Office 365 integration with PingFederate

Introduction

Office 365 is Microsoft's cloud-based Office solution. Out of two variants of Office 365 that Microsoft offers (desktop option, where users have Office applications (e.g.: Word, etc) installed locally on desktops, but documents and files are stored in the cloud; and a web client, where both documents and applications are stored in the Cloud.

SSO using PingFederate to O365 can be accomplished multiple ways: PingFederate with SAML, PingFederate with WS-Federation/WS-Trust, or an O365 SaaS Connector. In this below exercise, we will use SAML 2.0.

Objectives

- Configure O365 SP connection in PingFederate
- Configure O365 federation setting to authentication with PingFederate

Good to Know

- SAML 2.0 Authentication Protocol
- Authentication flows: IDP initiated (via PingFederate URL) SP initiated (Office 365 URL)

Pre-Requisite

- Office 365 should have a valid, non-default domain and is populated with a test user in it
- Validate that domain has authentication marked as 'managed'.
- Admin must have administrative access to PingFederate and Office 365

- Install the Microsoft Azure Active Directory Module for Windows PowerShell
- Configure data store and PCV in PingFederate to authenticate the users requiring Office 365 application access
- Specify the SAML 2.0 IDP EntityID in the PingFederate>Systems>Server>Protocol Settings
- Validate if AzureAD user has immutableID set, if not set immutableID attribute for the user using below command, as this is required attribute for the federation to work
- Set-MsolUser -UserPrincipalName "" -ImmutableId $value

Steps to follow at PingFederate

Create a PingFederate SP connection for Office 365:

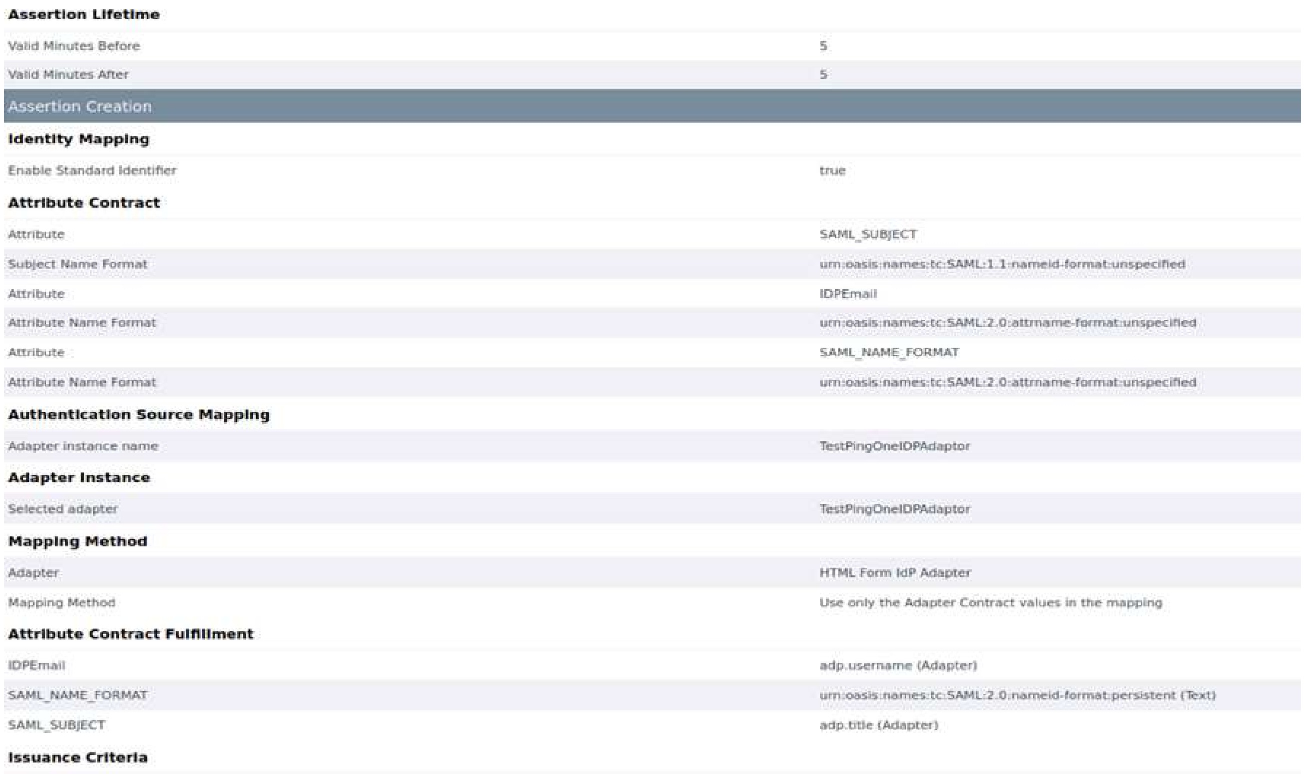
- Download the Office 365 SAML metadata from **https://nexus.microsoftonlinep.com/federationmetadata/saml20/federationmetadata.xml**
- Configure using Browser SSO profile SAML 2.0.
- Import the metadata from the downloaded Office 365 metadata file.
- Enable the following SAML Profiles:
  - IdP-Initiated SSO
  - SP-Initiated SSO
  - SP Initiated SLO
-
  - In Assertion Creation>Authentication Source Mapping>Attribute Contract Fulfilment, extend the contract to add the following

