

2019

Azure AD Access Model

PLAYBOOK

Document Control Sheet

Document Information

Document Name	Azure AD Access Model Playbook
Document Author	
Version	1.0
Status	Draft
Date	20 September 2019

Document Edit History

Version	Date	Edits	Prepared/Revised By
1.0	20 September 2019	Developed	Scott Judson

Table of Contents

1 Adding yourself as Account Administrator 1

1.1 Access the MAC tool (Modern Access Control)..... 1

1.2 Select 'Manage my access' 1

1.3 Search for your AWS and Azure account ID..... 1

1.4 Select the Azure or AWS Security Group and click 'Review' 1

1.5 Submit the access request 2

2 Checking out your elevated password 3

2.1 Login to Secret Server..... 3

2.2 Navigate from left-hand panel to 'Privileged AD Access' → 'Privileged Admins' →
'us.deloitte.com' 3

2.3 Select the secret for your elevated account..... 3

2.4 Click 'View' 3

2.5 Provide a reason for viewing the secret (e.g. "aws") and click 'Save' 3

2.6 Next to the password filed, click the lock icon to reveal your elevated password 4

3 Accessing your AWS account 6

3.1 Login to My Apps portal..... 6

3.2 Select the tile with your account name to login to the AWS console..... 6

4 Giving others access to your AWS account..... 7

4.1 Requestor should login to MAC tool 7

4.2 Request is dependent on two approvals 7

5 Accessing Azure Resource Group Account..... 7

5.1 Log in to MS Azure Portal..... 7

5.2 Sign-In with USA Admin Account..... 7

5.3 Connect with USA Admin Account and Thycotic Secret Server Password 7


5.4 Azure Multi-Factor Authentication 7

1 Adding yourself as Account Administrator

1.1 Access the MAC tool (Modern Access Control)

- <https://mac.us.deloitte.com/>
- You need to be connected to Deloitte network or VPN
- Login using your Deloitte credentials

Welcome



Login

1.2 Select 'Manage my access'

1.3 Search for the Security Group you are being added to (refer to your team leader for additional details)

Examples:

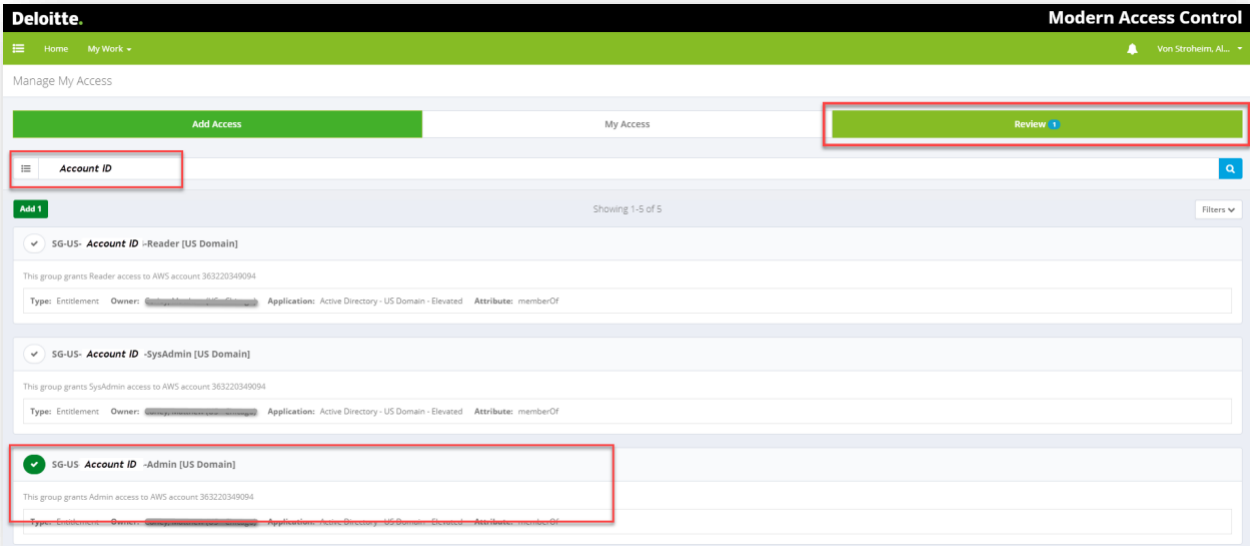
If you Have an AWS Account

Format: SG-US-<account ID> <Role Name>	
Examples for G-US-<account ID>-Admin':	
Security Group Name	Role
SG-US-<account ID>-Admin	Admin
SG-US-<account ID>-sysadmin	sysadmin
SG-US-<account ID>-poweruser	poweruser
SG-US-<account ID>-DBadmin	DBadmin
SG-US-<account ID>-reader	reader

