Authorship: https://www.linkedin.com/in/sedoykin

Disclaimer:

No guarantees or responsibilities are provided. You perform all actions at your own risk!

Teamcenter & OKTA MFA

Briefly: Here, we will try to integrate two-factor authentication based on OKTA with Teamcenter.

Contents

Authorship: https://www.linkedin.com/in/sedoykin

Disclaimer:

No guarantees or responsibilities are provided. You perform all actions at your own risk!

Introduction

Here we will try to implement two-factor authentication based on OKTA for Teamcenter. Guys, be prepared that this document might not work in your specific conditions, as there are too many uncertainties. However, I hope that it will provide the right directions for your research.

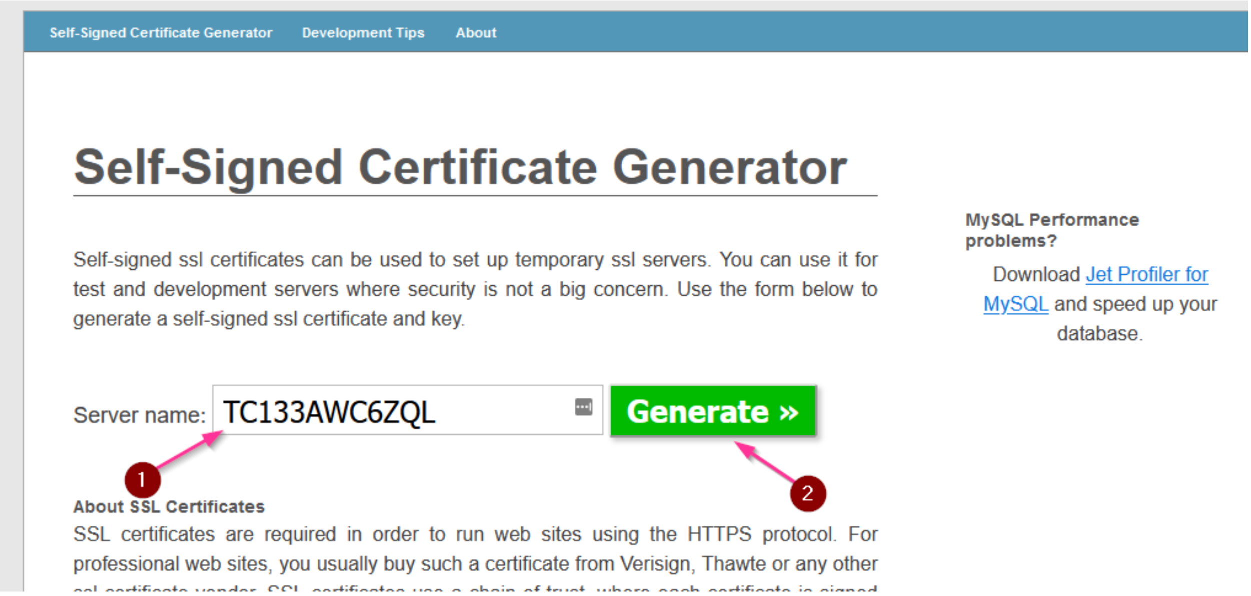
Authorship: https://www.linkedin.com/in/sedoykin
Disclaimer:
No guarantees or responsibilities are provided. You perform all actions at your own risk!

Prerequisites

- Teamcenter 13.3 (TcSS 13.3) + AWC 6
- Tomcat 9.0+
- Single server for all of TC components
- Hostname: *TC133AWC6ZQL
- All software installed in C:\Siemens
- OneLogin (okta.com) dev account:
  - *siemensdisrus-admin.okta.com
- Will be used SAML as technology for provide authorize data
- We will not use LDAP catalog on-premise!

Steps on the Teamcenter Infrastructure Side

1. **Generating self-signed certificates** - **https://www.selfsignedcertificate.com/**



Self-Signed Certificate Generator

Self-signed ssl certificates can be used to set up temporary ssl servers. You can use it for test and development servers where security is not a big concern. Use the form below to generate a self-signed ssl certificate and key.

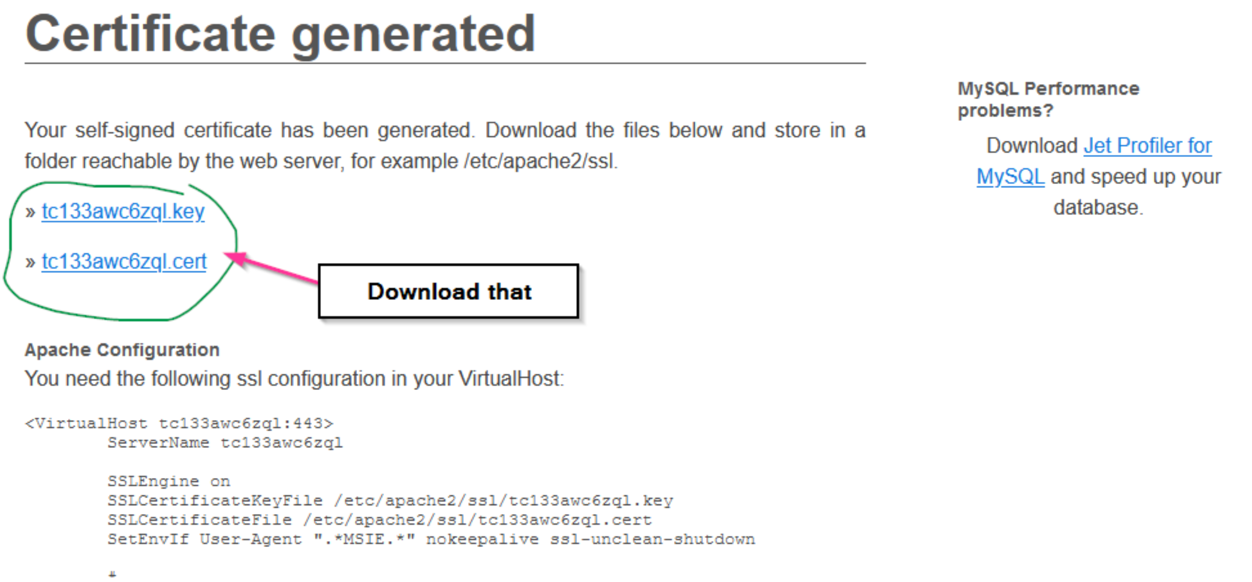
Server name: TC133AWC6ZQL **Generate »**

About SSL Certificates

SSL certificates are required in order to run web sites using the HTTPS protocol. For professional web sites, you usually buy such a certificate from Verisign, Thawte or any other ssl certificate vendor. SSL certificates use a chain of trust, where each certificate is signed

MySQL Performance problems?

Download Jet Profiler for MySQL and speed up your database.



Certificate generated

Your self-signed certificate has been generated. Download the files below and store in a folder reachable by the web server, for example /etc/apache2/ssl.

» tc133awc6zql.key

» tc133awc6zql.cert

Apache Configuration

You need the following ssl configuration in your VirtualHost:

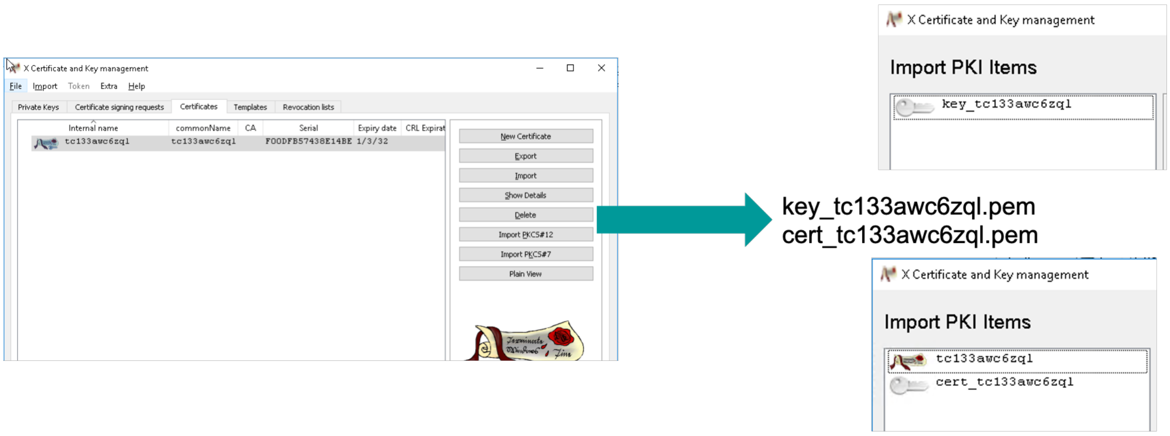
```
<VirtualHost tc133awc6zql:443>
        ServerName tc133awc6zql

        SSLEngine on
        SSLCertificateKeyFile /etc/apache2/ssl/tc133awc6zql.key
        SSLCertificateFile /etc/apache2/ssl/tc133awc6zql.cert
        SetEnvIf User-Agent ".*MSIE.*" nokeepalive ssl-unclean-shutdown
```

MySQL Performance problems?

Download Jet Profiler for MySQL and speed up your database.

2. **Convert key and cert to PEM format**
    a. Download https://hohnstaedt.de/xca
    b. Via XCA application, convert cert and key to PEM files



X Certificate and Key management

Internal name	commonName	CA	Serial	Expiry date	CRL Expirat
tc133awc6zql	tc133awc6zql		F00DFB57438E14BE	1/3/32	

key_tc133awc6zql.pem
cert_tc133awc6zql.pem

X Certificate and Key management

Import PKI Items

key_tc133awc6zql

X Certificate and Key management

Import PKI Items

tc133awc6zql
cert_tc133awc6zql

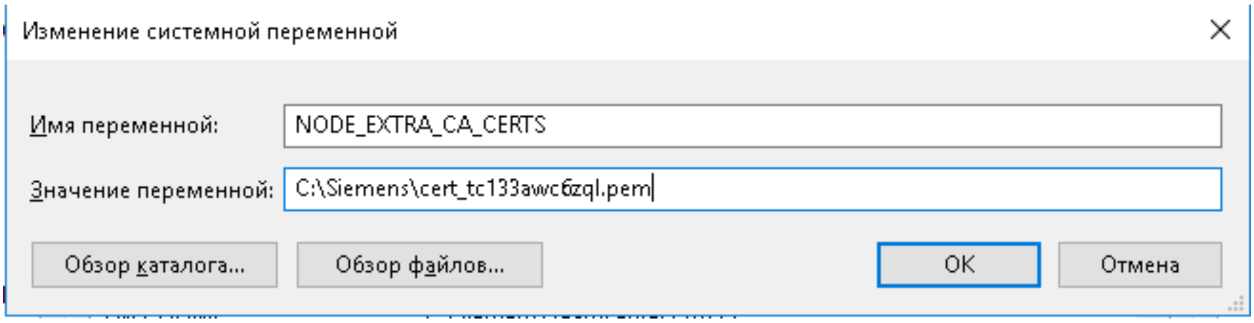
3. **Move the:**

key_tc133awc6zql.pem

cert_tc133awc6zql.pem

files to C:\Siemens and c:\Siemens\Tomcat9SSO\conf\

Create the next system variable (it needs for AWC)



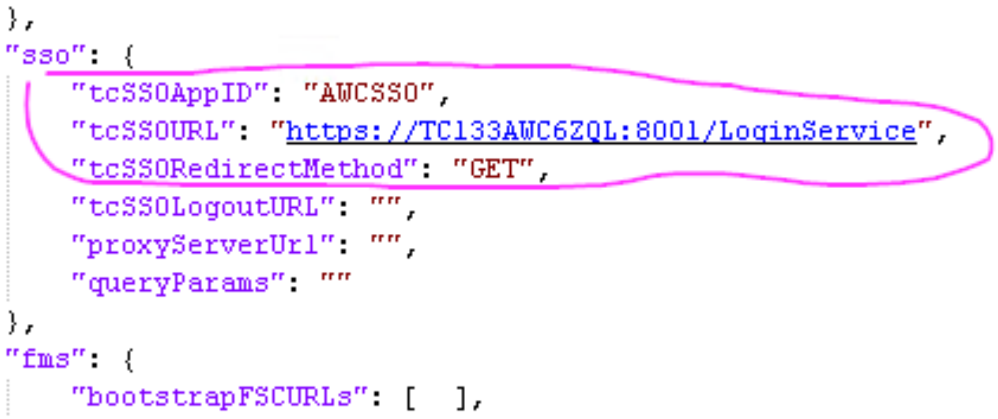
Изменение системной переменной

Имя переменной: NODE_EXTRA_CA_CERTS

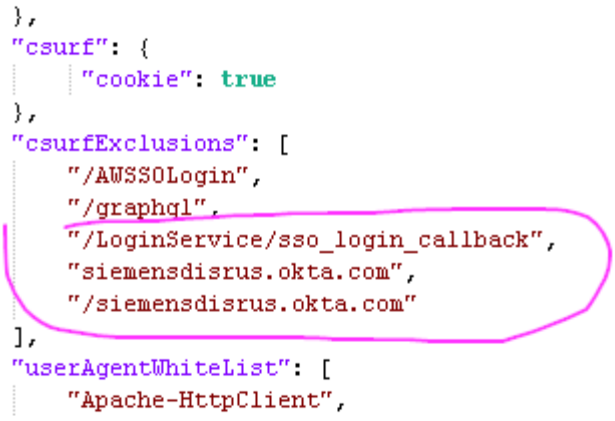
Значение переменной: C:\Siemens\cert_tc133awc6zql.pem