Attribute	**Description**
SAML_SUBJECT	The value of this assertion attribute must be the same as the Azure AD user's ImmutableID.
IDPEmail	Pass this attribute value in assertion as the O365 UPN value of the user.
SAML_NAME_FORMAT	Map this attribute value to this text: **urn:oasis:names:tc:SAML:2.0:nameid-format: persistent**

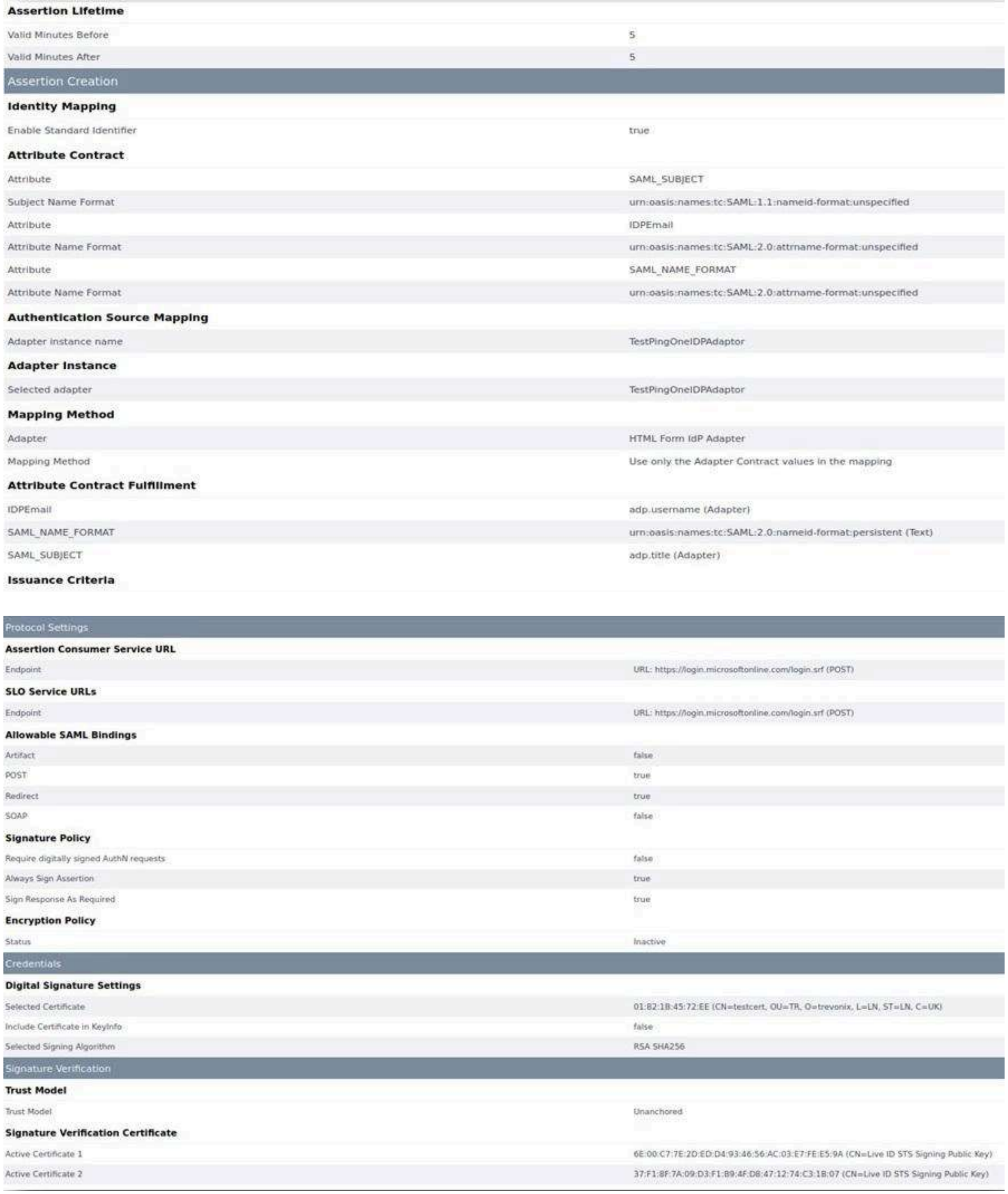
  - In Protocol Settings>Allowable SAML Bindings, enable POST and REDIRECT
  - In Protocol Settings>Signature Policy, select Always Sign Assertion
  - In Credentials>Digital Signature Settings, select the PingFederate signing certificate
    - If a signing certificate is not created, create one at PingFederate under Security>Signing
  - Decryption keys and certificates
  - Save the configuration
  - Export the signing certificate

