ivanti

Guide

ivanti

CONTENTS

1. **Ivanti Access 69** **5**
2. **New features summary** **6**
3. **Introducing Ivanti Access** **7**
   - 3.1. Ivanti Access overview 8
   - 3.2. Component interaction 10
   - 3.3. Authentication flow with Ivanti Access 12
   - 3.4. Authentication flow with Ivanti Access + Standalone Sentry 13
   - 3.5. After the user is authenticated in an Ivanti Access deployment 15
   - 3.6. Accessing the cloud service from a desktop, laptop, or an unmanaged device 16
   - 3.7. Setup overview for Ivanti Access 17
4. **Getting Started with Ivanti Access** **21**
   - 4.1. Before you set up Ivanti Access 22
   - 4.2. Working with Ivanti Access administrative portal 25
     - 4.2.1. Changing the password 27
     - 4.2.2. Resetting the password recovery key 28
     - 4.2.3. Configuring 2-step verification 30
   - 4.3. Working with Ivanti Access in Ivanti Neurons for MDM administrative portal 32
     - 4.3.1. Changing the Password for Ivanti Neurons for MDM portal 34
     - 4.3.2. Admins 35
   - 4.4. Ivanti Access Global Dashboard 36
5. **Set up Ivanti Access with UEM** **40**
   - 5.1. Overview of configuration with Ivanti Neurons for MDM 41
     - 5.1.1. Configuring Ivanti Access in Ivanti Neurons for MDM 42
     - 5.1.2. Configuring Ivanti Tunnel in Ivanti Neurons for MDM 44
     - 5.1.3. Configuring Ivanti Neurons for MDM in Ivanti Access 46
   - 5.2. Overview of configuration with Ivanti EPMM 48
     - 5.2.1. Configuring Ivanti Access in Ivanti EPMM 49
     - 5.2.2. Configuring Ivanti Tunnel in Ivanti EPMM 51
     - 5.2.3. Configuring Ivanti EPMM in Ivanti Access 52
   - 5.3. Deregistering Ivanti Access from UEM 54
6. **Set up Ivanti Access + Standalone Sentry** **55**
   - 6.1. Adding a profile 56
   - 6.2. Registering a Standalone Sentry 59
   - 6.3. Viewing Standalone Sentry information 61
   - 6.4. Standalone Sentry actions 63
   - 6.5. Profile overview 65
7. **Federated Pairs** **66**
   - 7.1. Configuring federated pairs 67
   - 7.2. Use Cases for distinctive deployments 69
   - 7.3. Signing certificates 70
   - 7.4. Service provider (SP) metadata 72
   - 7.5. IdP initiated login 74
   - 7.6. SAML response signature 75
   - 7.7. Encrypting SAML assertions 76
   - 7.8. Identity provider (IdP) metadata 78
   - 7.9. Office 365 settings 80
   - 7.10. Cookbook for Ivanti Connect Secure 86
   - 7.11. Active Logon Policy for Office 365 89
   - 7.12. Publishing a profile 92
   - 7.13. Azure Hybrid Domain-Join with Ivanti Access 93
   - 7.14. View federated pairs 94
   - 7.15. Renewing the SSL certificate 97
   - 7.16. Uploading proxy metadata 98
   - 7.17. Verifying traffic flow 99
   - 7.18. Cookbook for Ivanti Neurons 100
8. **Delegated IdP** **102**
   - 8.1. Delegated IdP overview 103
   - 8.2. Authentication flow with Access as the delegated IdP 104
   - 8.3. Configuring Ivanti Access as the delegated IdP 106

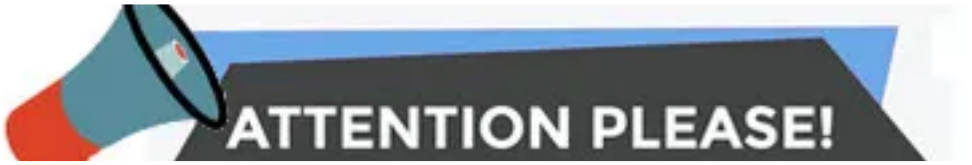
9. Conditional Access ... **113**
9.1. Conditional policies ... 114
9.1.1. Adding a new conditional policy ... 115
9.2. Conditional rules ... 116
9.2.1. Adding a conditional rule ... 117
9.3. Predefined conditional rules ... 118
9.4. Customizable conditional rules ... 119
9.5. Policy chaining ... 129
9.6. Example setup with conditional rules ... 130
9.7. Managing policies and rules ... 131
9.8. Enabling the compliance remediation page ... 133
10. Configuring Mobile App Single Sign-on (SSO) ... **134**
11. Split Tunneling ... **137**
11.1. Enabling split tunneling ... 139
11.2. Adding domains for split tunneling ... 140
12. Branding ... **141**
12.1. Branding overview ... 142
12.2. Adding a remediation page ... 146
12.3. Redirecting device users to a URL ... 147
12.4. Creating a customized message ... 148
13. Session Revocation ... **150**
13.1. About session revocation ... 151
13.2. Configuring Session Revocation ... 152
13.3. Session revocation report ... 154
13.4. What users see if session revocation is configured ... 155
14. Zero Sign-on with Ivanti Access ... **156**
14.1. Overview ... 157
14.2. Configuring Zero Sign-on in Ivanti Neurons for MDM ... 161
14.3. Configuring Zero Sign-on in Ivanti EPMM ... 163
14.4. Configuring Zero Sign-on in Ivanti Access ... 165
14.4.1. Setting Zero Sign-on security and user experience ... 166
14.4.2. Passwordless authentication to service providers on unmanaged devices ... 170
14.4.2.1. Password-less login from unmanaged devices ... 171
14.4.3. Password less login to cloud services for managed desktops ... 174
14.4.3.1. Password-less log in to desktops ... 175
14.4.3.2. Password-less log in to cloud services from managed desktops ... 176
14.4.3.3. Password-less login from managed devices ... 177
14.4.4. Zero Sign-on from desktops managed by Jamf and SCCM ... 180
14.4.4.1. Configuring UEM with Jamf in Ivanti Access ... 182
14.4.4.2. Configuring UEM with SCCM in Ivanti Access ... 184
14.4.5. What users see for FIDO2 ... 189
14.5. Authenticate ... 192
14.5.1. Configuring Authenticate on Ivanti Neurons for MDM ... 193
14.5.1.1. Configuring macOS for Authenticate ... 194
14.5.1.2. Configuring privacy preference for accessibility permission ... 195
14.5.1.3. Adding and distributing a macOS application for Authenticate ... 196
14.5.1.4. Adding and distributing a Windows application for Authenticate ... 197
14.5.2. Configuring Authenticate on Jamf ... 198
14.5.3. What users see for Authenticate ... 199
14.6. Client Registration Settings ... 205
15. Zero sign-on support in Ivanti Access using FIDO hardware keys for unmanaged desktops ... **206**
15.1. Configuring attribute mapping and migration in federation ... 207
15.2. Configuring user portal ... 208
15.3. Logging into user portal ... 209
15.3.1. Registering the security key for FIDO authentication ... 210
15.3.2. Registering the biometric for Zero Sign-on authentication ... 211
15.4. Accessing service provider using security key or biometric ... 212
16. Authenticator Only with Ivanti Access ... **213**
16.1. About Authenticator Only with Ivanti Access ... 214
16.2. Configuring Authenticator Only on Ivanti Neurons for MDM ... 218
16.3. Viewing Authenticator Only on Ivanti Neurons for MDM ... 221
16.4. Configuring Authenticator Only on Ivanti EPMM ... 223

16.5. Viewing Authenticator Only on Ivanti EPMM ... 225
16.6. What users see for Authenticator Only ... 226
17. Multi-factor Authentication with UEM Client ... 233
17.1. About multi-factor authentication with UEM client ... 234
17.2. Overview of configuring multi-factor authentication with UEM client ... 236
17.3. Configuring multi-factor authentication in Ivanti Access ... 237
17.4. What users see for multi-factor authentication in UEM client ... 240
18. Multi-factor Authentication with Authenticator ... 243
18.1. About multi-factor authentication with Authenticator ... 244
18.2. Configuring multi-factor authentication in Ivanti Access for Authenticator ... 247
18.3. Adding the Authenticator app to Ivanti EPMM ... 250
18.4. Adding the Authenticator app to Ivanti Neurons for MDM ... 255
18.5. What users see for multi-factor authentication ... 259
18.6. Lost Device Access Procedure ... 263
19. Access Certificates ... 265
19.1. Certificates ... 266
19.2. User Certificates ... 267
19.3. Certificate expiry notifications ... 270
19.4. Updating certificates for an SP or IdP ... 272
20. Reports ... 275
20.1. About reports ... 276
20.2. Ivanti Access reports ... 277
20.3. Errors Report ... 283
20.4. Zero Sign-on Reports ... 285
20.5. Audit Log ... 287
20.6. SaaS Sign-on ... 290
21. Settings ... 292
21.1. Admins ... 293
21.2. Working with Test IDP ... 297
21.3. Working with Test SP ... 298
22. Troubleshooting ... 300
22.1. Password is not prompted by Email+ application when using Ivanti Access for Office 365 ... 301
22.2. Salesforce from Web@Work does not display authentication page ... 302
22.3. Salesforce produces incorrect metadata with invalid Entity ID ... 303
23. Appendix ... 304
23.1. Configuring Ivanti Neurons for MDM for SSO certificates ... 305
23.2. Configuring Ivanti EPMM for SSO certificates ... 307
23.3. Configuring LDAP in Ivanti Neurons for MDM for session revocation ... 309
23.4. Configuring LDAP in Ivanti EPMM for session revocation ... 310
23.5. Customizing certificates for single sign-on in Ivanti Access ... 311
23.6. Back up and restore Office 365 settings ... 314
23.7. Configuring Ivanti Access Splunk application ... 316
24. Third-Party Attributes ... 321
25. About Zero Sign-on with MobileIron Access ... 322
26. Configuring Zero Sign-on ... 324
27. Configuring Zero Sign-on in Ivanti Access ... 326

1. Ivanti Access 69

June 2026

Access allows access to enterprise cloud resources based on user and device posture, and whether apps are managed or not. Non-AppConnect managed apps and AppConnect apps are supported. Authentication traffic for managed apps uses Tunnel and for AppConnect apps uses AppTunnel. In addition, conditional rules can be configured to allow access for unmanaged applications, as well as, manage access from mobile devices, laptops, and desktops.



New features summary

2. New features summary

These are cumulative release notes. If a release does not appear in this section, then there were no associated new features and enhancements.

Ivanti Access 69 - New features summary

- **Integrating Ivanti Neurons Federation via Ivanti Access**: Ivanti Access now features a dedicated catalog tile for **Ivanti Neurons**, allowing it to act as a SAML service provider in federation pairs with IDPs like Okta.
  For the Ivanti Neurons configuration, see **Cookbook for Ivanti Neurons**.

3. Introducing Ivanti Access

Ivanti Access is a cloud service which secures access to enterprise content in business cloud services such as Box, G Suite, Office 365, Dropbox, and Salesforce. Ivanti Access secures access based on the following:

- device identity
- user identity
- app identity

The following topics provide an overview about Ivanti Access :

3.1. Ivanti Access overview

Ivanti Access allows access to enterprise cloud resources based on user and device posture, and whether apps are managed or not. Non-AppConnect managed apps and AppConnect apps are supported. Authentication traffic for managed apps uses Ivanti Tunnel and for AppConnect apps uses AppTunnel. In addition, conditional rules can be configured to allow access for unmanaged applications, as well as, manage access from mobile devices, laptops, and desktops.

Deployment modes

Ivanti Access consists of two modes of deployment.

- Ivanti Access
  In an Ivanti Access deployment, Access integrates directly with a UEM to get device posture and compliance information from the UEM.
- Ivanti Access + Standalone Sentry
  In an Ivanti Access + Standalone Sentry, Access integrates with Standalone Sentry to get device posture and compliance. In this deployment, Ivanti Access has two components:
  - The Ivanti Access administrative portal, which is a SaaS service. Federated pair setup and configurations are done in the Ivanti Access administrative portal.
  - The Access gateway, which runs on Standalone Sentry, enforces conditional access policies and provides native mobile app single sign-on (SSO).

Ivanti Access in either deployment provides the following features:

- Integration with business cloud service providers (SP).
- Integration with identity providers (IdP). Conditional rules to allow, block, and warn Access.
- Secure access to enterprise cloud based services.
- Federated authentication with SAML or WS-Fed.
- Visibility into users, devices, and apps accessing cloud services.
- Prevention of unauthorized devices and apps from accessing cloud based services.

Naming convention

Unless otherwise noted, Ivanti Access refers to both Ivanti Access and Ivanti Access + Standalone Sentry deployments.

User interface

Ivanti Access is available in the Ivanti Access administrative portal or in the Ivanti Neurons for MDM portal. To work with either of these instances, use on of the following options:

- If your Ivanti Access deployment does not integrate with Ivanti Neurons for MDM, then Access features are available in the Ivanti Access administrative portal. For more information, see **Working with Ivanti Access administrative portal**.
- If your Ivanti Access deployment integrates with Ivanti Neurons for MDM, then the Access features are available in Ivanti Neurons for MDM in the left navigation pane. The Ivanti Neurons for MDM and Ivanti Access tabs are available in one console in Ivanti Neurons for MDM. For more information about this user experience, see **Working with Ivanti Access in Ivanti Neurons for MDM administrative portal**.
  Working with Ivanti Access in Ivanti Neurons for MDM administrative portal

Support and compatibility

For information on support and compatibility, see the Ivanti Access Release Notes.

3.2. Component interaction

This section provides an overview of how the various components in an Ivanti Access deployment interact with each other. The following table describes how various components interact with Ivanti Access.

Component	Ivanti Access	Ivanti Access + Standalone Sentry
Ivanti Access administrative portal	All Access related configurations , monitoring, reporting are done in the Ivanti Access administrative portal.	All Access related configurations , monitoring, reporting are done in the Ivanti Access administrative portal.
UEM	Managed apps which use Ivanti Tunnel, the Ivanti Tunnel app, and configurations are pushed from UEM. Ivanti Access gets device posture information from UEM.	Managed apps which use Ivanti Tunnel, the Ivanti Tunnel app, and configurations are pushed from UEM.
Ivanti Tunnel	Ivanti Tunnel establishes trust with Ivanti Access. Only authentication traffic to Ivanti Access goes through Ivanti Tunnel. To trigger Ivanti Tunnel, apply the Ivanti Tunnel VPN configuration to the managed apps and AppConnect apps.	Ivanti Tunnel establishes trust with Ivanti Access. Only authentication traffic to Ivanti Access goes through Ivanti Tunnel. To trigger Ivanti Tunnel, apply the Ivanti Tunnel VPN configuration to the managed apps and AppConnect apps.
Standalone Sentry	Not applicable.	• Gets the following from the Ivanti Access administrative portal - SP and IdP federated pairings - conditional rules for access control - SSL certificates and signing certificates (X.509 certificate and corresponding private key) Ivanti Access gets device posture information from Standalone Sentry. Standalone Sentry: • Captures information on which users, devices, and apps authenticate to enterprise cloud service. This information is reported in the Ivanti Access administrative portal. Standalone Sentry Communicates with the Ivanti Access administrative portal on port 443. Standalone Sentry syncs up with Ivanti Access at 15-minute intervals. To force update the configuration changes to Standalone Sentry, use the following CLI command in CONFIG mode: accs config-fetch update

UEM compliance actions and policies

Policies configured in a UEM define the checks on device posture and compliance actions if the device in non compliant. Access does the following if devices are out of compliance:

- Ivanti Access blocks connection to cloud service if devices are non compliant (violate an UEM policy) and also have a blocking action set up against the corresponding policy. If there is a non blocking action (such as email, monitor, notify) for a policy violation, Ivanti Access does not take any action.
- For Ivanti EPMM, Ivanti Access quarantines connection to cloud service if the devices are non compliant (violate an UEM policy) and also have a quarantine action set up against the corresponding policy.
  However, for Ivanti Neurons for MDM, Ivanti Access does not take any action against a corresponding quarantine policy.

In addition, you can configure Ivanti Access to revoke a session token if a device is non compliant. For more information on device compliance for session revocation, see **About session revocation**.

Device posture information on Compliant and Non-compliant modes

- Ivanti Access will have device posture information within 5 minutes to perform compliance actions after device moves from Non-Compliant to Compliant in Ivanti Neurons for MDM.
- Ivanti Access will have device posture information within 25 minutes to perform compliance actions after device moves from Compliant to Non-Compliant in Ivanti Neurons for MDM.

> When a device goes out of compliance, Access blocks the data path. This blocked status of the device can be viewed on Ivanti Neurons for MDM under Devices > Overview.
>
> 

For more information on UEM compliance actions and policies, see the respective Ivanti EPMM or Ivanti Neurons for MDM guides.

3.3. Authentication flow with Ivanti Access

The following describe the authentication flow with Ivanti Access.

- Managed non-AppConnect app using Ivanti Tunnel
- AppConnect apps with Ivanti Access enabled (Ivanti EPMM only)

> This section is not applicable if you are deploying Access + Standalone Sentry.

Managed non-AppConnect app using Ivanti Tunnel

The following describes the authentication flow when a managed non-AppConnect app accesses a enterprise cloud service.

Figure 1. Authentication flow for a managed non-appconnect app



1.	A managed app triggers Ivanti Tunnel.
2.	If the device is in compliance, Ivanti Tunnel establishes a secure connection with Ivanti Access.
3.	The managed app connects to the service provider (SP) through Ivanti Tunnel.

Split Tunneling is enabled: If split tunneling is enabled, and the split tunneling does not require tunneled connection to the service provider, the app connects directly with the service provider.

4.	If the managed app does not have a valid session token, the SP issues a SAML 2.0 AuthN Request to the app and redirects the app to Ivanti Access.
5.	Ivanti Access issues a secondary SAML AuthN Request based on the AuthN Request in step 4. The AuthN Request is issued via SAML and points the user to the identity provider (IdP).
6.	If the user does not have a current valid session token, the identity provider (IdP) requests the user's credentials. If the credentials match, the IdP issues a SAML Assertion to the user. The SAML Assertion identifies the user and redirects the user to Access.
7.	The user presents the SAML Assertion to Ivanti Access. If conditional rules for access control allow, Ivanti Access issues a secondary SAML Assertion to the user. The secondary SAML Assertion identifies the user and redirects the user to the cloud service (SP).
8.	The user presents the secondary SAML Assertion to the cloud service (SP). The SP verifies the secondary SAML Assertion and creates a session token to the app. The session token gives the user access to the SP.

AppConnect apps with Ivanti Access enabled (Ivanti EPMM only)

AppConnect apps with Ivanti Access enabled automatically use HTTP tunnel to Ivanti Access.

3.4. Authentication flow with Ivanti Access + Standalone Sentry

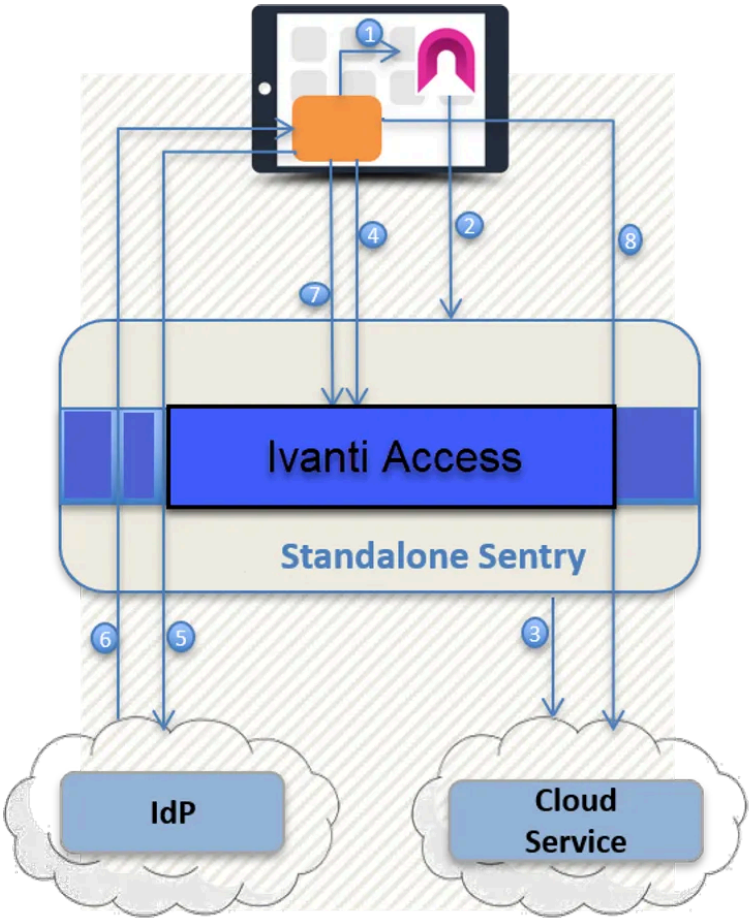
The following describe the authentication flow in an Ivanti Access + Standalone Sentry deployment.

- Managed non-AppConnect app using Ivanti Tunnel and Standalone Sentry
- AppConnect apps using AppTunnel with Ivanti Access + Standalone Sentry

Managed non-AppConnect app using Ivanti Tunnel and Standalone Sentry

The following describes the authentication flow when a managed non-AppConnect app accesses a enterprise cloud service in an Ivanti Access + Standalone Sentry deployment.

Figure 1. Authentication flow for a managed non-appconnect app



1.	A managed app triggers Ivanti Tunnel.
2.	If the device is in compliance, Ivanti Tunnel establishes a secure connection with Standalone Sentry.
3.	The managed app connects to the service provider (SP) through Ivanti Tunnel.

Split Tunneling is enabled: If split tunneling is enabled, and the split tunneling does not require tunneled connection to the service provider, the app connects directly with the service provider.

4. If the managed app does not have a valid session token, the SP issues a SAML 2.0 AuthN Request to the app and redirects the app to Ivanti Access on Standalone Sentry.

5. Ivanti Access issues a secondary SAML AuthN Request based on the AuthN Request in step 4. The AuthN Request is issued via SAML and points the user to the identity provider (IdP).

6. If the user does not have a current valid session token, the identity provider (IdP) requests the user's credentials. If the credentials match, the IdP issues a SAML Assertion to the user. The SAML Assertion identifies the user and redirects the user to Access.

7. The user presents the SAML Assertion to Access on Standalone Sentry. If conditional rules for access control allow, Ivanti Access issues a secondary SAML Assertion to the user. The secondary SAML Assertion identifies the user and redirects the user to the cloud service (SP).

8. The user presents the secondary SAML Assertion to the cloud service (SP). The SP verifies the secondary SAML Assertion and creates a session token to the app. The session token gives the user access to the SP.

AppConnect apps using AppTunnel with Ivanti Access + Standalone Sentry

Authentication traffic for managed apps goes to Ivanti Tunnel. For AppConnect apps that use AppTunnel, authentication traffic automatically goes through Ivanti Access. By default, AppTunnel traffic is trusted by Ivanti Access.

3.5. After the user is authenticated in an Ivanti Access deployment

After a session token is created, data between the managed app or AppConnect app and the cloud service continues to flow through Tunnel and AppTunnel. Data does not flow through Ivanti Access. The user will have to authenticate again only after the expiration of the session token. The length of the session token is configured on the cloud service.

3.6. Accessing the cloud service from a desktop, laptop, or an unmanaged device

Conditional rules configured in Ivanti Access can be used to define which apps and devices can authenticate with the cloud service provider (SP). You can configure a conditional rule to allow an unmanaged app to access the SP. By default, conditional rules are not applied to managed apps using Ivanti Tunnel and to AppConnect apps using Ivanti Tunnel or AppTunnel. The default conditional rule can be set to allow, block, or warn apps and devices if conditional rules do not match. If the default conditional rule is set to Allow when all other conditional rules do not match, authentication traffic will be allowed through Ivanti Access. In this setup, the app will be able to authenticate with the IdP.

Ivanti Access provides a set of predefined and customizable rules. For more information about conditional rules, see **Conditional Access**.