4. **Configuring AWC for access via HTTPS**

   Open **config.json** (c:\Siemens\Teamcenter13\microservices\gateway-1.6.0\config.json)



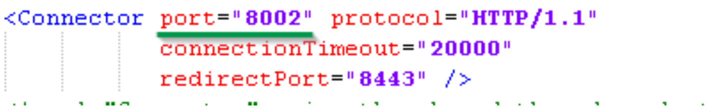
```
},
"sso": {
    "tcSSOAppID": "AWCSSO",
    "tcSSOURL": "https://TC133AWC6ZQL:8001/LoginService",
    "tcSSORedirectMethod": "GET",
    "tcSSOLogoutURL": "",
    "proxyServerUrl": "",
    "queryParams": ""
},
"fms": {
    "bootstrapFSCURLs": [  ],
```



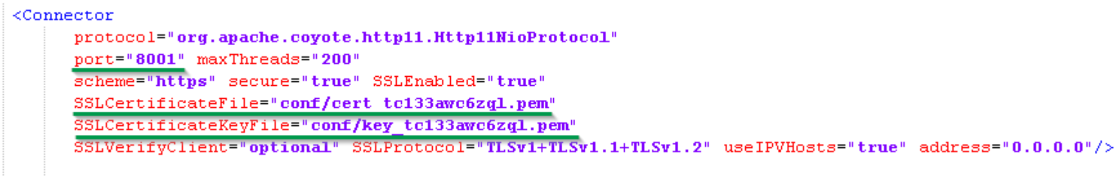
```
},
"csurf": {
    "cookie": true
},
"csurfExclusions": [
    "/AWSSOLogin",
    "/graphql",
    "/LoginService/sso_login_callback",
    "siemensdisrus.okta.com",
    "/siemensdisrus.okta.com"
],
"userAgentWhiteList": [
    "Apache-HttpClient",
```

5. **Configuring Tomcat for deploying TcSS components**

   Open server.xml (c:\Siemens\Tomcat9SSO\conf\server.xml)



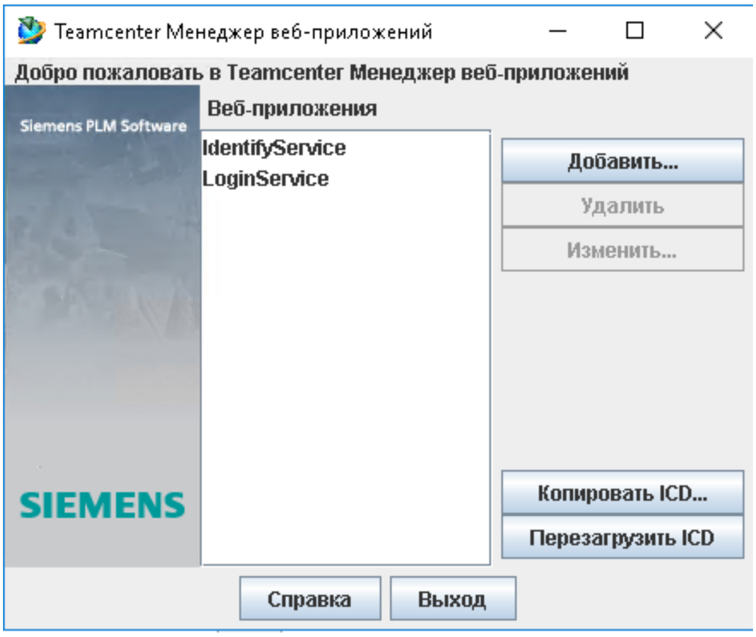
```
<Connector port="8002" protocol="HTTP/1.1"
           connectionTimeout="20000"
           redirectPort="8443" />
```



```
<Connector
      protocol="org.apache.coyote.http11.Http11NioProtocol"
      port="8001" maxThreads="200"
      scheme="https" secure="true" SSLEnabled="true"
      SSLCertificateFile="conf/cert_tc133awc6zql.pem"
      SSLCertificateKeyFile="conf/key_tc133awc6zql.pem"
      SSLVerifyClient="optional" SSLProtocol="TLSv1+TLSv1.1+TLSv1.2" useIPVHosts="true" address="0.0.0.0"/>
```

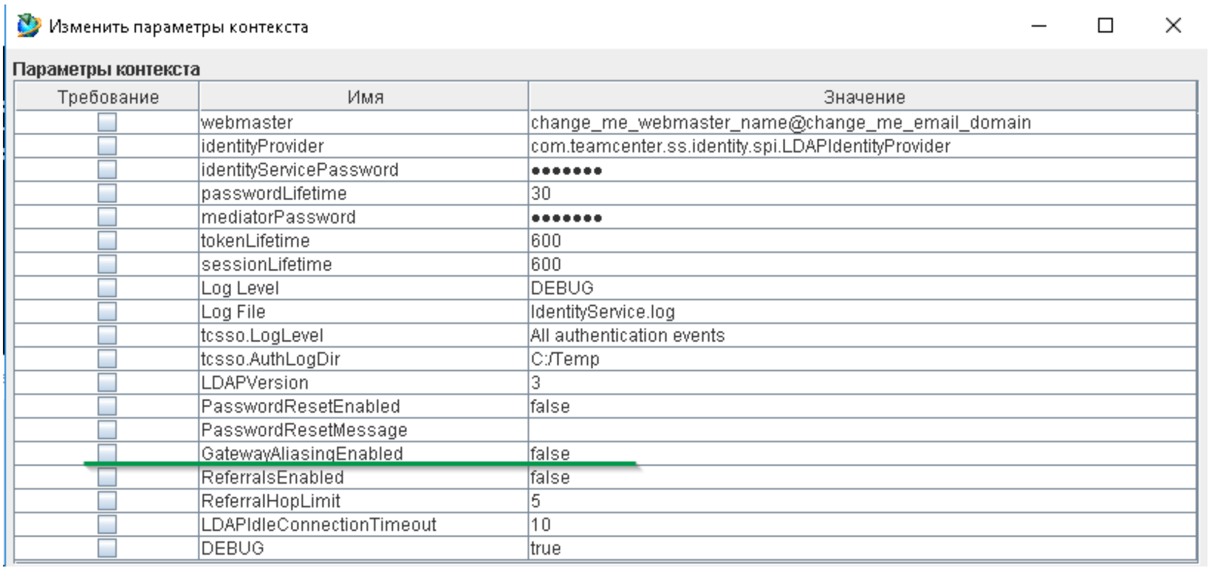
6. **Creating Login and Identify Services**

   Ohhh, for details go to: https://docs.sw.siemens.com/en-US/product/282219420/doc/PL20210421143201885.tss00001/html/xid373993



Веб-приложения:

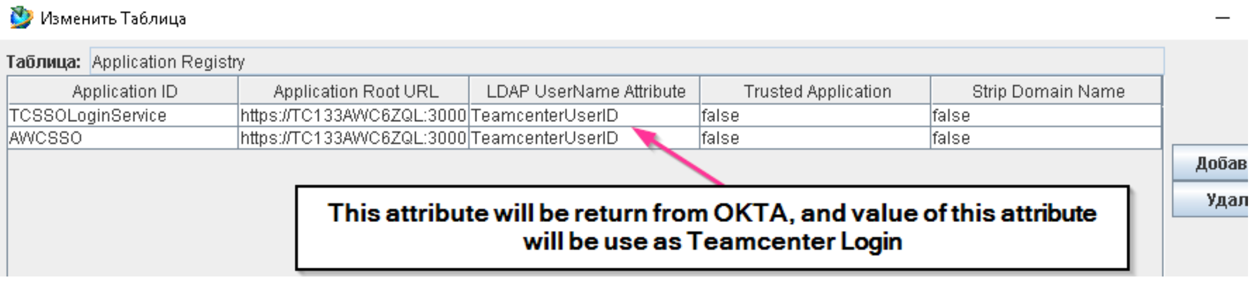
IdentifyService
LoginService



Изменить параметры контекста

Параметры контекста

Требование	Имя	Значение
☐	webmaster	change_me_webmaster_name@change_me_email_domain
☐	identityProvider	com.teamcenter.ss.identity.spi.LDAPIdentityProvider
☐	identityServicePassword	•••••••
☐	passwordLifetime	30
☐	mediatorPassword	•••••••
☐	tokenLifetime	600
☐	sessionLifetime	600
☐	Log Level	DEBUG
☐	Log File	IdentityService.log
☐	tcsso.LogLevel	All authentication events
☐	tcsso.AuthLogDir	C:/Temp
☐	LDAPVersion	3
☐	PasswordResetEnabled	false
☐	PasswordResetMessage	
☐	GatewayAliasingEnabled	false
☐	ReferralsEnabled	false
☐	ReferralHopLimit	5
☐	LDAPIdleConnectionTimeout	10
☐	DEBUG	true



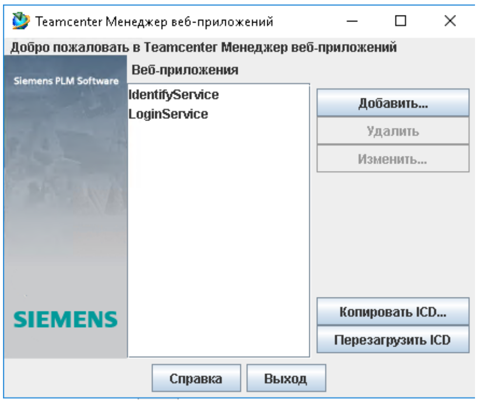
Изменить Таблица

Таблица: Application Registry

Application ID	Application Root URL	LDAP UserName Attribute	Trusted Application	Strip Domain Name
TCSSOLoginService	https://TC133AWC6ZQL:3000	TeamcenterUserID	false	false
AWCSSO	https://TC133AWC6ZQL:3000	TeamcenterUserID	false	false

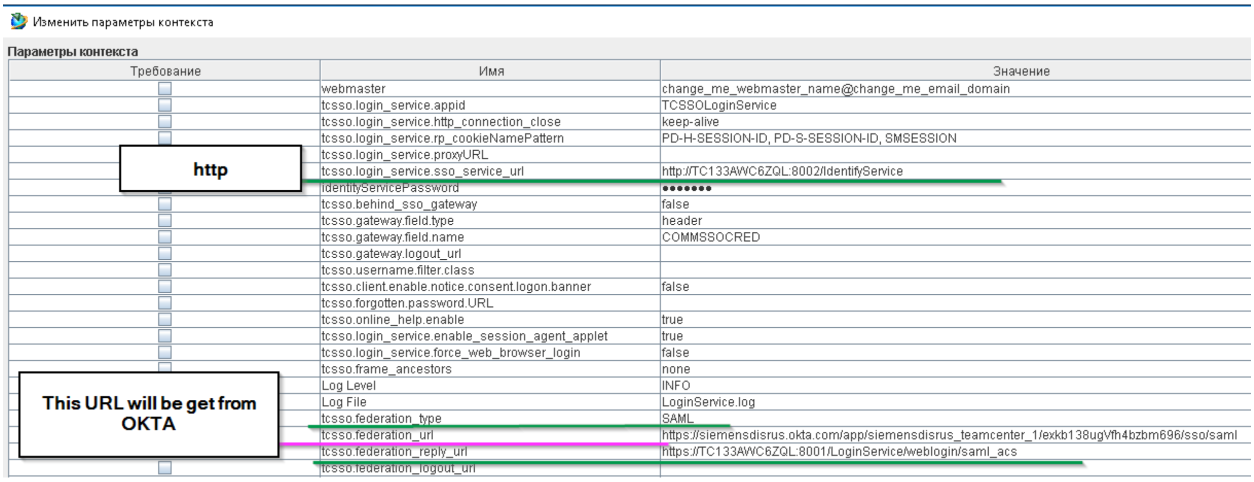
This attribute will be return from OKTA, and value of this attribute will be use as Teamcenter Login