- Export and then open the metadata file and copy the values for:
  - the entityID.
  - SSO URL(https://<your value>/idp/SSO.saml2)
  - SLO (https://<your value>/idp/SLO.saml2)
  -

Example:



Assertion Lifetime	
Valid Minutes Before	5
Valid Minutes After	5
Assertion Creation	
Identity Mapping	
Enable Standard Identifier	true
Attribute Contract	
Attribute	SAML_SUBJECT
Subject Name Format	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
Attribute	IDPEmail
Attribute Name Format	urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified
Attribute	SAML_NAME_FORMAT
Attribute Name Format	urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified
Authentication Source Mapping	
Adapter instance name	TestPingOneIDPAdaptor
Adapter Instance	
Selected adapter	TestPingOneIDPAdaptor
Mapping Method	
Adapter	HTML Form IdP Adapter
Mapping Method	Use only the Adapter Contract values in the mapping
Attribute Contract Fulfillment	
IDPEmail	adp.username (Adapter)
SAML_NAME_FORMAT	urn:oasis:names:tc:SAML:2.0:nameid-format:persistent (Text)
SAML_SUBJECT	adp.title (Adapter)
Issuance Criteria	



Assertion Lifetime	
Valid Minutes Before	5
Valid Minutes After	5
Assertion Creation	
Identity Mapping	
Enable Standard Identifier	true
Attribute Contract	
Attribute	SAML_SUBJECT
Subject Name Format	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
Attribute	IDPEmail
Attribute Name Format	urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified
Attribute	SAML_NAME_FORMAT
Attribute Name Format	urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified
Authentication Source Mapping	
Adapter instance name	TestPingOneIDPAdaptor
Adapter Instance	
Selected adapter	TestPingOneIDPAdaptor
Mapping Method	
Adapter	HTML Form IdP Adapter
Mapping Method	Use only the Adapter Contract values in the mapping
Attribute Contract Fulfillment	
IDPEmail	adp.username (Adapter)
SAML_NAME_FORMAT	urn:oasis:names:tc:SAML:2.0:nameid-format:persistent (Text)
SAML_SUBJECT	adp.title (Adapter)
Issuance Criteria	

Protocol Settings	
Assertion Consumer Service URL	
Endpoint	URL: https://login.microsoftonline.com/login.srf (POST)
SLO Service URLs	
Endpoint	URL: https://login.microsoftonline.com/login.srf (POST)
Allowable SAML Bindings	
Artifact	false
POST	true
Redirect	true
SOAP	false
Signature Policy	
Require digitally signed AuthN requests	false
Always Sign Assertion	true
Sign Response As Required	true
Encryption Policy	
Status	Inactive
Credentials	
Digital Signature Settings	
Selected Certificate	01:82:1B:45:72:EE (CN=testcert, OU=TR, O=trevonix, L=LN, ST=LN, C=UK)
Include Certificate in KeyInfo	false
Selected Signing Algorithm	RSA SHA256
Signature Verification	
Trust Model	
Trust Model	Unanchored
Signature Verification Certificate	
Active Certificate 1	6E:00:C7:7E:2D:ED:D4:93:46:56:AC:03:E7:FE:E5:9A (CN=Live ID STS Signing Public Key)
Active Certificate 2	37:F1:8F:7A:09:D3:F1:89:4F:D8:47:12:74:C3:1B:07 (CN=Live ID STS Signing Public Key)