3.7. Setup overview for Ivanti Access

This section provides an overview of the setup required for implementing access control to cloud services using Ivanti Access and contains the following:

- Before you configure Ivanti Access
- Overview of steps to set up Ivanti Access
- Authentication options

Before you configure Ivanti Access

Before you start configuring Ivanti Access the following infrastructure setup is required:

- **Federated authentication**
  Ivanti Access supports federated authentication using SAML and WS-Fed. Refer to the documentation provided by your SP and IdP for information on how to set up federated authentication using SAML or WS-Fed.
- **Standalone Sentry enabled for AppTunnel**
  By default, Ivanti Access trusts all AppTunnel traffic.
  Required only for Ivanti Access + Standalone Sentry deployment.
- **Ivanti Tunnel or AppConnect**
  Ivanti Access control for managed apps requires Ivanti Tunnel. Access control for AppConnect apps requires either Ivanti Tunnel or AppTunnel.
  AppTunnel is supported only with an Ivanti Access + Standalone Sentry deployment.
- **App distribution**
  Managed apps are distributed through Ivanti EPMM or Ivanti Neurons for MDM.

For related documentation, see the following:

- Ivanti EPMM documentation
  For information on how to set up AppTunnel, AppConnect, Ivanti Tunnel, and app distribution see the following documents: at:
  - For information on how to setup AppTunnel see the *Sentry Guide* at Sentry Product Documentation.
  - For information on how to configure Ivanti Tunnel see *Ivanti Tunnel Guide* at Ivanti Tunnel for Android Product Documentation
  - For information on how to set up an AppConnect app and how to distribute managed apps using Ivanti EPMM, see the following at AppConnect Guide.
    Ensure that the Ivanti Tunnel (iOS) VPN setting is selected in the app configuration for non-AppConnect apps.
- Ivanti Neurons for MDM documentation
  For information on how to set up AppTunnel, AppConnect, Ivanti Tunnel, and app distribution on Ivanti Neurons for MDM, see Ivanti Neurons for MDM Product Documentation or by clicking on Help in your Ivanti Neurons for MDM instance.

Overview of steps to set up Ivanti Access

The setup for Ivanti Access is done in the Ivanti Access administrative portal.

- Basic configuration
- Advanced configuration

- Split tunneling configuration
- Delegated IdP

Basic configuration

1. Get started with the set up.
   See Getting Started with Ivanti Access.
2. If your deployment uses Standalone Sentry, then register and assign Standalone Sentry to Ivanti Access.
   See Set up Ivanti Access + Standalone Sentry.
   OR
   If your deployment is Ivanti Access (without Standalone Sentry), set up integration with UEM.
   See Set up Ivanti Access with UEM.
3. Set up a cloud service provider (SP) and identity provider (IdP) federated pair.
   See Federated Pairs.
4. Upload Proxy metadata to the cloud service and identity provider.
   See Uploading proxy metadata.
5. Publish the profile.
   See Publishing a profile.
6. Verify traffic flow.
   See Verifying traffic flow.

Advanced configuration

1. Set up conditional rules for access control. Conditional rules allow you to define which applications and IP network ranges can access a cloud resource.
   See Conditional Access.
2. Set up session revocation, which allows you to terminate or revoke the session token if a device is out of compliance and the compliance action is blocked or a device is retired.
   See Session Revocation.
3. Set up mobile app single sign-on (SSO) to allow users to access enterprise cloud services from their managed mobile devices without having to enter passwords.
   See Configuring Mobile App Single Sign-on (SSO).
4. Set up Zero Sign-on to allow users access to enterprise cloud services from their unmanaged devices without having to enter passwords.
   See Zero Sign-on with Ivanti Access.
5. Set up multi-factor authentication using the UEM client to allow users to access their enterprise cloud services from an unmanaged device using multi-factor authentication in addition to their enterprise credentials.
   See Multi-factor Authentication with UEM Client.
6. Set up Ivanti Access desktop trust agent to verify and establish trust for unmanaged Windows 7 and Windows 10 desktops.
   See *Desktop Trust Agent Guide*.

Split tunneling configuration

In an Ivanti Access deployment, all authentication traffic for the federated pairs configured in Access goes through Ivanti Access using Ivanti Tunnel VPN. Depending on the type of Access deployment, all other traffic through Ivanti Tunnel VPN goes directly to

the destination server or through Standalone Sentry. Split tunneling allows you to control which traffic goes through Standalone Sentry to on-premise enterprise resources and which traffic goes directly to the destination.

For information about configuring Ivanti Access as the delegated IdP, see **Split Tunneling**.

Delegated IdP

In most cases, Ivanti Access is deployed as an intermediary between the service provider (SP) and the identity provider (IdP). In such a deployment, Ivanti Access acts as a proxy to the IdP and all federated SP traffic goes through Ivanti Access. In some cases, you may want to retain the existing SP-IdP federated setup, but deploy Ivanti Access to federate a sub set of the traffic, such as traffic from mobile devices. In such cases Ivanti Access can be deployed as a delegated IdP rather than as a proxy to the IdP.

For information about configuring split tunneling, see **Delegated IdP**.

Authentication options

With a basic Ivanti Access setup, when users initially attempt to log in to an enterprise cloud service from their managed device, they are prompted for their username and password. In addition, Ivanti Access allows you to set up various authentication options to allow your users ease of access from both managed and unmanaged devices to enterprise cloud services. The following table describes these options. See **Advanced configuration** for information on how to set up the various authentication options.

Feature	Purpose	Description
Mobile app single sign-on		
Native mobile application single sign-on (SSO)	Password less access from managed device.	Password less certificate-based single sign-on from managed devices. Users do not need to enter their username and password.
SaaS sign-on		
Zero Sign-on	Password less access from managed device.	Password less certificate-based single sign-on from managed devices. Users do not need to enter their username and password.
	Password less access from unmanaged devices.	A QR code is presented to users attempting to access a cloud service from their unmanaged device. Scanning the QR code with their managed device authenticates the user and allows access from the unmanaged device. Users have the option to enable push notifications or one-time passcode (OTP). If enabled, a push notification is sent to the managed device on subsequent logins from the unmanaged device. Alternately, users can use OTP. Users do not need to enter their username and password.
Multi-factor authentication	Ivanti Access from unmanaged devices.	Two factor authentication allows users to access cloud services from unmanaged devices. Users enter their username and password on the unmanaged device. A push notification is sent to the user's managed device. If accepted, users can access the cloud service from their unmanaged device. Alternately, users can use OTP.
Desktop trust agent		
Desktop trust agent	Ivanti Access from unmanaged Windows 7 and Windows 10 desktops.	The desktop trust agent verifies and establishes trust for unmanaged Windows 7 and Windows 10 desktops, thus allowing access to cloud services

4. Getting Started with Ivanti Access

The following topics let you configure Ivanti Access:

- Before you set up Ivanti Access
- Working with Ivanti Access administrative portal
  - Changing the password
  - Resetting the password recovery key
  - Configuring 2-step verification
- Working with Ivanti Access in Ivanti Neurons for MDM administrative portal
  - Changing the Password for Ivanti Neurons for MDM portal
  - Admins
- Ivanti Access Global Dashboard

4.1. Before you set up Ivanti Access

Verify that you have the following items before configuring Ivanti Access.

- **Deployment Type**
- **Federated authentication**
- **Ivanti Access credentials**
- **Standalone Sentry information**
  Gather Standalone Sentry information if you plan to have Standalone Sentry in your Ivanti Access deployment.
- **Certificates for Ivanti Access + Standalone Sentry**
- **Signing certificate**

Deployment Type

Ivanti Access supports deployment with Standalone Sentry or Ivanti Access (as a service). Before you begin with Ivanti Access, ensure that you understand the deployment types.

For more information, see **Ivanti Access overview**.

Federated authentication

Ivanti Access supports federated authentication using SAML and WS-Federation.

Before you begin with Ivanti Access, ensure that you are able to login to every service provider you intend to use with Access using federated identity from your identity provider(s).

> Federated authentication setup is not required for implementing certificate-based SSO with Ivanti Access.

Ivanti Access credentials

When you sign up for Ivanti Access, an email is forwarded to you by your sales representative.

The email contains the following important information that you will need for accessing the system:

- URL for the Ivanti Access administrative portal
- local administrator login credentials

Be sure to retrieve the information in the email before proceeding.

Root Admin credentials lets you perform the following tasks:

- Sign in to Ivanti Access administrative portal
- Create cloud service provider (SP) and identity provider (IdP) federated pairs
- Set up access control rules
- User management
- Activate or deactivate admins
- Self Serve

- Configuration Management
- Analytics and Dashboard
- Register Standalone Sentry
- View reports

Standalone Sentry information

If your deployment is Ivanti Access + Standalone Sentry, add a secondary hostname to the Standalone Sentry you use for access control. The primary DNS FQDN is reserved for Standalone Sentry for AppTunnel. The secondary hostname will be reserved for the Access module on the Standalone Sentry. You will use the second hostname when you first log in to the Ivanti Access administrative portal and go through the setup wizard.

Certificates for Ivanti Access + Standalone Sentry

Ensure that you have an SSL certificate to use with Ivanti Access. You will also require signing certificates when you set up a cloud service provider (SP) and identity provider (IdP) federated pair.

SSL certificate for Ivanti Access

The SSL certificate must be in PKCS 12 format and issued by a publicly trusted certificate authority (CA). The issuer can be an intermediate or root CA. The common name (CN) in the certificate must be exactly the same name as the second hostname reserved for the Access module on Standalone Sentry. You will upload this certificate when you go through the setup wizard.

Generating an SSL certificate (PKCS12 file) for Ivanti Access

If you don't already have a PKCS12 file, you can use OpenSSL to generate a PKCS12 file. Ignore this section if you already have a PKCS12 file.

Execute the following commands to generate a PKCS12 file:

1. Generate a certificate signing request (CSR) to submit to a certificate authority (CA). Enter the following command in OpenSSL:

   openssl req -out CSR.csr -new -newkey rsa:2048 -nodes -keyout privateKey.key
2. Forward the CSR.csr file to the CA for signing.The CA returns a .crt (example: certificate.crt) file.
3. Combine the certificate and private keys into a PKCS12 file.
   To combine the certificate and private keys into a PKCS12 file, enter the following OpenSSL command:

   openssl pkcs12 -export -out certificate.p12 -inkey privateKey.key -in certificate.crt -certfile CACert.crt
   - CACert.crt contains the CA's cert chain that signed certificate.crt.
   - You must upload certificate.p12 in the Ivanti Access administrative portal.
   - You will be asked for an export password. You will use the export password when you upload the certificate in Ivanti Access.

Signing certificate

Ivanti Access uses signing certificates to sign authentication requests and SAML assertions. A default signing certificate specific to your Access instance is automatically provided. When you set up a federated pair in the Ivanti Access administrative portal, you are also provided with the option to either generate a new signing certificate or upload a certificate of your choosing. If you do not want

to use the default certificate, you can use the option to generate or upload a new certificate. For more information, see **Federated Pairs**.

> The SSL certificate should not be used in lieu of a signing certificate.

4.2. Working with Ivanti Access administrative portal

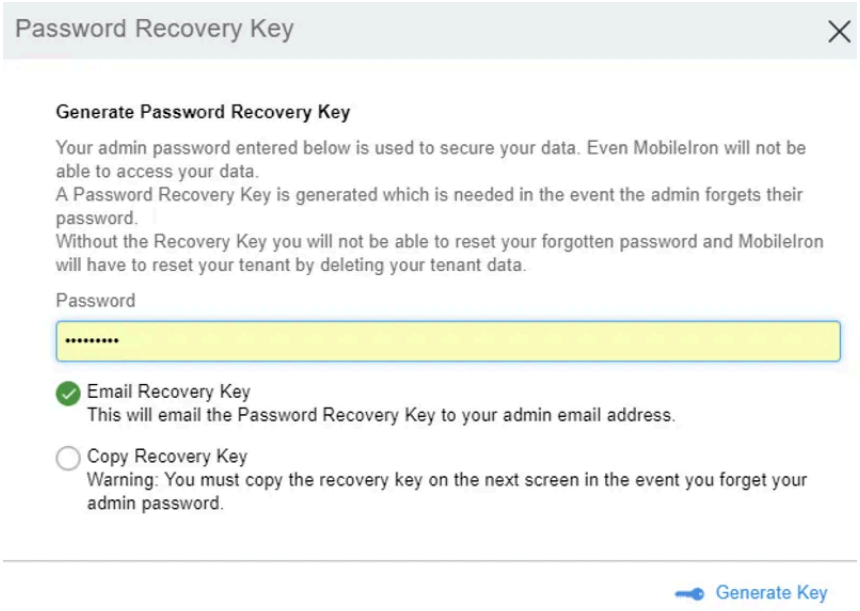
You can access the Ivanti Access administrative portal from a web browser. Use the credentials provided in the welcome email to sign in to the Ivanti Access administrative portal.

If you wish to use the new user interface, see **Working with Ivanti Access in Ivanti Neurons for MDM administrative portal**.

Procedure

1. In a supported browser, enter the Access URL provided in the welcome email.
   Example: https://access-na1.ivanti.com
   The URL may vary depending on the region.
   Administrator accounts lock temporarily for a short period after multiple consecutive invalid password attempts on initial log in.
2. For Username, enter the email address provided in the Welcome email.
3. For Password, enter the password provided in the Welcome email.
4. Click Sign In. The **Change Password** window displays.
   Figure 1. Change password

5. For Current Password, enter the password provided in the Welcome email.
6. For New Password, enter a new password.
7. For Confirm New Password, re-enter the same password that was used for New Password and click **Done**. The log in screen appears. Enter the new credentials to log in to Ivanti Access.
8. Enter the new password to log in to Ivanti Access.
   The **Password Recovery Key** window displays, which provides options for receiving the password recovery the key.
   Figure 2. Password recovery key



1. Enter the **New Password** in the text box.
2. Select one of the following options to backup your Recovery Key.
   - Email Recovery key: This option lets you email the Password Recovery Key to your administrator email address.

- Copy Recovery key: This option lets you copy the Password Recovery Key to a file in your local drive. A warning to receive an email for recovery key appears when you click Copy Recovery Key option.
  Figure 3. Warning for password recovery key

  After login, if you forget your password, click Account Settings > **Change Password**. The window to change your password opens. You must use the password recovery key to change your password.

If you forget your password and lose your password recovery key, you will not have access to the Access administrative portal. Contact the Root Admin or the Super Admin to reset the password. If the Root Admin forgets the password, contact Support.

11. Click **OK** > **Generate Key**.
12. Click Continue to get started with the setup wizard.
13. Click Get Started to select the preferred deployment type.
    The screen to select Ivanti Access or Ivanti Access + Standalone Sentry appears.
    Once you select the deployment type and click Done, you will not have the option to change your selection.
14. Click Done.
15. Click to start configuring account settings.
    The email for the administrator account and the Tenant GUID is visible.

Next steps

- For an Ivanti Access (without Standalone Sentry) deployment, see **Set up Ivanti Access with UEM**.
- For an Ivanti Access + Standalone Sentry deployment, see **Set up Ivanti Access + Standalone Sentry**.

Related topics

- **Changing the password**
- **Resetting the password recovery key**
- **Configuring 2-step verification**
- **Ivanti Access Global Dashboard**

4.2.1. Changing the password

After you initially sign in to the Ivanti Access administrative portal using the credentials provided by Ivanti, you may want to change the password. Your enterprise security policies may require you to change your password periodically.

When you attempt to enter a password for more than six times, the account is locked. You must wait for sometime to log in again.

> After login, if you forget your password, click Account Settings > **Change Password**. The window to change your password opens. You must use the password recovery key to change your password.

Procedure

1. In the Ivanti Access administrative portal, click Account Settings > Change Password.

The Change Password dialog appears.

2. For Current Password, enter the current password.
3. For New Password, enter the new password.
4. For Confirm New Password, re-enter the new password.
5. Click Done.

Password requirements

A new password must match the following requirements:

- Password length should be between 8 and 32 characters
- No spaces
- Not more than 2 identical characters in a row (For example: 111 not allowed)
- Sequential characters are not allowed (For example: 123 or abcde)
- At least one lower case letter (a-z)
- At least one upper case letter (A-Z)
- At least one number (0-9)
- At least one symbol [~ ! @ # $ % ^ & * ( ) _ + : ; < > ? { } [ ] |]

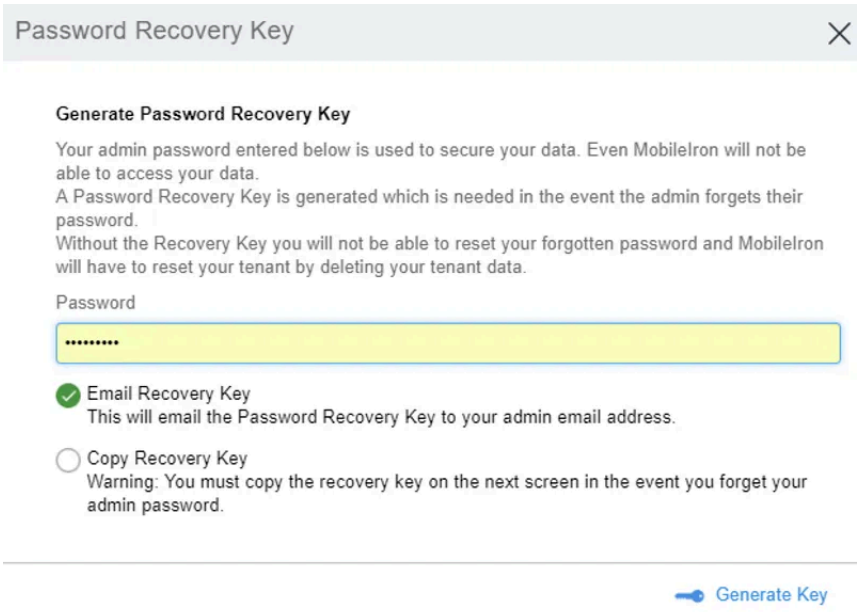
4.2.2. Resetting the password recovery key

You can change the password recovery key in the Ivanti Access administrative portal.

Procedure

1. In the Ivanti Access administrative portal, click Account Settings > Reset Password Recovery Key.

The Password Recovery Key dialog appears.



2. Enter your password in the text box.
3. Select one of the following options to backup your Recovery Key.

- Email Recovery key: This option emails the Password Recovery Key to your admin email address.
- Copy Recovery key: This option lets you copy the Password Recovery Key to a file in your local drive.

You can use this key to recover your password in case you forget the password.

4. Click **Generate Key**.

> If you forget your password and lose your password recovery key, you will not have access to the Ivanti Access administrative portal.

Resetting your password

The password recovery key is required to reset the password from the log in screen. However, when a tenant logs in, recovery key is not required to reset the password. You cannot reuse the last three passwords including the current password when you reset a password.

Procedure

1. On the Ivanti Access Log in page, click Reset Password.

You will be prompted to create a new password.

2. For Username, enter your username.

3. For Recovery Key, enter your password recovery key.

You can copy and paste the key.

4. For New Password, enter a new password.

5. For Confirm New Password, re-enter the new password.

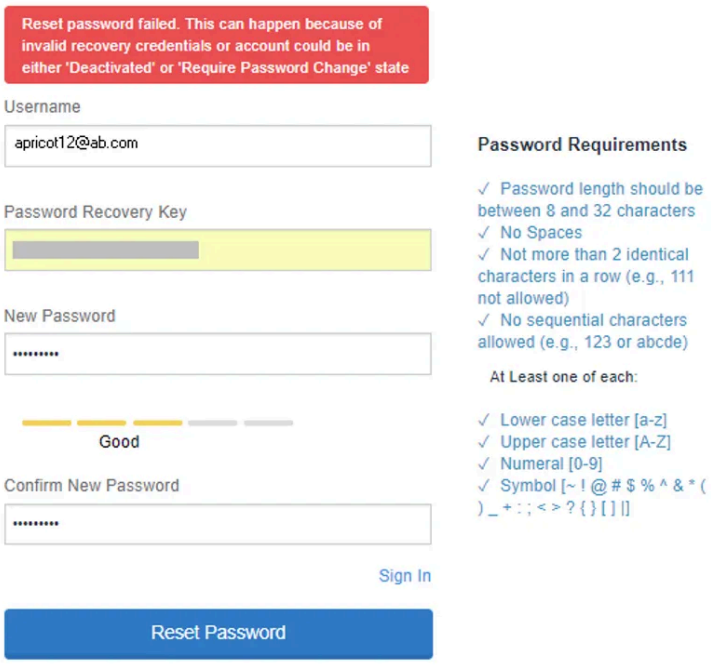
6. Click on Reset Password.

You will be returned to the Sign In dialog.

7. Enter the new password to sign in to the Ivanti Access administrative portal.

Resetting your password can sometimes fail for the following reasons. Ensure that you check the error and verify the reason.

- Invalid recovery credentials
- Account could be in either 'Deactivated' or 'Require Password Change' state



4.2.3. Configuring 2-step verification

2-Step verification adds another layer of security that requires not only a password and user name but also a verification code to sign in to the Access administrative portal. The verification code is generated by either Authenticator or Google Authenticator. You configure 2-step verification in the Ivanti Access administrative portal.

You can enable 2-step verification only for your account. You cannot enable 2-step verification for other administrators or vice versa. If 2-step verification is enabled, you are prompted to enter your credentials and the verification code to access Access account. If the verification code is not available, you cannot sign in to the Ivanti Access administrative portal.

- 2-Step verification with Google Authenticator is supported on iOS and Android devices. 2-Step verification with Authenticator is supported only on iOS devices.
- If 2-Step verification fails, verify if your device is in sync with the local time

Before you begin

- Verify that you have created an Ivanti Access account.
- For iOS devices, verify that you have downloaded the Authenticator app or Google Authenticator app from iOS App Store .

OR

For Android devices, verify that you have downloaded the Google Authenticator app from Android Google Play Store.

Procedure

1. In the Ivanti Access administrative portal, click Account Settings > 2-Step Verification.
2. Click the **Off** toggle.

A **Warning** is displayed.

3. To configure 2-step verification, click **Continue,** then Next.

A QR code is displayed.

Figure 1. QR code for 2-step verification

4. On your device, launch the authenticator app.
5. From the authenticator app, scan the QR code displayed in Ivanti Access.

Alternately, for Google Authenticator only, click the Enter Time based Secret Key link to generate a secret key. Enter the generated secret key in Google Authenticator. The secret key is unique to every verification.

A 6-digit code is generated in the authenticator app.

6. In the Ivanti Access administrative portal, click Next to enter the 6-digit code.

Figure 2. Enter 6-digit code



7. In Enable 2-Step Verification enter the 6-digit code.
8. Click Done.

To verify whether 2-step verification is on or off, in Access, go to **Settings** > **Admins**. The 2-Step Verification column displays the status.

To generate a verification code for 2-step verification for signing in to Ivanti Access:

- If you are using Google Authenticator, launch the app.
- If you are using Authenticator, launch the app, and go to Settings > Admin OTP.

Disabling 2-Step Verification

Administrators can disable 2-step verification for their own account only. However, a Super Admin can disable 2-step verification for an Admin or Read Only Admin. If an administrator with Admin or Read Only Admin role loses their phone or has issues with 2-step verification, they can contact their Access Super Admin to reset 2-step verification for their account. If a Super Admin is not available, contact Ivanti Support. An email notification is sent to the administrator if a Super Admin or Ivanti Support disables 2-step verification for an account. However, email notification is not sent when administrators disable the 2-Step Verification for their own account. For more information about administrator roles, see **Admins**.

2-Step verification can be disabled from Account Settings > 2-Step Verification in the admin portal.

Before you begin

- Verify that 2-Step Verification is enabled.

Procedure 1

1. In the Access administrative portal, go to Account Settings > 2-Step Verification.
2. Click the toggle to change the setting to **OFF**.

Procedure 2

1. In the Access administrative portal, click **Settings** > **Admins**.
2. Click the toggle in the 2-Step Verification column for your account to change the setting to **OFF**.

This method is not available to administrators with Read-only permission.

Signing out of the Ivanti Access administrative portal

If you do not sign out, the session will timeout in 30 minutes.

Procedure

1. In the Ivanti Access administrative portal, click Account Settings > Sign Out.

When you sign in to Access again, launch an authenticator app and generate a verification code. You will be prompted to enter the verification code in addition to your username and password.