7. Creating Login and Identify Services



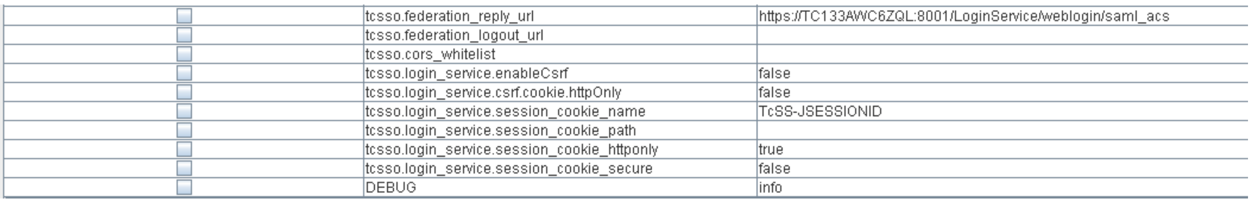
Веб-приложения

IdentifyService
LoginService



Параметры контекста

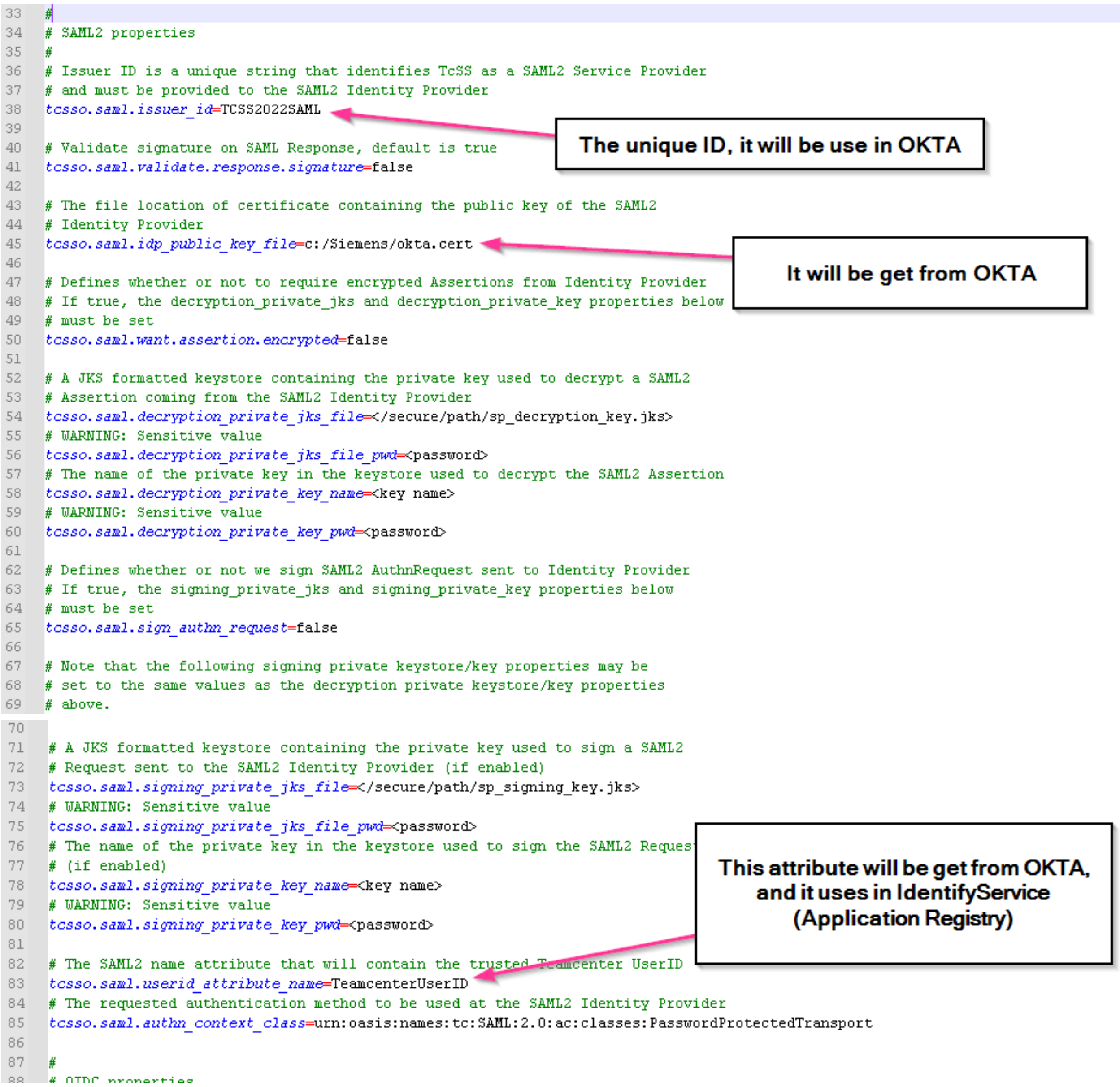
Требование	Имя	Значение
□	webmaster	change_me_webmaster_name@change_me_email_domain
□	tcsso.login_service.appid	TCSSOLoginService
□	tcsso.login_service.http_connection_close	keep-alive
□	tcsso.login_service.rp_cookieNamePattern	PD-H-SESSION-ID, PD-S-SESSION-ID, SMSESSION
	tcsso.login_service.proxyURL	
	tcsso.login_service.sso_service_url	http://TC133AWC6ZQL:8002/IdentifyService
	identityServicePassword	•••••••
□	tcsso.behind_sso_gateway	false
□	tcsso.gateway.field.type	header
□	tcsso.gateway.field.name	COMMSSOCRED
□	tcsso.gateway.logout_url	
□	tcsso.username.filter.class	
□	tcsso.client.enable.notice.consent.logon.banner	false
□	tcsso.forgotten.password.URL	
□	tcsso.online_help.enable	true
□	tcsso.login_service.enable_session_agent_applet	true
□	tcsso.login_service.force_web_browser_login	false
□	tcsso.frame_ancestors	none
	Log Level	INFO
	Log File	LoginService.log
	tcsso.federation_type	SAML
	tcsso.federation_url	https://siemensdisrus.okta.com/app/siemensdisrus_teamcenter_1/exkb138ugVfh4bzbm696/sso/saml
	tcsso.federation_reply_url	https://TC133AWC6ZQL:8001/LoginService/weblogin/saml_acs
□	tcsso.federation_logout_url	



□	tcsso.federation_reply_url	https://TC133AWC6ZQL:8001/LoginService/weblogin/saml_acs
□	tcsso.federation_logout_url	
□	tcsso.cors_whitelist	
□	tcsso.login_service.enableCsrf	false
□	tcsso.login_service.csrf.cookie.httpOnly	false
□	tcsso.login_service.session_cookie_name	TcSS-JSESSIONID
□	tcsso.login_service.session_cookie_path	
□	tcsso.login_service.session_cookie_httponly	true
□	tcsso.login_service.session_cookie_secure	false
□	DEBUG	info

8. **Configuring federation.properties (1)**

   Open **federation.properties**(c:\Siemens\SSOSrv\LoginService\webapp_root\WEB-INF\classes\federation.properties)



```
#
# SAML2 properties
#
# Issuer ID is a unique string that identifies TcSS as a SAML2 Service Provider
# and must be provided to the SAML2 Identity Provider
tcsso.saml.issuer_id=TCSS2022SAML

# Validate signature on SAML Response, default is true
tcsso.saml.validate.response.signature=false

# The file location of certificate containing the public key of the SAML2
# Identity Provider
tcsso.saml.idp_public_key_file=c:/Siemens/okta.cert

# Defines whether or not to require encrypted Assertions from Identity Provider
# If true, the decryption_private_jks and decryption_private_key properties below
# must be set
tcsso.saml.want.assertion.encrypted=false

# A JKS formatted keystore containing the private key used to decrypt a SAML2
# Assertion coming from the SAML2 Identity Provider
tcsso.saml.decryption_private_jks_file=</secure/path/sp_decryption_key.jks>
# WARNING: Sensitive value
tcsso.saml.decryption_private_jks_file_pwd=<password>
# The name of the private key in the keystore used to decrypt the SAML2 Assertion
tcsso.saml.decryption_private_key_name=<key name>
# WARNING: Sensitive value
tcsso.saml.decryption_private_key_pwd=<password>

# Defines whether or not we sign SAML2 AuthnRequest sent to Identity Provider
# If true, the signing_private_jks and signing_private_key properties below
# must be set
tcsso.saml.sign_authn_request=false

# Note that the following signing private keystore/key properties may be
# set to the same values as the decryption private keystore/key properties
# above.

# A JKS formatted keystore containing the private key used to sign a SAML2
# Request sent to the SAML2 Identity Provider (if enabled)
tcsso.saml.signing_private_jks_file=</secure/path/sp_signing_key.jks>
# WARNING: Sensitive value
tcsso.saml.signing_private_jks_file_pwd=<password>
# The name of the private key in the keystore used to sign the SAML2 Reques
# (if enabled)
tcsso.saml.signing_private_key_name=<key name>
# WARNING: Sensitive value
tcsso.saml.signing_private_key_pwd=<password>

# The SAML2 name attribute that will contain the trusted Teamcenter UserID
tcsso.saml.userid_attribute_name=TeamcenterUserID
# The requested authentication method to be used at the SAML2 Identity Provider
tcsso.saml.authn_context_class=urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport

#
# OIDC properties
```

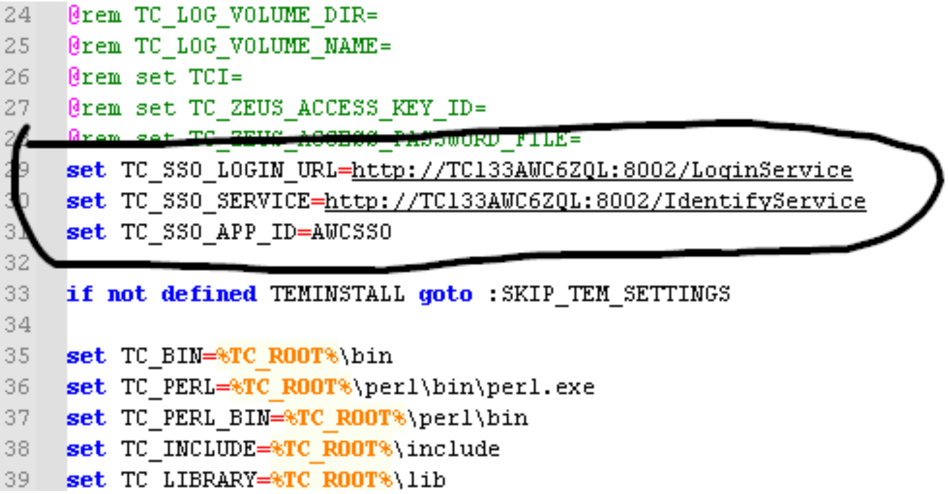
The unique ID, it will be use in OKTA

It will be get from OKTA

This attribute will be get from OKTA, and it uses in IdentifyService (Application Registry)

9. **Configuring Teamcenter core**

   Open **tc_profilevars.bat** (C:\Siemens\tcdata\tc_profilevars.bat)



```
@rem TC_LOG_VOLUME_DIR=
@rem TC_LOG_VOLUME_NAME=
@rem set TCI=
@rem set TC_ZEUS_ACCESS_KEY_ID=
@rem set TC_ZEUS_ACCESS_PASSWORD_FILE=
set TC_SSO_LOGIN_URL=http://TC133AWC6ZQL:8002/LoginService
set TC_SSO_SERVICE=http://TC133AWC6ZQL:8002/IdentifyService
set TC_SSO_APP_ID=AWCSSO

if not defined TEMINSTALL goto :SKIP_TEM_SETTINGS

set TC_BIN=%TC_ROOT%\bin
set TC_PERL=%TC_ROOT%\perl\bin\perl.exe
set TC_PERL_BIN=%TC_ROOT%\perl\bin
set TC_INCLUDE=%TC_ROOT%\include
set TC_LIBRARY=%TC_ROOT%\lib
```

