#### IT RCSA - Infrastructure

Entity	Apple Bank	
Test Name	Appre Datin	
Test Name Test Date	11 minasuccure 4/9/2021	
Process	IT-IFR-P9 Single Sign-On	
Sub-process	Single Sign-On	
Risk # and Description	IT-IFR-R09 - The absence of a single sign-on solution may increase the risk surface of the bank, by allowing multiple paths of access and therefore increasing the potential for attacks such as the phishing and man-in-the-middle attacks.	
Control # and Description	IT-IFR-C15 Single Sign-On Single Sign-On (SSO) is implemented to reduce and centralize the log-in credentials to the ABS information assets.	
Level of Risk	High	
Control Frequency	As Needed	
Process Owner	Debi Gupta	
Procedures Performed for Validating Population	Inquiry, Observation, Inspection	
SII(s) or Exception(s) Number(s)	Self Reported by Information Security	

Test Sample

## Single Sign-On settings for application ABLE

Control Test Procedures			
Test Step	Test Procedure		
A1	Determine that there is a list of applications that are single sign-on enabled	Pg. 2, 3, 4, 5	
B1	Determine that the single sign-on connection is secured, based on an authentication and authorization standard	Pg. 6	
B2	Determine that the single sign-on connection is secured, based on a digest and signature standard	Pg. 7	
В3	Determine that the single sign-on connection is secured, based on a directory synchronization between OKTA and Active Directory	Pg. 8, 9, 10, 11, 12	
		_	

See OKTA additional settings for Multi Factor to enforce SSO (pg. 13-18)

