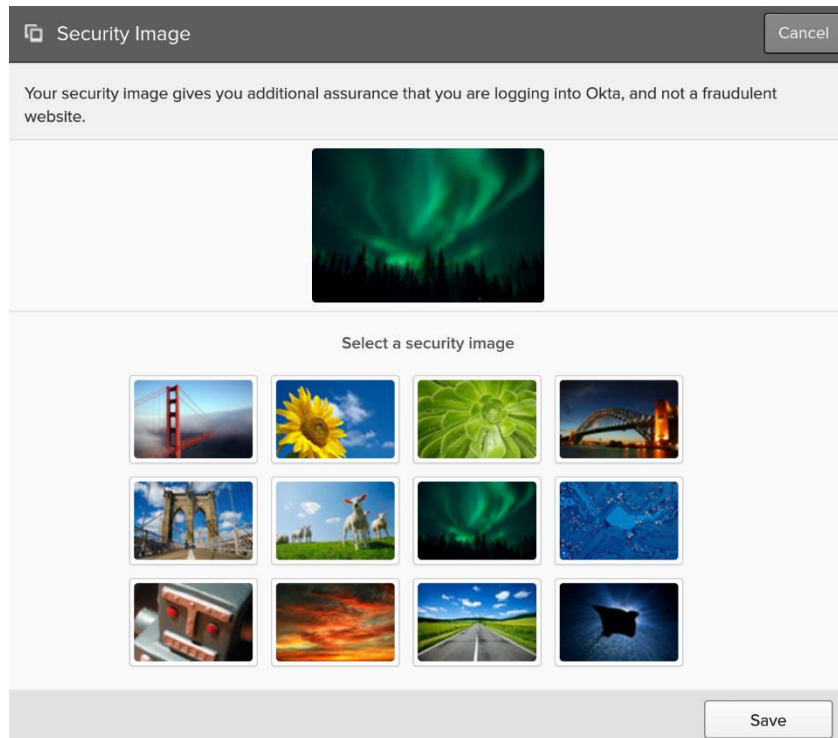
YubiKey 5

Last used 2 months ago

Remove

Google Authenticator

Set up

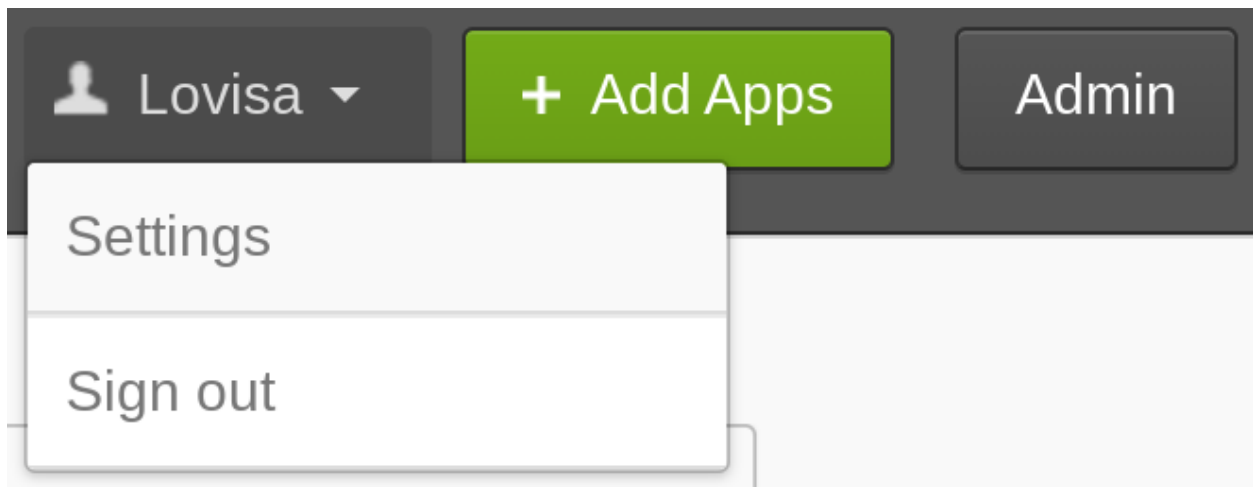


 HenkJan

Admin

Settings

Sign out



The screenshot shows a dark grey header bar. On the left, there is a user profile section with a person icon and the name "Lovisa" followed by a downward arrow. In the center, there is a green button with a white plus sign and the text "Add Apps". On the right, there is a dark grey button with the text "Admin". A white dropdown menu is open below the "Lovisa" profile, containing two items: "Settings" and "Sign out".