Steps to follow at Office 365

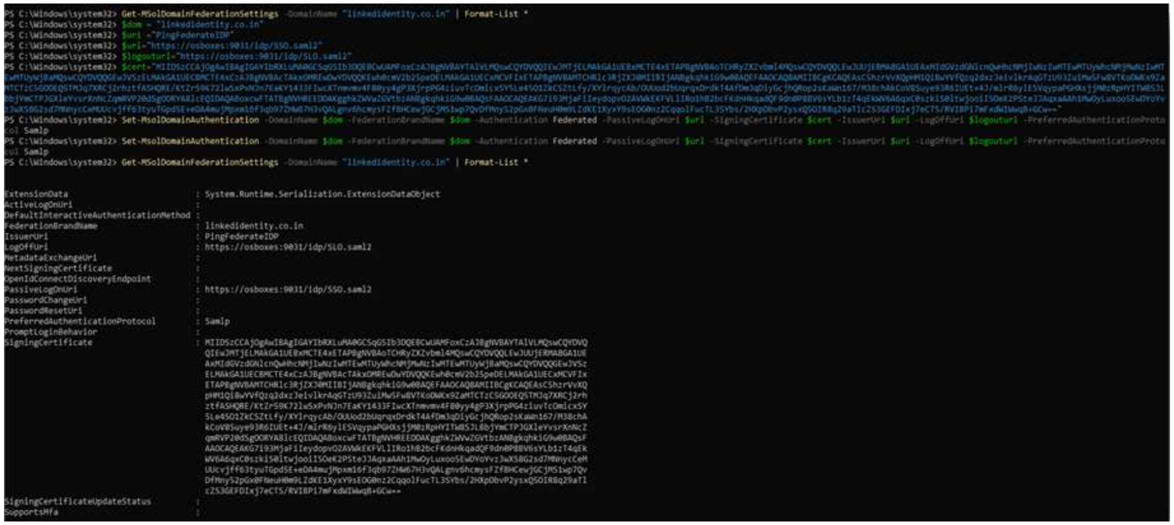
Run Windows PowerShell Command Prompt window (run as administrator) on any internet connected computer.

- Run command: Install-Module MSOnline
- Enter $cred = Get-Credential.
  - Enter the username and password of your Office 365 administrator account in the pop-up
- Connect with MsolService.
  - Connect-MsolService -Credential $cred
- List your domains.
  - Get-MsolDomain
- Select the domain for which you would like to enable SSO.
  - $dom = "<Your O365 domain>"

Set the PingFederate metadata details in the Office 365 configuration as below:

- Set the uri parameter to the PingFederate entityID value.
  - $uri = "<Your entityID>"
- Set the url parameter to the PingFederate Location for SSO value.
  - $url= "<Your Passive Log on Uri>"
- Set the logouturl parameter to the PingFederate Location for SLO value.
  - $logouturl= "<Your Log Off Uri>"
- Open the downloaded signing certificate in Notepad, copy the encoded contents, and paste them into the command below to set the certificate parameter.
- $cert= "<Your certificate contents>"
- Run the following command to setup SAML SSO for your domain
- Set-MsolDomainAuthentication -DomainName $dom -FederationBrandName $dom -Authentication Federated -PassiveLogOnUri $url -SigningCertificate $cert -IssuerUri $uri – LogOffUri $logouturl -PreferredAuthenticationProtocol Samlp
- Run the following command to see the completed SSO settings
  - Get-MSolDomainFederationSettings -DomainName "<Your O365 domain>" | Format-List *