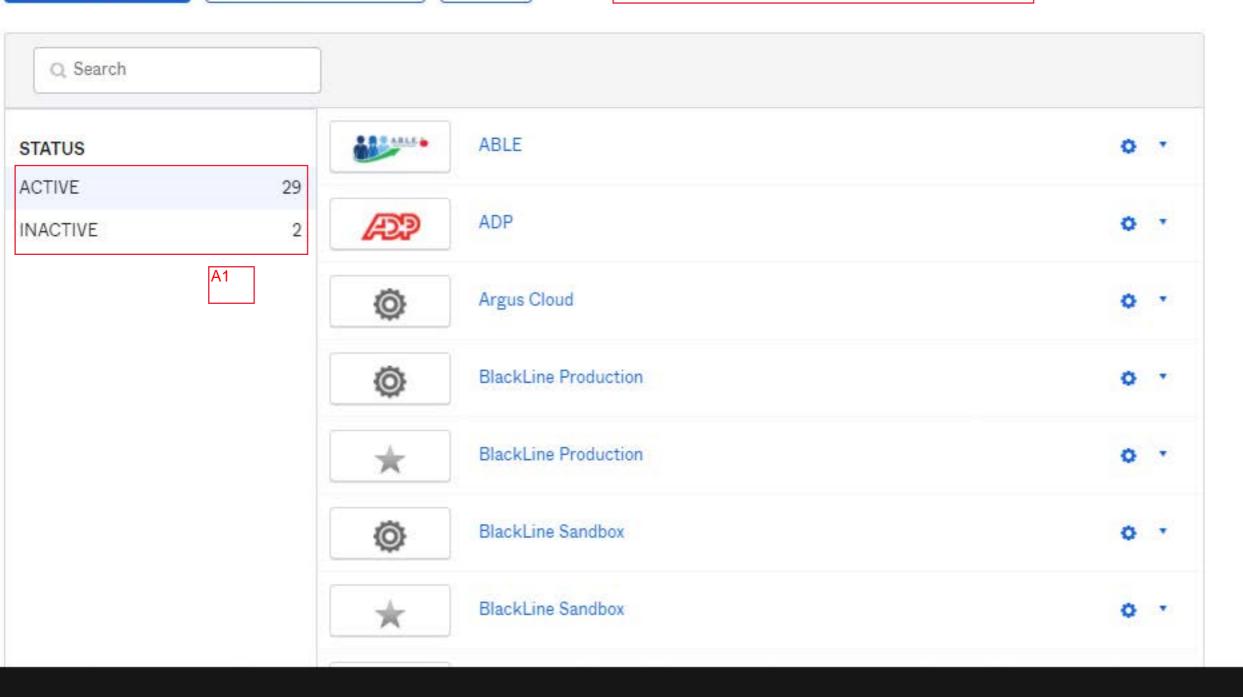


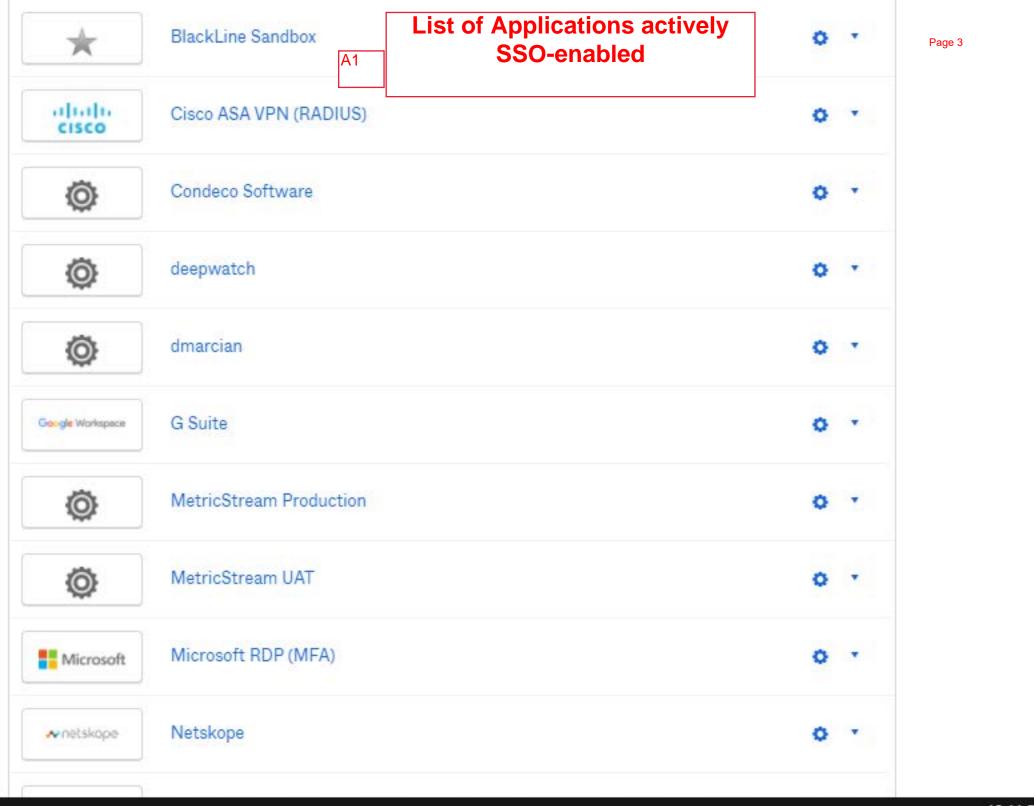
👼 Add Application

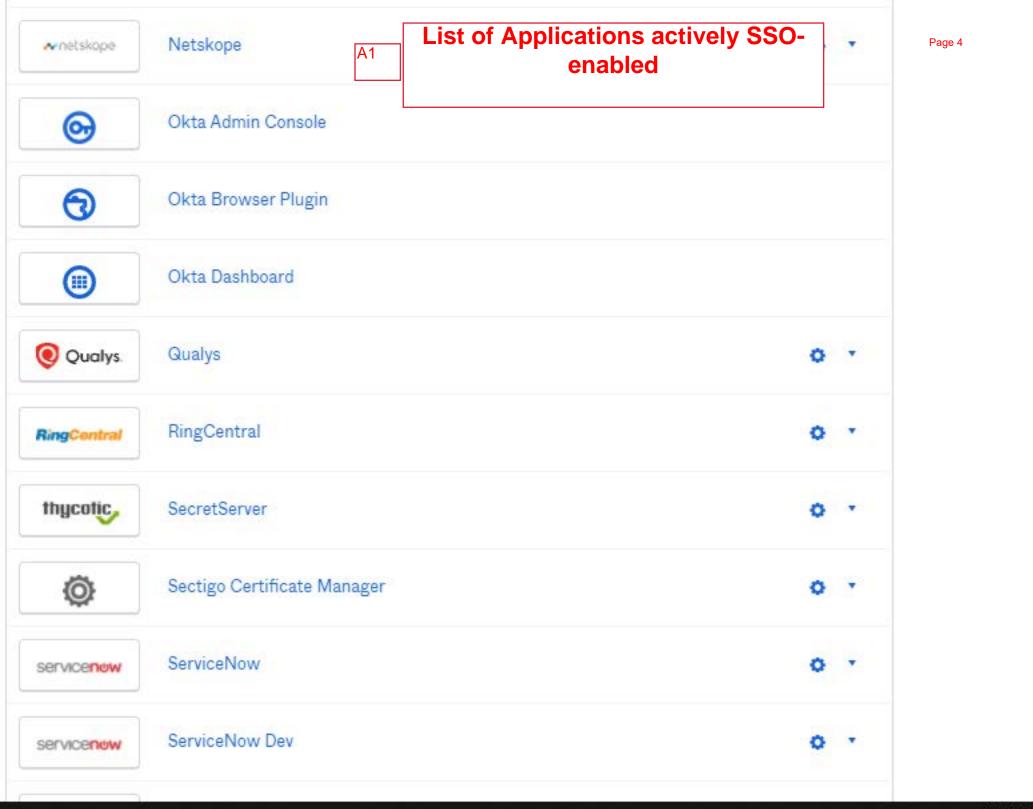
Assign Users to App

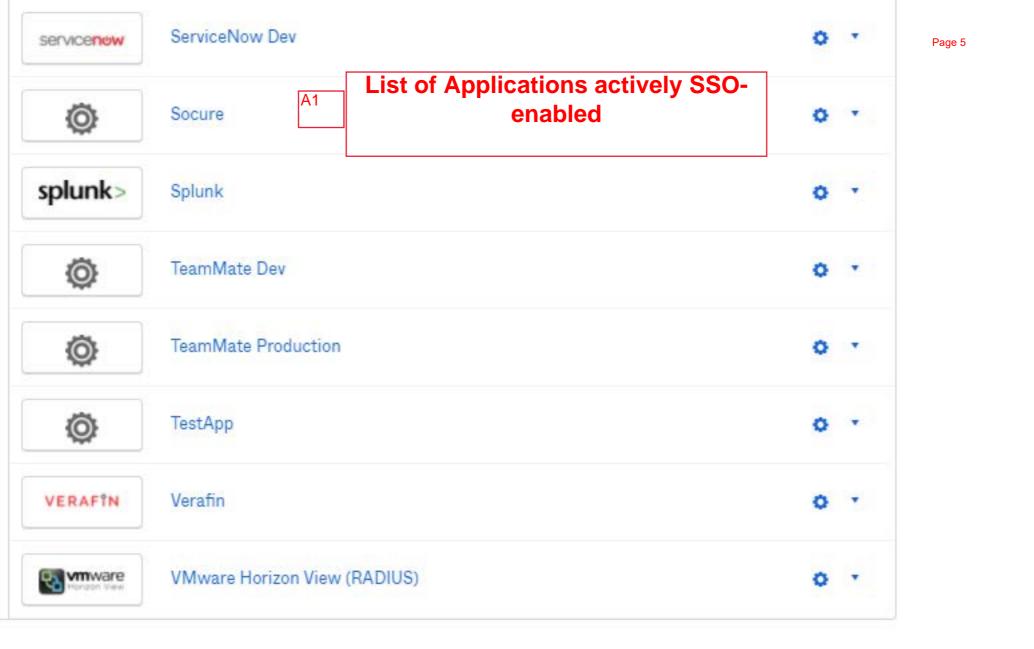
More ▼

List of Applications actively SSOenabled









## General Settings

All fields are required unless marked optional. Some fields may no longer be editable. Page 6