4.3. Working with Ivanti Access in Ivanti Neurons for MDM administrative portal

You can access the Ivanti Access administrative portal from a web browser. If your deployment uses Ivanti Neurons for MDM, sign in with your Ivanti Neurons for MDM credentials. If your deployment uses Ivanti EPMM, use the credentials provided in the welcome email to sign in to the Ivanti Access administrative portal.

The features such as resetting the password recovery key and configuring 2-step verification are not supported for Access in the Ivanti Neurons for MDM administrative portal.

Procedure

1. In a supported browser, enter the URL for your Ivanti Neurons for MDM tenant.
   Example: https://na2.ivanti.com/login.html
   For Access: login.ivanti.com
   The URL will vary depending on your region.
2. Enter your Ivanti Neurons for MDM administrator account.
3. Click Sign In and enter the Password.
4. Click Sign In again.
   The Ivanti Neurons for MDM portal opens.
5. Click the Accesstab to view the admin portal.
6. Click Get Started to select the preferred deployment type.
   The screen to select Access or Access + Standalone Sentry appears.

Once you select the deployment type and click Done, you will not have the option to change your selection.

7. Select the deployment type as Access or Access + Standalone Sentry.

   Access is configured and the Access admin portal opens.

8. Click  to start configuring account settings.
   The email for the administrator account and the Tenant GUID is visible.

- For an Ivanti Access (without Standalone Sentry) deployment, see **Set up Ivanti Access with UEM**.
- For an Ivanti Access + Standalone Sentry deployment, see **Set up Ivanti Access + Standalone Sentry**

Account settings

Click Access > Account to view the links to documentation, support, your Access tenant GUID, your administrator account information, and links to change your password and sign out.

Related topics

- Changing the Password for Ivanti Neurons for MDM portal

4.3.1. Changing the Password for Ivanti Neurons for MDM portal

After you initially sign in to the Ivanti Neurons for MDM administrative portal using the credentials provided, you may want to change the password. Your enterprise security policies may require you to change your password periodically.

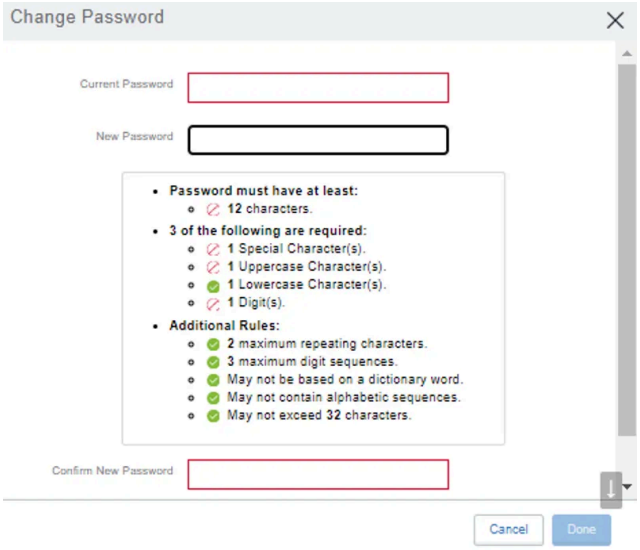
When you attempt to enter a password for more than six times, the account is locked. You must wait for sometime to log in again.

> I f you forget your password, click Forgot Password in the log in page. An email is sent to the user associated with the username with instructions to reset the password.

Procedure

1. In the Ivanti Access administrative portal, click Account Settings > Change Password.

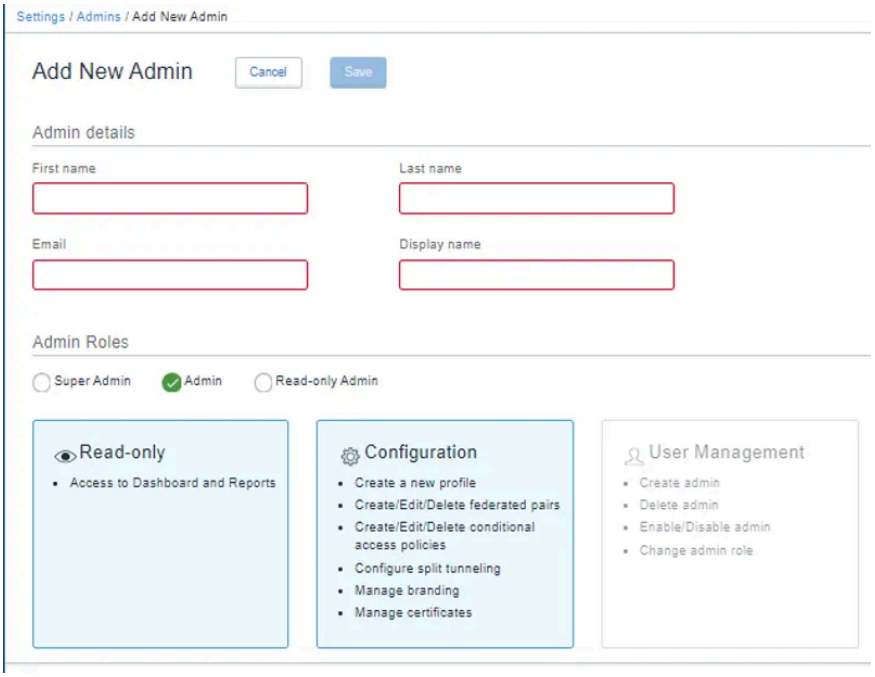
The Change Password dialog appears.



2. For Current Password, enter the current password.
   The password requirements are listed when you click to enter the password.
3. For New Password, enter the new password.
4. For Confirm New Password, re-enter the new password.
5. Click Done.

4.3.2. Admins

The **Admins** tab lets you create and delete profiles for administrators to manage the Ivanti Access portal. It also lets you activate and deactivate (enable or disable) the administrators.



> The Reset Password and 2-Step verification is not available for Admins with Access and Ivanti Neurons for MDM portal.

When a new Admin is created, you will receive an email with an activation link to reset the password.

Admins added in the Access tab will not have any Cloud role. They will only see the Access tab. Admins added in the Ivanti Neurons for MDM tab may have Access roles as well as Cloud roles depending on what they are assigned.



The following options are not available in the Ivanti Neurons for MDM portal:

- The Status column is not available for the Admin created.
- The reset admin password option is also removed in Ivanti Neurons for MDM portal.

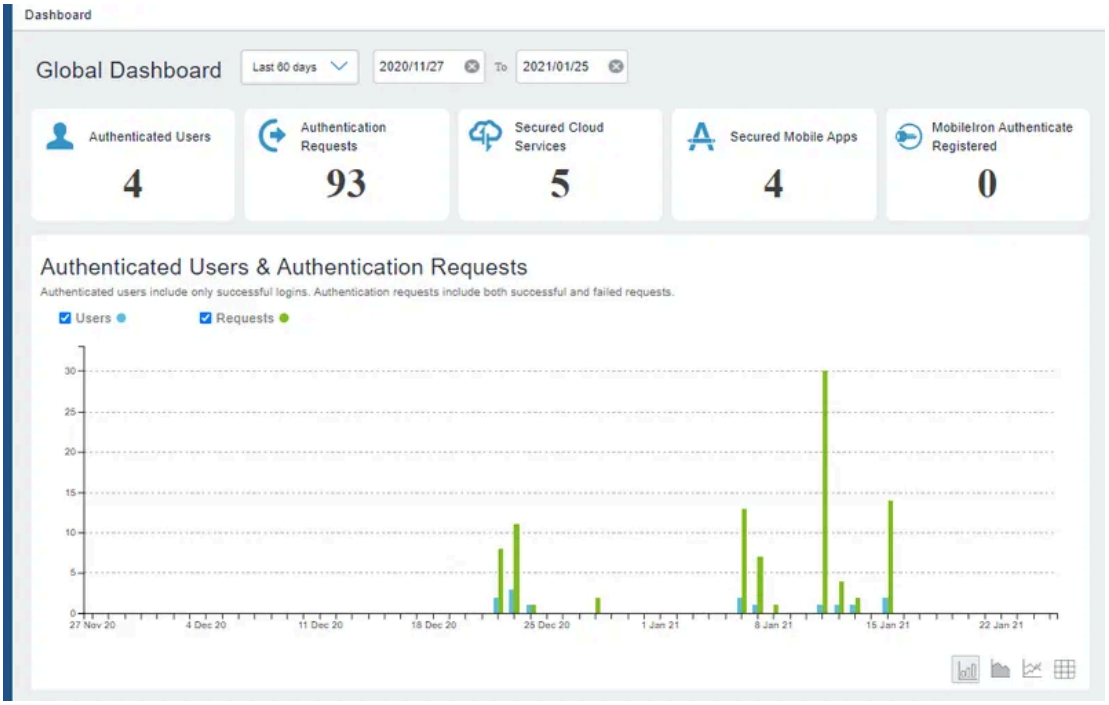
For more information on Adding an administrator, creating and deleting profiles, see **Admins**.

4.4. Ivanti Access Global Dashboard

The Ivanti Access Global Dashboard is designed to support data management. The dashboard is categorized into sections such as Authenticated Users, Authentication Requests, Secured Cloud Services, Secured Mobile Apps, Authenticated Users & Authentication Requests, Top Secured Services, Top Services By Authenticated Users, Mobile Apps Blocked, and Block & Allow Requests.

You can view the dashboard data for any preferred period. The dashboard displays real time data when the reports are submitted to Ivanti Access by Sentry. It takes about 15 minutes to refresh the data.

You can click on the trend graphs to fetch the overlay card for a preferred date. The overlay card displays the report for the appropriate date you selected. To view the complete report, click **View All Data**. The **Reports** tab displays the complete report.



Each data set on the dashboard can be viewed in multiple different graphical formats, such as a bar graph, line graph, pie graph, or in a tabular format. The tabular form also displays the time that the data is aggregated by Coordinated Universal Time (UTC).

Sections	Description
Authenticated Users	Provides the number of allowed or blocked users that are authenticated by the identity providers.
Authentication Requests	Provides the number of allowed or blocked requests that are targeting the cloud services. It also provides information about the requests that have processing exceptions.
Secured Cloud Services	Provides information about Federated Pairs. Each active Federated Pair is a service.
Secured Mobile Apps	Provides the number of unique applications that are accessed by the user.
Authenticate Registered	Provides the number of Authenticate registered desktops. It helps the admin view the percentage of desktops they intend to have registered and then accordingly admin can register more desktops.
Authenticated Users & Authentication Requests	Provides a graphical representation for the authenticated users and requests trends.
Top Secured Services	Provides the number of blocked requests based on the top secured services.
Top Services By Authenticated Users	Provides the number of authenticated users for every service.
Mobile Apps Blocked	Provides a graphical representation about the blocked services.
Allow, Block & Warn Requests	Provides a graphical representation about the allowed and blocked hits based on any appropriate combination such as Rule, SAML pair, and policies. It also provides information about the warn requests to secured cloud services using specific policies and rules.
Authentication by OS Platforms	Provides a graphical representation about the Service Provider actions by aggregate OS such as iOS, Android, Windows, Macintosh, Linux, and other unknown platforms.
Authentication by Managed Apps	Provides a graphical representation about the list of Managed Apps that are accessing the Service Provider. When a managed app that is not available in Ivanti Access database is accessed, a bar named Unknown is displayed in the graph. These apps will be monitored and added to the database in the future releases.

GeoIP Map

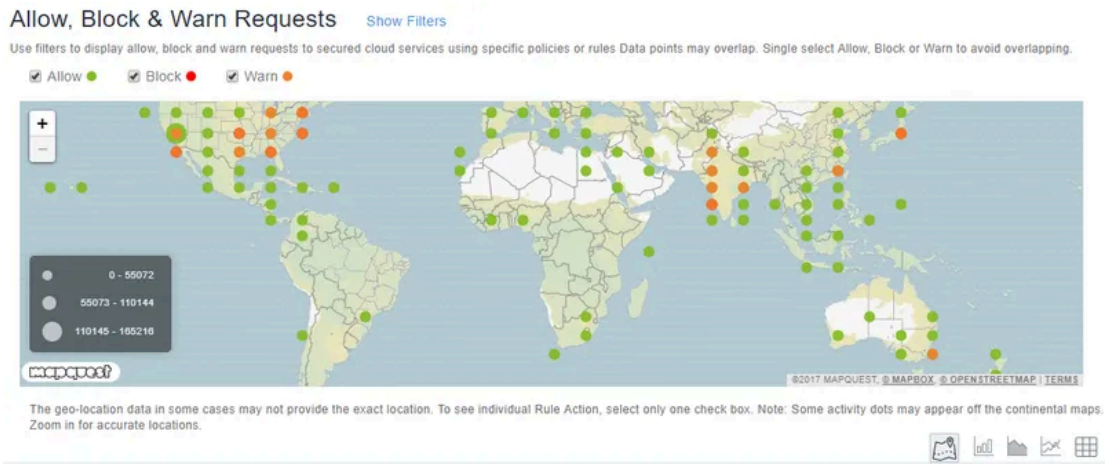
The Allow, block, and warn requests data to secured cloud services is available based on geolocation. In the Allow, Block, and Warn Requests section of the dashboard, click to view geolocation.

GeoIP identifies the location and other characteristics such as over lay card displaying IP address, username, time stamp of end users for a wide range of applications including content personalization, fraud detection, traffic analysis, and compliance. The GeoIP map provides the following features:

- Count of Allow/Block/Warn requests

- Zoom in and Zoom out to have better precision of the data
- Horizontal scrolling to view a particular section of the map
- Filters to narrow down the data set
- Checkboxes to select Allow, Block, or Warn requests
- The geolocation data in some cases may not provide the exact location.
- To see individual Rule Action, select only one check box.
- Some activity dots may appear off the continental maps. Zoom in for accurate locations.

Figure 1. Geolocation for allow, block, and warn requests



Viewing details for allow, block, or warn requests

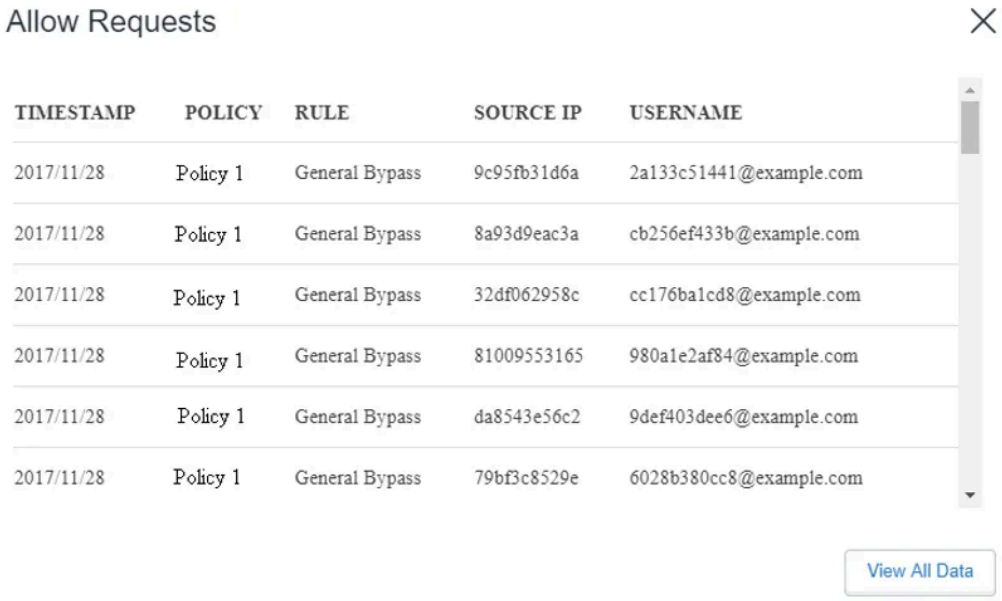
The Allow, Block, or Warn requests are displayed on the GeoIP map at various locations. You can determine the users logged in from a specific location to assess and mitigate the risks . Clarity is provided through reverse lookup. When you mouse over the Geo bubble, the callout which appears, displays the count of Allow, Block, and Warn requests.

Procedure

1. On the GeoIP map, click the Geo Bubble for Allow, Block, or Warn request.

The Allow Requests, Block Requests, or Warn Requests window displays based on your selection.

Figure 2. Request details



2. Click **View All Data**.

The Reports page opens to display the Geolocation details.

5. Set up Ivanti Access with UEM

Access integrates with a unified endpoint management (UEM) platform to get device posture and compliance information. To set up the integration, you configure Access integration in the UEM and verify the integration in Ivanti Access. The UEM are

- Ivanti EPMM
- Ivanti Neurons for MDM

You can integrate up to six Ivanti Neurons for MDM instances and multiple Ivanti EPMM servers (no limit) in your deployment.

> The configuration with UEM described in these sections only apply to Ivanti Access (without Standalone Sentry) deployments.

The following topics help you configure UEM and Ivanti Access:

5.1. Overview of configuration with Ivanti Neurons for MDM

Complete the following tasks to set up Ivanti Neurons for MDM integration with Ivanti Access:

1. Configuring Ivanti Access in Ivanti Neurons for MDM
2. Configuring Ivanti Neurons for MDM in Ivanti Access
3. Configuring Ivanti Tunnel in Ivanti Neurons for MDM

5.1.1. Configuring Ivanti Access in Ivanti Neurons for MDM

Set up Access on Ivanti Neurons for MDM.

Before you begin

- Make a note of the URL for your Access instance, and the Access administrator username and password. The URL for your Access instance is one of the following:

-	https://access-na1.mobileiron.com
-	https://access-eu1.mobileiron.com

- Ensure that you have Manage Ivanti Access Integration role in Ivanti Neurons for MDM.
- You have the credentials for the Ivanti Access administrator account you will use to set up Ivanti Access in Ivanti Neurons for MDM. Ivanti recommends creating a separate administrator account in Ivanti Access that is specifically used for UEM integration with Ivanti Access. Ensure that the account does not have 2-step verification enabled.

Procedure

1.	In Ivanti Neurons for MDM, go to Admin > Access.

Figure 1. configure ivanti access on ivanti neurons for mdm

2.	Enter the following:
-	Access Admin URL: URL for Access
-	Access Admin Username: User name for the Access administrator account you created for Access integration.
-	Access Admin Password
3.	Click Register.

Ivanti Access is registered with Ivanti Neurons for MDM and the following displays:

Figure 2. ivanti access registration



Next steps

Configuring Ivanti Neurons for MDM in Ivanti Access.

Related topics

See the *Ivanti Neurons for MDM Guide* for information about setting roles.

5.1.2. Configuring Ivanti Tunnel in Ivanti Neurons for MDM

Ivanti Tunnel creates a secure connection between the managed device and Ivanti Access for authenticating users accessing enterprise cloud resources.

Before you begin

- Add a Certificate Authority and create an Identity Certificate setting in Ivanti Neurons for MDM.
  - Add the Certificate Authority in Admin > Certificate Authority.
  - Create an Identity Certificate setting in Configuration > Add > Identity Certificate.
    For Certificate Distribution, select Dynamically Generated and for Source, select the certificate you configured in Admin > Certificate Authority.
- If you were using a Sentry profile to configure Ivanti Access in Ivanti Neurons for MDM, reconfigure your setup to use an Access profile before deploying Ivanti Tunnel 3.1.0 for iOS through the most recently released version as supported by Ivanti. To set up an Access profile, see **Configuring Ivanti Access in Ivanti Neurons for MDM**.
- For Android enterprise, app configuration is done when adding the app to the UEM for distribution. The following procedure applies to all supported OS except Android enterprise. However, configuration information provided in this procedure also applies when you configure Android enterprise. For information on how to add Ivanti Tunnel for Android enterprise to Ivanti Neurons for MDM, see the relevant section in the *Ivanti Tunnel Guide*.
  If you are configuring Ivanti Tunnel for Android enterprise and using Access Profile only, Ivanti recommends adding configuring AllowedAppList to specify the apps for which authentication traffic goes through Ivanti Tunnel.

Procedure

1. In Cloud, go to Configurations > +Add.
2. Search for Ivanti Tunnel and click Ivanti Tunnel.
3. Select the OS type for the configuration.
4. Create a separate Ivanti Tunnel configuration for each OS type.
5. Enter a name for the configuration.
6. Select one of the following:
7. Access Profile Only - Select if Ivanti Tunnel traffic goes only to Access.
8. Sentry + Access Profile - Select if Ivanti Tunnel VPN supports both traffic to Access for authentication to enterprise cloud resources and through Standalone Sentry to on-premise enterprise resources. This option is available for iOS and Android only.
9. If you selected Sentry + Access Profile for profile mode, select the Sentry profile and the iOS or Android service you created in the Sentry profile.
10. For Ivanti Tunnel for Android configuration, do the following:
11. For Client Cert. Alias, for Ivanti Tunnel for Android only, select the same certificate configuration you select for SCEP Identity.
12. For SCEP Identity, select the Identity Certificate configuration you created for Ivanti Tunnel.
13. For Ivanti Tunnel for Windows 10 configuration, do the following:
14. For SCEP Identity, select the Identity Certificate configuration you created for Ivanti Tunnel.
15. For Define Ivanti Tunnel App Settings, select Advanced.

16. Enter the following key-value pairs:

Key	Value
AppTriggerList/0/App/Id	App Id that will trigger Ivanti Tunnel. Example: %PROGRAMFILES% (x86)\Google\Chrome\Application\chrome.exe
TrafficFilterList/0/App/Id	App Id that will tunnel traffic through Ivanti Tunnel. Example: %PROGRAMFILES% (x86)\Google\Chrome\Application\chrome.exe
RouteList/0/Address	If your Cloud tenant is *.access-na1.mobileiron.com enter: 18.232.253.154 If your Cloud tenant is *.access-eu1.mobileiron.com enter: 18.194.253.44
RouteList/0/PrefixSize	32
TrafficFilterList/0/RoutingPolicyType	SplitTunnel
RouteList/1/Address	If your Ivanti Neurons for MDM tenant is *.access-na1.mobileiron.com enter: 18.232.30.29 If your Ivanti Neurons for MDM tenant is *.access-eu1.mobileiron.com enter: 18.194.99.243
RouteList/1/PrefixSize	32

10. Leave all defaults as is and click Next.

If you are configuring Ivanti Neurons for MDM and Ivanti Tunnel for Android enterprise and using Access Profile only, Ivanti recommends adding configuring AllowedAppList to specify the apps for which authentication traffic goes through Ivanti Tunnel.

11. Select the distribution for the configuration and click Done.
12. In Ivanti Access,
13. Navigate to the UEM tab.
14. Select the Ivanti Neurons for MDM UEM and click the Sync UEM button.
15. Enter the credentials and click Verify and Done.

This step is required to pull the Ivanti Tunnel certificates from the UEM and established trust between Ivanti Tunnel and Ivanti Access.

Next steps

1. Add Ivanti Tunnel to Ivanti Neurons for MDM. For information on how to add Ivanti Tunnel to Ivanti Neurons for MDM, see the relevant section in the *Ivanti Tunnel Guide* for the device OS.

2. Set up SP and IdP federated pairs.

See **Service provider (SP) metadata** and **Identity provider (IdP) metadata**.

Related topics

For more information about configuring and distributing Ivanti Tunnel see the *Ivanti Tunnel Guide* for the OS.

5.1.3. Configuring Ivanti Neurons for MDM in Ivanti Access

You configure your Access tenant in Ivanti Neurons for MDM and verify the integration in Ivanti Access in the UEM tab.

Before you begin

Ensure the following:

- Your Ivanti Access tenant is configured in Ivanti Neurons for MDM. See **Configuring Ivanti Access in Ivanti Neurons for MDM**
- You have the credentials for the Ivanti Neurons for MDM administrator account you will use to verify the connection from Ivanti Access to Ivanti Neurons for MDM. Ivanti recommends creating a separate administrator account in Ivanti Neurons for MDM that is specifically used for UEM integration with Access. Ensure that the account,
  - is a single user, not an API user.
  - has Access administrator, Common Platform Service (CPS), and Device Read Only roles.

Procedure

1. Click UEMon the left navigation pane in Ivanti Access.

Figure 1. UEM tab



2. In UEMs tab, click Connect to Verify to complete the UEM registration process.
   The Verify UEM Tenant window appears.

Figure 2. Verify UEM Tenant



3. Enter the following:

- UEM Username: User name for the Ivanti Neurons for MDM administrator account you created for Access integration.
- UEM Password: Password for the administrator account.