If you Have an Azure Account

Format: SG-US AZU AME CON <Project Name> <Role Name>	
Examples for OracleOfferingDFTEESZ project:	
Security Group Name	Role
SG-US AZU AME CON OracleOfferingDFTEESZ NPD Contributor	Contributor
SG-US AZU AME CON OracleOfferingDFTEESZ NPD SecurityReader	SecurityReader
SG-US AZU AME CON OracleOfferingDFTEESZ NPD MonitoringReader	MonitoringReader
SG-US AZU AME CON OracleOfferingDFTEESZ NPD CostManagementReader	Financial Controller

1.4




1.5 Submit the access request

- You will have to name your project manager for approval
- Your manager will then need to login to the MAC tool and approve the request
- please refer to this page for additional information; <https://wt.deloitteresources.com/solutions/iam/pages/mac.aspx>

Account changes update
Modern Access Control

Changes requested for your elevated account have been processed with the following results:

Approved

Operation	Account	Entitlement	Comments
Add		SG-US Cloud CON CBOIRS-SBX [US Domain]	

Your account was successfully provisioned and has been granted the approved access listed above.

2 Checking out your elevated password

2.1 Login to Secret Server

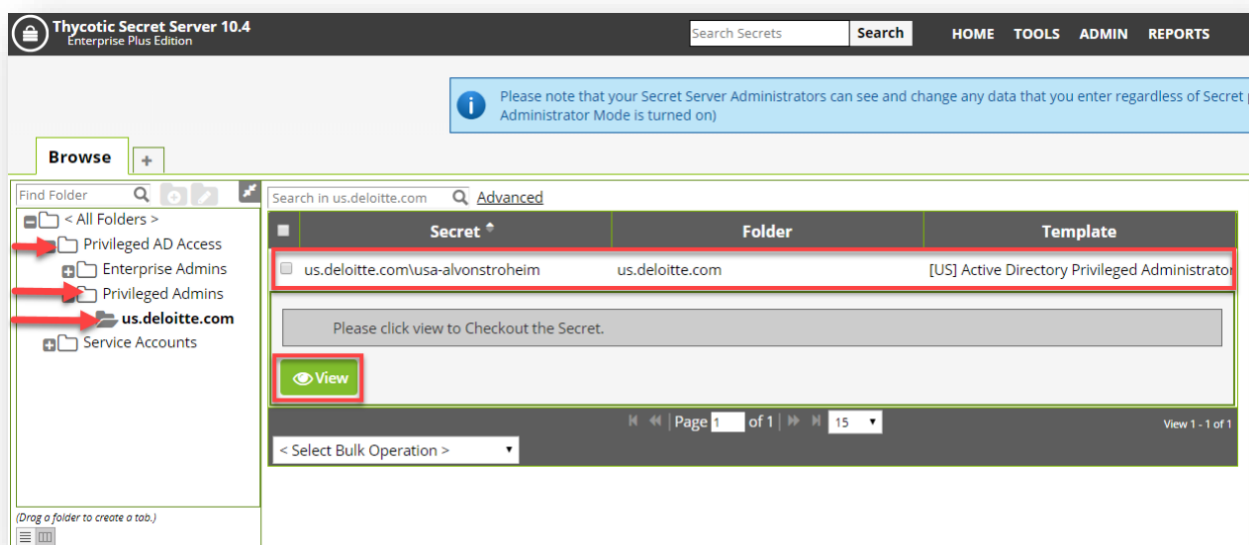
- <https://uspcs.us.deloitte.com/USPCS/>
- You need to be on Deloitte network or VPN

2.2 Navigate from left-hand panel to 'Privileged AD Access' → 'Privileged Admins' → 'us.deloitte.com'

2.3 Select the secret for your elevated account

- Your Deloitte username prefixed with "usa-"

2.4 Click 'View'



2.5 Provide a reason for viewing the secret (e.g. "aws") and click 'Save'

Thycotic Secret Server 10.4
Enterprise Plus Edition

Search Secrets Search HOME TOOLS ADMIN REPORTS

us.deloitte.com\usa-alvonstroheim ([US] Active Directory Privileged Administrator)

Please enter the reason that you are viewing this Secret.