## Need provisioning for this app?

Okta doesn't provide user
provisioning for this app yet, but it
can be added with on-premises
provisioning.
Contact your Okta sales
representative to enable support.
Learn more

SAML Settings

GENERAL

Single Sign On URL

https://able.applebank.com/lms/index.php?
r=SimpleSamlApp/SimpleSamlApp/modules/saml/sp/saml2acs.php/default-sp

Recipient URL

https://able.applebank.com/lms/index.php?
r=SimpleSamlApp/SimpleSamlApp/modules/saml/sp/saml2-

SSO URL => SSO is authenticated and authorized based on SAML standard through a portal service

B1

SSO URL

Page 7

SSO Settings for ABLE

Signature, Digest Algorithm

32

PasswordProtectedTransport

None (disabled)

Yes

SAML Issuer ID http://www.okta.com/\${org.externalKey}

#### ATTRIBUTE STATEMENTS

authnContextClassRef

Assertion Inline Hook

Honor Force Authentication

Name Format Value

user.login Unspecified user.login

nspecified user.iogin

#### GROUP ATTRIBUTE STATEMENTS

Name Format Filter

SSO Settings for ABLE Support by OKTA

SAML User ID managed through OKTA

**B**3

11:58 AM 4/30/2021

SSO Settings for ABLE Support by OKTA

General Sign On Mobile Import Assignments REPORTS Assign v Convert Assignments Q Search... Groups \* Current Assignments Filters Assignment Priority Recent Unassignments People Okta ABLE Access Enabled X APPLEBANK.NY.com/GROUPS/Okta Sync/Okta Groups ABLE Access Enabled SELF SERVICE You need to enable self OKTA-synchronization service for org managed apps **B**3 before you can use self service for this app. Go to self service settings Requests Disabled Approval

Edit

Dashboard

Directory

OMM

Security

Workflow

Reports

Settings

Applications

Applications

Self Service

V

V

^

V

V

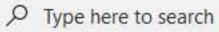
V

V

V

OK6 Cell (US)













@ 2021 Okta, Inc.