The following status displays in Access based on the connection:

Status	Description
Connected	Ivanti Access and Ivanti Neurons for MDM are connected.
Not Verified	The Ivanti Neurons for MDM Credentials are not verified by Access. Enter the credentials to complete the workflow.
Deregistered	Ivanti Access is deregistered.
Unreachable	Server is unable to connect to Ivanti Neurons for MDM.
Incorrect Password or Permissions	The UEM permissions or password is incorrect.

4. Click Verify.
5. Click Done.

6. Select the host added and click Sync UEMin the right-pane.
   This action fetches the Ivanti Tunnel profiles from UEM and pushes to gateway.

Next steps

Configure Ivanti Tunnel in Ivanti Neurons for MDM. See **Configuring Ivanti Tunnel in Ivanti Neurons for MDM**.

5.2. Overview of configuration with Ivanti EPMM

Set up Ivanti EPMM integration with Ivanti Access configuration in the following order:

- Configuring Ivanti Access in Ivanti EPMM
- Configuring Ivanti Tunnel in Ivanti EPMM
- Configuring Ivanti EPMM in Ivanti Access

5.2.1. Configuring Ivanti Access in Ivanti EPMM

Configure Ivanti Access in Ivanti EPMM.

Before you begin

- Add a Certificate Enrollment setting in Ivanti EPMM. You will upload the associated CA certificate in Access to establish trust between Ivanti Tunnel and Ivanti Access.

For more information about Certificate Enrollment settings, see the *Ivanti EPMM Device Management Guide* for your device operating system. For Android enterprise, see the Ivanti EPMM Device Management Guide for Android.

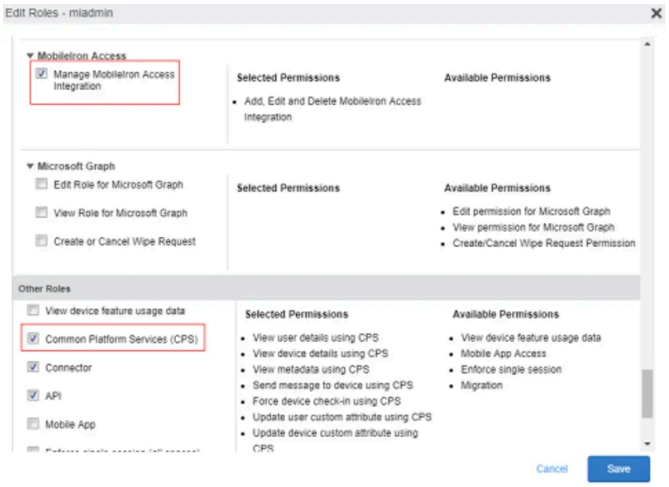
- Ensure that you have Manage Ivanti Access Integration and Common Platform Services (CPS) roles enabled in Ivanti EPMM. To enable roles, in the Ivanti EPMM Admin Portal, go to Admin > Admins > select the administrator > click Actions > Edit Roles.

After updating roles, sign out and then sign in again to the Ivanti EPMM Admin Portal for the changes to take effect.

- Ensure that 2-step verification is turned off for the administrator in Access.
- Make a note of the URL for your Access instance, and the Access administrator username and password. The URL for your Access instance is one of the following:

-	https://access-na1.mobileiron.com
-	https://access-eu1.mobileiron.com

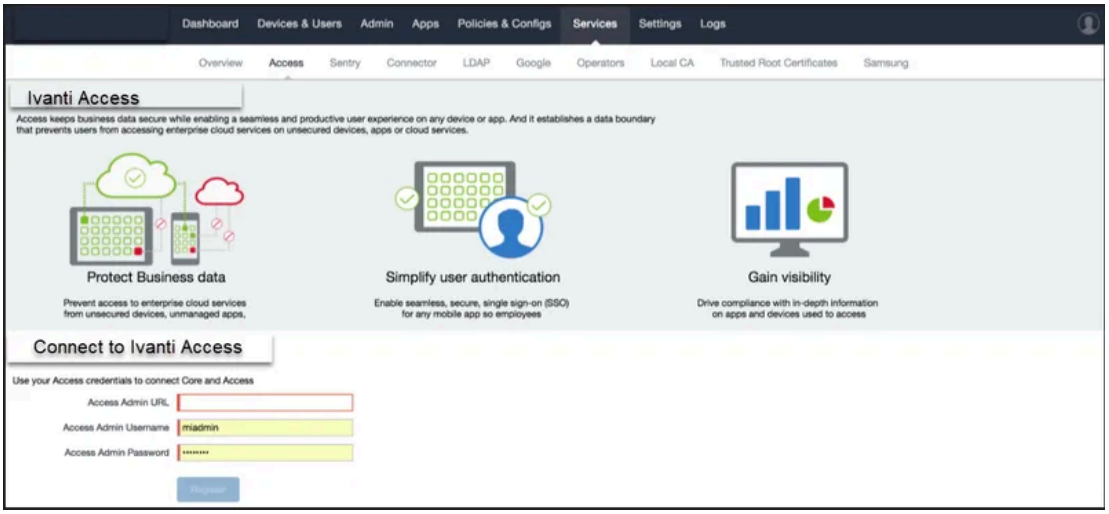
Figure 1. adding roles in ivanti epmm



Procedure

1.	In the Ivanti EPMM Admin Portal, go to Services > Access.

Figure 2. configure access



	2.	Enter the following:
	-	Access Admin URL: URL for Access.
	-	Access Admin Username: Username for an Access administrator.
	-	Access Admin Password.
	3.	Click Register.

Access is registered with Ivanti EPMM.

Figure 3. access registration



Next steps

Configure Ivanti Tunnel in Ivanti EPMM for Ivanti Access. See **Configuring Ivanti Tunnel in Ivanti EPMM**.

5.2.2. Configuring Ivanti Tunnel in Ivanti EPMM

Ivanti Tunnel creates a secure connection between the managed device and Ivanti Access for authenticating users accessing enterprise cloud resources.

Before you begin

- Ensure that you have registered Ivanti Access with Ivanti EPMM.
- Ensure that you have added Ivanti Tunnel to Ivanti EPMM.

For information on how to add Ivanti Tunnel to Ivanti EPMM, see the relevant section in the *Ivanti Tunnel Guide* for the device OS.

Procedure

1. In Ivanti EPMM, go to Polices & Configs > Configurations.
2. Click Add New > VPN.

Figure 1. add ivanti tunnel vpn setting

3. For Connect Type, select the Ivanti Tunnel or Ivanti Tunne(Android).

Create a separate Ivanti Tunnel configuration for each OS type.

4. Enter a name for the configuration.
5. Select the check box for Enable Access.
6. For Identity Certificate, select the Certificate Enrollment configuration you created earlier to establish trust between Ivanti Tunnel and Ivanti Access.
7. Click Save.

- The Enable Access setting is also available in the AppConnect App Configuration and Web@Work configuration. The setting allows these apps to direct authentication traffic to Access. The setting is available only if Services > Access is configured in the Ivanti EPMM Admin Portal. Otherwise, the setting is grayed out.
- Federated traffic from Docs@Work through Access is only supported with Ivanti Tunnel. However, using Ivanti Tunnel to CIFs services will fail. Federated traffic through AppTunnel and an Ivanti Access (without Standalone Sentry) deployment is not supported for Docs@Work. Selecting Enable Access in the Docs@Work configuration does not have an impact.
- Google Apps (GApps) require Chrome to direct authentication traffic through Ivanti Access.

Next steps

Configure Ivanti Access in Ivanti EPMM. See **Configuring Ivanti EPMM in Ivanti Access**.

5.2.3. Configuring Ivanti EPMM in Ivanti Access

The Ivanti EPMM with which Ivanti Access integrates is configured in the UEM tab in Ivanti Access.

When Ivanti EPMM is in maintenance, you must configure the load balancers to return 503 , Service Unavailable.

Before you begin

- Ensure that you have completed the steps detailed in the following:

- Configuring Ivanti Access in Ivanti EPMM

- Configuring Ivanti Tunnel in Ivanti EPMM

- Make a note of the following:

- FQDN for Ivanti EPMM.

- The username and password for an administrator with Common Platform Services (CPS) and Device Read Only roles in Ivanti EPMM.

- Ivanti recommends creating a separate administrator account in Ivanti EPMM that is specifically used for UEM integration with Access.

Procedure

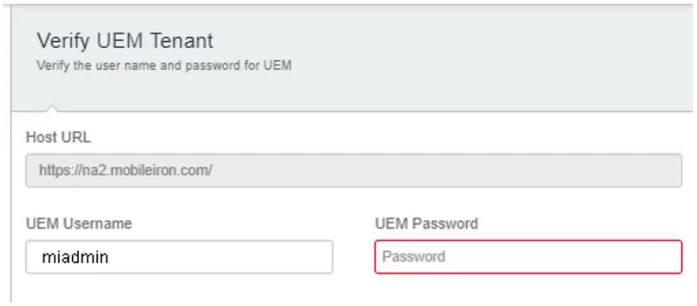
1. Click UEM on the left navigation pane in the Ivanti Access administrative portal.

The UEM panel with the host details appears.

2. Click Connect to Verify either in the UEM Username column or in the right hand panel.

The Verify UEM Tenant window appears.

Figure 1. Verify UEM Tenant



3. Enter the following details:

- Host URL:The fully qualified domain name (FQDN) of Ivanti EPMM.

The field is automatically populated and not editable.

-	UEM Username: A user with Common Platform Services (CPS) and Device Read Only roles assigned in Ivanti EPMM.

	-	UEM Password

The following status is displayed in Ivanti Access based on the connection:

Status	Description
Connected	Access and Ivanti EPMM are connected.
Not Verified	The Ivanti EPMM Credentials are not verified by Access. Enter the credentials to complete the workflow.
Deregistered	Access is deregistered.
Unreachable	Server is unable to connect to Ivanti EPMM.
Incorrect Password or Permissions	The UEM permissions or password is incorrect.

	4.	Click Verify.

The Ivanti Tunnel certificate is pulled and establishes trust between Ivanti Tunnel and Ivanti Access.

	5.	Click Done.

Next steps

Set up SP and IdP federated pairs. See **Federated Pairs**.

5.3. Deregistering Ivanti Access from UEM

To stop using Ivanti Access with UEM, deregister the Access profile configured in the UEM and delete the UEM in Ivanti Access.

> Deregistering the Access profile in UEM and deleting the UEM in Access can be done in any order. It is, however, important to do both.

Before you begin

- Ensure that the Access profile in UEM is no longer in use and that there is no data associated with the profile. This means that Enable Access is disabled in any Iavnti Tunnel VPN profile, AppConnect App Configuration, Docs@Work, or Web@Work configuration.

Procedure

1. In the UEM, navigate to the Access profile.

In the Ivanti EPMM Admin Portal, go to Services > Access.

In Ivanti Neurons for MDM, go to Admin > Infrastructure > Access.

2. Click Deregister to remove the Access profile.

A Deregister Access Profile window displays.

3. Depending on your UEM, click Confirm or Deregister Access Profile to deregister.

Enter the Access Admin Username and Password to deregister.

4. In the Access administrative portal, click UEM.

5. Click Deletein the right panel to remove UEM.

The Delete UEM window appears.

6. Click Delete UEM.

UEM is removed from Ivanti Access.

6. Set up Ivanti Access + Standalone Sentry

In Access + Standalone Sentry deployment, Access gets device posture and compliance information from Standalone Sentry. To make Standalone Sentry known to Access, register Standalone Sentry to Access, then assign the Sentry to the Access profile.

> Standalone Sentry registration and setup is not applicable to a Access (as a service) deployment. Skip this section if you are deploying Access (as a service).

Overview of steps to set up Ivanti Access + Standalone Sentry

The following describe the tasks to set up Ivanti Access + Standalone Sentry:

- **Adding a profile**
- **Registering a Standalone Sentry**
- **Assigning Standalone Sentry to a profile**

6.1. Adding a profile

If you selected Ivanti Access + Standalone Sentry, the Add Profile screen appears. Use the Profile page to create a profile for Ivanti Access and set up Ivanti Access + Standalone Sentry.

Before you begin

- The certificate must be signed by a trusted third-party CA, and must have its associated private key as part of the PKCS 12 file.
- The certificate must comply with security requirements. See Error conditions for SSL certificate. For more information about error conditions, see **Adding a profile** . If the SSL certificate does not comply with the security requirements, then the following error displays.

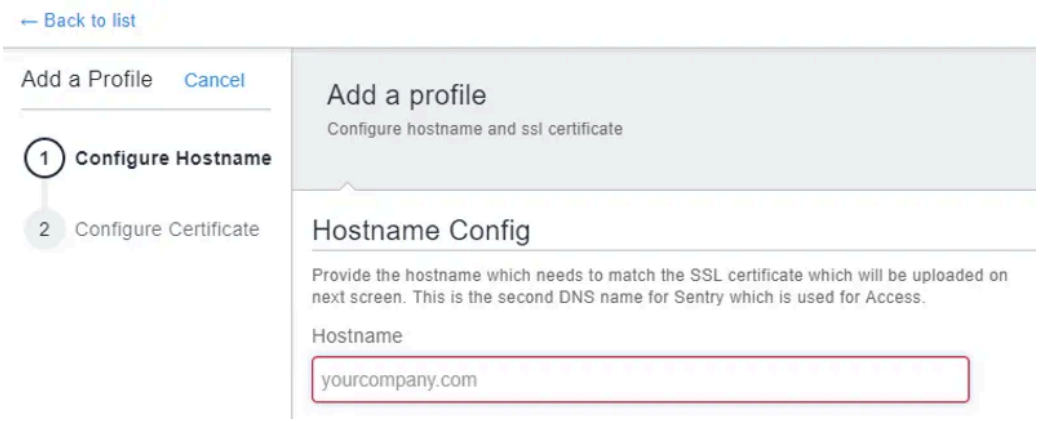
- Associate the SSL certificate with the Sentry second hostname.

Procedure

1.	For Hostname, enter the second hostname for the Standalone Sentry.

The second hostname will be associated with Ivanti Access.

Figure 1. Configure hostname



2.	Click on Next.

Figure 2. Configure certificate

3.	Click Add new certificate to upload the SSL certificate associated with the second hostname.

Figure 3. add new certificate

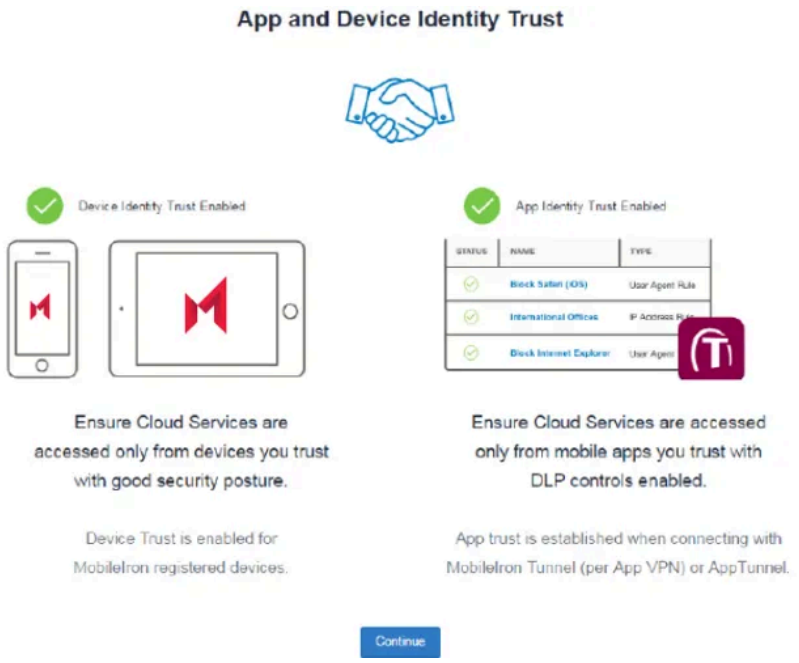
4.	For Certificate Name, enter a name by which you can identify the certificate.
5.	For Certificate Password, enter the password required to open the certificate.

6. Click Choose File to navigate to the location of the certificate file or drag and drop the certificate file.

7. Click Add SSL Certificate to complete the process of adding the certificate.

8. Click Done to complete the profile setup.

Figure 4. Complete profile setup



9. Click Continue to view the profile in the Overview page.

You will now have created a profile. You can now add a cloud service provider (SP) and identity provider (IdP) federated pair to this profile.

Next steps

Register a Standalone Sentry to Ivanti Access. See **Registering a Standalone Sentry**.

Related topics

See **Federated Pairs** for information about adding an SP and an IdP federated pair.

Error conditions for SSL certificate

The SSL certificate you upload to the Sentry profile must meet the security requirements from Apple. If the certificate does not meet the security requirements the system displays error messages. Ivanti Access checks for the following error conditions:

- SHA-1 server certificate or issuing authority detected.
- Server certificate or issuing authority contains RSA key size less than 2048 bits.
- Server certificate does not contain DNS name of the server in the Subject Alternative Name extension.

The following conditions are applicable only if the server certificate is issued after July 1, 2019 as indicated in the certificate. For more information, see the requirements provided by Apple: **https://support.apple.com/en-us/HT210176**

- Server certificate does not contain an ExtendedKeyUsage (EKU) extension containing the id-kp-serverAuth OID.
- TLS server certificates have validity period of more than 825 days.

6.2. Registering a Standalone Sentry

Use the Standalone Sentry command line interface (CLI) to register Standalone Sentry to Ivanti Access.

Procedure

	1.	SSH to Standalone Sentry.
	2.	Log in as an administrator.
	3.	Enter the following commands:

Enable

Configure terminal

accs registration <tenant url> <user>.

<tenant url>: The tenant URL you received in the welcome email.

Do not use /cms in the tenant url.

<user>: The local admin email for Ivanti Access you received in the welcome email.

You will be prompted to enter the tenant admin password. This is the admin password your received in the welcome email.

End

Show accs registration

Example of Standalone Sentry registration to Ivanti Access

The following example shows the CLI and output for registering Standalone Sentry to Ivanti Access.

Last login: Fri Feb 19 16:58:43 2016 from 10.10.15.2

****

* Sentry CLI *

* *

* *

****

Welcome miadmin it is Tue Feb 23 22:24:51 UTC 2016

sentry@mycompany.com> enable

Password:

sentry@mycompany.com# configure terminal

Enter configuration commands, one per line.

sentry@mycompany.com/config# accs registration https://access-na1.mobileiron.com foo@example.com

Enter password for user "foo@example.com":

Registration succeeded. Details:

"tenantURL" : "https://access-na1.mobileiron.com",

"tenantUsername" : "foo@example.com",

"registrationTimeMs" : 1456267371581,

"crtUuid" : "17592186044416",

"crtUsername" : "17592186044416"

}

sentry@mycompany.com/config# end

sentry@mycompany.com# show accs registration

{

"tenantURL" : "https://access-na1.mobileiron.com",

"tenantUsername" : "foo@example.com",

"registrationTimeMs" : 1456267371581,

"crtUuid" : "17592186044416",

"crtUsername" : "17592186044416"

}sentry@mycompany.com#

Next steps

Assign the Standalone Sentry to a profile. See **Assigning Standalone Sentry to a profile**.

Related topics

Example of Standalone Sentry registration to Ivanti Access

6.3. Viewing Standalone Sentry information

You can view the Standalone Sentry information that you have added in Access. The registered Standalone Sentry checks-in every fifteen minutes to Ivanti Access. When Sentry does not check-in, authentication failures to cloud service providers might occur. When Sentry does not check-in for an hour, Ivanti Access displays an alert in the Sentry tab to resolve the issues. The administrator is also notified with an email every 30 minutes for 24 hours to diagnose the issues and resolve the check-in issue. The email notification is stopped after 24 hours.

> If the Standalone Sentry that was registered to Access is no longer in use, unassign the Standalone Sentry from the profile to stop getting alerts.

Procedure

1. Click **Sentry** in the left navigation pane of Access administrative portal after you have registered the Standalone Sentry.

You can now assign the Standalone Sentry to a profile.

The Supported versions of Standalone Sentry are also listed on this page.

2. Enter the administrator's password to assign the Standalone Sentry to a profile.

3. To view the detailed report of the Standalone Sentry that you have added, select the appropriate Sentry. The detailed report displays on the right pane.

Report	Description
Overview	The Overview section provides the following information: • ID • Status • Last Activity Time • Registration Time
Inventory	The Inventory report provides the following information: • Hostname • Machine Size • Product Version • Fips Enabled • Portal Url • Service Start Time • UEM Hostname • UEM Server Type
Configuration	The Configuration report provides information about the status of the Sentry configuration.
Registration	The Registration report provides information about the status of Sentry registration.

6.4. Standalone Sentry actions

You can take the following actions on a Standalone Sentry:

- Assign the Standalone Sentry to a profile.
- Unassign the Standalone Sentry to a profile.
- Delete the Standalone Sentry.

Assigning Standalone Sentry to a profile

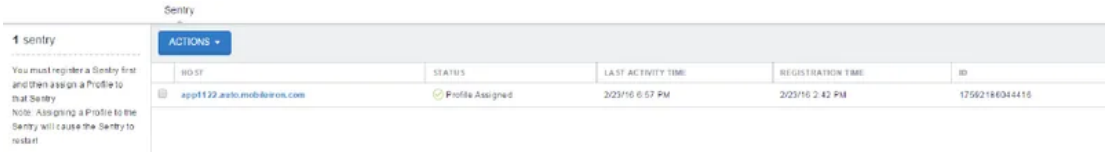
Assigning Standalone Sentry to Ivanti Access profile allows Access to get device posture and compliance information from that Standalone Sentry.

Procedure

1. In the Sentry page, select the Standalone Sentry.
2. Click Actions >Assign to assign the Standalone Sentry to the profile.

The Standalone Sentry Status displays as Profile Assigned.

Figure 1. sentry profile assigned



Unassigning Standalone Sentry from a profile

Unassign Standalone Sentry if it is no longer in use.

Procedure

1. In the Sentry page, select the Standalone Sentry.
2. Click Actions > Unassign to unassign the Standalone Sentry to the profile.

The Standalone Sentry Statusdisplays as Profile Unassigned.

Deleting a Standalone Sentry

When you delete a Standalone Sentry, it will be unregistered when the Standalone Sentry syncs with the Ivanti Access administrative portal.

Before you begin

Unassign the Standalone Sentry from an Ivanti Access profile. See Unassigning Standalone Sentry from a profile.

Procedure

1. In the Sentry page, select the Standalone Sentry.
2. Click Actions > Delete.
3. Click on Delete Sentry.

The Standalone Sentry will no longer be listed in the Sentry page.

> The Standalone Sentry will be unregistered when it next syncs with the Ivanti Access administrative portal.

6.5. Profile overview

The Profile > Overview page provides an overview of the steps to enable access control for cloud services.

If you have an Ivanti Access + Standalone Sentry deployment, the page also provides a snapshot of Standalone Sentry under Profile Details. You can edit the hostname and SSL certificates from the Overview page.

A profile is a set of configurations that can be assigned to a Standalone Sentry. It consists of a single hostname and its SSL configuration, IdP and SP proxy pairs, and conditional rules that control access to the IdP and SP proxy pairs. You can have multiple IdP and SP proxy pairs and conditional rules in the profile.

> For Ivanti Access + Standalone Sentry, you can assign a profile to multiple Standalone Sentry.

Editing the profile

The edit function allows you to update the Standalone Sentry second hostname and SSL certificate for Ivanti Access.

Procedure

1. In **Profile Details**, click the text box to edit the details.

Item	Description	Default
Hostname	The second hostname for Standalone Sentry. The second hostname is associated with Access on Standalone Sentry.	Hostname entered during initial setup.
SSL Certificate Alias	The SSL certificate for Ivanti Access. Select from the drop down list.	Certificate uploaded during initial setup
Add new certificate	Click to add a new SSL certificate.	

2. Click ✔ to save the changes or ✖ to cancel.

The changes are applied when the Standalone Sentry syncs with the Ivanti Access administrative portal.

7. Federated Pairs

Ivanti Access acts as a proxy between the service provider (SP) and identity provider (IdP). In a federated pair set up, Ivanti Access appears as a service provider (SP) to your identity provider (IdP) and as an IdP to your SP. A federated pair is the original IdP and SP pair for which Access is used as the proxy.