Example:



```
PS C:\Windows\system32> Get-MSolDomainFederationSettings -DomainName "linkedidentity.co.in" | Format-List *
PS C:\Windows\system32> $dom = "linkedidentity.co.in"
PS C:\Windows\system32> $uri ="PingFederateIDP"
PS C:\Windows\system32> $url="https://osboxes:9031/idp/SSO.saml2"
PS C:\Windows\system32> $logouturl="https://osboxes:9031/idp/SLO.saml2"
PS C:\Windows\system32> $cert="MIIDSzCCAjOgAwIBAgIGAYIbRXLuMA0GCSqGSIb3DQEBCwUAMFoxCzAJBgNVBAYTAlVLMQswCQYDVQQIEwJMTjELMAkGA1UEBxMCTE4xETAPBgNVBAoTCHRyZXZvbml4MQswCQYDVQQLEwJUUjERMA8GA1UEAxMIdGVzdGNlcnQwHhcNMjIwNzIwMTEwMTUyWhcNMjMwNzIwMTEwMTUyWjBaMQswCQYDVQQGEwJVSzELMAkGA1UE
[illegible]
[illegible]
[illegible]
[illegible]cZS3GEFDIxj7eCT5/RVIBPi7mFxdWIWwqB+GCw=="
PS C:\Windows\system32> Set-MsolDomainAuthentication -DomainName $dom -FederationBrandName $dom -Authentication Federated -PassiveLogOnUri $url -SigningCertificate $cert -IssuerUri $uri -LogOffUri $logouturl -PreferredAuthenticationProto
col Samlp
PS C:\Windows\system32> Set-MsolDomainAuthentication -DomainName $dom -FederationBrandName $dom -Authentication Federated -PassiveLogOnUri $url -SigningCertificate $cert -IssuerUri $uri -LogOffUri $logouturl -PreferredAuthenticationProto
col Samlp
PS C:\Windows\system32> Get-MSolDomainFederationSettings -DomainName "linkedidentity.co.in" | Format-List *


ExtensionData                          : System.Runtime.Serialization.ExtensionDataObject
ActiveLogOnUri                         :
DefaultInteractiveAuthenticationMethod :
FederationBrandName                    : linkedidentity.co.in
IssuerUri                              : PingFederateIDP
LogOffUri                              : https://osboxes:9031/idp/SLO.saml2
MetadataExchangeUri                    :
NextSigningCertificate                 :
OpenIdConnectDiscoveryEndpoint         :
PassiveLogOnUri                        : https://osboxes:9031/idp/SSO.saml2
PasswordChangeUri                      :
PasswordResetUri                       :
PreferredAuthenticationProtocol        : Samlp
PromptLoginBehavior                    :
SigningCertificate                     : MIIDSzCCAjOgAwIBAgIGAYIbRXLuMA0GCSqGSIb3DQEBCwUAMFoxCzAJBgNVBAYTAlVLMQswCQYDVQ
                                         QIEwJMTjELMAkGA1UEBxMCTE4xETAPBgNVBAoTCHRyZXZvbml4MQswCQYDVQQLEwJUUjERMA8GA1UE
                                         AxMIdGVzdGNlcnQwHhcNMjIwNzIwMTEwMTUyWhcNMjMwNzIwMTEwMTUyWjBaMQswCQYDVQQGEwJVSz
                                         ELMAkGA1UECBMCTE4xCzAJBgNVBAcTAkxOMREwDwYDVQQKEwh0cmV2b25peDELMAkGA1UECxMCVFIx
                                         ETAPBgNVBAMTCHRlc3RjZXJ0MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsCShzrVvXQ
                                         pHM1Qi8wYVfQzq2dxzJeivlkrAqGTzU93ZulMwSFw8VTKoDWKx9ZaMTCTzCSGOOEQSTMJq7XRCj2rh
                                         ztfASHQBE/KtZr59K72lwSxPvNJn7EaKY1433FIwcXTmmvmv4F80yy4gP3XjrpPG4ziuvTcOmicxSY
                                         5Le4SO1ZkCSZtLfy/XYlrqycAb/OUUod2bUqrqxDrdkT4AfDm3qDiyGcjhQRop2sKawn167/M38chA
                                         kCoVBSuye9JR6IUEt+4J/mlrR6ylESVqypaPGHXsjjMNzRpHYITWBSJLBbjYmCTPJGXleYvsrXnNcZ
                                         qmRVP20dSgOORYA8lcEQIDAQABoxcwFTATBgNVHREEDDAKggh0ZWVwZGVtbzANBgkqhkiG9w0BAQsF
                                         AAOCAQEAKG7193MjaFiIeydopvO2AVWkEKFVLlIRo1hB2bcFKdnHkqadQF9dn0P88V6sYLb1zT4qEk
                                         WV6A6qxC0szki50ltwjoolISOeK2PSteJJAqxaAAh1MwOyLuxooSEwDYoYvzJwXS8G2sd7MNnycCeM
                                         UUcvjff63tyuTGpdSE+eDA4mujMpxm16f3qb97ZHW67H3vQALgmv6hcmysFIf8HCewjGCjMS1wp7Qv
                                         DfMny52pGx0FNeuH0m9LIdKE1XyxY9sEOG0nz2CqqolFucTL3SYbs/2HXpDbvP2ysxQ5OIR8q29aTl
                                         cZS3GEFDIxj7eCT5/RVIBPi7mFxdWIWwqB+GCw==
SigningCertificateUpdateStatus         :
SupportsMfa                            :
```