Privacy





Version 2021.04.2

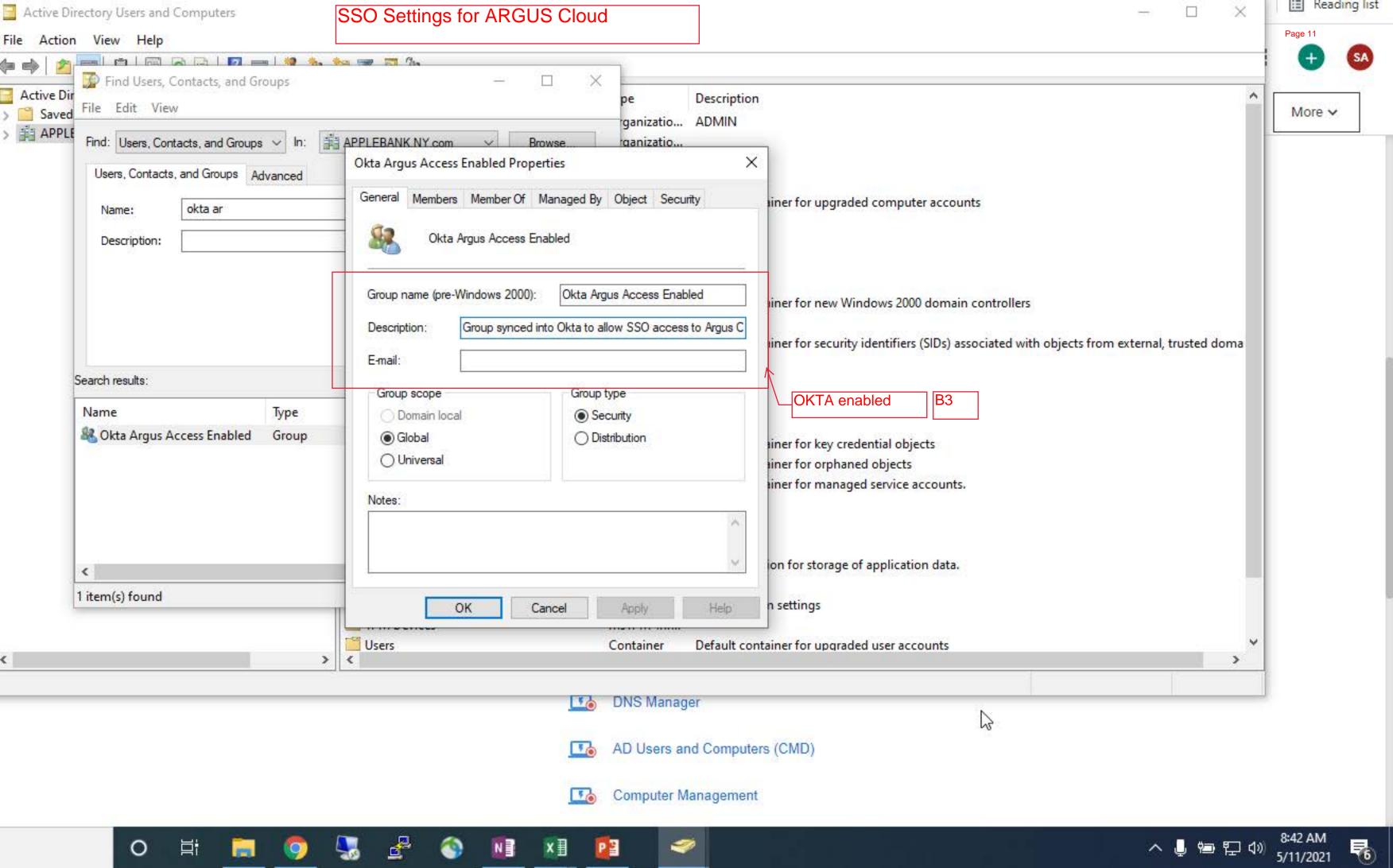


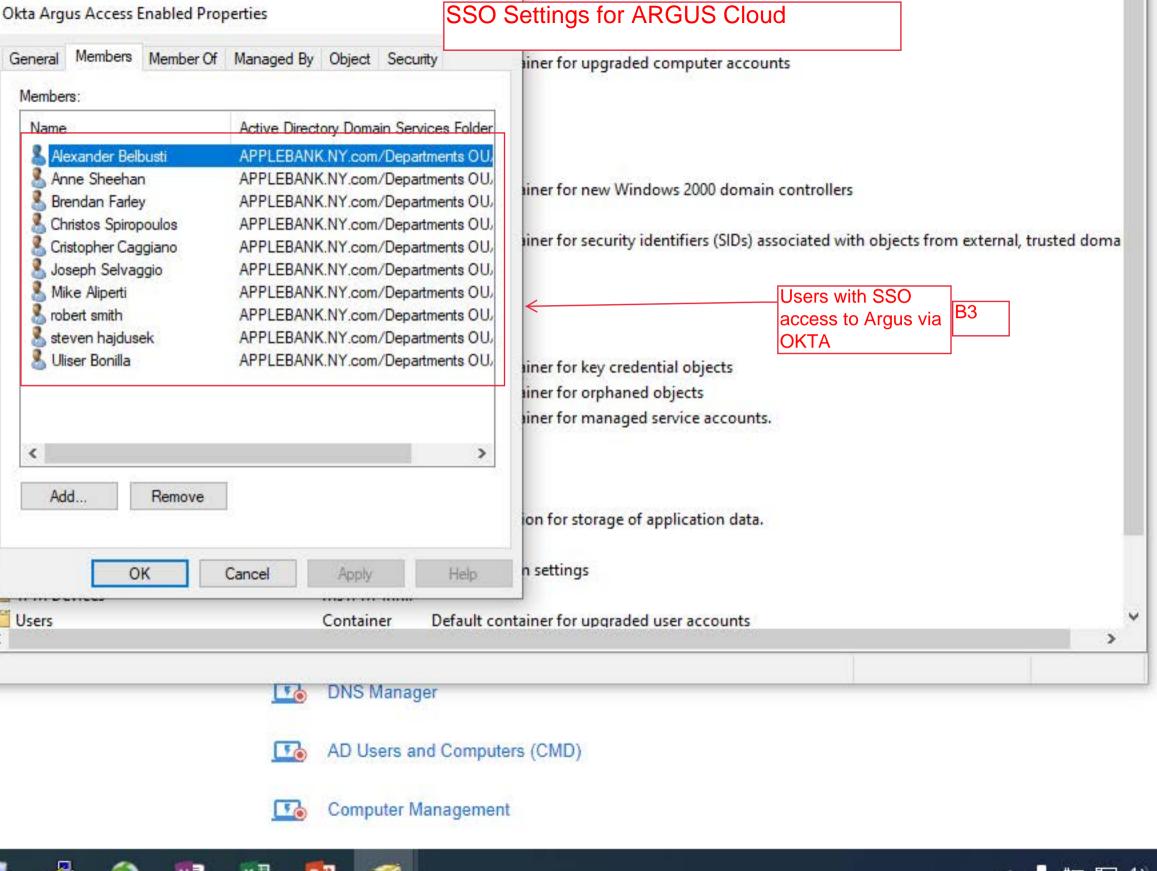


Status site Download Okta Plugin Feedback



Page 10



















5/11/2021

	Page 1
Additional SSO Security Settings	, ago ,
1) Multi Factor Authentications (MFA)	

Active \*

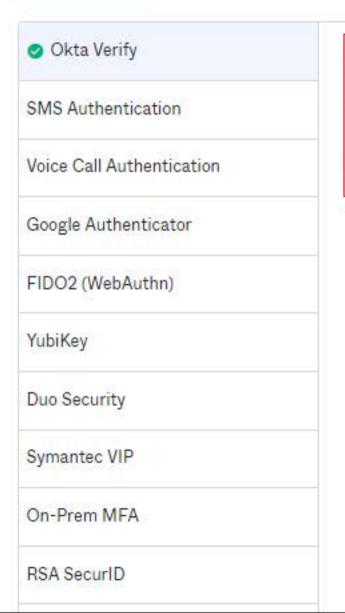
Edit



#### **OKTA MULTIFACTOR SETTINGS**

Factor Types

Factor Enrollment



# Okta Verify

After configuring this factor, users signing in to Okta see that extra verification is required. If Okta Verify is selected they will be instructed to download the Okta Verify App. Once installed, the user will be prompted to enter the generated six digit number to gain access.