This following describes the steps required to set up a three-way trust between the SP, IdP, and Access and contains the following:

7.1. Configuring federated pairs

A federated pair is the identity provider (IdP) and service provider (SP) pair for which Ivanti Access is used as the intermediary. Federated pairs are configured in Federated Pairs. The Federated Pairs link in the left navigation pane changes to Federation if delegated IdP is enabled.

Before you begin

Before you configure a federated pair, ensure the following:

1. You have an existing federated authentication setup, using SAML or WS-Fed, between the cloud service provider (SP) and the identity provider (IdP).
2. The existing federated authentication setup between the SP and IdP works without Ivanti Access in the path.
3. You have the SP and IdP metadata.
    - For instructions on getting cloud service provider (SP) metadata see the following Knowledge Base article **How do I access Service Provider (SP) metadata?**
    - For instructions on getting identity provider metadata see the Knowledge Base article at **How do I access Identity Provider (IdP) metadata?**

- Microsoft Azure Active Directory as an IdP is qualified only with Salesforce (SP) and G Suite (SP).
- Microsoft Azure Active Directory as an IdP is not supported with Office 365 (SP).
- G Suite as an IdP is qualified only with Salesforce (SP) and Facebook Workplace (SP).
- G Suite as an IdP is not supported with Office 365 (SP).
- OneLogin as an IdP is not supported with Office 365 (SP).
- WebEx as an SP is qualified only with Microsoft ADFS (IdP) and Okta (IdP).
- For Office 365 Using WS-Federation only the following IdP are supported: Microsof ADFS and Ping Identity.

Procedure

1. In the Ivanti Access administration portal, go to Profile > Federated Pairs.
2. Click +Add New Pair.
   The set of supported cloud service providers displays.
3. Click the appropriate service provider to configure service provider settings.
   To add a service provider that is not listed, select either **Custom SAML Service Provider** or **Custom WS-Federation Service Provider.**
   Concur is a compatible app. Concur as a service provider is tested only with Okta and Microsoft ADFS.
4. Enter the requested information for the service provider.
   The requested information includes the signing certificate, encryption certificate for SAML assertions, service provider metadata, checkbox to validate signature for authentication requests sent by service provider, and the option to configure single sign-on (SSO).
   If you had previously uploaded signing certificates, select the certificate from the Signing Certificate drop-down list. Ivanti also provides a default signing certificate, which is also available in the drop-down list.
    - Previously, the service provider signing certificates existed but were not validated and user could log in to the service provider regardless of the signing certificate status. Now, a checkbox is introduced to validate the service provider signature and log an error in the Reports > Access. For the existing federated pairs, the checkbox is disabled and for the

new federated pairs, it is enabled by default. This field is supported for Salesforce and Custom SAML service provider only.

- When configuring a Federated Pair, the checkbox labeled "Validate signature for authentication requests" should be enabled. For backward compatibility, this option is unchecked for the existing pairs. Ensure that the SP/IdP metadata is updated and enable the checkbox.

5. Click Next.
   The set of supported identity providers displays.
6. Click the appropriate identity provider to configure identity provider settings.
7. Enter the requested information.
   The requested information includes the signing certificate and the identity provider metadata.
8. Click Done to complete the federated pair configuration.
9. Click OK in the Federated Pairs Setup is Complete message.
   The new pair is displayed on the Federated Pairs tab in Access.

You can also edit a federated pair. On the Federation page, click ✎ for the federated pair that you want to edit. When editing a federated pair, you can switch from add metadata URL to upload metadata or vice versa or only provide the metadata URL for the federated pair.

Related topics

- **Signing certificates**
- **Generating a signing certificate in Ivanti Access**
- **Service provider (SP) metadata**
- **Configuring Mobile App Single Sign-on (SSO)**
- **IdP initiated login**
- **SAML response signature**
- **Identity provider (IdP) metadata**
- **Office 365 settings**
- For more information on configuring federated pairs, see **Ivanti Access cookbooks**.

Next steps

1. Publish the profile.
   See **Publishing a profile**.
2. Upload metadata from Access to SP and IdP.
   See **Uploading proxy metadata**.
3. Verify traffic flow.
   See **Verifying traffic flow**.

7.2. Use Cases for distinctive deployments

Some customers have distinctive deployment scenarios with custom service provider and identity providers. This section lists some of the use cases that are distinctive and can serve a requirement in other deployments.

Jabber and Ivanti Access

An Ivanti EPMM user can leverage Access to provide Zero Sign-on or conditional access for a Jabber client. Jabber can be used to protect messaging and calling voice data requirements. This deployment uses MI Packet Ivanti Tunnel for Jabber (service provider) and Ping Federate (identity provider) with Access.

For more information on MI Packet Ivanti Tunnel and Ivanti Access deployment, see the **KB article**.

7.3. Signing certificates

Ivanti Access uses standard PKI to sign authentication requests and assertions used for federation. A default signing certificate is created for every Access instance. If you do not want to use the default certificate, you can generate a new signing certificate in the Ivanti Access administrative portal or add a PKCS 12 file containing a certificate and private key to use for signing federation messages.

- Adding a signing certificate in Ivanti Access
- Generating a signing certificate in Ivanti Access

SSL certificates should not be used in lieu of the signing certificate. This use case is not supported.

You can use the same signing certificate for the SP as well as the IdP.

Adding a signing certificate in Ivanti Access

The following provides the steps for adding a signing certificate in Access.

Before you begin

- Ensure that you have a PKCS 12 format file (.PFX or .P12) that contains your signing certificate and corresponding private key.

Procedure

1. In the service provider or identity provider configuration, click Advanced Options.
2. Click Add a new certificate.
3. Enter the following information:

Item	Description
Certificate Name	Enter an identifying name for the signing certificate.
Certificate Password	Enter the password for the signing certificate.
Choose File	Click to navigate to the location of the certificate or drag and drop the certificate to this location.

4. Click Add Signing Certificate to add the signing certificates.

The certificate is available to select from the Signing Certificate drop-down list.

The certificate is also listed in the Access Certificates tab.

Generating a signing certificate in Ivanti Access

The following provides the steps for generating a signing certificate in Ivanti Access.

Procedure

1. In the service provider or identity provider configuration, click Advanced Options.
2. Click Generate certificate to generate and add the signing certificate.

3. For Certificate Name, enter a name to identify the signing certificate.
4. Click Generate Signing Certificate.

The Certificate Name displays in the Signing Certificate drop-down list.

The certificate is also listed in the Access Certificates tab.

7.4. Service provider (SP) metadata

When a federated pair uses SP metadata URL, metadata is monitored. Ivanti Access monitors SP metadata present in the system with the metadata at the URL. Metadata monitoring occurs every 24 hours. The fields such as Entity ID, ACS URL, and Signing cert pem are monitored and evaluated for changes.

Use one of the options described in the following table to upload SP metadata to Access. When any changes are detected across any of these fields between metadata present in the system and the metadata at the URL, Access raises an alert with an email to all the administrators. It also displays an alert in the Ivanti Access portal. The administrator then uses the sync metadata option to update the federated pair with these changes.

> Ivanti Access verifies the validity of the service provider metadata certificate file and sends email notifications. For more information, see **Certificate expiry notifications**.

If the SP certificate expires, your device end users will not be able to authenticate and access corporate services federated through Ivanti Access admin portal.

The following table describes the options for uploading service provider (SP) metadata.

Option	Description
Upload Metadata	Click Choose File to navigate to the metadata file to add or drag and drop the file. The metadata file automatically populates the data Access.
Add Metadata	Enter the following information: • Entity ID • Assertion Consumer Service URL Click **Add New** to add multiple Assertion Consumer Service (ACS) URLs. The option to add multiple ACS URLs is available for Custom SAML SP and Custom WS-Fed SP only. For more information about multiple ACS URLs, see **Assertion Consumer Service (ACS) URLs**. Select Auth requests signed to enter a Base64 Encoded Cert. Use the Add Metadata option to add metadata for G Suite. For more information, see **Metadata for G Suite**.
Metadata URL	Enter the metadata URL. If there are changes to the metadata on the SP at the configured URL, Ivanti Access sends an email notification to the Access administrator. In Access > Federated Pairs, the following alert message displays for the federated pair: SP metadata has changed. For the federated pair, click Actions > Sync SP metadata to update the metadata file in Ivanti Access. An email notification is sent to the Ivanti Access administrator after the sync.

Assertion Consumer Service (ACS) URLs

Configure Assertion Consumer Service (ACS) URLs if you want to configure multiple destinations for the service provider (SP). For example, you may want your sales and customer support teams to go to separate locations on the service. Based on the intended destination, the SP encodes a different ACS URL in the authentication request. Access directs traffic to the ACS URL in the

Authentication Request if it matches the ACS URL configured in Access. If an ACS URL is not provided in the Authentication Request or the ACS URL does not match the ACS URL configured in Access, the traffic goes to the default destination.

The option to add multiple ACS URLs is available for only for Custom SAML SP and Custom WS-Fed SP only.

Metadata for G Suite

G-Suite does not provide a metadata file, therefore, for G Suite, select the Add Metadata option to add the service provider metadata to Ivanti Access. Enter the following:

- Entity ID: google.com/a/
- Assertion Consumer Service URL: https://www.google.com/a//acs

For PingIdentity only, select the check box for Auth requests signed. In the Base 64 Encoded Cert text box, paste the Base 64 Encoded Cert from PingIdentity.

See also, the **Knowledge Base** article.

7.5. IdP initiated login

The Enable IdP initiated login for this SP option is available for configuration for custom service providers (SP) only. However, the option is enabled by default for Concur SP. The option is disabled for all other SPs.

Select the Enable IDP initiated login for this SP option if your service provider redirects to the IdP login page, instead of sending a SAML AuthnRequest to the IdP.

Enabling IdP initiated login lets Access expose an IdP URL that generates a SAML request to the original IdP. However, if the Use Ivanti Tunnel Certificate for SSO option is also enabled, Access generates a SAML response to the SP based on the user's Ivanti Tunnel certificate.

7.6. SAML response signature

The ability to choose the SAML response signature is available for custom service providers (SP) only.

This option is available for service providers that require the SAML Response to be signed instead of signing the SAML Assertion inside the SAML Response.

The Sign Assertion option is selected by default. You can select the Sign Response option if appropriate.

> SAML Responses received by Ivanti Access must always have the Assertion signed. However, the Response must not be signed.

7.7. Encrypting SAML assertions

Enabling encryption of SAML assertions adds another layer of security. Enable this feature in a mobile app single sign-on setup if the SP supports SAML assertion decryption. The SAML assertions are encrypted such that the assertions can be decrypted only with the private keys held by the service provider.

- Encryption of SAML assertions is disabled by default.
- Responses can be signed while carrying a signed encrypted Assertion, but the Response itself is not encrypted.
- Do not use the signing certificate for encrypting SAML assertions and vice-versa.
- The following service providers (SP) support encryption of SAML assertions:
  - Salesforce
  - Custom SAML Service Provider
  - Custom WS-Federation Service Provider
- A default certificate for encryption is automatically available in your Ivanti Access tenant.
- Enabling SAML assertion encryption, enables additional options for Native Mobile Application Single Sign-On (SSO). These options allow you select the data encryption algorithm and the key transport algorithm for single sign-on.

Before you begin

See **Configuring Mobile App Single Sign-on (SSO)**for information about setting up single sign-on.

Procedure

1. In the service provider configuration for Salesforce, Custom WS-Federation Service Provider or for Custom SAML Service Provider, go to Encryption Certificate.
2. Click the check box for Encrypt SAML assertion.

The default encryption certificate is automatically selected.

3. (Optional) To use a different certificate than the default certificate, do one of the following:
   - select a certificate from the drop-down list.
   - click Generate certificate or Add new certificate.

Adding a new certificate for SAML assertion encryption

The following provides the steps for adding a new certificate for SAML assertion encryption.

Before you begin

- Ensure that you have a PKCS 12 format file (.PFX or .P12) that contains the certificate and corresponding private key.

Procedure

1. In the service provider (SP) configuration, in the Encryption Certificate section, click Add new certificate.
2. Enter the following information:

Item	Description
Certificate Name	Enter an identifying name for the encryption certificate.
Certificate Password	Enter the password for the encryption certificate.
Choose File	Click to navigate to the location of the encryption certificate or drag and drop the certificate to this location.

3. Click Add Encryption Certificate to add the new certificate.
   The certificate is now available to select from the drop-down list.
   The certificate is also listed in Profile >Access Certificates.

Generating a certificate for SAML assertion encryption

The following provides the steps for generating a certificate for SAML assertion encryption.

Procedure

1. In the service provider (SP) configuration, in the Encryption Certificate section, click Generate certificate.
2. For Certificate Name, enter a name to identify the certificate.
3. Click Generate Encryption Certificate.
   The certificate is now available to select from the drop-down list.
   The certificate is also listed in Profile > Access Certificates.

Related topics

- Adding a new certificate for SAML assertion encryption

- Generating a certificate for SAML assertion encryption

7.8. Identity provider (IdP) metadata

When a federated pair uses IdP metadata URL, metadata is monitored. Ivanti Access monitors IdP metadata present in the system with the metadata at the URL. Metadata monitoring occurs every 24 hours. The fields such as Entity ID, Redirect SSO URL, Post SSO URL, and Signing cert pem are monitored and evaluated for changes.

Use one of the options described in the following table to upload IdP metadata to Ivanti Access. When any changes are detected across any of these fields between metadata present in the system and the metadata at the URL, Access raises an alert with an email to all the administrators. It also displays an alert in the Ivanti Access portal. The administrator then uses the sync metadata option to update the federated pair with these changes.

Use one of the options described in the following table to upload IdP metadata to Ivanti Access.

> Ivanti Access verifies the validity of the identity provider metadata certificate file and sends email notifications. For more information, see **Certificate expiry notifications**.

If the IdP certificate expires, your device end users will not be able to authenticate and access corporate services federated through Access admin portal.

Option	Description
Upload Metadata	Click Choose File to navigate to the metadata file to add or drag and drop the file. The metadata file automatically populates the data in Ivanti Access.
Add Metadata	Enter the following information: • Entity ID • Post SSO URL • Redirect SSO URL • Base64 Encoded Cert
Metadata URL	Enter the metadata URL. For ADFS, enter the metadata URL for the ADFS server in the following format: https://<*ADFS DOMAIN NAME*>/FederationMetadata/2007-06/FederationMetadata.xml. If the ADFS server is internal, expose the URL through the firewall. If there are changes to the metadata on the IDP at the configured URL, Ivanti Access sends an email notification to the Ivanti Access administrator. In Access > Federated Pairs, the following alert message displays for the federated pair: IDP metadata has changed. For the federated pair, click Actions> Sync IDP metadata to update the metadata file in Ivanti Access. An email notification is sent to the Ivanti Access administrator after the sync.

About Microsoft ADFS metadata

For a SAML pair configured with Microsoft ADFS, you can upload the metadata, configure a metadata URL, or add the metadata. Changing the initial configuration of the metadata to a different form depends on how you configured the metadata initially. The following table describes the initially configured form and the forms to which it can be modified.

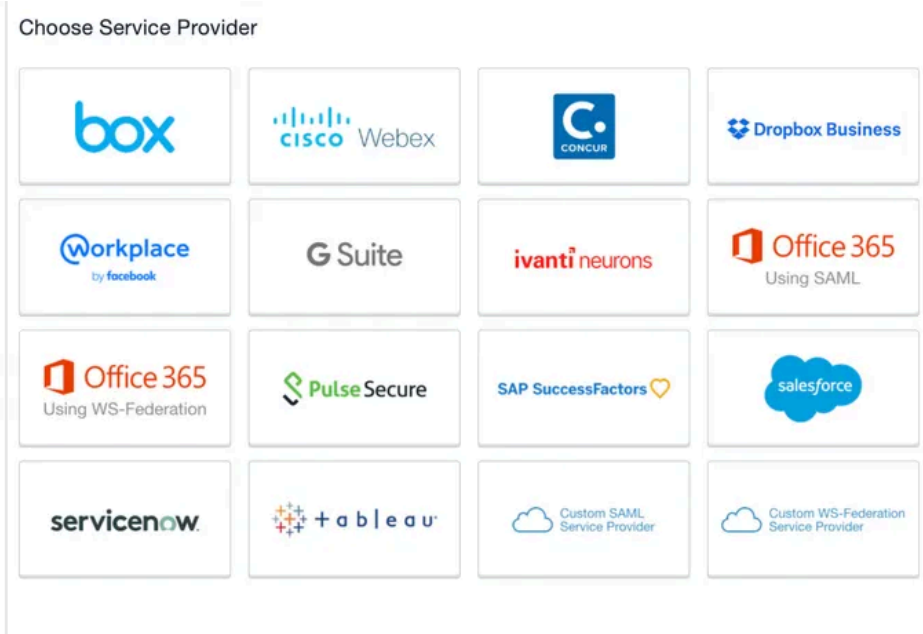
Initial SAML pair configuration using	Can be modified to
Upload metadata	Metadata URL. However, it cannot be modified to Add Metadata.
Metadata URL	Upload Metadata. The existing URL configuration is overridden by the uploaded metadata, and the URL is no longer tracker. The metadata configuration cannot be modified to Add Metadata.
Add Metadata	Cannot be modified to other options.

7.9. Office 365 settings

Office 365 is configured using either WS-Federation or SAML federation authentication protocols. Select one of the following service provider options in the Choose Service Provider page to configure Office 365 settings:

- Office 365 Using SAML
- Office 365 Using WS-Federation

Figure 1. Choose service provider



The following describes the settings specific to Office 365 as the service provider:

- **Office 365 settings using SAML authentication**
- Office 365 settings using WS-Federation authentication
- **PowerShell commands for Office 365**
- **Backup and restore Office 365 federation settings**
- **Multi-domain issuer**
- Active Logon Policy for Office 365

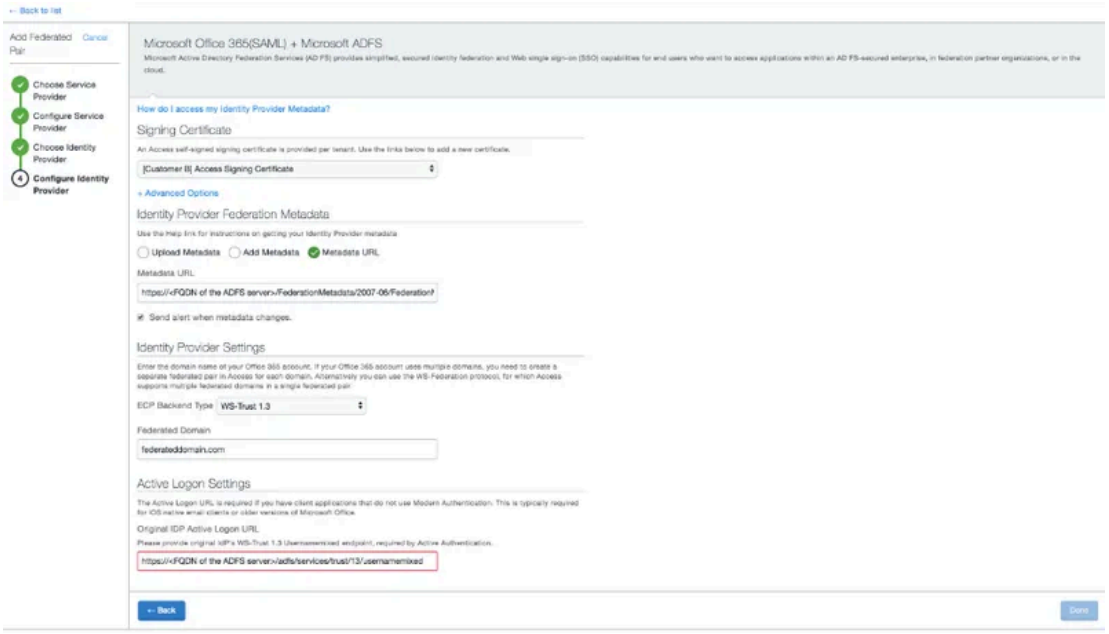
Office 365 settings using SAML authentication

The following describes the additional Office 365 settings available for configuration if your service provider is Office 365 Using SAML. These settings are available in the IdP configuration page:

- **ECP Backend Type:** Select from the drop-down list. Specifies the ECP backend type to connect to the IdP.
- **Federated Domain**: Enter the value for Office 365.
  Example: mycompany.com.
- Active Logon Settings: Enter the Active Logon URL in the text box for **Original IDP Active Logon URL.** The Active Logon URL varies depending on the ECP backend type and the IdP. If your IdP is Microsoft ADFS, the Original IDP Active Logon URL text box is pre-populated with the Active Logon URL. Update the URL with the correct ADFS domain.

- Example for ADFS using ECP WS-Trust 1.3:
  https://<FQDN of the ADFS server>/adfs/services/trust/13/usernamemixed.
- Example for ADFS using WS-Trust2005:
  https://<FQDN of the ADFS server>/adfs/services/trust/2005/usernamemixed

Figure 2. IdP settings for Office 365 as the service provider using SAML



Office 365 settings using WS-Federation authentication

The following describes the additional Office 365 settings available for configuration if your service provider is Office 365 Using WS-Federation.

The option to enable multiple federated domains is available in the Office 365 service provider configuration page.

- Support Multiple Domains: Select the check box to enable multiple federated domains to use the same federated pair in Ivanti Access.

The options to configure MEX metadata and the Active Logon URL are available in the IdP configuration page.

MEX metadata and Active Logon URL expose SOAP Web Service endpoints and define how other endpoints interact with the SOAP Web Service endpoints. Ivanti Access publishes MEX metadata based on the MEX metadata configuration provided by the original IdP. Access only exposes the endpoints that are supported and configured in the MEX metadata of the original IdP. Only WS-Trust 1.3 and WS-Trust 2005 protocols for usernamemixed are supported. Configuring MEX metadata allows for support for applications such as Microsoft Dynamics 365 and Microsoft SQL Server. In addition, Windows Transport endpoint is supported with Ivanti Access + Standalone Sentry deployments only.

For more information about enabling Windows Transport endpoints see **Azure Hybrid Domain-Join with Ivanti Access**.

Select one of the following methods to provide the MEX metadata configuration from the original IdP:

- Enable Mex Metadata: Select the check box to provide metadata configuration from the original IdP. Choose one of the following:
  - **MEX metadata URL**: Enter the URL for the MEX metadata for the original IdP.
    Example for ADFS MEX Metadata URL : https://<FQDN of the ADFS server>/adfs/services/trust/mex

Note: Federation metadata import through URL might fail if the server does not present certificate chain issued by trusted certificate authorities. For the MEX metadata URL, the corresponding server must present full certificate chain issued by trusted certificate authority.

- Upload MEX metadata: Upload the MEX metadata file from the original IdP.

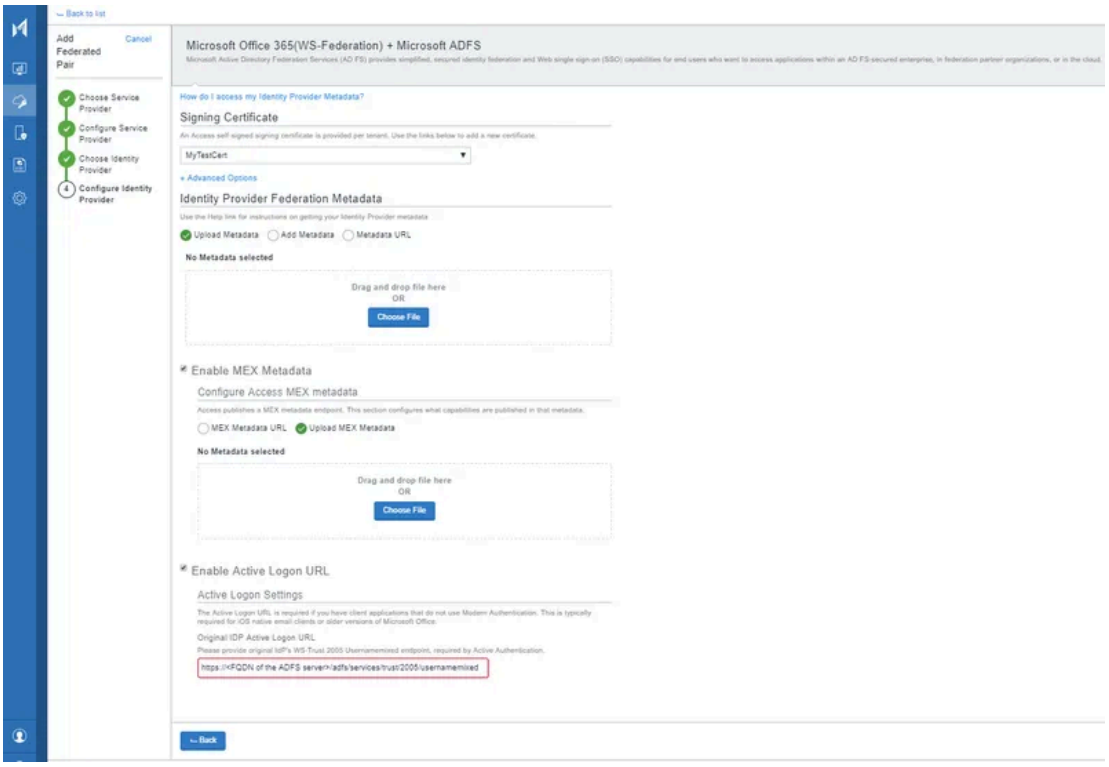
Deselect the check box to disable MEX metadata.

