

IT RCSA - Infrastructure

Entity	Apple Bank
Test Name	IT Infrastructure
Test Date	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
B3	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)

List of Applications actively SSO-enabled

[Add Application](#) [Assign Users to App](#) [More ▾](#)

STATUS

ACTIVE	29
INACTIVE	2

A1



ABLE



ADP



Argus Cloud



BlackLine Production



BlackLine Production

































BlackLine Sandbox



BlackLine Sandbox



	BlackLine Sandbox	List of Applications actively SSO-enabled		
	Cisco ASA VPN (RADIUS)			
	Condeco Software			
	deepwatch			
	dmarcian			
	G Suite			
	MetricStream Production			
	MetricStream UAT			
	Microsoft RDP (MFA)			
	Netskope			

A1



Netskope

A1

List of Applications actively SSO-enabled

Page 4



Okta Admin Console



Okta Browser Plugin



Okta Dashboard



Qualys



RingCentral

RingCentral



thycotic

SecretServer



Sectigo Certificate Manager



serviceNow

ServiceNow



















serviceNow

ServiceNow Dev



List of Applications actively SSO-enabled

A1

	ServiceNow Dev	 ▼
	Socure	 ▼
	Splunk	 ▼
	TeamMate Dev	 ▼
	TeamMate Production	 ▼
	TestApp	 ▼
	Verafin	 ▼
	VMware Horizon View (RADIUS)	 ▼

App Settings

SSO Settings for ABLE

[Edit](#)

Application label

ABLE

Application visibility

- ☐ Do not display application icon to users
- ☐ Do not display application icon in the Okta Mobile app

Auto-launch

- ☐ Auto-launch the app when user signs into Okta.

Application notes for end users

Application notes for admins

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

[Edit](#)

GENERAL

Single Sign On URL

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

Recipient URL	https://able.applebank.com/lms/index.php? r=SimpleSamlApp/SimpleSamlApp/modules/saml/sp/saml2- acs.php/default-sp
Destination URL	https://able.applebank.com/lms/index.php? r=SimpleSamlApp/SimpleSamlApp/modules/saml/sp/saml2- acs.php/default-sp
Audience Restriction	https://able.applebank.com/lms/index.php

SSO URL

SSO Settings for ABLE

Default Relay State	
Name ID Format	Transient
Response	Signed
Assertion Signature	Signed
Signature Algorithm	RSA_SHA256
Digest Algorithm	SHA256
Assertion Encryption	Unencrypted
SAML Single Logout	Disabled
authnContextClassRef	PasswordProtectedTransport

Signature, Digest
Algorithm

B2

authnContextClassRef

PasswordProtectedTransport

Honor Force Authentication

Yes

Assertion Inline Hook

None (disabled)

SAML Issuer ID

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

ATTRIBUTE STATEMENTS

Name

Name Format

Value

user.login

Unspecified

user.login

GROUP ATTRIBUTE STATEMENTS

Name

Name Format

Filter

SSO Settings for ABLE Support by OKTA

Page 8

SAML User ID
managed through
OKTA

B3



Active ▾



[View Logs](#) [Monitor Imports](#)

SSO Settings for ABLE
Support by OKTA

[General](#) [Sign On](#) [Mobile](#) [Import](#) [Assignments](#)

Assign ▾

Convert Assignments

Search...

Groups ▾

Filters	Priority	Assignment	
People	1	<div>Okta ABLE Access Enabled APPLEBANK.NY.com/GROUPS/Okta Sync/Okta ABLE Access Enabled</div>	<div><div></div><div></div></div>
Groups			

OKTA-synchronization
B3

REPORTS

- [Current Assignments](#)
- [Recent Unassignments](#)

SELF SERVICE

You need to enable self service for org managed apps before you can use self service for this app.
[Go to self service settings](#)

Requests Disabled
Approval -

Edit

- Dashboard
- Directory
- Applications
- Applications
- Self Service
- OMM
- Security
- Workflow
- Reports
- Settings

← Back to Applications



Argus Cloud

Active



View Logs

Monitor Imports

- General
- Sign On
- Mobile
- Import
- Assignments

Assign

Convert Assignments

Search...