10. **Deploying TcSS services**

    Copy these files:

    c:\Siemens\SSOSrv\IdentifyService\deployment**\IdentifyService.war**
    c:\Siemens\SSOSrv\LoginService\deployment**\LoginService.war**

    to:

    c:\Siemens\Tomcat9SSO**\webapps**

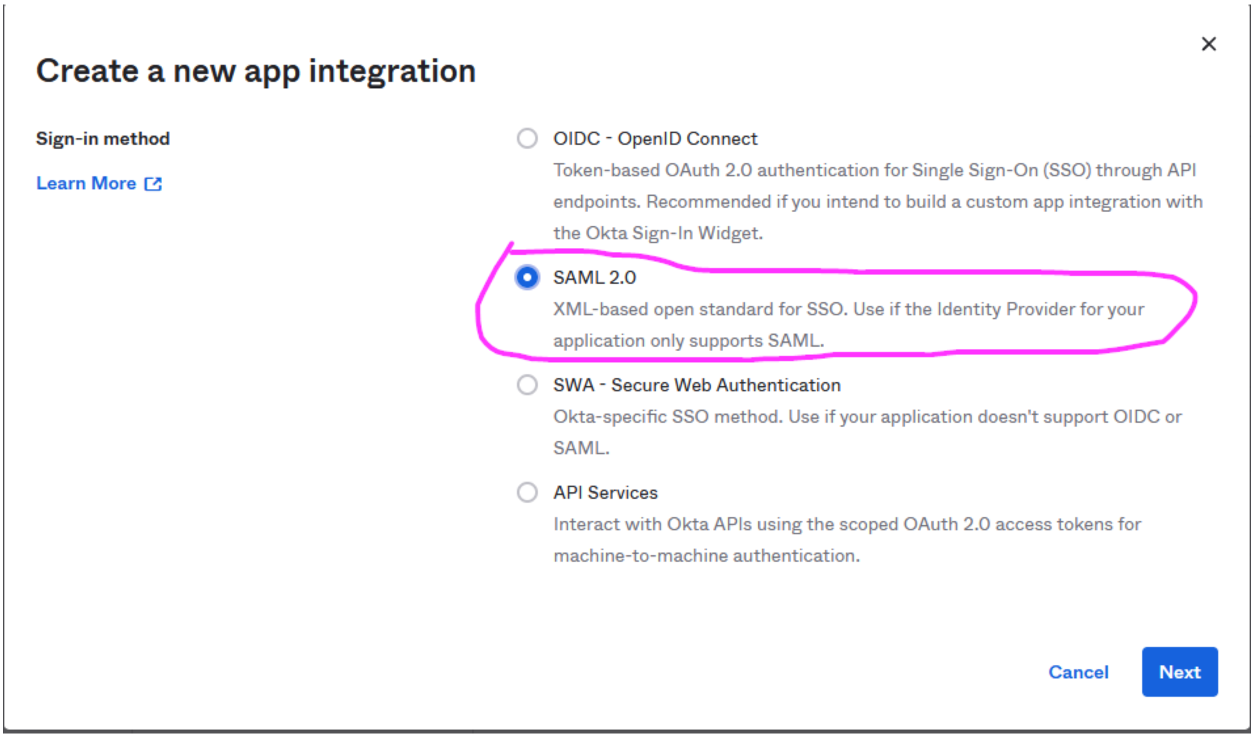
Authorship: https://www.linkedin.com/in/sedoykin

Disclaimer:

No guarantees or responsibilities are provided. You perform all actions at your own risk!

Steps on the OKTA service side

1. **You should have dev account, it is free for developing purpose** after get it you should create new SAML integration application



Create a new app integration

Sign-in method

Learn More

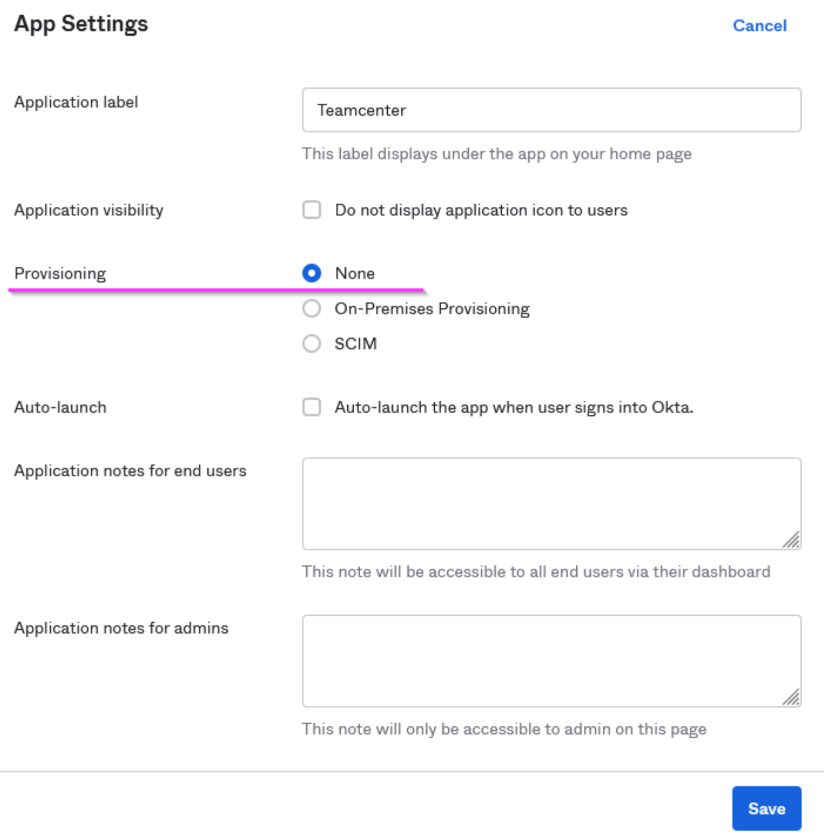
○ OIDC - OpenID Connect
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.

● SAML 2.0
XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.

○ SWA - Secure Web Authentication
Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.

○ API Services
Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

2. Configuring SAML integration application



App Settings

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

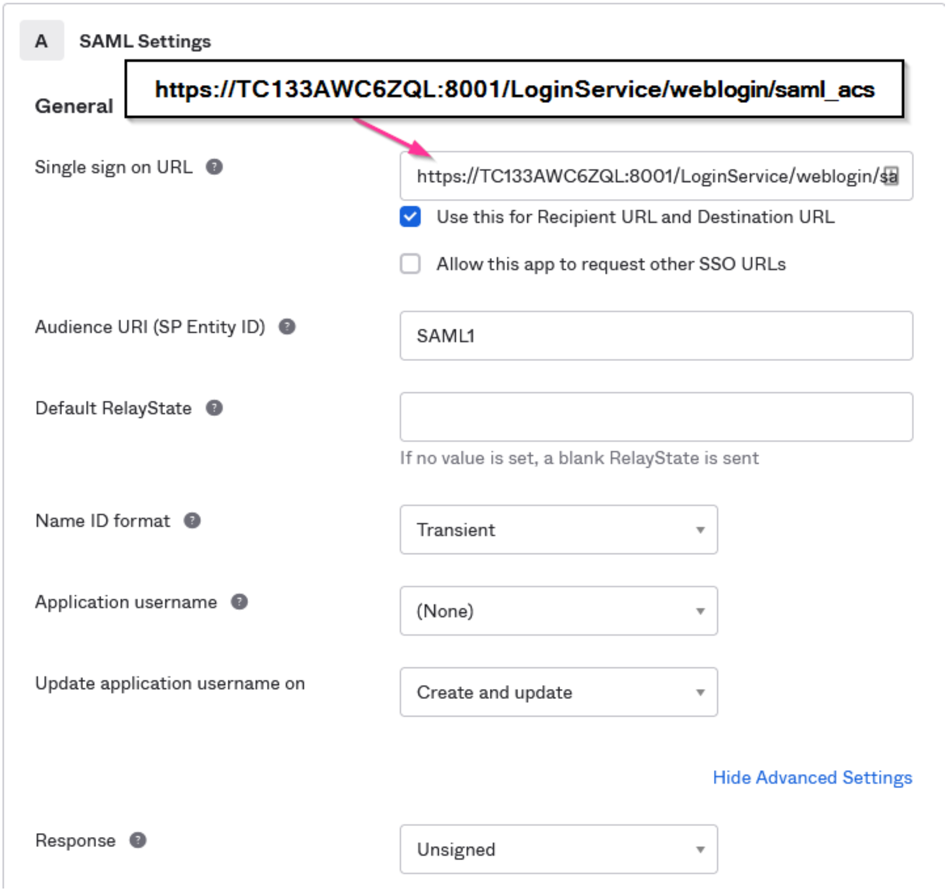
Application visibility: □ Do not display application icon to users

Provisioning: ● None
○ On-Premises Provisioning
○ SCIM

Auto-launch: □ Auto-launch the app when user signs into Okta.

Application notes for end users:
This note will be accessible to all end users via their dashboard

Application notes for admins:
This note will only be accessible to admin on this page



A SAML Settings

General

https://TC133AWC6ZQL:8001/LoginService/weblogin/saml_acs

Single sign on URL: https://TC133AWC6ZQL:8001/LoginService/weblogin/sa
☑ Use this for Recipient URL and Destination URL
□ Allow this app to request other SSO URLs

Audience URI (SP Entity ID): SAML1

Default RelayState:
If no value is set, a blank RelayState is sent

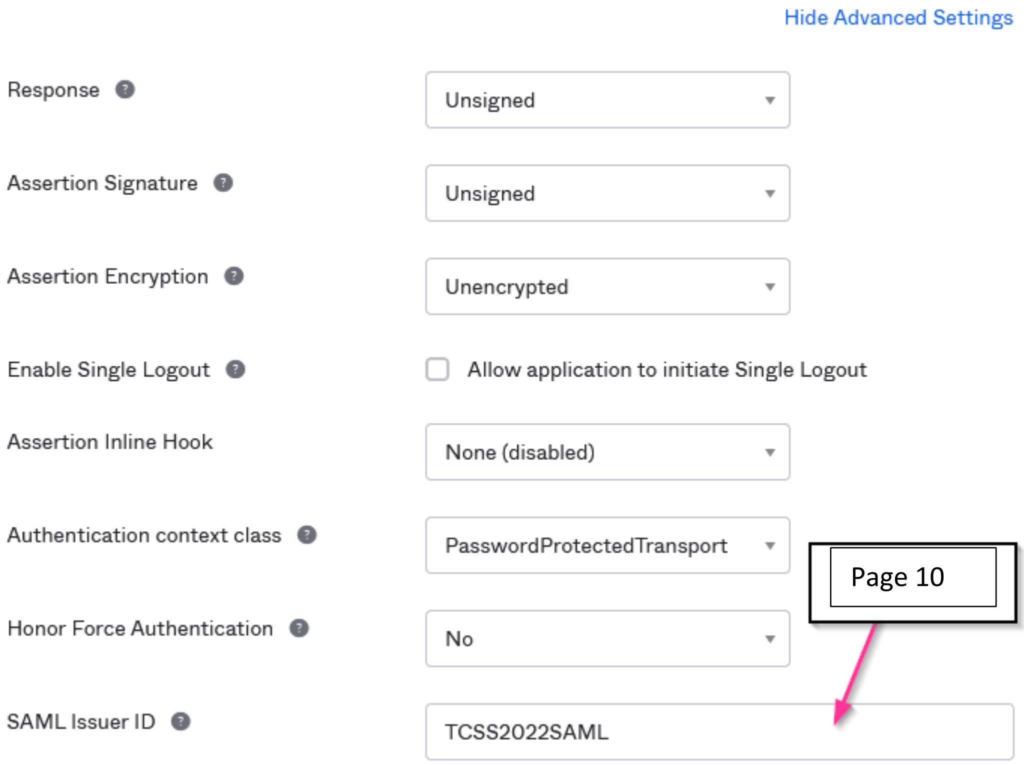
Name ID format: Transient

Application username: (None)