- Enable Active Logon URL: Select the check box to enable Active Logon URL. Enter the Active Authentication URL for the original IdP. You enable Active Logon URL to handle Active Auth traffic. This is required for applications, such as some email applications, that support only active authentication. Ivanti Access exposes only WS-Trust 2005 usernamemixed endpoints. If your IdP is Microsoft ADFS, the Original IDP Active Logon URL text box is pre-populated with the Active Logon URL. Update the URL with the correct ADFS domain.
  Example:
  https://<FQDN of the ADFS server>/adfs/services/trust/2005/usernamemixed
  Deselect the check box to disable Active Logon URL.

> Native iOS clients, Android email clients, and Email+ use active authentication.

See also **Active Logon Policy for Office 365**.

Figure 3. Office 365 settings using WS-Federation authentication



Authentication with Microsoft PowerShell commands

Ivanti Access supports the use of Microsoft PowerShell commands, such as Connect-MgGraph and Connect-SPOService, to get authorization tokens to authenticate endpoints with Azure ID. This support allows administrators to set up authentication for service provider (SP) accounts that belong to a federated domain.

- PowerShell commands, such as Connect-SPOService, are ActiveAuth transactions. Therefore, ensure that an Active Logon Policy is applied. Otherwise, the ActiveAuth traffic is bypassed and no rules are evaluated.
- Ensure that the latest version of Microsoft Graph PowerShell SDK is installed when running PowerShell scripts from Ivanti Access pair for setting up Office 365.

For Ivanti Access + Standalone Sentry deployments, the feature is not enabled by default. The feature is enabled using command line interface (CLI) commands in Standalone Sentry. The commands are available in Standalone Sentry 9.6.0 through the latest version as supported by Ivanti.

> Do not enable the feature on a Standalone Sentry that is configured for ActiveSync. The feature is not supported on a Standalone Sentry that is configured for ActiveSync.

To enable the feature in Ivanti Access + Standalone Sentry deployments, enter the following command in Standalone Sentry command line interface (CLI) in CONFIG mode:

config# debug sentry ignore-line-breaks true

To disable the feature in Ivanti Access + Standalone Sentry deployments, enter the following command in Standalone Sentry command line interface (CLI) in CONFIG mode:

config# debug sentry ignore-line-breaks false

Restart the Standalone Sentry service for the configuration changes to take effect. To restart Standalone Sentry service, enter the following command in EXEC PRIVELEGE mode:

sentry# service tomcat restart

The 'service tomcat restart' may impact traffic.

Would you like to proceed? {yes|[no]} : yes

To view whether the feature is enabled or not in Standalone Sentry, enter the following show command in EXEC PRIVELEGE mode:

sentry# show sentry ignore-line-breaks

org.apache.xml.security.ignoreLineBreaks: false

- False indicates that the feature is disabled.
- True indicates that hte feature is enabled.

PowerShell commands for Office 365

The commands to federate Azure AD with Ivanti Access are provided as a PowerShell batch script, which can be downloaded from the Ivanti Access administrative portal. After you create a federated pair with Office 365 in Access, the link to download the PowerShell batch script becomes available in the federated pair listing in Profile > Federated pairs.

> Ensure that the latest version of Microsoft Graph PowerShell SDK is installed when running PowerShell scripts from Ivanti Access pair for setting up Office 365.

To use the PowerShell commands, download the PowerShell script and run the script in PowerShell with the following command:

script_name.ps1 -domain mydomain.com

In the above command:

- script_name is the name of the downloaded PowerShell script.
- mydomain.com is the Microsoft Azure AD domain.

Ensure that you have PowerShell Administrator permissions.

Figure 4. Download PowerShell commands

Backup and restore Office 365 federation settings

To backup and restore the Office 365 federation settings, see **Back up and restore Office 365 settings**.

Multi-domain issuer

If you are federating using the WS-Federation protocol, you can use the same federated pair for multiple AD domains suffixes that federate with the same Office 365 tenant.

In cases where multi-domain issuer is enabled, Ivanti Access composes the multi-domain issuer from the domain in the UPN. If the UPN domain is the sub domain, the issuer will not match with the root domain issuer in Azure AD. Configure the attribute AzureDomain in the ADFS, if you have a domain forest (multiple ADs joined in the forest). In such cases, the issuer URI suffix is derived from the value of the attribute name AzureDomain in the assertion from the original IdP.

For ADFS 3.0, to add the AzureDomain attribute, add the following claim rules to the relying party trust:

- Query DistinGuishedName from AD
- c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD AUTHORITY"]
  => add(store = "Active Directory", types = ("http://somedomain.com/phase1"), query = ";DistinGuishedName;", param = c.Value);
  Parse DistinGuishedName to compose root domain
- c:[Type == "http://somedomain.com/phase1"]
  => add(Type = "http://somedomain.com/phase2", Value = RegExReplace(c.Value, "^(?:.*?)DC=(?<domain1>[^'DC']*),DC=(?<domain0>[^'DC']*)$", "$.$"));
  Issue root domain and AzureDomain attribute
  c:[Type == "http://somedomain.com/phase2"]
  => issue(Type = "http://schemas.xmlsoap.org/claims/AzureDomain", Value = c.Value);

For ADFS 4.0, to add the AzureDomain attribute, add the following claim rules to the relying party trust:

- Query DistinguishedName from AD
- c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]
  => add(store = "Active Directory", types = ("http://somedomain.com/phase1"), query = ";distinguishedName;", param = c.Value);
  Parse DistinguishedName to compose root domain
- c:[Type == "http://somedomain.com/phase1"]
  => add(Type = "http://somedomain.com/phase2", Value = RegExReplace(c.Value, "^(?:.*?)DC=(?<domain1>[^'DC']*),DC=(?<domain0>[^'DC']*)$", "$.$"));
  Issue root domain and AzureDomain attribute

```
c:[Type == "http://somedomain.com/phase2"]
=> issue(Type = "http://schemas.xmlsoap.org/claims/AzureDomain", Value = c.Value);
```

7.10. Cookbook for Ivanti Connect Secure

Ivanti Connect Secure can work as SAML service provider. Use Okta or any appropriate IDP and configure a Customer SP federation pair on Ivanti Access using Ivanti Connect Secure SP and IDP.

This cookbook considers Okta as the identity provider.

> If the user tries to configure Request Header rule with Header Name as “Referer”, the configured header rule will not be evaluated by Ivanti Access. This occurs as by default, Ivanti Connect Secure does not send Referer Header in the SAML request.

Complete the following procedure to configure Ivanti Connect Secure.

Before you begin

- Ensure your global SAML configuration is correct
  - Login to Ivanti Connect Secure admin portal.
  - Under System > Configuration > SAML, select Settings.
    Validate or populate Host FQDN for SAML with the FQDN of your Ivanti Connect Secure Appliance
  - Click Save.

Creating metadata file for Ivanti Connect Secure

1. Login to Ivanti Connect Secure admin portal.
2. Under System > Configuration > SAML, select New Metadata Provider.
3. Enter a Name such as Access_ZSO.
4. Select Remote for location.
5. Enter the Download URL provided by Okta.
6. Verify the Identity Provider for roles.
7. Click Save.
   It takes a few moments for the values to populate from the Metadata Service. Refresh the page to see if download was successful or not.

Downloading metadata on Ivanti Connect Secure

1. Login to Ivanti Connect Secure admin portal.
2. Under Authentication > Auth. Servers choose new SAML Server and click New Server.
3. Enter a Name such as Access_ZSO.
4. Select 2.0 for SAML Version.
5. Select Metadata for Configuration Mode.
6. Select the Identity Provider Entity Id from your Okta SAML Metadata Provider (In **Creating metadata file for Ivanti Connect Secure**).
7. Select POST for SSO Method.
8. Select the Okta SSO Certificate.

9. Select a valid Device Certificate for Signing.
10. Click Save.
11. Edit the Authentication Server created and click Download Metadata.

Configuring Federated Pair on Ivanti Access

1. Login to Access admin portal.
2. Click Profile> Federation > Add Pair.
3. Select Pulse Secure as the service provider.
4. Upload Pulse SAML metadata.xml saved in **Downloading metadata on Ivanti Connect Secure**.
5. Select Use Ivanti Tunnel Certificates for SSO .
6. Click Next.
7. Select Okta as the identity provider in the catalog.
8. Upload the Okta Metadata.
9. Click Done.
10. Publish the profile.

Updating Ivanti Connect Secure configuration to federate with Ivanti Access

1. Login to Ivanti Connect Secure admin portal.
2. Edit the metadata provider created in **Creating metadata file for Ivanti Connect Secure**.
3. Enter the Access IDP Metadata (Upload to SP) download URL.
4. Click Save.
   Refresh the page to ensure that the new metadata is downloaded successfully.
5. Edit the SAML Auth server created in **Downloading metadata on Ivanti Connect Secure**.
6. Edit and update the Identity Provider Entity ID to newly updated access url.
7. Select the Access SSO Certificate.
8. Click Save.

Updating Okta configuration to federate with Ivanti Access

1. Login to Okta admin portal and edit the Metadata Provider.

Additional configurations on Pulse Secure required for end-end flow

The following configuration is for users with ZSO enabled on Ivanti Access admin portal.

Enable ZSO for user portal

Configure Users Realm to use SAML Auth Server

1. Login to Pulse admin portal > Users > User Realm > New User Realm.
2. Enter a name for realm and select SAML Auth server in Authentication.

3. Click Save.
4. Under Role mapping, create a new rule with username * and select Users role from the list.
5. Click Save.

Configure Sign In Policy for ZSO

1. Login to Pulse admin portal > Authentication > Sign In > Sign In Policies.
2. Click New URL.
3. Select User type > Users.
4. Enter "*/zso" as the Sign-in URL.
5. In Authentication realm, select User Picks from a list of authentication realm and select the User realm configured for ZSO.
6. Click Save.

Enable ZSO for Admin Portal

Configure Admin Realm to use SAML Auth Server

1. Login to Pulse admin portal > Admin > Admin Realm > New Admin Realm.
2. Enter a name for realm and select SAML Auth server in Authentication.
3. Click Save.
4. Under Role mapping, create a new rule with username * and select Users role from the list.
5. Click Save.

Configure Sign In Policy for ZSO

1. Login to Pulse admin portal > Authentication > Sign In > Sign In Policies.
2. Click New URL.
3. Select User type > Administrators.
4. Enter "*/zso" as the Sign-in URL.
5. In Authentication realm, select User Picks from a list of authentication realm and select the Admin realm configured for ZSO.
6. Click Save.

Enable ZSO for Pulse Client

Configure VPN Profile for Pulse Client

1. Login to Pulse admin portal > Users > Resource Policies > VPN Tunneling > Connection profile.
2. Create a New Profile.
3. Enter a name for the profile.
4. In IPv4 address assignment, select IPv4 address pool and enter a pool of IP address. For example: 10.10.10.1-100
5. Click Save.

7.11. Active Logon Policy for Office 365

A passive logon policy (passive or modern authentication) is configured by default for Office 365 federated pairs. If your Office 365 email application does not support passive authentication, use the Active Logon Policy option to assign a separate conditional policy to authenticate the active authentication (ActiveAuth) traffic for the Office 365 federated pair. The Active Logon Policy option becomes available after the Office 365 federated pair is created.

Passive authentication is based on a browser-based connection to Office 365, which supports redirects. The following describe the federated authentication flow with passive authentication:

1. The user-agent (browser) connects to Office 365.
2. Office 365 responds with a 301 redirect to the identity provider.
3. The user-agent follows the redirect to the identity provider.
4. The identity provider presents a login form for end users to enter their credentials.
   The credentials can be in the form of user name and password, certificate, or another alternative method.
5. The identity provider generates a response that contains an authentication Assertion and a browser-based mechanism, either redirect or JavaScript, to auto-submit the Assertion to Office 365.
6. The user-agent uses the browser-based mechanism to submit the Assertion to Office 365.
7. Office 365 validates the Assertion, thus allowing the user to log in.

Active authentication does not support browser-based connection to Office 365. Therefore, it does not

- support 301 redirects
- render HTML or form-based entry
- do JavaScript-based automatic form submission.

The federated authentication flow for active authentication is as follows:

1. Users enter their account credentials in the email application.
2. The email application sends the user credentials to Office 365.
3. Office 365 forwards the user credentials to the identity provider.
4. The identity provider returns an Assertion in the response to Office 365.
5. Office 365 validates the Assertion allowing the user to log in.

For an Office 365 federated pair configured in Ivanti Access, if there are no policies assigned to ActiveAuth traffic, the ActiveAuth traffic is bypassed and no rules are evaluated. If you are using email applications that support only active authentication, to allow these applications to authenticate with Office 365, assign an Active Logon policy to the Office 365 federated pair. See **Office 365 settings**.

> Native iOS clients, Android email clients, and Email+ use active authentication.

When you assign a policy from the Active Logon Policy drop-down, the conditional rules in the assigned policy are evaluated for ActiveAuth traffic. The following conditional rules are not applicable to ActiveAuth traffic:

- Trusted App and Device Rule
- Ivanti Tunnel Rule

- Multi-Factor Authentication
- Android for Work Registration
- iOS Native Email OAuth
- Desktop Trust Rule

Assigning an active logon policy

The option to assign a policy for active logon is available in Profile > Federated Pairs, in the listing for the Office 365 federated pair.

Before you begin

Ensure that you have created a separate conditional policy to use for ActiveAuth traffic. When you create a conditional policy, the policy becomes available in the Active Logon Policy drop down when you are assigning the policy. To create a conditional policy, see **Conditional Access**.

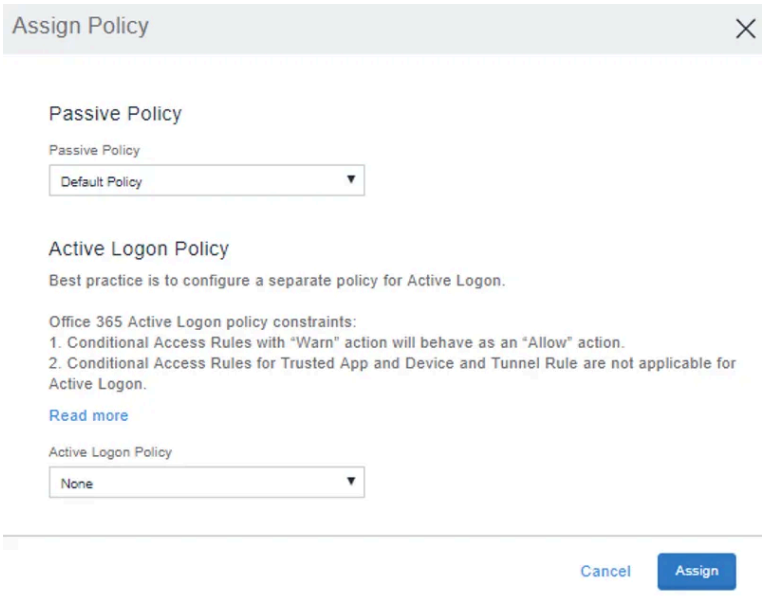
> Ivanti recommends that you configure a separate conditional policy for Active Logon.

Procedure

1. In Ivanti Access, go to Profile > Federated Pairs.
2. In the listing for the Office 365 federated pair, click .

The **Assign Policy** window opens.

Figure 1. Assign logon policy



3. Select the policy from the following options:

Passive Policy: Select the Passive policy from the drop-down list for browser-based solution.

Active Logon Policy: Select the Active Logon policy from the drop-down list for client-based solution.

Select **None** from Active Logon drop down list, if you do not want Active Authentication traffic to evaluate any policy's rule condition.

	4.	Click **Assign**.

7.12. Publishing a profile

Publishing the profile makes the changes available. In an Ivanti Access (without Standalone Sentry) deployment, publishing the profile makes the changes live. Typically, it takes less than two minutes for the changes to take effect.

In a deployment with Ivanti Access + Standalone Sentry, the changes are made available to the Standalone Sentry paired with the profile. Standalone Sentry picks up the changes when it next syncs. If there are any changes, Standalone Sentry consumes the changes.

Standalone Sentry syncs every 15 minutes with the Ivanti Access administrative portal. Therefore, it might take up to 15 minutes for the changes to take effect. However, you can force an update from the Standalone Sentry command line.

If there is a delay of fifteen minutes for Sentry to be updated, then to manually force an update, use Sentry CLI *accs config-fetch{update| force-update}*.

The following changes cause Standalone Sentry to restart:

- Fetching updates for the first time
- Access hostname changes
- Access SSL cert changes
- Access port changes

Before you begin

Under the menu options, click **View Changes** to verify the changes.

> The profile Publish button is hidden when there is no change in the profile since the last publish. The Publish button is enabled only when the profile is modified since the last publish. Whenever the changes to configuration are reverted, the publish button disappears. It disappears if there is no actual change to the profile, since the last publish.

Procedure

1. In the Ivanti Access administrative portal, go to Profile > Overview.
2. Click Publish.

Publish is only available if a pair has been created.

3. Click OK.

7.13. Azure Hybrid Domain-Join with Ivanti Access

Azure AD Join Configuration allows an administrator to enable Windows Transport endpoint for Windows device registration with Azure AD.

For more information, see the **KB article**.

7.14. View federated pairs

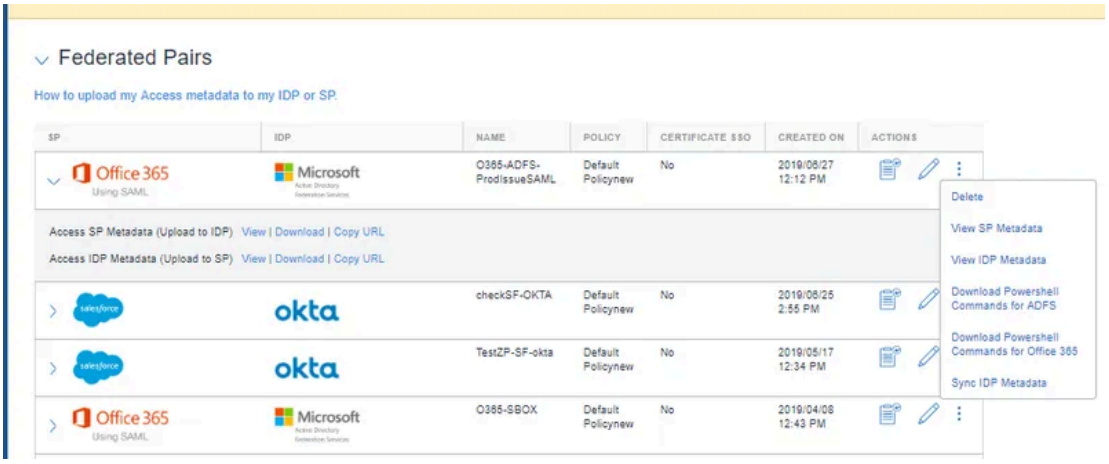
You can view the list of configured federated pairs in the Ivanti Access administration portal in Profile > Federated Pairs.

- Information and metadata for a SP and IdP pair
- Assigning a policy to a federated pair
- Editing a federated pair
- Deleting a federated pair

Information and metadata for a SP and IdP pair

For information and metadata for a federated pair, expand the row for the federated pair or click on the icons under Actions.

Figure 1. Federated pairs details



Item	Description
Name	Name you entered for the federated pair.
Policy	Name of the conditional policy applied to the federated pair. For an Office 365 federated pair, the Passive Policy name is displayed.
Certificate SSO	Indicates whether certificate-based single sign-on is configured for the pair.
Access SP Metadata (Upload to IdP)	Ivanti Access generates proxy metadata by combining the service provider metadata and the signing certificate. You upload the Access (SP) metadata to the IdP. • Click Download to download the Access proxy metadata for the SP. • Click View to view the Access proxy metadata for the SP. • Click **Copy URL** to copy the proxy metadata and upload to IdP.
Access IDP Metadata (Upload to SP)	Ivanti Access generates proxy metadata by combining the IdP metadata and the signing certificate. You upload the Access (IdP) proxy metadata to the cloud service provider. • Click the Download to download the Access proxy metadata for the IdP. • Click the View to view the Access proxy metadata for the IdP. • Click **Copy URL** to copy the proxy metadata and upload to SP.
Actions	
Assign policy icon	Click to assign a conditional policy. For an Office 365 federated pair, you can choose a passive policy or an active logon policy.
Edit icon	Click to edit the settings for the federated pair.
Vertical three dots	Click for additional actions available for the federated pair: • Delete: Click to delete the federated pair • View SP Metadata: Click to view the metadata you uploaded for the cloud service provider (SP) . • View IDP Metadata: Click to view the metadata you uploaded for the identity provider (IdP). • Download PowerShell Commands for ADFS: Click to download the PowerShell script to run the commands. • Download PowerShell Commands for Office 365: Click to download the PowerShell script to run the commands.

Assigning a policy to a federated pair

If a policy is not applied to a federated pair, the default policy is applied.

> During the initial setup, Ivanti recommends that you do not make changes to the default policy.

Procedure

1. In the Ivanti Access administration portal, go to Profile > Federated Pairs.
2. For the federated pair, click .
3. In the Assign Policy dialog, from the Policy drop down list select a policy.

4. Click Assign.
5. Click Publish.

If you do not Publish the changes, the updates are not applied.

Related topics

- Office 365 settings.
- Conditional Access.

Editing a federated pair

If you make changes to a federated pair, change the metadata file, or the signing certificate, you must upload an updated proxy metadata file to the service provider and the IdP.

Procedure

1. In the Ivanti Access administration portal, go to Profile > Federated Pairs.
2. For the federated pair, click Actions > Edit.
3. After editing, click Publish.

If you do not Publish the changes, the updates are not applied.

Deleting a federated pair

The following provides the steps for deleting a federated pair.

Procedure

1. In the Access administration portal, go to Profile > Federated Pairs.
2. For the federated pair, click Actions > Delete.
3. In the pop-up box, click Delete.
4. After deleting, click Publish.

If you do not Publish the changes, the updates are not applied.

> Delete, removes the Federated pair from Ivanti Access. However, to also remove Access from the federated login path to the service provider, you must establish or restore the direct federation between your service provider and identity provider.

7.15. Renewing the SSL certificate

The following describes the steps to add a new SSL certificate when the current SSL certificate expires.

Procedure

1. Login to the Ivanti Access with administrator credentials.
2. In the **Overview** tab, scroll down to **Profile Details**.
3. Click the certificate in the **SSL Certificate Alias** field.
4. Click **Add new certificate**. The **Add SSL Certificate** windows displays.
5. Enter the **Certificate Name** and **Certificate Password**.
6. Under **SSL Certificate Upload,** click **Choose File**.
7. Upload the new SSL certificate to renew the certificate.
8. Click **Add SSL Certificate**.

The SSL certificate is now renewed.

7.16. Uploading proxy metadata

Ivanti Access generates proxy metadata by combining the cloud service provider (SP) or the identity provider (IdP) metadata and the signing certificate. The proxy meta data is automatically generated when you configure the SP and IdP in the Ivanti Access administrative portal.

You upload the proxy meta data to the SP and the IdP. When you upload the proxy meta data to the (SP) and the (IdP), you establish a three-way trust between the SP, IdP, and Access. All authentication traffic now goes through Access.