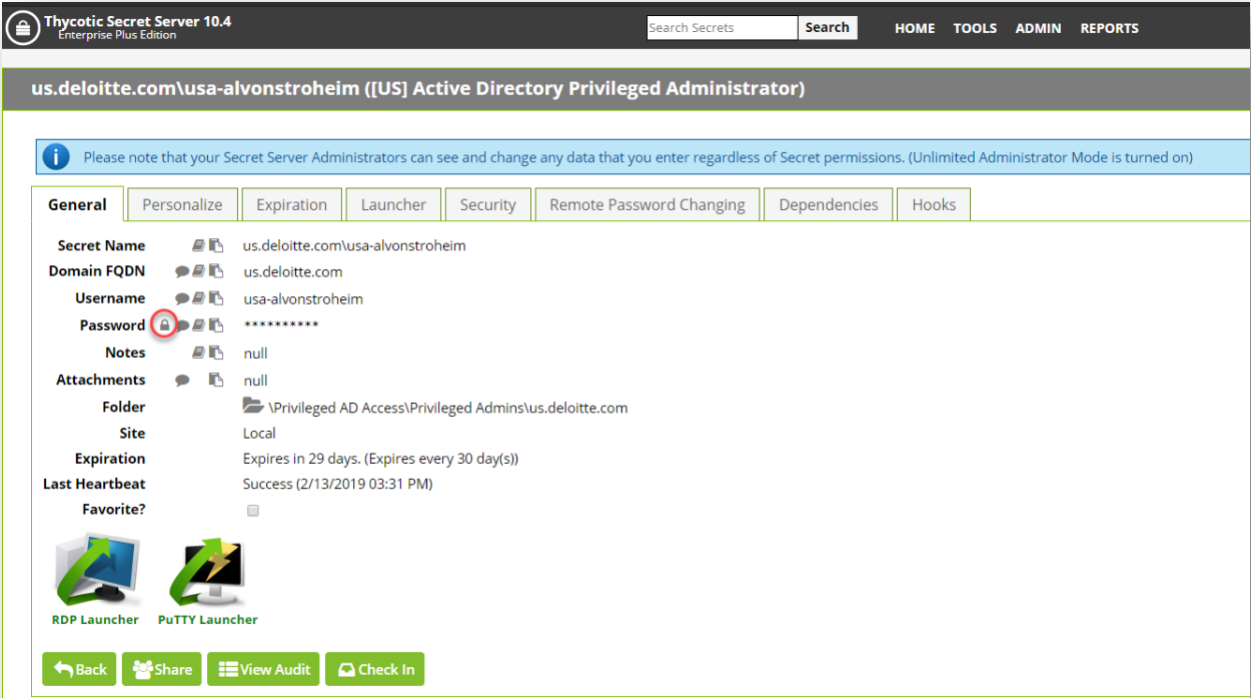
Secret Name us.deloitte.com\usa-alvonstroheim

Reason for View * AWS

Save Cancel

2.6 Next to the password filed, click the lock icon to reveal your elevated password

- You will need to login daily to Secret Server to retrieve your updated password