Update application username on: Create and update

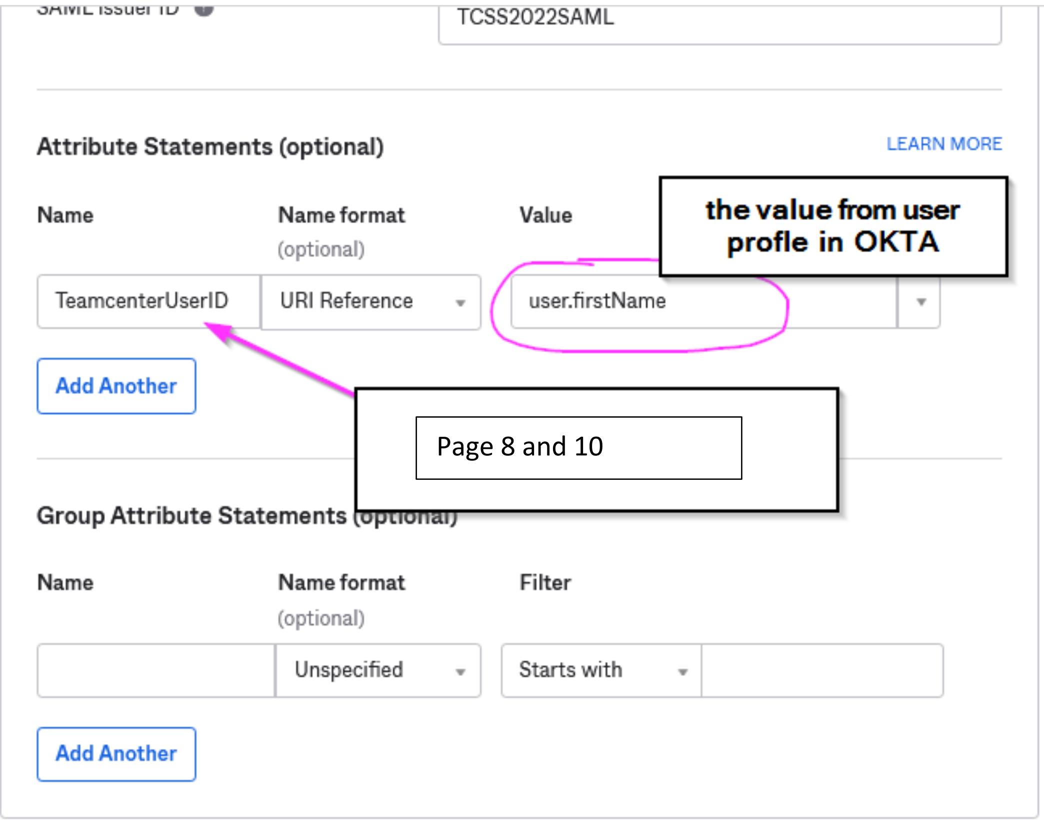
Response: Unsigned

Configuring SAML integration application



Response	Unsigned
Assertion Signature	Unsigned
Assertion Encryption	Unencrypted
Enable Single Logout	□ Allow application to initiate Single Logout
Assertion Inline Hook	None (disabled)
Authentication context class	PasswordProtectedTransport
Honor Force Authentication	No
SAML Issuer ID	TCSS2022SAML

Page 10



SAML Issuer ID TCSS2022SAML

Attribute Statements (optional)

Name	Name format (optional)	Value
TeamcenterUserID	URI Reference	user.firstName

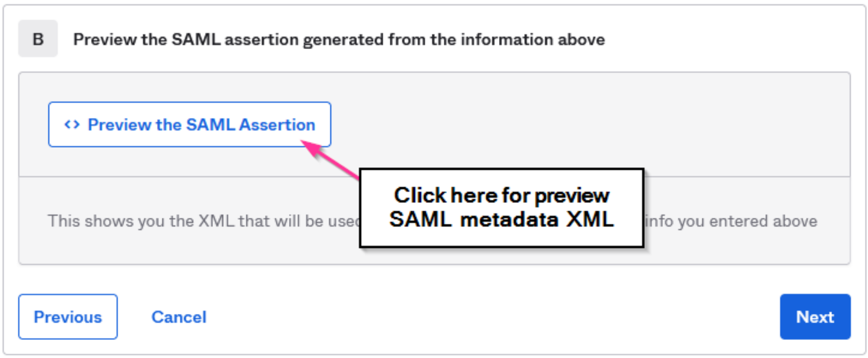
the value from user profle in OKTA

Page 8 and 10

Group Attribute Statements (optional)

Name	Name format (optional)	Filter	
	Unspecified	Starts with	

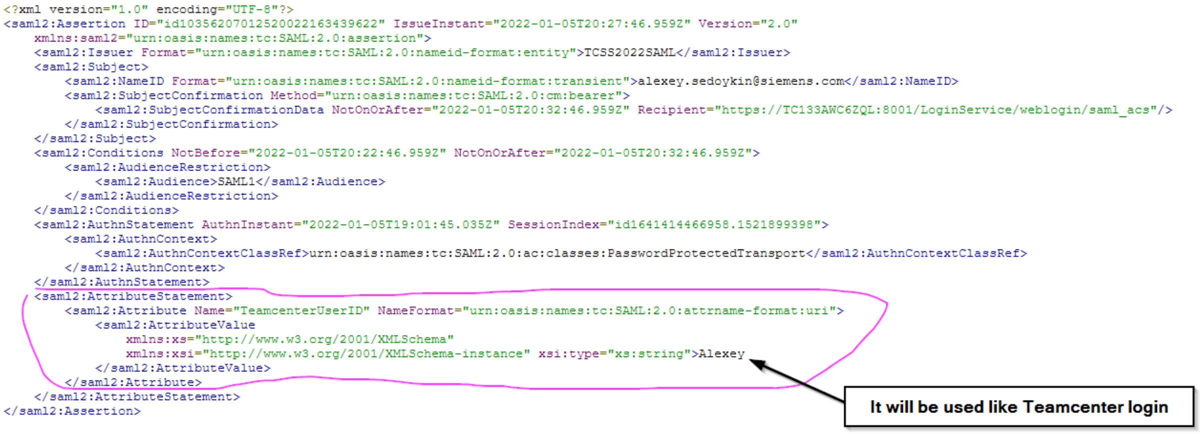
Configuring SAML integration application



B Preview the SAML assertion generated from the information above

This shows you the XML that will be used … info you entered above

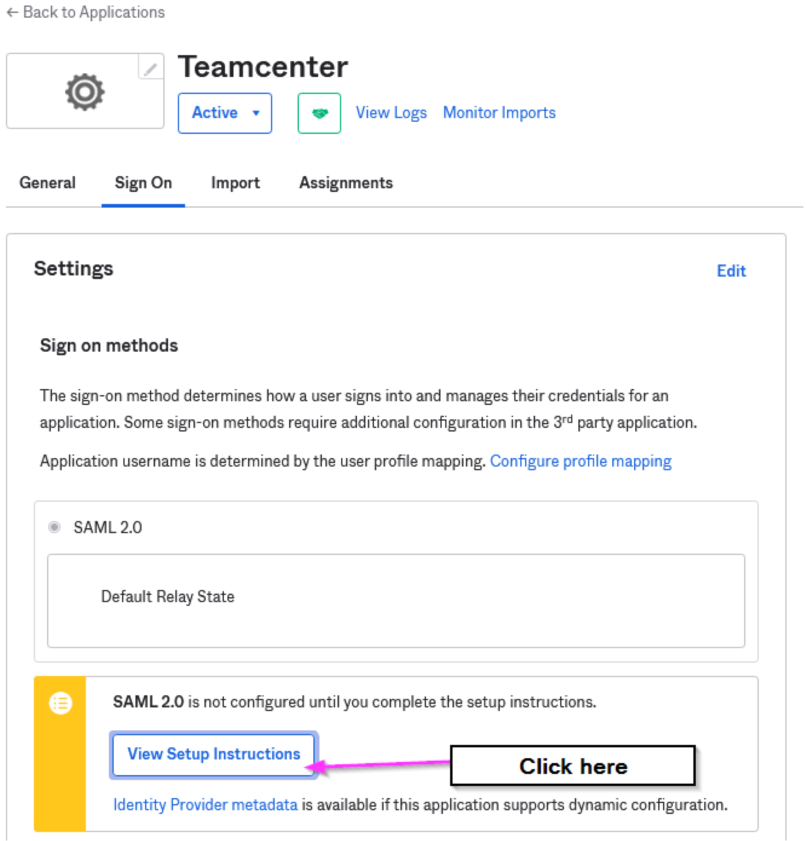
Click here for preview SAML metadata XML



```
<?xml version="1.0" encoding="UTF-8"?>
<saml2:Assertion ID="id103562070125200221634396 22" IssueInstant="2022-01-05T20:27:46.959Z" Version="2.0"
    xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
    <saml2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">TCSS2022SAML</saml2:Issuer>
    <saml2:Subject>
        <saml2:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient">alexey.sedoykin@siemens.com</saml2:NameID>
        <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
            <saml2:SubjectConfirmationData NotOnOrAfter="2022-01-05T20:32:46.959Z" Recipient="https://TC133AWC6ZQL:8001/LoginService/weblogin/saml_acs"/>
        </saml2:SubjectConfirmation>
    </saml2:Subject>
    <saml2:Conditions NotBefore="2022-01-05T20:22:46.959Z" NotOnOrAfter="2022-01-05T20:32:46.959Z">
        <saml2:AudienceRestriction>
            <saml2:Audience>SAML1</saml2:Audience>
        </saml2:AudienceRestriction>
    </saml2:Conditions>
    <saml2:AuthnStatement AuthnInstant="2022-01-05T19:01:45.035Z" SessionIndex="id1641414466958.1521899398">
        <saml2:AuthnContext>
            <saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</saml2:AuthnContextClassRef>
        </saml2:AuthnContext>
    </saml2:AuthnStatement>
    <saml2:AttributeStatement>
        <saml2:Attribute Name="TeamcenterUserID" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
            <saml2:AttributeValue
                xmlns:xs="http://www.w3.org/2001/XMLSchema"
                xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">Alexey
            </saml2:AttributeValue>
        </saml2:Attribute>
    </saml2:AttributeStatement>
</saml2:Assertion>
```

It will be used like Teamcenter login

Configuring SAML integration application



← Back to Applications

Teamcenter

Settings

Sign on methods

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

Application username is determined by the user profile mapping. Configure profile mapping

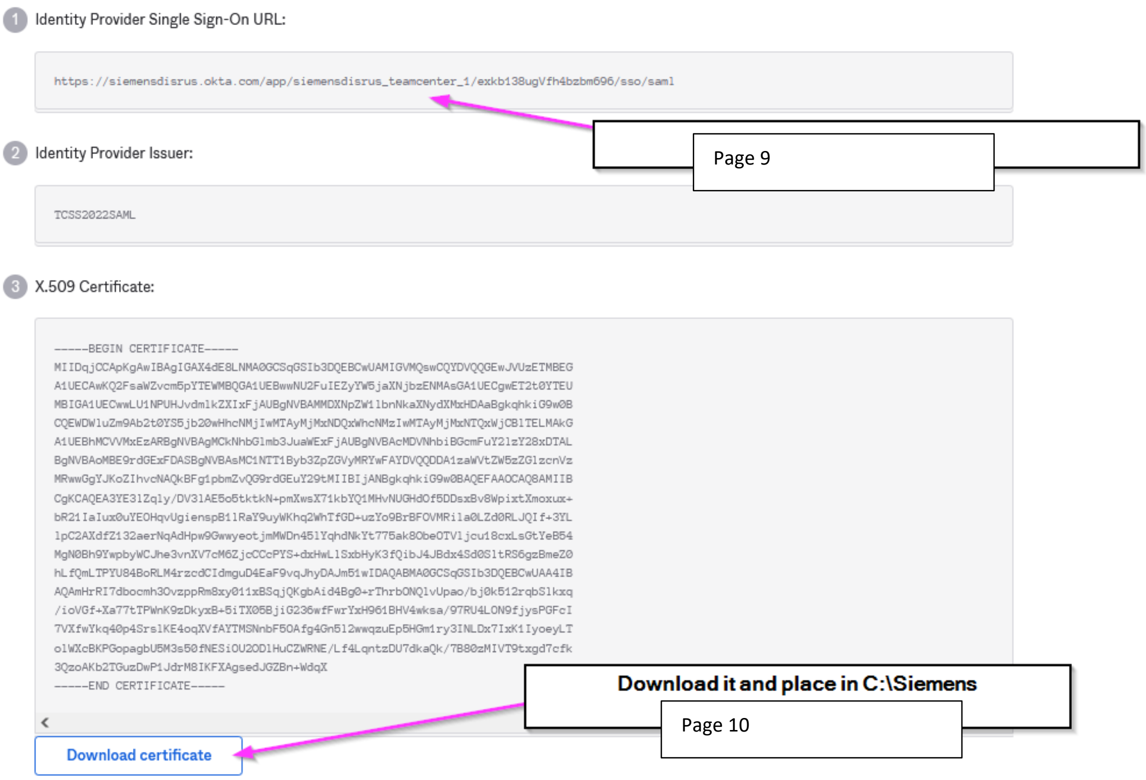
● SAML 2.0

Default Relay State

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

Click here

Identity Provider metadata is available if this application supports dynamic configuration.