Before you begin

If your deployment is Ivanti Access + Standalone Sentry:

- Ensure that a Standalone Sentry is registered on the Ivanti Access administrative portal.
- The Standalone Sentry is assigned to the profile.
- The profile with configured federated pair is published to Standalone Sentry.

Procedure

1. Get the proxy metadata from the Ivanti Access administrative portal:

Go to Profile > Federated Pairs.

Expand the row for the federated pair.

For the Access service provider proxy metadata, click the Download link adjacent to Access(SP) Metadata.

You will upload the Access(SP) Metadata file to the identity provider (IdP).

For the Access identity provider proxy metadata, click the Download link adjacent to Access(IDP) Metadata

You will upload the Access(IDP) Metadata file to the cloud service provider (SP).

2. Upload the proxy metadata to cloud service provider (SP).

3. Upload the proxy metadata to identity provider (IdP).

Related topics

- For instructions on uploading the IdP proxy metadata to an SP, see the **Knowledge Base article**.
- For instructions on uploading the SP proxy metadata to an IdP, see the **Knowledge Base article**.

7.17. Verifying traffic flow

After you upload proxy metadata to the cloud service provider (SP) and identity provider (IdP), traffic will flow through Ivanti Access and Standalone Sentry. You can verify that authentication and access to the cloud service is working.

Procedure

1. On a mobile device use the service provider's app to access the cloud service. You should be able to access the cloud service successfully.
2. On a desktop, access the cloud service. You should be able to access the cloud service successfully.
3. On the Access administrative portal, check Reports > Access.

The Reports > Access page displays the authentication traffic to which the default rule is applied. Standalone Sentry sycns with the Ivanti Access administrative portal every 15 minutes. It may take up to 15 minutes for the authentication traffic to display in Reports > Access.

4. Use the debug accs check-in access-report CLI command that forces Sentry to sync Access reports to the Ivanti Neurons for MDM console.

Next steps

- Set up conditional rules.

See **Conditional Access**.

7.18. Cookbook for Ivanti Neurons

Integrating Ivanti Neurons as a SAML Service Provider with Ivanti Access

Ivanti Neurons can work as SAML service provider. Use Okta or any appropriate IDP and configure a Customer SP federation pair on Ivanti Access using the dedicated Ivanti Neurons SP catalog item and your chosen IDP.

This cookbook considers Okta as the identity provider.

> **Custom Rules**: You can apply custom conditional access policies to this federation. For example, you can configure Network Rules in Ivanti Access to restrict user logins for Ivanti Neurons to a specific IP range.

Before you begin

- Ensure your global SAML configuration is correct.
- Ensure you have the required administrative privileges in Ivanti Neurons, Ivanti Access, and Okta.
- For configuring an external authenticator provider in Neurons, see **External Authentication (SSO)**.

Phase 1: Preparing Metadata

Creating the Identity Provider metadata record in Ivanti Neurons

1. Login to the Ivanti Neurons admin portal.
2. Navigate to the SSO/SAML configuration section.
3. Select **Other IdP** to create a new external authentication provider.
4. Select **Enabled Signed Requests** and then click **Apply Changes**.
5. Select **Download SP metadata**.
6. Upload the Access IdP metadata. For further details, refer Phase 2 and Phase 3.
7. Click **Continue**.

> Encrypted assertions are not supported in Ivanti Access.

Phase 2: Configuring the Federated Pair on Ivanti Access

Setting up the Federation Pair

1. Login to the Ivanti Access admin portal.
2. Navigate to **Profile** > **Federation** > **Add Pair**.
3. From the service provider catalog, select the dedicated **Ivanti Neurons** tile.

> Do not use the 'Custom SAML' option; selecting the Neurons tile ensures proper analytics tracking.

1. Upload the Ivanti Neurons 'SAML metadata.xml' that you downloaded in the previous phase.
2. Click **Next**.
3. Select **Okta** as the identity provider from the catalog.

4. Upload the Okta Metadata.
5. Click **Done**.

Phase 3: Finalizing the Integration

Updating Ivanti Neurons to federate with Ivanti Access

1. Login to the Ivanti Neurons admin portal.
2. Edit the metadata provider you created earlier.
3. Update the configuration to point to the **Access IDP Metadata (Upload to SP)** option.
4. Ensure that the Identity Provider Entity ID is updated to the newly generated Access URL.

Updating Okta configuration

1. Login to the Okta admin portal.
2. Edit the application configuration for this setup to recognize the Ivanti Access integration as the trusted entity routing the authentication.
3. While configuring Okta Console, as listed in **Okta Authentication (SAML)**, ensure to update the attributes in **Configure SAML** > **Attribute Statements**, as follows:
    1. (Mandatory) **Name**: 'email', **Value**: 'user.email'. Click **Add Another**.
    2. (Optional) **Name**: 'given_name', **Value**: 'user.firstName'. Click **Add Another**.
    3. (Optional) **Name**: 'family_name', **Value**: 'user.lastName'.

    > The data in the above fields is case-sensitive.

Publish the Profile

Once all configurations and rules are set, publish the profile in Ivanti Access to apply the changes.

- Return to the Ivanti Neurons admin portal. Click **Continue** > **Validate Settings**. The validation takes place automatically. You will receive a confirmation screen if login is successful.

(Optional) Configuring Conditional Network Rules

If you need to restrict Ivanti Neurons access to specific networks:

1. In the Ivanti Access admin portal, open your newly created Ivanti Neurons federation pair.
2. Navigate to the **Custom Rules** option.
3. Select **Network Rule**.
4. Define the permitted IP range to restrict login access to those specific IPs.
5. Click **Save**.

8. Delegated IdP

The following provide more information about setting up Ivanti Access as a delegated IdP:

8.1. Delegated IdP overview

In most cases Ivanti Access is deployed as a proxy between the service provider (SP) and the identity provider (IdP). In such a deployment, all federated SP traffic goes through Ivanti Access. In some cases, you may want to retain the existing SP-IdP federated setup, but deploy Access to federate a sub set of the traffic, such as traffic from mobile devices. In such cases, Ivanti Access can be deployed as a delegated IdP rather than as a proxy to the IdP. If Access is deployed as a delegated IdP, the original IdP is seen as an SP by Ivanti Access.

Ivanti Access can be deployed as the delegated IdP only for the following IdPs:

- Idaptive
- Microsoft ADFS
- Okta
- PingFederate

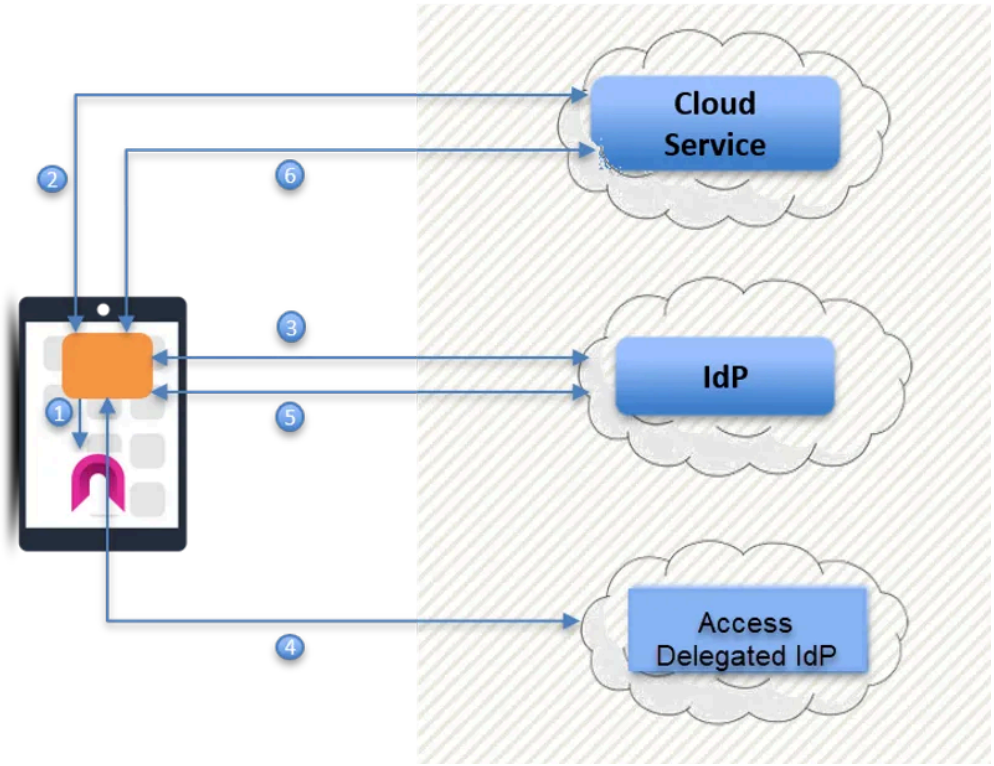
In an Ivanti Access configured as a delegated IdP:

- To authenticate managed devices, configure certificate single sign-on (SSO) in the UEM.
- To authenticate unmanaged devices, you have the option to enable Unmanaged Device Authentication in Ivanti Access. If authentication for unmanaged devices is enabled, the unmanaged device is redirected to the original IdP for forms-based authentication.

8.2. Authentication flow with Access as the delegated IdP

The following graphic provides the authentication flow with Access as delegated IdP for managed devices:

Figure 1. Authentication flow with Access as the delegated IdP



1.	Users access a service provider (SP) from a managed app. The managed app triggers Ivanti Tunnel.
2.	If the app does not have a valid session token, the SP issues an authentication request to the app and redirects the app to the identity provider (IdP).
3.	The IdP issues a secondary authentication request based on the authentication request in step 2 and points the user to Ivanti Access (delegated IdP).
4.	Ivanti Access identifies the user based on the certificate used to establish the Ivanti Tunnel VPN. Based on the information provided in the Ivanti Tunnel certificate, Access generates an authentication response to the app and redirects to the original identity provider (IdP). Access determines the contents of the authentication response based on the Native Mobile Application Single Sign-On (SSO) configuration in Access, which includes the user identifying information that the SP expects.
5.	The original IdP generates an authentication response to the app based on the authentication response in step 4 and redirects to the original SP.

6.	The SP verifies the user information and creates a session token to the app. The session token gives the user access to the SP.

8.3. Configuring Ivanti Access as the delegated IdP

Setting up Access as the delegated IdP requires configuration in UEM, Access, and in the IdP as well. Ivanti Access supports delegation for the following IdPs: Idaptive, Microsoft ADFS, Okta, and PingFederate.

> Only authentication from managed devices is allowed for Delegated IDP with Idaptive pair.

The setup described here does not apply to an Ivanti Access + Standalone Sentry deployment. If your deployment is Ivanti Access + Standalone Sentry, see the following KB article: **Access as Delegated IDP**.

Overview of tasks

1. In UEM, configure certificates for single sign-on. If single sign-on is configured, Ivanti Access authenticates the user. Otherwise, the user is redirected to the original IdP for forms-based authentication.
2. In Ivanti Access, enable Delegated IdP in Settings > Tenant Settings.
3. In Ivanti Access, and set up the original IdP in Profile > Federation > Add Pair > Delegated IdP.
4. In the original IdP, set up delegation to Ivanti Access.

Before you begin

Ensure the following:

- You have an existing federated authentication set up between the cloud service provider (SP) and the supported identity provider (IdP).
- In a delegated IdP setup, Access sees the IdP as an SP. Therefore, download the SP metadata from the IdP. If you are enabling authentication for unmanaged devices, also download the IdP metadata from the IdP. The following table provides links to instructions on how to get the metadata for your IdP.

IdP	For instructions on how to get the metadata go to	Supported methods for providing metadata in Access
Idaptive	Download the metadata. See the Cookbook for Idaptive.	Upload metadata
ADFS	Download metadata from https://<YourADFS>/FederationMetadata/2007-06/FederationMetadata.xml	Upload metadata Enter metadata URL
Okta (Manual Setup)	See the Cookbook for Okta. See the "How to get Metadata from Okta as SP for Access" section for instructions on downloading the SP metadata from Okta. See the "How to get Metadata from Okta as IdP for Access" section for instructions on downloading the IdP metadata from Okta. Required only for enabling authentication for unmanaged devices.	Upload metadata Enter metadata URL
Okta (Automated Setup)	Cookbook for configuring Okta as delegated IDP See "Step 1: Creating an application and download the metadata for Okta" section for instructions on downloading the metadata from Okta. : If the okta admin wants to unhide the Access application created from the automated workflow, they can do so by from Okta console. For more information , see the cookbook.	
PingFederate	See the "Configure PingFederate for Delegated-IdP flow" section in Cookbook for PingFederate.	Upload metadata Enter metadata URL

- If single sign-on is configured in UEM, SCEP obtains user information from LDAP. Therefore, ensure that the LDAP settings in UEM fetch the appropriate attributes from LDAP.
  The Ivanti Tunnel certificate is setup to include the mapping to a certificate field for certificate native mobile application single sign-on (SSO). The following tables describe the certificate field mapping for Ivanti Neurons for MDM and Ivanti EPMM.

LDAP for Ivanti Neurons for MDM deployments	Certificate	SAN Type in SCEP
Idaptive		
$	$	RFC 822 Name
ADFS		
$	$	RFC 822 Name
$	$	Distinguished Name
$	$	Not Applicable
Okta and Ivanti Neurons for MDM deployments		
$	$	RFC 822 Name
PingFederate and Ivanti Neurons for MDM deployments		
$	$	RFC 822 Name
F5		
$	$	RFC 822 Name

LDAP for Ivanti EPMM deployments	Certificate	SAN Type in SCEP
Idaptive		
EmailAddress	$EMAIL$	RFC 822 Name
ADFS		
sAMAccountName	$USERID$	RFC 822 Name
distinguishedName	$USER_DN$	Distinguished Name
Okta		
userPrincipalName	$EMAIL$	RFC 822 Name
PingFederate		
userPrincipalName	$EMAIL$	RFC 822 Name
F5		
userPrincipalName	$EMAIL$	RFC 822 Name

- To make it easier to configure mobile application single sign-on, upload a sample Ivanti Tunnel certificate and assign user friendly names to each field in the certificate. For more information, see **User Certificates**.

Procedure

1. In Ivanti Access, go to Settings > Tenant Settings.
2. For Delegated IDP, click the toggle to ON to enable delegated IdP.
3. Navigate to Profile > Federation.



4. Click Add Pair and select Delegated IdP.



5. Click the appropriate IdP to configure identity provider settings.
   Select Custom Identity Provider for any other provider other than the available identity providers.
6. Select the signing certificate.
   A default signing certificate is selected. You can select a different signing certificate from the drop-down list.
7. Select "Validate signature for authentication requests sent by the service provider". For backward compatibility, this option is unchecked for the existing pairs. Ensure that the SP/IdP metadata is updated and enable the checkbox.
8. (Optional) Select the check box for Encrypt SAML assertions.
9. Upload the service provider (SP) metadata from the original identity provider (IdP).
10. For mobile app single sign-on do the following:
11. From the **Reference Client Certificate** drop-down list, select the sample Ivanti Tunnel certificate.
12. In the SAML Subject Configuration section:

- For Type,
  If your IdP is Idaptive, select Email.
  If your IdP is ADFS, select Persistent.

If your IdP is Okta, select Email.
If your IdP is PingFederate, select Email.

- For Get Value From, select SAN of type rfc822Name.
  The instance maps to the order it is listed in the certificate configuration in UEM.

13. (Only if your IdP is ADFS) In the SAML Attribute Configuration section:

SAML Attribute Configuration is not needed for Okta and PingFederate, irrespective of the SP.

Name	Get Value from	Additional transforms
UserID	SAN of type rfc822Name	-
UserDomain	SAN of type directoryName: Instance 1	dn:domain

4. If you selected Encrypt SAML assertions, select the encryption algorithms.
   The options for encryption algorithms are only visible if you selected Encrypt SAML assertions.
5. Click Next.
6. (Optional for Okta Manual Setup) For Unmanaged Device Authentication, check Enable policy and configurations for handling authentication of Unmanaged Mobile Devices via IDP.
   Enabling the option directs authentication traffic from unmanaged devices to the original IdP for forms-based authentication.
   If the original IdP is Okta or PingFederate, the option to upload IdP metadata becomes available.
   This option is not available for ADFS because the metadata for ADFS, uploaded earlier in the configuration, includes both SP and IdP metadata.

> This set up is for Okta manual setup only. Follow the Cookbook for Okta automated setup for automated setup.

Figure 1. unmanaged devices authentication



13. (Optional) For Okta or PingFederate, if you enabled Unmanaged Device Authentication, upload the IdP metadata downloaded from the respective IdP.
14. Click Done to complete the configuration.
15. In Profile > Federation, click on the IdP listed in Delegated IdP and download the Access IDP Metadata. If Unmanaged Device Authentication is enabled, you will also see Access SP Metadata. Download the Access SP metadata as well.
16. (Optional) If your IdP is ADFS, click Download the Powershell Command for ADFS.

> If there are changes to the SP or delegated IDP metadata, Access detects these changes and notifies the administrator via email.
> The following alert message also displays for the federated pair in Access > Delegated IDP: SP/Application metadata (IDP) has changes. For the delegated IDP, click Actions > Sync SP/Application metadata (IDP) to update the metadata file in Ivanti Access.
> An email notification is sent to the Ivanti Access administrator after the sync.

Next steps

- Set up the IdP for delegation to Ivanti Access. This includes uploading the Access IdP, and the Access SP, if applicable, metadata to the IdP. Upload the Access IdP metadata in the IDP where delegations are configured. Upload the Access SP

metadata in the IdP where service providers are configured. Do one of the following:

- If your IdP is ADFS, run the PowerShell script in ADFS. This is the same PowerShell script you downloaded from Ivanti Access. The PowerShell script contains the commands to setup delegation to Ivanti Access.
  See **PowerShell commands for ADFS**.
  See also Using Ivanti Access as a Delegated IdP for ADFS.
- If your IdP is Okta, see Okta as Delegated IdP (Manual Setup) and Okta as Delegated IdP (Automated Setup).
- If you IdP is PingFederate, see Ivanti Access as Delegated IdP for PingFederate

- If you enabled unmanaged device authentication, ensure that the conditional policies applied to the Delegated IdP configuration does not block unmanaged devices.

Related topics

- **Signing certificates**
- **Identity provider (IdP) metadata**
- **Encrypting SAML assertions**
- **Conditional policies**

PowerShell commands for ADFS

Ivanti Access provides PowerShell scripts for the following:

- Set up Ivanti Access as the delegated IdP in ADFS
- Create a new Ivanti Access theme in ADFS for iPads running iOS 13

The PowerShell scripts eliminate the need to copy and paste the commands. The PowerShell scripts can be downloaded from Profile > Federation and run on your machine.

The following describes how to use the PowerShell scripts:

- **Running the PowerShell scrip to set up Ivanti Access as the delegated IdP in ADFS**
- **Using the PowerShell script to create a new Ivanti Access theme in ADFS for iPadOS 13 upgrades**

Running the PowerShell scrip to set up Ivanti Access as the delegated IdP in ADFS

The commands to set up Access as the delegated IdP in ADFS are provided as a PowerShell batch script that can be downloaded and run on your machine. After you create a delegation for ADFS in Access, the link to download the PowerShell batch script becomes available in the listing for the delegated IdP in Profile > Federation.

Running the script as described allows you to set up Access as a Claims Provider Trust in ADFS. When Access presents its claims to ADFS, ADFS serves the corresponding Relying Party, such as Office 365 or Salesforce, and allows the user to authenticate to the Relying Party. The Relying Party, such as Office 365 or Salesforce, must also be configured in ADFS.

If authentication of unmanaged devices is enabled in the delegated IdP configuration in Access, the PowerShell script also adds Access as a Relying Party with all required claims in ADFS.

Before you begin

- Ensure that you have PowerShell Administrator permissions.
- Depending on your ADFS version, run one of the following commands to get the Active Directory identifier:
  - For ADFS 4.0: (Get-AdfsClaimsProviderTrust -Name "Active Directory").Identifier

- For ADFS 3.0: Get-ADFSProperties
  Look for the value for Identifier.

Procedure

1. Download the PowerShell script.
   1. In Access, go to Profile > Federation.
   2. For the ADFS listed, click the three vertical dots in Actions.
   3. Click Download Powershell Commands for ADFS to download the script.
2. Run the following command in PowerShell:
   .\MICROSOFT_ADFS_SP_WSFED-script.ps1 -activeDirectoryIdentifier "ActiveDirectoryIdentifier" -sourceAdfsWebThemeName default -targetAccessWebThemeName "AccessThemeName"
   You will be prompted to enter values specific to your environment.
   For ActiveDirectoryIdentifier, enter your enterprise Active Directory identifier.
   For AccessThemeName, enter any name. This the web theme name for Access. ADFS automatically creates the web theme name based on the name you enter.

Using the PowerShell script to create a new Ivanti Access theme in ADFS for iPadOS 13 upgrades

The iPadOS 13 upgrade PowerShell script creates a new Access theme in ADFS so that authentication traffic from iPads running iPadOS 13 is redirected to Ivanti Access.

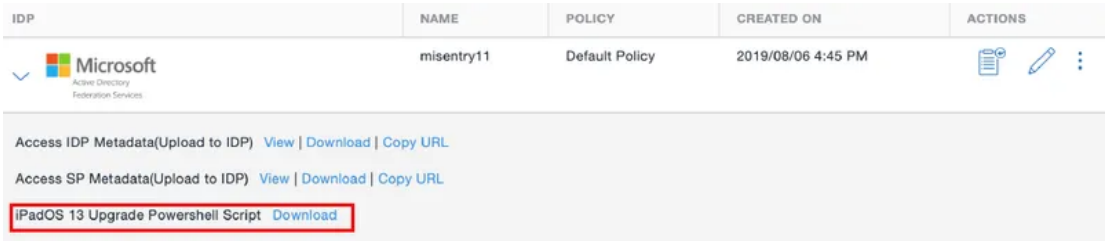
- The iPadOS 13 upgrade PowerShell script becomes available only if you have an existing delegated IdP setup with ADFS. If you are creating a new delegated IdP setup with ADFS, follow the procedure in **Running the PowerShell scrip to set up Ivanti Access as the delegated IdP in ADFS**.
- The upgrade script does not overwrite or delete any existing web theme in your environment. It creates a new theme from an existing source theme that you specify.

Before you begin

Ensure that you have PowerShell Administrator permissions.

Procedure

1. Download the PowerShell script.
2. In Access, go to Profile > Federation.



   1. For the ADFS listed, for iPadOS 13 Upgrade Powershell Script, click Download.

1. Run the following command in PowerShell:
   MICROSOFT_ADFS_SP-iPadOS13-upgrade-script.ps1
2. Enter values that are specific to your environment.
   For ActiveDirectoryIdentifier, enter your enterprise Active Directory identifier.

Run one of the following commands to get the Active Directory identifier based on the version of ADFS:

- For ADFS 4.0: (Get-AdfsClaimsProviderTrust -Name "Active Directory").Identifier
- For ADFS 3.0: Get-ADFSProperties
  Locate the value for Identifier.

3. Enter the source web theme name from which to create the new web theme.
   Enter the existing Access web theme name. A duplicate of the Access web theme is created.
4. Enter a new target web theme name for the new web theme.
   ADFS automatically creates a new web theme name based on the name you enter.
   If you provide an existing web theme name, the script prompts you to enter a new name.

After the new web theme is created, you are presented with the following options:

- Apply customized ADFS web theme to all Relying Party Trusts: Select this option to apply the new web theme to all Relying Party Trusts.
- Do not apply ADFS web theme now. Exit: Select this option to save the web theme and exit PowerShell without applying to any Relying Party Trusts. If you need to apply the new web theme to only some Relying Party trusts in your environment, contact your ADFS administrator.

9. Conditional Access

Ivanti Access allows you to define which applications and IP network ranges can access a cloud resource. You define the apps and IP network ranges that can access the cloud resource in conditional policies and rules in Ivanti Access.

The following provide additional information on setting up conditional policies and rules:

9.1. Conditional policies

A conditional policy is a set of conditional rules, which can be applied to a federated pair. A conditional policy can contain multiple conditional rules.