Groups

Filters	Priority	Assignment
People		
Groups	1	<div>Okta Argus Access Enabled APPLEBANK.NY.com/GROUPS/Okta Sync/Okta Argus Access Enabled</div>

OKTA enabled

B3

REPORTS

- Current Assignments
- Recent Unassignments

SELF SERVICE

You need to enable self service for org managed apps before you can use self service for this app.
[Go to self service settings](#)

Requests Disabled

Approval -

Edit

SSO Settings for ARGUS Cloud

Active Directory Users and Computers

File Action View Help

Find Users, Contacts, and Groups

Find: Users, Contacts, and Groups In: APPLEBANK NY.com

Users, Contacts, and Groups Advanced

Name: okta ar

Description:

Search results:

Name	Type
Okta Argus Access Enabled	Group

1 item(s) found

Okta Argus Access Enabled Properties

General Members Member Of Managed By Object Security

Okta Argus Access Enabled

Group name (pre-Windows 2000): Okta Argus Access Enabled

Description: Group synced into Okta to allow SSO access to Argus C

E-mail:

Group scope

☐ Domain local

☒ Global

☐ Universal

Group type

☒ Security

☐ Distribution

Notes:

OK Cancel Apply Help

OKTA enabled

B3

DNS Manager

AD Users and Computers (CMD)

Computer Management

SSO Settings for ARGUS Cloud

Okta Argus Access Enabled Properties

General Members Member Of Managed By Object Security

Members:

Name	Active Directory Domain Services Folder
Alexander Belbusti	APPLEBANK.NY.com/Departments OU,
Anne Sheehan	APPLEBANK.NY.com/Departments OU,
Brendan Farley	APPLEBANK.NY.com/Departments OU,
Christos Spiropoulos	APPLEBANK.NY.com/Departments OU,
Cristopher Caggiano	APPLEBANK.NY.com/Departments OU,
Joseph Selvaggio	APPLEBANK.NY.com/Departments OU,
Mike Aliperti	APPLEBANK.NY.com/Departments OU,
robert smith	APPLEBANK.NY.com/Departments OU,
steven hajdusek	APPLEBANK.NY.com/Departments OU,
Uliser Bonilla	APPLEBANK.NY.com/Departments OU,

<

>

Add... Remove

OK Cancel Apply Help

Container for upgraded computer accounts

Container for new Windows 2000 domain controllers

Container for security identifiers (SIDs) associated with objects from external, trusted domain

Container for key credential objects

Container for orphaned objects

Container for managed service accounts.

Container for storage of application data.

Container settings

Container Default container for upgraded user accounts

Users with SSO access to Argus via OKTA B3

- DNS Manager
- AD Users and Computers (CMD)
- Computer Management

Additional SSO Security Settings

1) Multi Factor Authentications (MFA)

OKTA MULTIFACTOR SETTINGS

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

Okta Verify

Active ▾

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

Edit

☒ Enable Push Notification

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

OKTA MULTIFACTOR SETTINGS

Add Multifactor Policy

1 MFA Enrollment

2 Okta RDP Access

3 External Consultants Enrollment

4 Default Policy

MFA Enrollment

Active Edit Delete

Description

Assigned to groups

Okta Gmail Remote Access Enabled

Eligible Factors

Okta VerifyOptional

Okta Verify with Push

Add Rule

Priority	Rule Name	Status
1	Enroll in MFA anywhere	Inactive

OKTA MULTIFACTOR SETTINGS
RDP (secure access) to SERVER

Add Multifactor Policy

1 MFA Enrollment

2 **Okta RDP Access**

3 External Consultants Enrollment

4 Default Policy

Okta RDP Access

Active ▾ Edit Delete

Description

Assigned to groups

Okta Server MFA Access Enabled

Eligible Factors

☒ Okta Verify

☒ Okta Verify with Push

Optional

Add Rule

Priority	Rule Name	Status
1	Allow RDP access to Network servers	Active ▾ ⓘ ✎ ✕

OKTA MULTIFACTOR SETTINGS
External Users Settings

Add Multifactor Policy

- 1 MFA Enrollment
- 2 Okta RDP Access
- 3 External Consultants Enrollment
- 4 Default Policy

External Consultants Enrollment

Active Edit Delete

Description

Assigned to groups

- External Consultants
- Okta CDI ServiceNow Access

Eligible Factors

- Okta Verify Optional
- Okta Verify with Push

Add Rule

Priority	Rule Name	Status
1	Consultants Enroll in MFA	Inactive

OKTA MULTIFACTOR SETTINGS
Default Policy

Add Multifactor Policy

- 1 MFA Enrollment
- 2 Okta RDP Access
- 3 External Consultants Enrollment
- 4 Default Policy

Default Policy

Edit

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

Assigned to groups
☒ Everyone

Eligible Factors
☒ Okta Verify
☒ Okta Verify with Push
Optional

Add Rule

Priority	Rule Name	Status
1	Default Rule	Active