1 Identity Provider Single Sign-On URL:

```
https://siemensdisrus.okta.com/app/siemensdisrus_teamcenter_1/exkb138ugVfh4bzbm696/sso/saml
```

Page 9

2 Identity Provider Issuer:

```
TCSS2022SAML
```

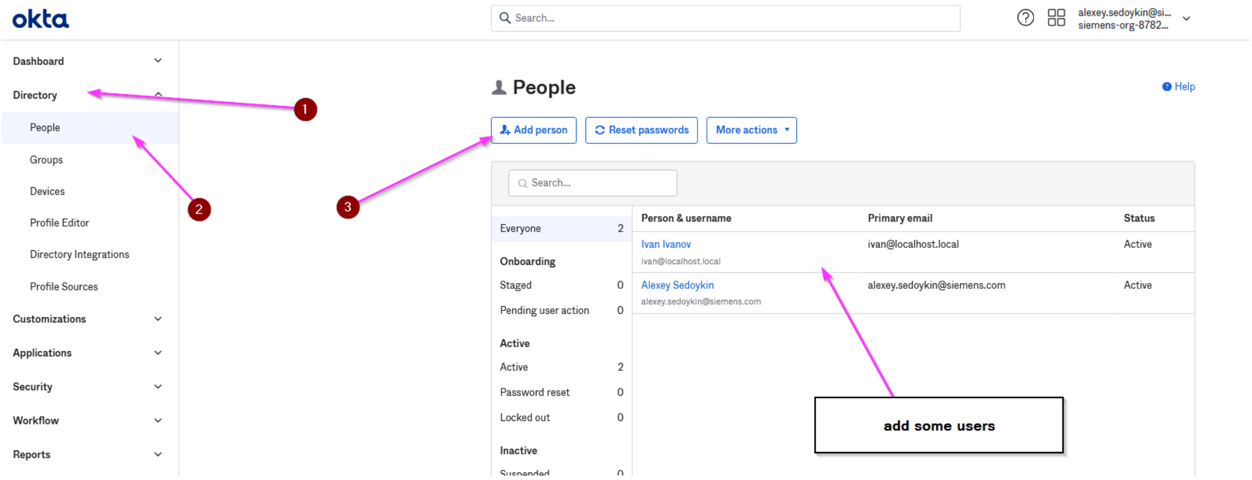
3 X.509 Certificate:

```
-----BEGIN CERTIFICATE-----
MIIDqjCCApKgAwIBAgIGAX4dE8LNMA0GCSqGSIb3DQEBCwUAMIGVMQswCQYDVQQGEwJVUzETMBEG
A1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsGA1UECgwET2t0YTEU
MBIGA1UECwwLU1NPUHJvdmlkZXIxFjAUBgNVBAMMDXNpZW1lbnNkaXNydXMxHDAaBgkqhkiG9w0B
CQEWDWluZm9Ab2t0YS5jb20wHhcNMjIwMTAyMjMxNDQxWhcNMzIwMTAyMjMxNTQxWjCBlTELMAkG
A1UEBhMCVVMxEzARBgNVBAgMCkNhbGlmb3JuaWExFjAUBgNVBAcMDVNhbiBGcmFuY2lzY28xDTAL
BgNVBAoMBE9rdGExFDASBgNVBAsMC1NTT1Byb3ZpZGVyMRYwFAYDVQQDDA1zaWVtZW5zZGlzcnVz
MRwwGgYJKoZIhvcNAQkBFg1pbmZvQG9rdGEuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA3YE3lZqly/DV3lAE5o5tktkN+pmXwsX71kbYQ1MHvNUGHdOf5DDsxBv8WpixtXmoxux+
bR21IaIux0uYEOHqvUgienspB1lRaY9uyWKhq2WhTfGD+uzYo9BrBFOVMRila0LZd0RLJQIf+3YL
lpC2AXdfZ132aerNqAdHpw9GwwyeotjmMWDn45lYqhdNkYt775ak8ObeOTVljcu18cxLsGtYeB54
MgN0Bh9YwpbyWCJhe3vnXV7cM6ZjcCCcPYS+dxHwLlSxbHyK3fQibJ4JBdx4Sd0SltRS6gzBmeZ0
hLfQmLTPYU84BoRLM4rzcdCIdmguD4EaF9vqJhyDAJm51wIDAQABMA0GCSqGSIb3DQEBCwUAA4IB
AQAmHrRI7dbocmh3OvzppRm8xy011xBSqjQKgbAid4Bg0+rThrbONQlvUpao/bj0k512rqbSlkxq
/ioVGf+Xa77tTPWnK9zDkyxB+5iTX05BjiG236wfFwrYxH961BHV4wksa/97RU4LON9fjysPGFcI
7VXfwYkq40p4SrslKE4oqXVfAYTMSNnbF5OAfg4Gn5l2wwqzuEp5HGm1ry3INLDx7IxK1IyoeyLT
olWXcBKPGopagbU5M3s50fNESiOU2ODlHuCZWRNE/Lf4LqntzDU7dkaQk/7B80zMIVT9txgd7cfk
3QzoAKb2TGuzDwP1JdrM8IKFXAgsedJGZBn+WdqX
-----END CERTIFICATE-----
```

Download it and place in C:\Siemens

Page 10

3. Adding users at OKTA account

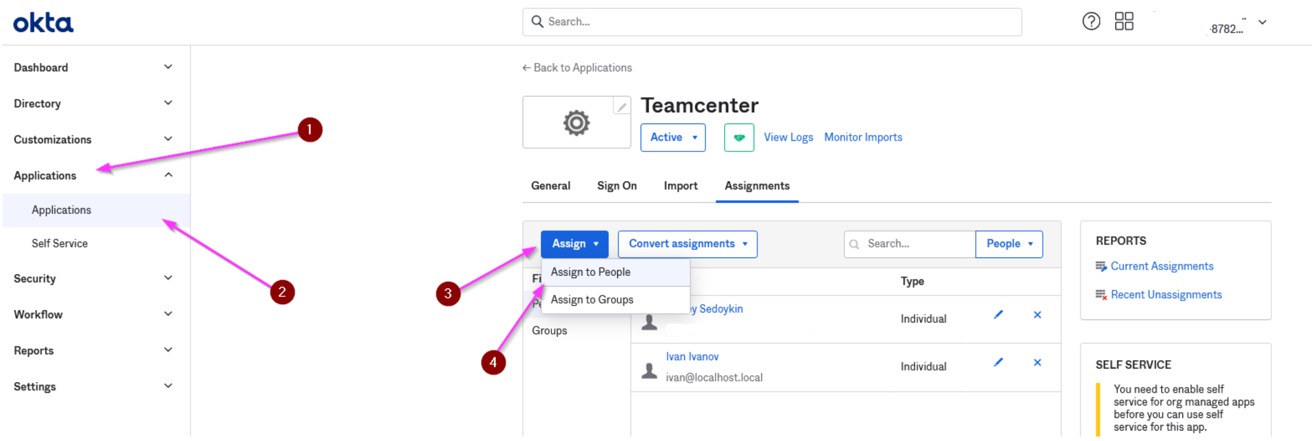


Everyone	2
Onboarding	
Staged	0
Pending user action	0
Active	
Active	2
Password reset	0
Locked out	0
Inactive	
Suspended	0

Person & username	Primary email	Status
Ivan Ivanov ivan@localhost.local	ivan@localhost.local	Active
Alexey Sedoykin alexey.sedoykin@siemens.com	alexey.sedoykin@siemens.com	Active

add some users

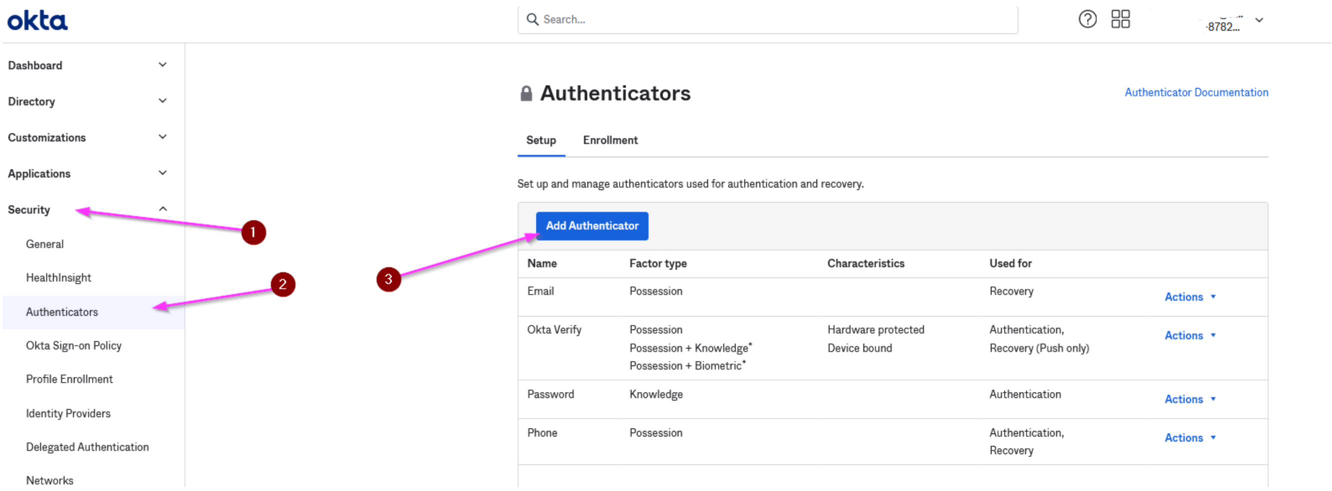
4. Assigning users at SAML integration application



	Type
...y Sedoykin	Individual
Ivan Ivanov ivan@localhost.local	Individual

You need to enable self service for org managed apps before you can use self service for this app.

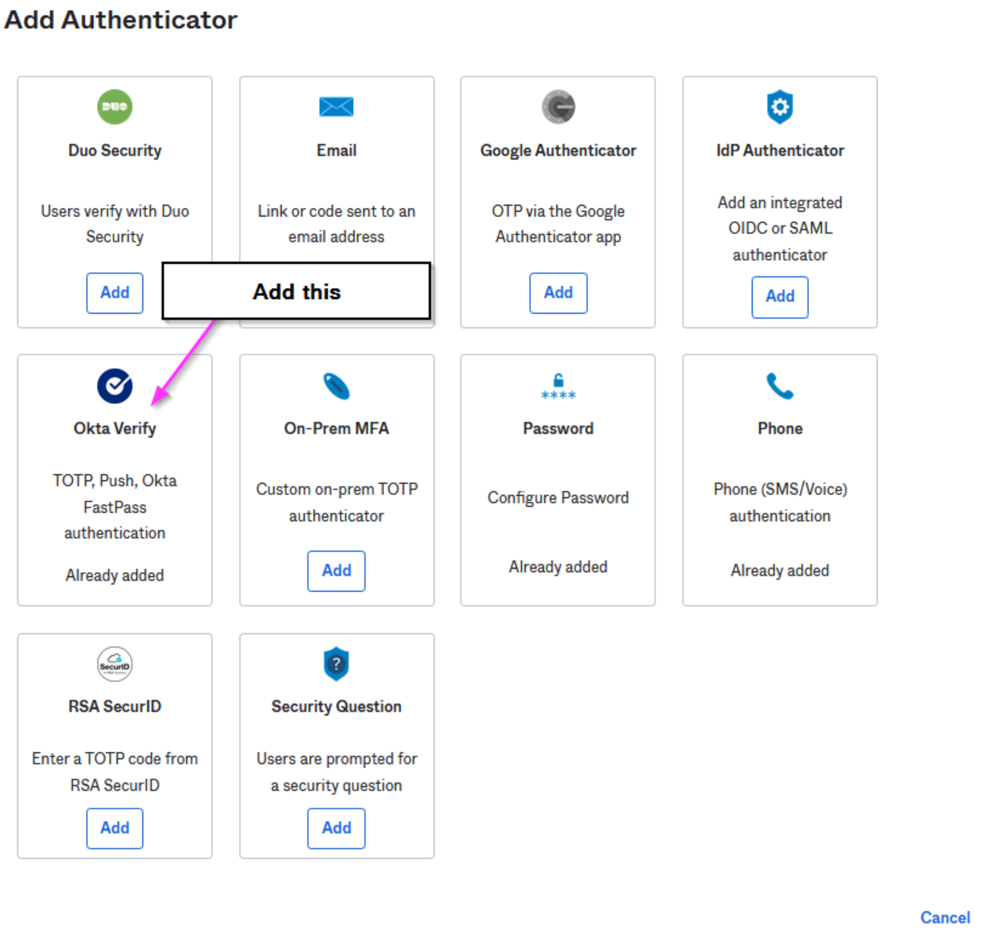
5. Adding MFA feature



Authenticators

Set up and manage authenticators used for authentication and recovery.