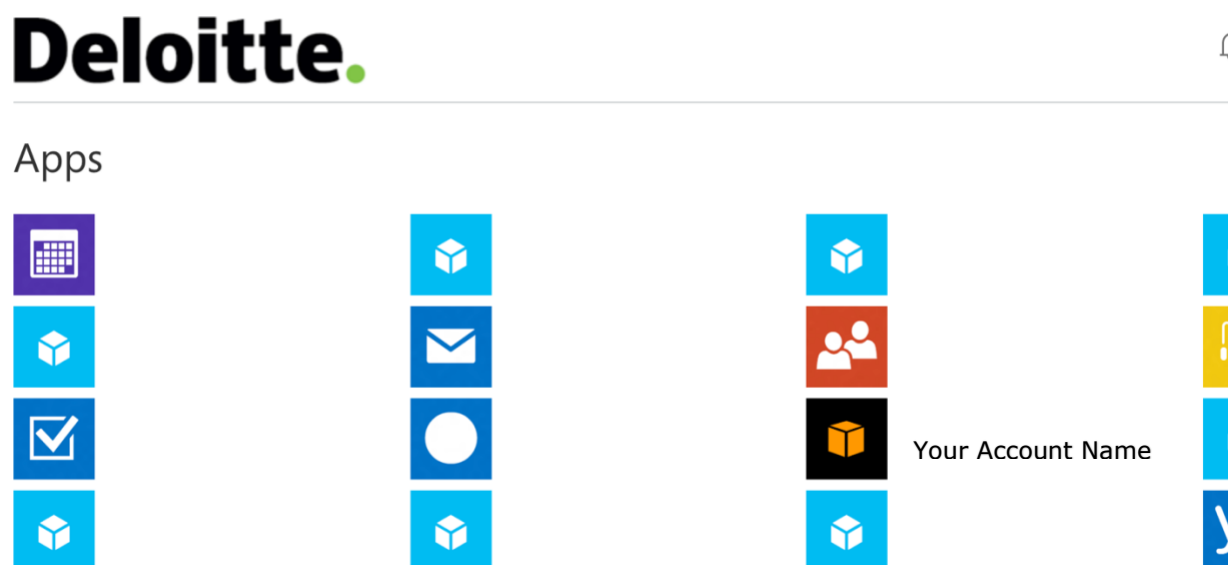


3 Accessing your AWS account (skip to next section for Azure)

3.1 Login to My Apps portal

- <https://myapps.microsoft.com/>
 - On Windows, you either need to use Firefox or run Chrome as a different user and then you'll be able to enter your usa-* credentials
 - For additional Information on how to access Apps portal please page :https://resources.deloitte.com/sites/onetechology/Documents_New/Business_of_IT/OneCloud/Tech-Elevated-Acct-Browser.pdf
 - On Mac, you will need to login using Firefox or use Chrome in incognito mode
- Login using the following credentials:
 - Username: "usa-username@deloitte.com"
 - Password: secret password
- Accounts are only accessible after manager approved in the MAC tool

3.2 Select the tile with your account name to login to the AWSconsole

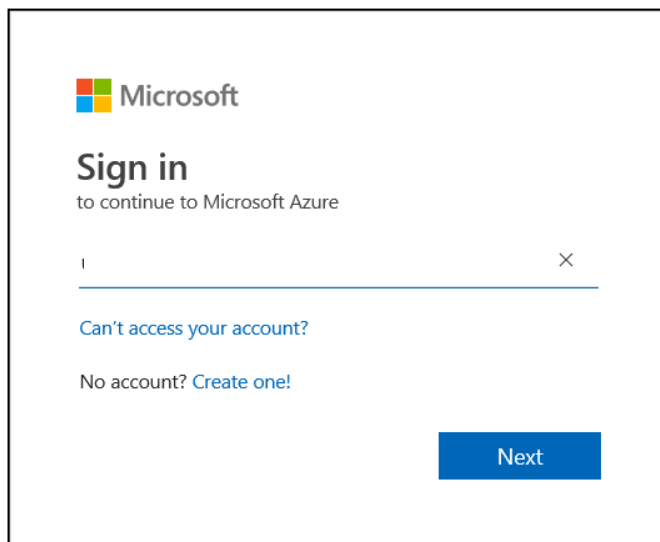


5 Accessing your Azure Resource Group account

5.1 Login to MS Azure Portal

- Open one of the following web browsers
- - Mozilla Firefox or MS Edge (**New Private Browsing Session**)
 - *Google Chrome will cause issues
- NOTE: Accounts are only accessible after manager approved in the MAC tool