## Chapter 7, API Management

### VALID KEYS

<b>Next</b>	84JpOm4yxD_cU6n0XVqJJUH-G_PbBkkRWUBNYG5c0oY
<b>Current</b>	UKIDIJ6DDvhJsh_bbpGdJCQX-cbCE17T7xxiv3RmZ4
<b>Previous</b>	g7mnAuYuCOF9XaWvWSdezpyUekdE0zgkaK78tlb2nHw

[← Back to Authorization Servers](#)

# My Demo App

Active ▾

Settings

Scopes

Claims

Access Policies

Token Preview

Settings

Rotate Signing Keys

Edit

## Add Rule

### Rule Name

TIP: Describe what this rule does

IF

Grant type is

Client acting on behalf of itself

Client Credentials

Client acting on behalf of a user

Authorization Code

Implicit

Resource Owner Password

AND

User is

Any user assigned the app

Assigned the app and a member of one of the following:

AND

Scopes requested

Any scopes

The following scopes:

THEN

Use this inline hook

None (disabled) ▾

AND

Access token lifetime is

1

Hours ▾

AND

Refresh token lifetime is

Unlimited ▾

but will expire if not used every

7

Days ▾

Create Rule

Cancel

### Add Policy

**Name**

**Description**

**Assign to**  All clients  
 The following clients:

**Value type**

**Filter** ? Only include groups that meet the following condition.

### Add Claim

**Name**

**Include in token type**

**Value type**

**Value** ?

[Expression Language Reference](#)

**Disable claim**  Disable claim

### Add Claim

Name

Include in token type Access Tok... ▾ Always ▾

Value type Expression ▾

Value <sup>?</sup>   
[Expression Language Reference](#)

Disable claim  Disable claim

Include in  Any scope  
 The following scopes:

Create Cancel

### Add Scope

Name   
For example: email

Description

Default scope  Set as a default scope

Metadata  Include in public metadata

Create Cancel

default

Active ▾

Settings

Scopes

Claims

Access Policies

Token Preview

---

Add Authorization Server

Name

Audience

Description

# API


Authorization Servers

Tokens

Trusted Origins

## Add Origin

Name

Origin URL 

Type

- CORS** Selecting 'CORS' enables the origin URL to access Okta APIs from Javascript.
- Redirect** Selecting 'Redirect' allows for browser redirection to 'Origin URL' after signing in or out.



ADD ORIGINS

Add Origin URLs to redirect users to custom screens or enable browser-based applications to access Okta APIs from Javascript (CORS).

Add Origin

Q Search...				
FILTERS	Name	Origin URL	Type	Actions
All Origins				
CORS				
Redirect				

## Chapter 8, Managing Access with Advanced Server Access

### 👤 Add Group to Project

Project

Server\_1

Group

read\_only

#### Server Account Permissions

Server accounts created by Advanced Server Access for members of this group will receive user-level permissions.

User

Server accounts created by Advanced Server Access for members of this group will receive administrative permissions.

Admin

#### Options

Sync group to servers

Create Group

# Server\_1

Actions

Details Groups Users Servers Enrollment Preauthorizations

Add Group to Project

find by name...

## User Groups

find by name...

NAME	TEAM ROLES	FEDERATION
04. devops		x
everyone		x
owners	Admin	x

## User Attributes

UNIX\_GID

150000

UNIX\_UID

150000

UNIX\_USER\_NAME

henkjan\_devries

WINDOWS\_USER\_NAME

henkjan\_devries

 **henkjan.devries**

 **Actions** ▾

Details

User Details

STATUS

✓ Active

FIRST NAME

HenkJan

LAST NAME

de Vries

FULL NAME

HenkJan de Vries

EMAIL

henkjan.devries@devoteam.com

### Update Team Attributes for 04. devops

Overriding a group's team attribute values may cause unintended collisions. Groups with colliding attribute values will not be synced to servers.

Attribute	Team Value
Unix GID *	<input type="text" value="180002"/>
Unix Group Name *	<input type="text" value="sft_devops"/>
Windows Group Name *	<input type="text" value="sft_devops"/>

**Update**

# Enter the following information from Okta

Once you have added Advanced Server Access to Okta, choose the "Sign On" tab under the application configuration, then click the "Identity Provider metadata" link.

Copy the URL below.

## IdP Metadata URL

<https://yourDomain.okta.com/app/eskdjfw293e/sso/saml/metadata>



To complete Advanced Server Access signup you'll need to authenticate with Okta. **Before proceeding, be sure to assign yourself to the Advanced Server Access application within Okta or you won't have permission to log in.**

[Authenticate With Okta](#)



SAML 2.0 is not configured until you complete the setup instructions.

[View Setup Instructions](#)

[Identity Provider metadata](#) is available if this application supports dynamic configuration.

### ADVANCED SIGN-ON SETTINGS

These fields may be required for a Okta Advanced Server Access proprietary sign-on option or general setting.

Base URL

Enter your Base URL. Refer to the Setup Instructions above to obtain this value.

Audience Restriction

Enter your Audience Restriction. Refer to the Setup Instructions above to obtain this value.

1 General Settings

General Settings - Required

Application label   
This label displays under the app on your home page

Application Visibility  Do not display application icon to users  
 Do not display application icon in the Okta Mobile App

General settings

All fields are required to add this application unless marked optional.

## Chapter 9, Leveraging Access Gateway for Your On-Premises Applications

### + New Protected Application : Sample Header Application

Access Gateway Sample Header -

**Settings**  
Define application

**Attributes**  
Define trusted attributes

**Policies**  
Define access rules