Name	Factor type	Characteristics	Used for	
Email	Possession		Recovery	Actions ▾
Okta Verify	Possession Possession + Knowledge* Possession + Biometric*	Hardware protected Device bound	Authentication, Recovery (Push only)	Actions ▾
Password	Knowledge		Authentication	Actions ▾
Phone	Possession		Authentication, Recovery	Actions ▾



Add Authenticator

Duo Security — Users verify with Duo Security — Add

Email — Link or code sent to an email address

Google Authenticator — OTP via the Google Authenticator app — Add

IdP Authenticator — Add an integrated OIDC or SAML authenticator — Add

Okta Verify — TOTP, Push, Okta FastPass authentication — Already added

On-Prem MFA — Custom on-prem TOTP authenticator — Add

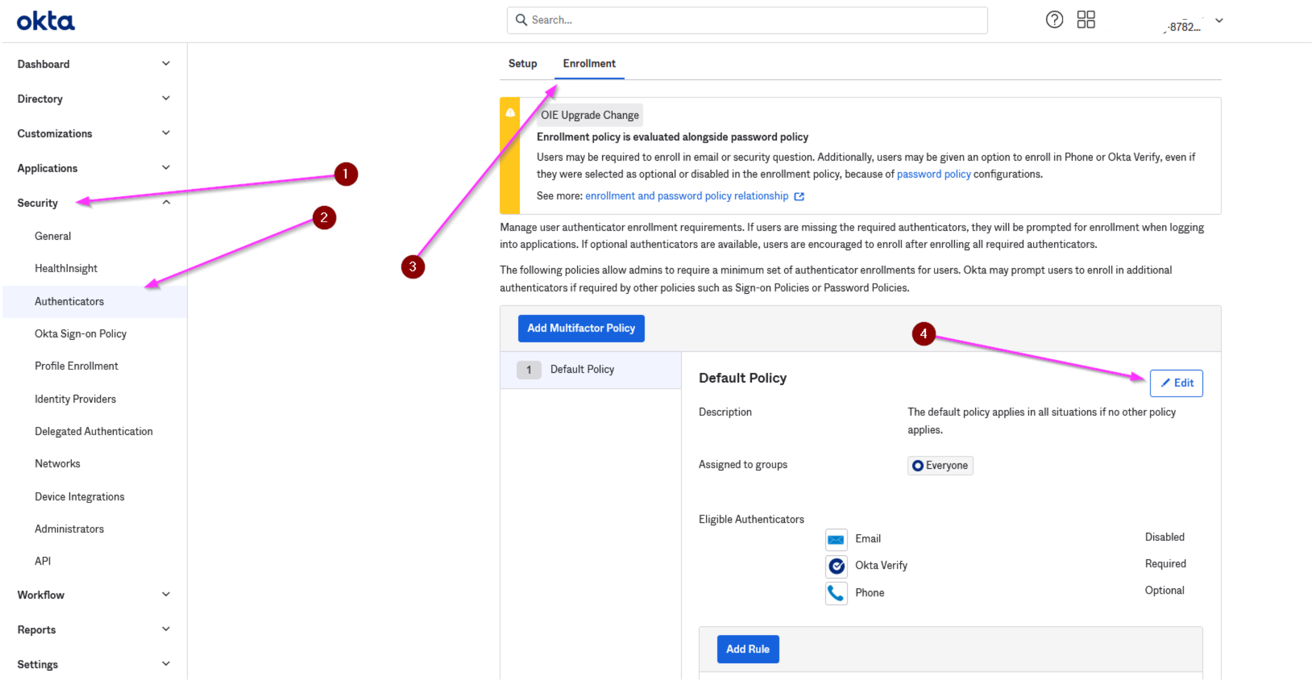
Password — Configure Password — Already added

Phone — Phone (SMS/Voice) authentication — Already added

RSA SecurID — Enter a TOTP code from RSA SecurID — Add

Security Question — Users are prompted for a security question — Add

Adding MFA feature



OIE Upgrade Change

Enrollment policy is evaluated alongside password policy

Users may be required to enroll in email or security question. Additionally, users may be given an option to enroll in Phone or Okta Verify, even if they were selected as optional or disabled in the enrollment policy, because of password policy configurations.

See more: enrollment and password policy relationship

Manage user authenticator enrollment requirements. If users are missing the required authenticators, they will be prompted for enrollment when logging into applications. If optional authenticators are available, users are encouraged to enroll after enrolling all required authenticators.

The following policies allow admins to require a minimum set of authenticator enrollments for users. Okta may prompt users to enroll in additional authenticators if required by other policies such as Sign-on Policies or Password Policies.

1 Default Policy

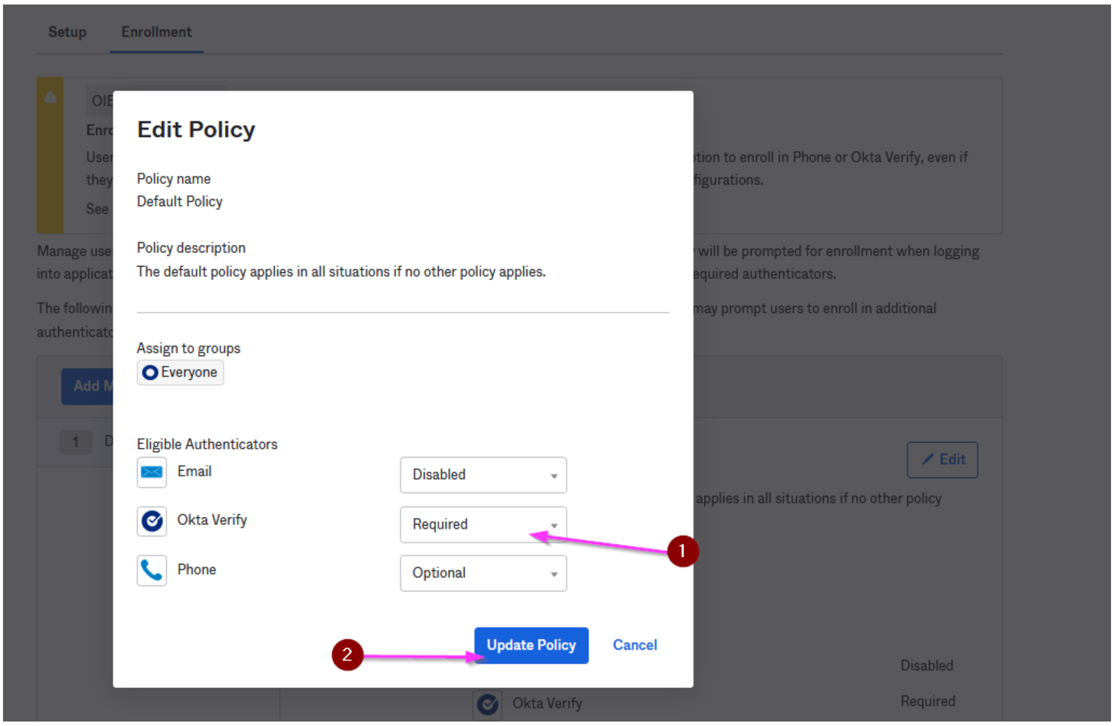
Default Policy

Description: The default policy applies in all situations if no other policy applies.

Assigned to groups: Everyone

Eligible Authenticators

Email	Disabled
Okta Verify	Required
Phone	Optional



Edit Policy

Policy name
Default Policy

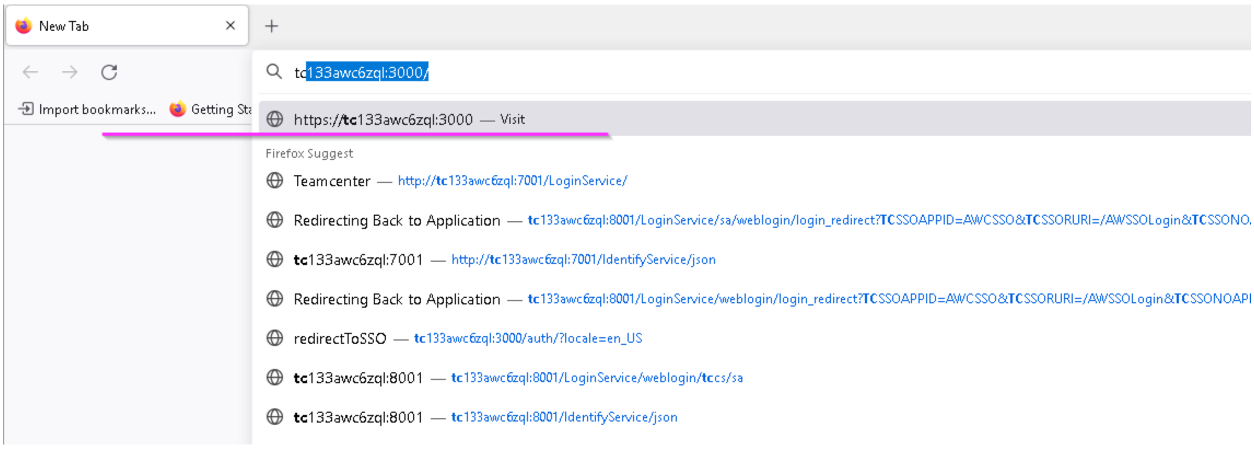
Policy description
The default policy applies in all situations if no other policy applies.

Assign to groups
Everyone

Eligible Authenticators

Email	Disabled
Okta Verify	Required
Phone	Optional

How can I check all this?!



tc133awc6zql:3000/

https://tc133awc6zql:3000 — Visit

Firefox Suggest

Teamcenter — http://tc133awc6zql:7001/LoginService/

Redirecting Back to Application — tc133awc6zql:8001/LoginService/sa/weblogin/login_redirect?TCSSOAPPID=AWCSSO&TCSSORURI=/AWSSOLogin&TCSSONO.