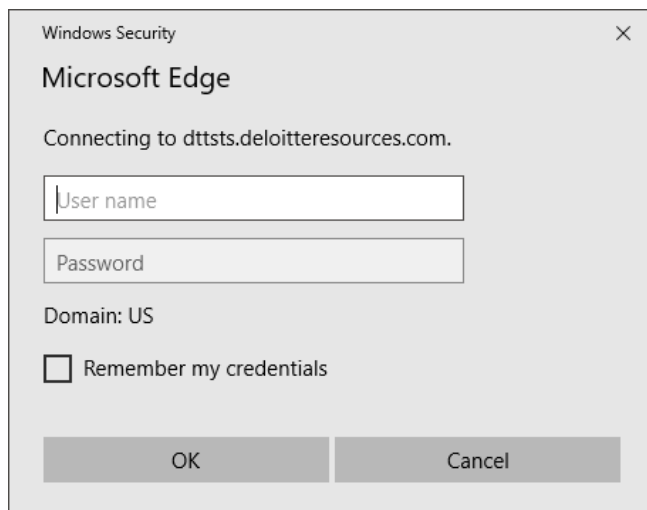
5.2 Sign-In with USA Admin Account ex: **usa-YourDeloitte Email** ex: **usa-jdoe@deloitte.com**



5.3 Connect with USA Admin Account and Thycotic Secret Server Password

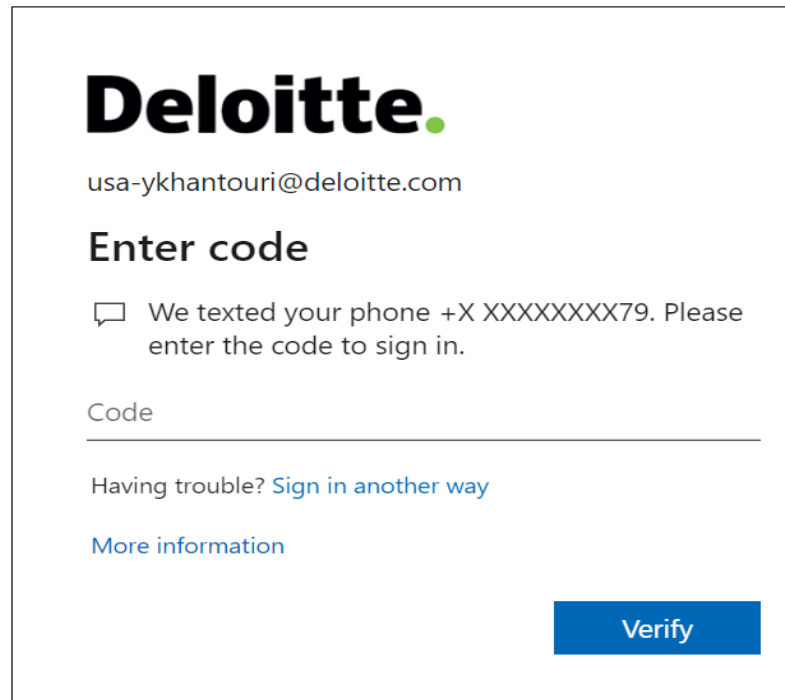
ex:

User Name: **usa-YourDeloitteAlias** ex: **usa-jdoe**
Password: **Thycotic Secret Server Password**



5.4 Azure Multi-Factor Authentication

Additional code will be sent to the user cellphone. Access to Azure portal will be provisioned once the code is entered.

A screenshot of a Deloitte multi-factor authentication interface. At the top is the Deloitte logo. Below it is the email address 'usa-ykhantouri@deloitte.com'. The main heading is 'Enter code'. A message with a speech bubble icon states: 'We texted your phone +X XXXXXXXX79. Please enter the code to sign in.' Below this is a text input field labeled 'Code'. Under the input field are two links: 'Having trouble? Sign in another way' and 'More information'. A blue 'Verify' button is located at the bottom right of the form.

Deloitte.

usa-ykhantouri@deloitte.com

Enter code

🗨 We texted your phone +X XXXXXXXX79. Please enter the code to sign in.

Code

Having trouble? [Sign in another way](#)

[More information](#)

Verify

Select "Resource Groups" or "Subscriptions" on the next screen, depending on how you have structured your environment.