Test the configuration

Test the PingFederate IDP-initiated SSO integration:

- Go to the PingFederate SSO application endpoint for the Office 365 SP connection
  - Example: https://osboxes:9031/idp/startSSO.ping?PartnerSpId=urn%3Afederation%3AMicrosoftOnline
- Complete PingFederate authentication
- You're redirected to your Office 365 domain

Test the PingFederate SP-initiated SSO integration:

- Go to https://portal.office.com
- Enter your email address
- After you're redirected to PingFederate, enter your PingFederate username and password
- You're redirected back to Office 365

Access Requests (https://trevonix.com/tag/access-requests/) Access Security (https://trevonix.com/tag/access-security/) ACloudIdaas (https://trevonix.com/tag/acloudidaas/) API Security (https://trevonix.com/tag/api-security/) cybersecurity (https://trevonix.com/tag/cybersecurity/) cyber threats (https://trevonix.com/tag/cyber-threats/) DAST (https://trevonix.com/tag/dast/) DynamicAuth (https://trevonix.com/tag/dynamicauth/) emerging threats (https://trevonix.com/tag/emerging-threats/) Entitle Management (https://trevonix.com/tag/entitle-management/) equipped (https://trevonix.com/tag/equipped/) Forgerock (https://trevonix.com/tag/forgerock/) Identity Analytics (https://trevonix.com/tag/identity-analytics/) Identity Governance (https://trevonix.com/tag/identity-governance/) Identity Life Cycle Management (https://trevonix.com/tag/identity-life-cycle-management/) Integration (https://trevonix.com/tag/integration/) Merger (https://trevonix.com/tag/merger/) mfa (https://trevonix.com/tag/mfa/) Mobile Access Points (https://trevonix.com/tag/mobile-access-points/) Office365 (https://trevonix.com/tag/office365/) Okta (https://trevonix.com/tag/okta/) Passwordless (https://trevonix.com/tag/passwordless/) Password Vault (https://trevonix.com/tag/password-vault/) ping (https://trevonix.com/tag/ping/) pingfederate (https://trevonix.com/tag/pingfederate/) Ping Identity (https://trevonix.com/tag/ping-identity/) Privilige Access (https://trevonix.com/tag/privilige-access/) profile Management (https://trevonix.com/tag/profile-management/) Resk Based (https://trevonix.com/tag/resk-based/) risks (https://trevonix.com/tag/risks/) Role Based Access (https://trevonix.com/tag/role-based-access/) SAST (https://trevonix.com/tag/sast/) Secure SDLC (https://trevonix.com/tag/secure-sdlc/) security (https://trevonix.com/tag/security/) Segregation of Duties (https://trevonix.com/tag/segregation-of-duties/) sensitive data (https://trevonix.com/tag/sensitive-data/) SingleSignOn (https://trevonix.com/tag/single-sign-on/) singleslide (https://trevonix.com/tag/singleslide/) strategies (https://trevonix.com/tag/strategies/) tailored (https://trevonix.com/tag/tailored/) victim (https://trevonix.com/tag/victim/) vigilance (https://trevonix.com/tag/vigilance/) Vulnerability Assessment (https://trevonix.com/tag/vulnerability-assessment/) Workflow Orchestration (https://trevonix.com/tag/workflow-orchestration/) Zero Trust (https://trevonix.com/tag/zero-trust/)