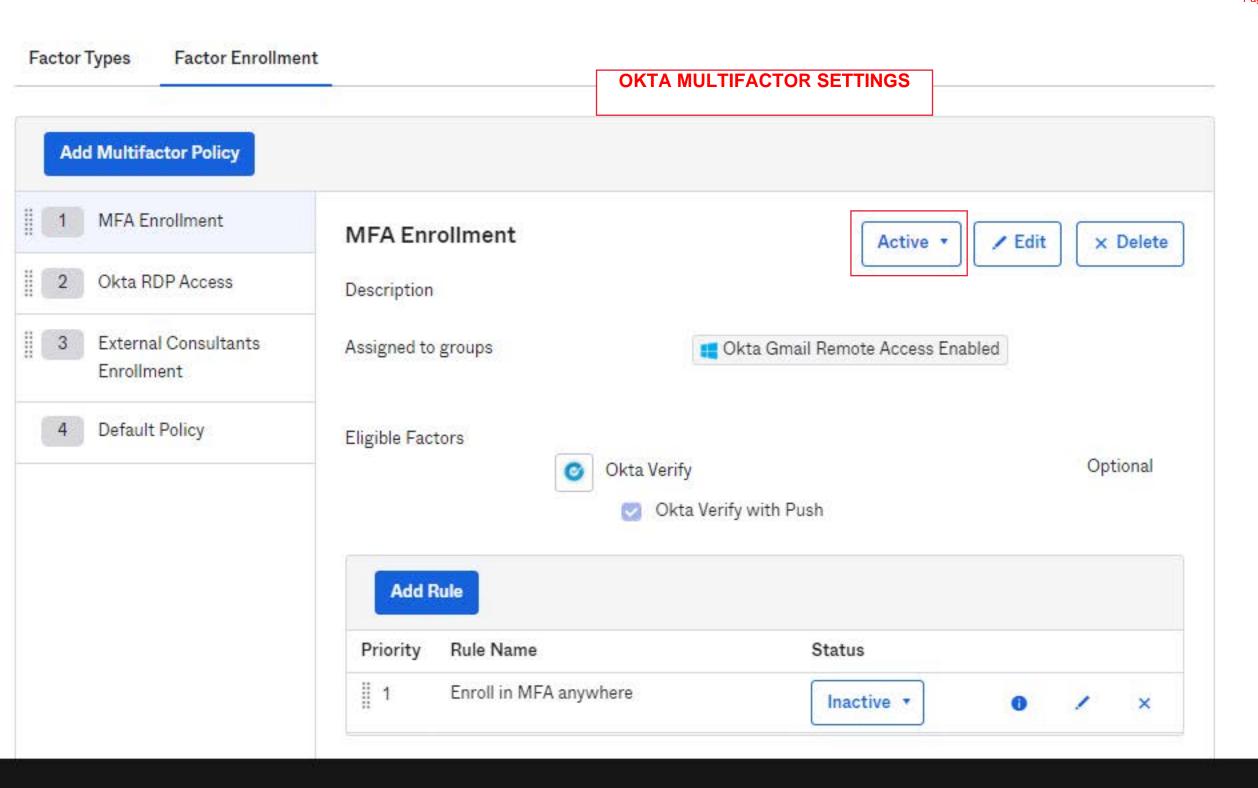
## Okta Verify Settings

Enable Push Notification

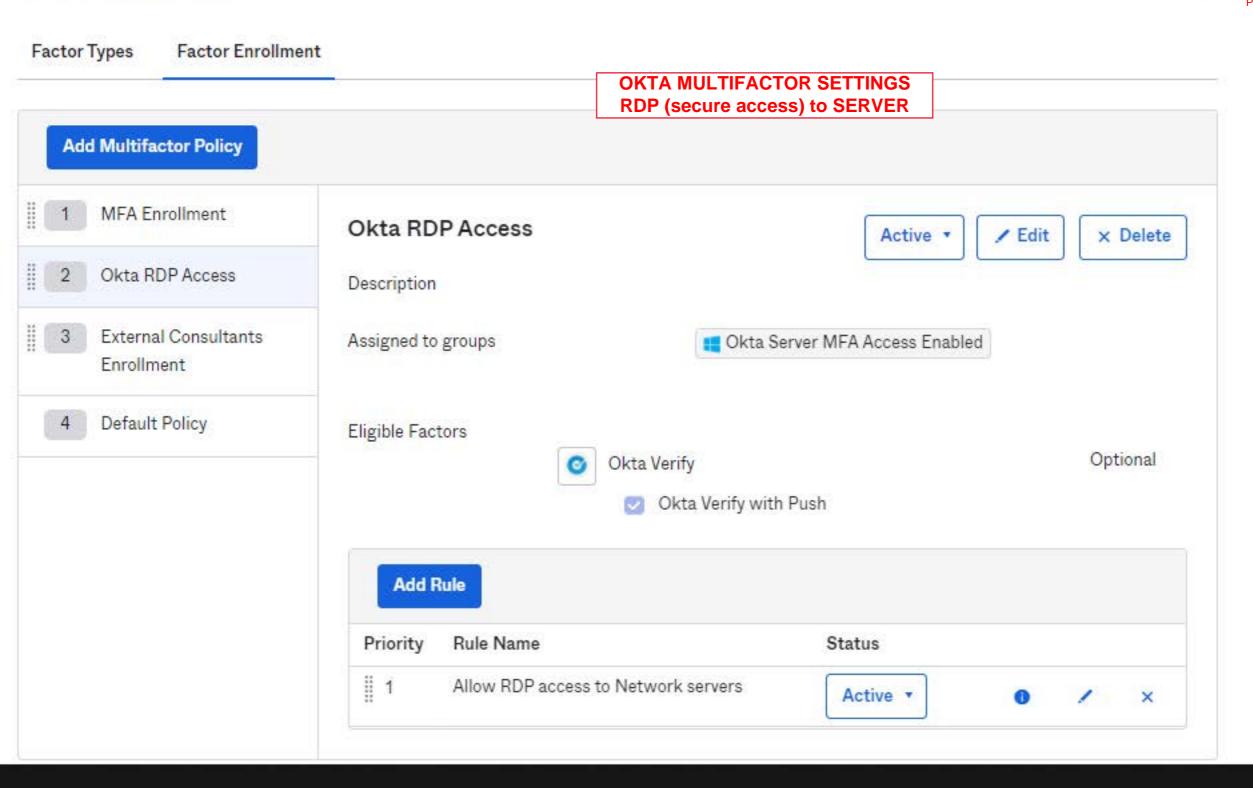
Require Touch ID or Face ID for Okta Verify (only on iOS)