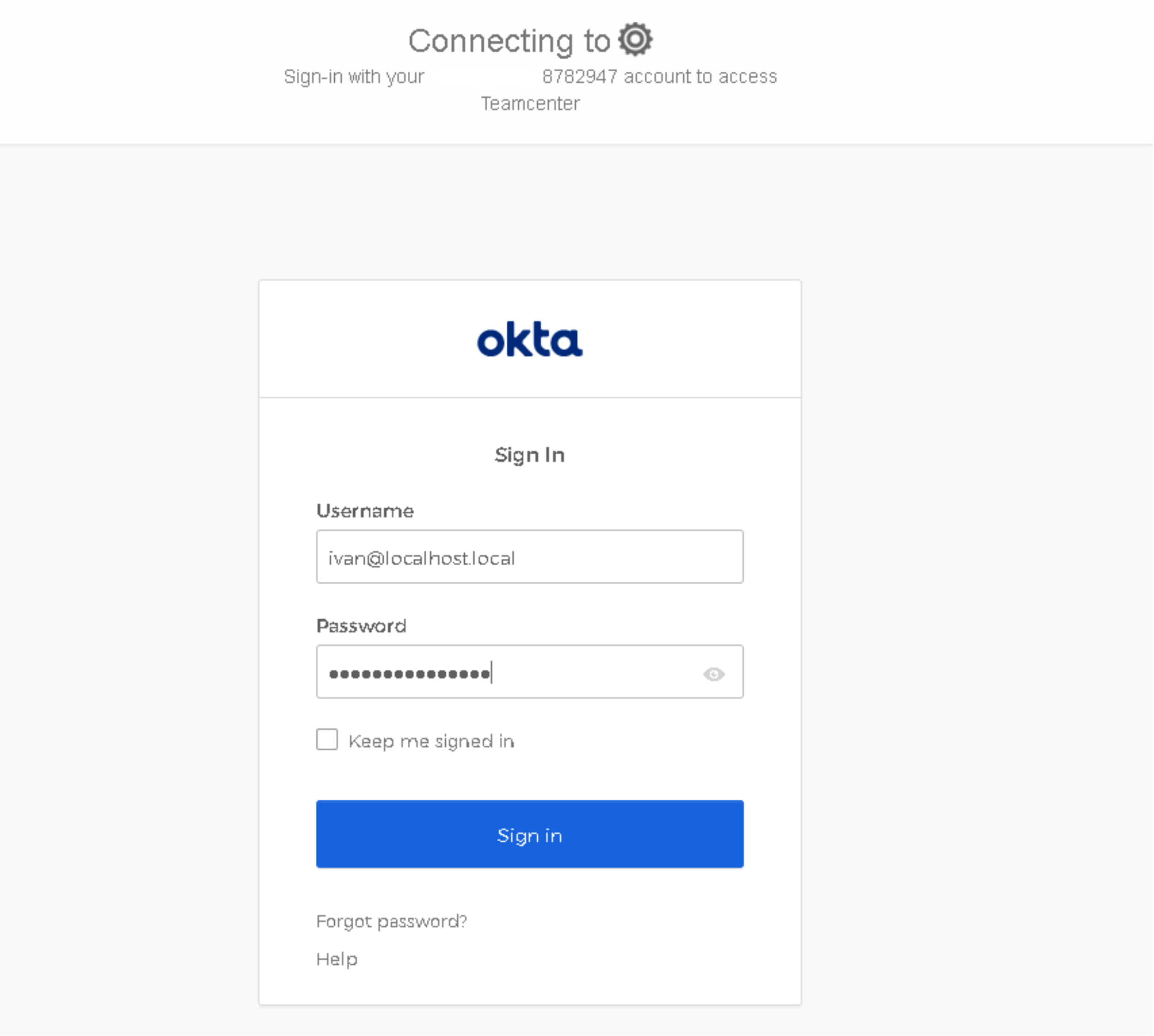
tc133awc6zql:7001 — http://tc133awc6zql:7001/IdentifyService/json

Redirecting Back to Application — tc133awc6zql:8001/LoginService/weblogin/login_redirect?TCSSOAPPID=AWCSSO&TCSSORURI=/AWSSOLogin&TCSSONOAPI

redirectToSSO — tc133awc6zql:3000/auth/?locale=en_US

tc133awc6zql:8001 — tc133awc6zql:8001/LoginService/weblogin/tccs/sa

tc133awc6zql:8001 — tc133awc6zql:8001/IdentifyService/json



Connecting to

Sign-in with your 8782947 account to access Teamcenter

okta

Sign In

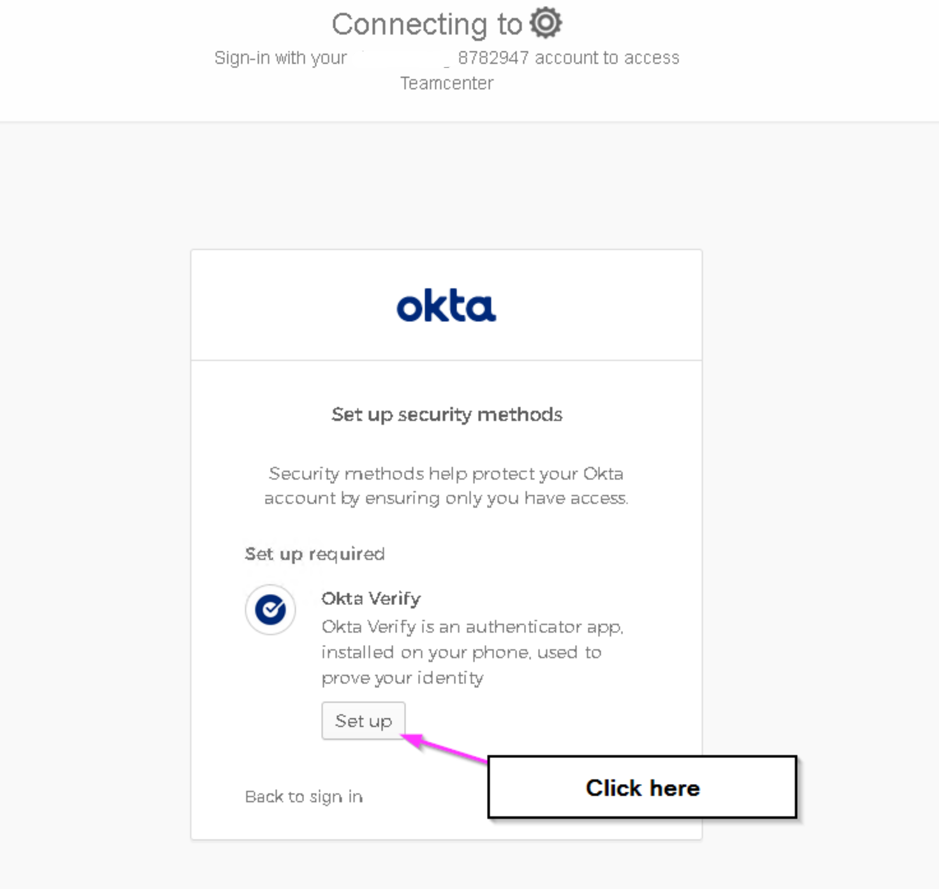
Username

ivan@localhost.local

Password

●●●●●●●●●●●●●●●

□ Keep me signed in



Connecting to

Sign-in with your _ 8782947 account to access Teamcenter

Set up security methods

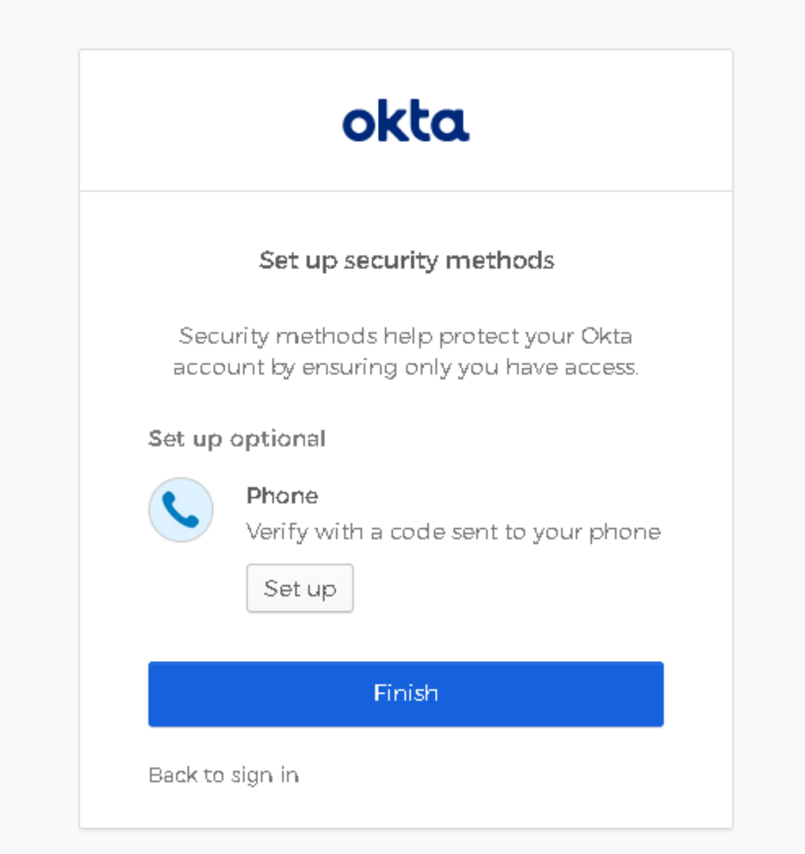
Security methods help protect your Okta account by ensuring only you have access.

Set up required

Okta Verify

Okta Verify is an authenticator app, installed on your phone, used to prove your identity

Click here



Set up security methods

Security methods help protect your Okta account by ensuring only you have access.

Set up optional

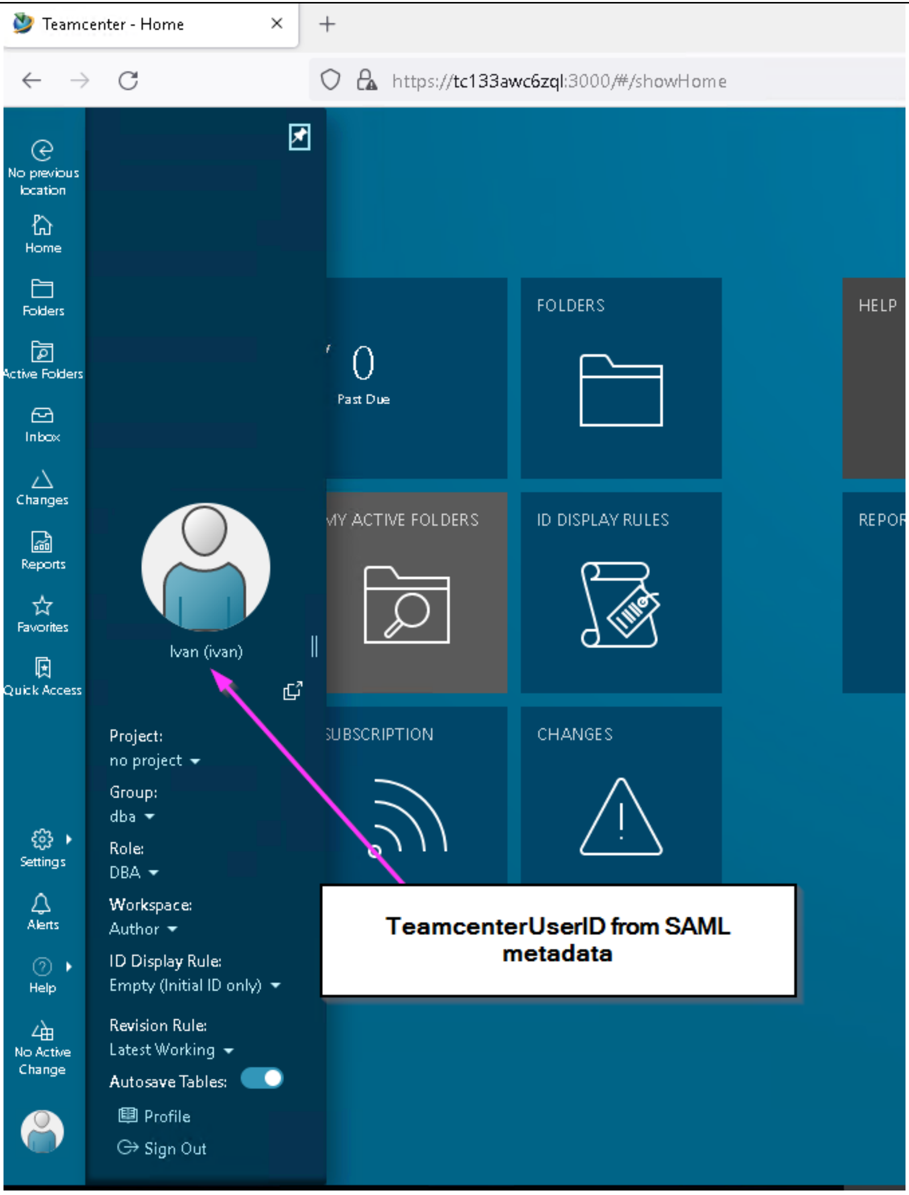
Phone

Verify with a code sent to your phone

Authorship: https://www.linkedin.com/in/sedoykin

Disclaimer:

No guarantees or responsibilities are provided. You perform all actions at your own risk!



Ivan (ivan)

Project: no project

Group: dba

Role: DBA

Workspace: Author

ID Display Rule: Empty (Initial ID only)

Revision Rule: Latest Working

Autosave Tables: ●

TeamcenterUserID from SAML metadata

THAT'S ALL, gOOd LUCK!