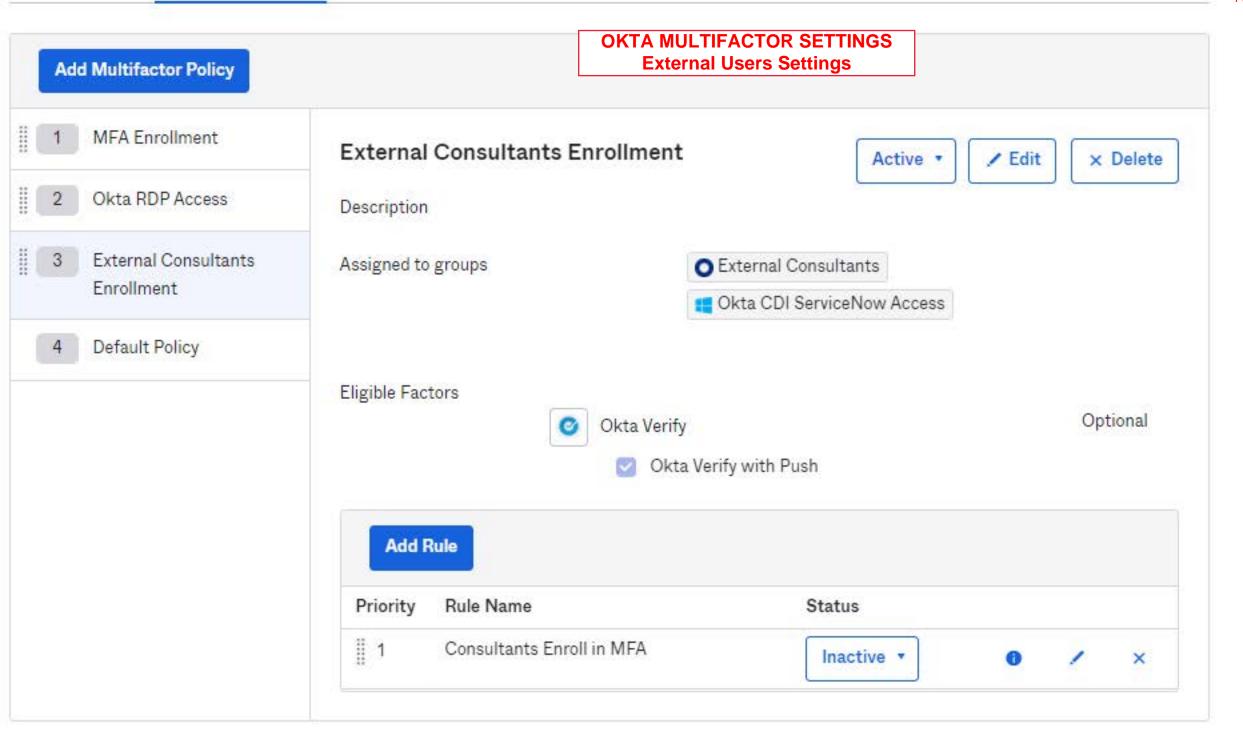








Factor Types Factor Enrollment



Factor Types

Factor Enrollment