A default policy is automatically created when you do the initial setup through the setup wizard. The default policy is automatically applied to a federated pair if no other policy is applied. You cannot delete the default policy, you can only edit it. The default policy automatically includes a set of predefined rules. You can create additional policies. However, only one policy can be applied to a federated pair with the exception of the Active Logon policy, which can be applied in addition to another policy.

You can do the following in a policy:

- Add or delete rules.
- Move rules up or down in the list.
- Change the action on a rule.
- Disable rules.

9.1.1. Adding a new conditional policy

To add a new conditional policy in Ivanti Access, go to Profile > Conditional Access.

Before you begin

Before you create conditional access policies and rules, verify that traffic is flowing as expected between Ivanti Access, the identity provider (IdP), and the cloud service provider (SP). See **Verifying traffic flow**

Procedure

1. In the Ivanti Access administrative portal, go to Profile > Conditional Access.
2. Click +Add Conditional Policy to add a new conditional policy. The new policy is created.
3. Edit this policy appropriately. You can enter a name and description for the policy.

The General Bypass rule is created by default when you add a new policy.

4. Click Publish to make the changes available.

9.2. Conditional rules

Conditional rules define which app, devices, or users are allowed or blocked access to the service provider. Conditional rules are contained in a policy. The rules are applied in the order they are listed in the policy. The top row is evaluated first. If the rule condition is not met, the next rule is evaluated. If rule condition is met, the action associated with the rule is taken and all other rules are skipped. You can change the order of the rules by moving the rule either up or down in the list.

Conditional rules allow or block access to a cloud resource based on the following:

- Ivanti Tunnel information
- User information
- IP network range

You can limit traffic to allow only the configured IP network range, or block traffic from the configured IP network range.

Go to Reports > Access to view the source IP for the authentication traffic.

- Source IP or headers added by a HTTP proxy or load balancer.
- User agent (app) accessing the cloud service

The user agent is a short string provided by the app accessing the cloud service. The user agent string identifies the app.

Go to Reports > Access to view the user agent string for the authentication traffic.

9.2.1. Adding a conditional rule

You add a conditional rule to a conditional policy.

Procedure

1. In the Ivanti Access administrative portal, go to Profile > Conditional Access.
2. Expand the policy row to which you want to add the conditional rule.
3. Click +Add Rule to add a new conditional rule.
4. Click a predefined or customizable rule.
5. Complete the requested fields for the rule.
6. Click Done to save the rule.

The rule appears at top of the list. To reorder the list, select the rule and move it to the preferred position in the list.

7. Click Publish to make the changes available.

Related topics

- **Predefined conditional rules**
- **Customizable conditional rules**

9.3. Predefined conditional rules

Ivanti Access provides a set of predefined conditional rules. These rules are automatically added to the default policy when the default policy is created. You cannot change a predefined rule. You can do the following to a predefined rule:

- Delete the rule.
- Change the action on the rule.
- Move the rule up or down in the list.
- Disable the rule.

The General Bypass rule is a special predefined rule that is automatically added to all new policies and it is the last rule in the policy. The rule cannot be moved up in the list or be disabled. You can only change the action on the rule.

Rule name	Description	Default action
Trusted App and Device	Determines whether all tunneled applications are allowed that incude using Ivanti Tunnel, Web@Work, Docs@Work, using AppTunnel or Ecosystem apps using AppConnect with AppTunnel.	Allow
Untrusted Apps on iPad	Blocks all applications that do not have Ivanti Tunnel VPN configuration.	
Untrusted Apps on iPhone	Blocks all applications that do not have Ivanti Tunnel VPN configuration.	Block
Untrusted Apps on MAC	Blocks all applications that do not have Ivanti Tunnel VPN configuration.	
Untrusted Apps on Android	Blocks all applications that do not have Ivanti Tunnel VPN configuration.	Block
Untrusted Apps on Windows	Blocks all applications that do not have Ivanti Tunnel VPN configuration.	Block
Android for Work Registration	Determines whether the untrusted devices are enabled to register for Android for work. If your deployment is Access + Standalone Sentry, ensure that your Standalone Sentry version is 8.5.0 through the most recent version as supported by Ivanti.	Allow
iOS Native Email OAuth	Controls (allow/block) access to the IdP from iOS native email client using OAuth with Office 365. This rule is not automatically added to the default policy.	Allow

9.4. Customizable conditional rules

You can customize the following set of conditional rules:

- **Tunnel Rule**. For more information, see Tunnel rule.
- **User Info Rule**. For more information, see User Info Rule.
- **Network Rule**. For more information, see Network Rule.
- **App Rule**. For more information, see App Rule.
- **Advanced Network Rule**. For more information, see Advanced Network Rule.
- Multi-Factor Authentication: For more information, see Multi-factor Authentication
- Request Header Rule: For more information, see Request Header Rule.
- Zero Sign-on Rule: For more information, see Multi-factor Authentication.
- **Desktop Trust Rule**. For information, see Desktop Trust Rule.
- **Device Ownership Rule** : For more information, see Device Ownership Rule.
- **Redirect to IDP**: For more information, see Redirect to IDP Rule.

Tunnel rule

Add a Tunneled rule to control access for tunneled apps. The following describes the fields in the Tunnel Rule.

Item	Description
Name	Enter a name for the rule.
Description	Enter descriptive text for the rule.
Action	From the drop down menu, select one of the following: Allow: Allows traffic from the specified Tunneled application. Block: Blocks traffic from the specified Tunneled application. **Warn:** Warns traffic from the specified Tunneled application. **Follow Policy**: Applies the conditional policy that you choose from the existing list.

User Info Rule

Add a User Info Rule to control access for an user or an user group. By default, all the fields in the SAML assertion, including subject and any attributes are matched against the values specified in this rule.

- Add attribute names in this rule if you want to match the values specified in this rule only to the attribute you specify here.
- If you want the values specified in this rule to match all attributes, use the attribute name "*".

Values can be user IDs or group IDs. If you configure your Identity Provider to include a group ID to match against, it enables you to configure a small list of group IDs instead of a large list of individual user IDs.

Item	Description
Name	Enter a name for the rule.
Description	Enter descriptive text for the rule.
SAML Assertion Field	Select the SAML Subject checkbox if you want the UserInfoRule to match the SAML Subject. The default option is set to true. Enter the Attribute Name. For example, *.abcd. If the username or the group is part of the Attributes in the SAML response, then the Attribute name must be added here or the * must match with all of the attributes if any in the SAML response.
Match With	From the drop-down menu, select one of the following: • **Add**: Lets you add users to the list to configure the rule. • **Upload to Append**: Lets you upload a text file with one user or group per line. • **Upload to Replace**: Lets you replace the existing list of users with a new list of users in a new text file. Ivanti recommends to use .txt format files to upload the users. The file must contain only one user per line.
Action	From the drop-down menu, select one of the following: • Allow: Allows traffic from the specified User or User group. • Block: Blocks traffic from the specified User or User group. • **Warn:** Warns traffic from the specified User or User group. • **Follow Policy**: Applies the conditional policy that you choose from the existing list.

Network Rule

Add a Network Rule to control access from an IP network range. The following describes the fields in a Network Rule.

Item	Description
Name	Enter a name for the rule.
Description	Enter descriptive text for the rule.
Action	From the drop down menu, select one of the following: Allow: Allows traffic from the specified IP address range. Block: Blocks traffic from the specified IP address range. **Warn:** Warns traffic from the specified IP address range. **Follow Policy**: Applies the conditional policy that you choose from the existing list.
Start IP Mask or CIDR Network Address	Enter the start address for the IP address range. The IP address can be in the form of an IPv4 address or CIDR.
End IP Mask or CIDR Network Address	Enter the end address for the IP range. The IP address can be in the form of an IPv4 address or CIDR.

App Rule

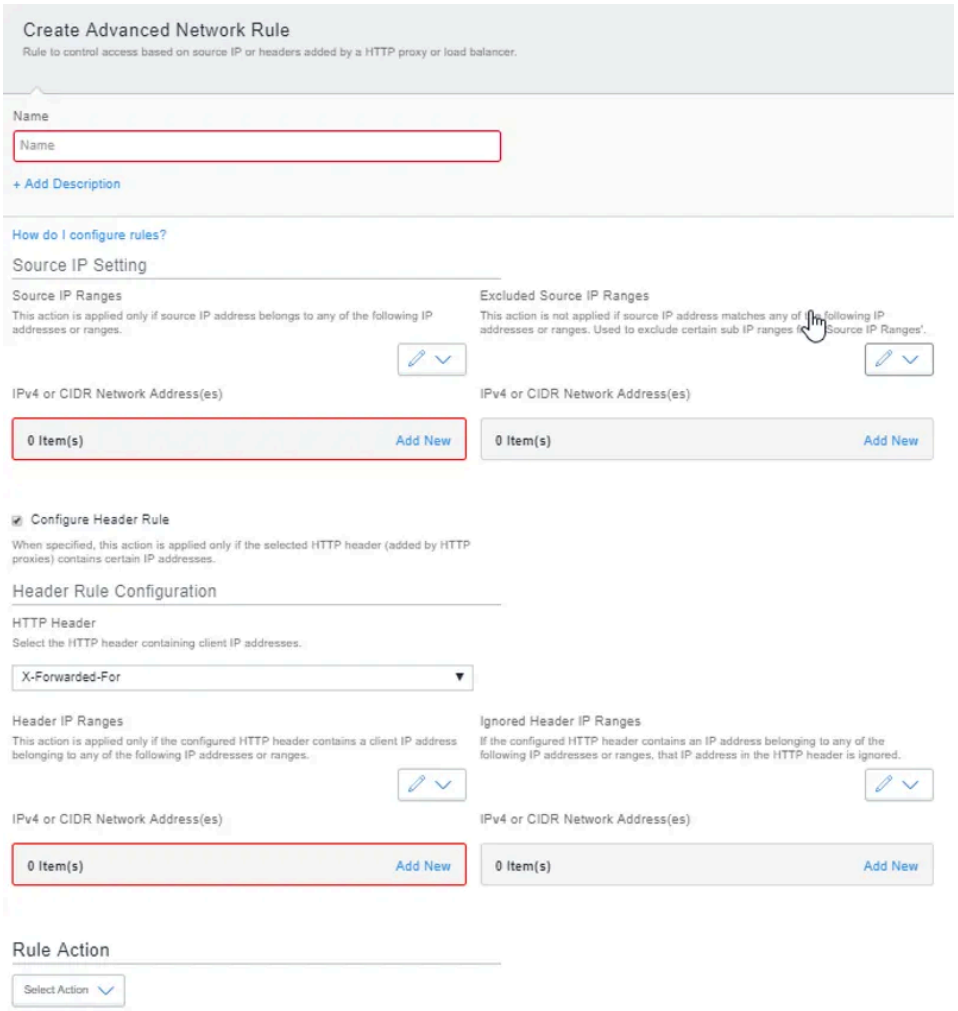
Add an App Rule for an app or device platform to allow or block the app or device platform. The following describes the fields in an App Rule.

Item	Description
Name	Enter a name for the conditional rule.
Description	Enter descriptive text for the conditional rule.
Action	From the drop down menu, select one of the following: Allow: Allows traffic from the specified Application. Block: Blocks traffic from the specified Application. **Warn:** Warns traffic from the specified Application. **Follow Policy**: Applies the conditional policy that you choose from the existing list.
Matching Algorithm	From the drop down menu, select one of the following: Regex: Select if you plan to use a regular expression for the user agent. Wildcard: Select if you plan to use wildcard for the user agent Literal: Select if the rule should exactly match the configured expression.
Expression	Enter an expression for the app, based on the matching algorithm you selected. Check the Reports view to see the user agents in the traffic for authentication.
Case Sensitive	Select if the rule should consider the case configured in the expression.
Partial Match	Select if the rule can be applied to a partial match of the configured expression.

Advanced Network Rule

Add an advanced network conditional rule to control access based on source IP and/or headers added by an HTTP proxy or load balancer. For more information, see the **KB article**.

Figure 1. adding advanced network rule



The following describes the fields in an Advanced Network Rule.

Item	Description
Name	Enter a name for the conditional rule.
Description	Enter descriptive text for the conditional rule.
Source IP Setting	
Source IP Ranges	• Click **Add New** to add the IP address manually. Enter the Source IP address range that must be IPv4 or CIDR Network Address. For example: 192.168.0.1 or 192.168.0.0/24 • Select **Upload to Append** to upload a fine and append the IP addresses to the existing IP address. Select **Upload to Replace** to replace all the IP address with the IP address from the uploaded file. Upload a text file containing the IP addresses in CIDR format or the normal IP Address format. The maximum number of allowed entries of IP address(es) in the text file is 1000 for successful upload of IP address(es).
Excluded Source IP Ranges	Exclude Source IP range is required when you have a large IP range that to configure for source IP and exclude subsets of that range from the consideration. For example: The rule must be configured for the range 192.168.0.0 – 192.168.0.255. However, you might not want IP ranges from this set. The IP ranges to be excluded are 192.168.0.0 – 192.168.0.3 and 192.168.0.8 – 192.168.0.11. Configure the source IP range as 192.168.0.0/24. In exclude IP range, add 192.168.0.0/30 and 192.168.0.8/30. Procedure • Click **Add New** to enter the sub IP address range that you wish to exclude from the Source IP ranges. For example: 192.168.0.1 or 192.168.0.0/24 • Use the drop-down list to **Upload to Append** or **Upload to Replace** an IP address range. You must upload a plain text file with each line containing an IP address or a CIDR network. The maximum number of IP range entries supported is 1000.
Configure Header Rule - Select the check-box to configure the Header Rule. By default, this checkbox is enabled. Deselect the checkbox to create a rule without headers.	
Header Rule Configuration	
HTTP Header	Select one of the HTTP header types containing client IP addresses. • X-Forwarded-For • X-MS-Forwarded-Client-IP
Header IP Ranges	• Click **Add New** to enter the Header IP range that contains a client IP address. For example: 192.168.0.1 or 192.168.0.0/24

Item	Description
	• Use the drop-down list to **Upload to Append** or **Upload to Replace** a Header IP range. You must upload a plain text file with each line containing an IP address or a CIDR network. The maximum number of IP range entries supported is 1000.
Ignored Header IP Ranges	Use the **Ignored Header IP Range** when you have multiple proxies that always get added to the header. • Click **Add New** to enter the IP address range that the IP address in the HTTP header is ignored. • Use the drop-down list to **Upload to Append** or **Upload to Replace** an IP Header range. You must upload a plain text file with each line containing an IP address or a CIDR network. The maximum number of IP range entries supported is 1000.
Action	From the drop down menu, select one of the following: Allow: Allows traffic from the specified Application. Block: Blocks traffic from the specified Application. **Warn:** Warns traffic from the specified Application. **Follow Policy**: Applies the conditional policy that you choose from the existing list.

Certain deployments masks an X-Forwarded-For header with Z-Forwarded-For before adding its own X-Forwarded-For header identifying the originating customer IP address. This prevents the internal IP addresses leaking out of the enforcement nodes. This provides the true static IP address of the user. Hence a request through the proxy will have a static IP address into X-Forwarded-For header. To set up the Advanced Network Rule that only leverages a static IP address as X-Forwarder-For header.

- Source IP Setting: 0.0.0.0/0
- Configure Header Rule (X-Forwarded-For) and upload a .txt file (including the static IP)
- Rule action: Allow
- Set the General bypass rule to Block.

All the source IPs are valid unless the IP matches, it is blocked by General bypass rule.

Multi-factor Authentication

For information about adding the multi-factor authentication rule, see **Multi-factor Authentication with Authenticator**

Zero Sign-on Rule

For more information about adding the Zero Sign-on rule, see **Zero Sign-on with Ivanti Access**

Desktop Trust Rule

For information about adding a desktop trust rule, see the *Ivanti Access Desktop Trust Agent Guide*.

Request Header Rule

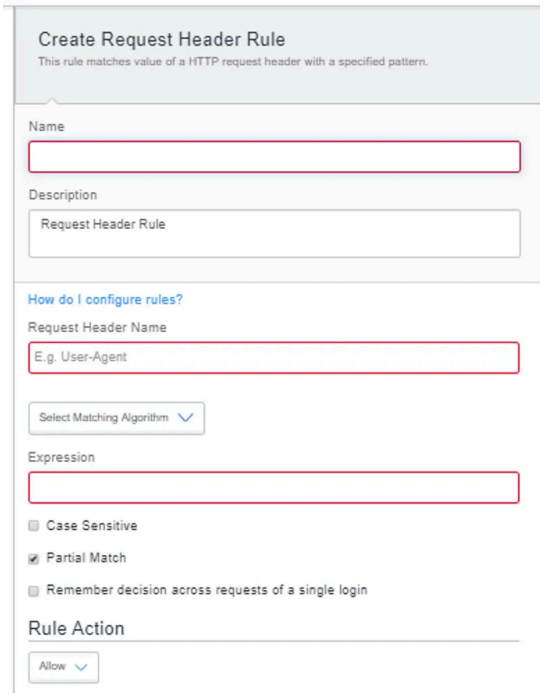
Add the Request Header Rule to match the value of a HTTP request header with a specified pattern. The Request Header rule is very similar to the App rule; however, you can select any header name other than just the User-Agent.

Use case: When the user has Access federated with Microsoft ADFS and Office 365 and then tries to register a device, it gets blocked by the untrusted Apps on Windows 10 rule. If you use the Azure Domain integration, then the actual MDM registration is also done by Azure.

Due to the current policies, there is no option to allow device registrations on these Windows 10 devices except from allowing Edge.

The new Request Header Rule thus helps to match the value of any HTTP request header with a specified pattern.

Figure 2. request header rule



The following table lists the fields in a Request Header Rule:

Item	Description
Name	Enter a name for the conditional rule.
Description	Enter descriptive text for the conditional rule.
Request Header Name	Enter any appropriate header name such as User-Agent.
Matching Algorithm	From the drop-down menu, select one of the following options: Regex: Select if you plan to use a regular expression the header name. Wildcard: Select if you plan to use wildcard for the header name. Literal: Select if the rule should exactly match the configured expression.
Expression	Enter an expression for the app, based on the matching algorithm you selected. Check the **Reports** view to see the header name that you mentioned in the traffic for authentication.
Case Sensitive	Select if the rule should consider the case configured in the expression.
Partial Match	Select if the rule can be applied to a partial match of the configured expression.
Remember decision across requests of a single login	Select this checkbox to remember the action for the first request and to apply the same action for the rest of the requests. This action skips the rule evaluation for the remaining requests of SP login.
Action	From the drop down menu, select one of the following: **Allow**: Allows traffic from the specified Application. **Block**: Blocks traffic from the specified Application. **Warn**: Warns traffic from the specified Application. **Follow Policy**: Applies the conditional policy that you choose from the existing list.

Device Ownership Rule

Add the Device Ownership Rule to control access based on the user's device ownership at the time of registration with Ivanti NMDM. You can impose stricter conditional access policies using this rule. The user's device ownership is identified using an API that is used for a complaint or non-complaint device check. To use this rule, a new rule must be created for each of the device ownership types. If the device ownership is selected as "Device Not Set" and no rule is created for "Device Not Set," by default, all traffic from all the applications is allowed.

The three different types of supported device ownerships are:

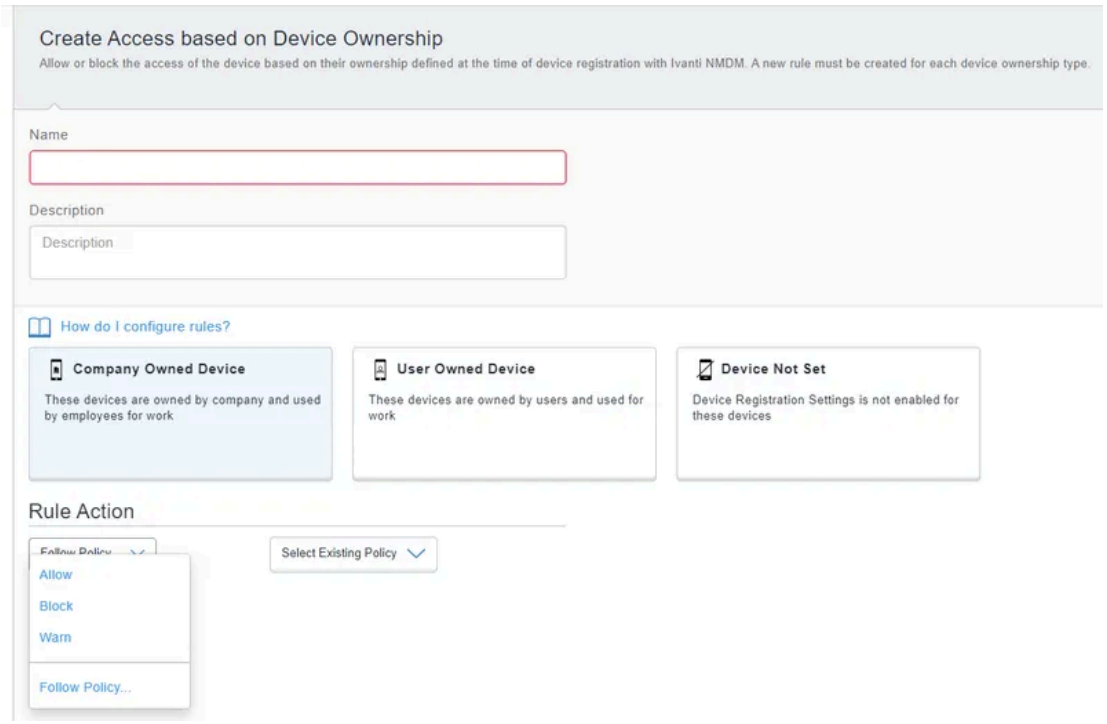
- Company Owned Device
- User Owned Device, and
- Device Not Set

To create the Device Ownership Rule:

1. Navigate to **Profile** > **Conditional Access** > **Add Conditional Policy** > **Add Rule**.
2. Click **Device Ownership** tile.
3. On the *Create Access based on Device Ownership* page, enter a name and description for the rule in the **Name** and **Description** fields, respectively.
4. Select an ownership tile for which you want to create the rule.

5. Select an action from the **Rule Action** dropdown for the selected ownership tile. If you select **Follow Policy** from the dropdown, then you must specify a policy in the **Select Existing Policy** dropdown.
6. Click **Done** to finish configuring the rule.

Figure 3. Device ownership rule



The following table lists the fields and elements associated with the Device Ownership Rule:

Item	Description
Name	Enter a name for the conditional rule.
Description	Enter descriptive text for the conditional rule.
Company Owned Device	Company owned devices used by the employees for work
User Owned Device	User owned devices used for work
Device Not Set	Device registration settings not enabled for devices during registration with Ivanti NMDM.
Rule Action	From the drop down menu, select one of the following: **Allow**: Allows traffic from the specified Application. **Block**: Blocks traffic from the specified Application. **Warn**: Warns traffic from the specified Application. **Follow Policy**: Applies the conditional policy that you choose from the existing list.
Select Existing Policy	An existing policy that could be applied to the rule. This dropdown displays when you select **Follow Policy** option in the **Rule Action** dropdown.

Redirect to IDP Rule

The Redirect to IDP rule lets you redirect to the configured IDP for authentication.

In managed or unmanaged devices flow, if redirect to IDP rule is evaluated, you are redirected to IDP for authentication.

For example, in managed devices, when the federated pairs are selected to perform single sign-on without the need to authenticate at the IdP end and if Redirect to IDP rule is evaluated, user is directed to IDP for authentication even though single sign-on is enabled at pair level.

To create the Redirect to IDP Rule:

1. Navigate to **Profile** > **Conditional Access** > **Add Conditional Policy** > **Add Rule**.
2. Click **Redirect to IDP** tile.
3. On the *Create Redirect to IDP Rule* page, enter a name and description for the rule in the **Name** and **Description** fields, respectively.
4. Select an action from the **Rule Action** dropdown. If you select **Follow Policy** from the dropdown, then you must specify a policy in the **Select Existing Policy** dropdown.
5. Click **Done** to finish configuring the rule.

9.5. Policy chaining

You can chain a conditional policy to a conditional rule in another policy. When the conditional rule is evaluated and the conditions in the rule are met, the conditional rules in the chained policy are also evaluated. This allows you to configure additional conditionals rules to be evaluated for the original rule. This is called policy chaining and allows additional flexibility in evaluating which apps and IP network ranges can access a cloud resource. You can choose a policy from the existing list of policies for a rule to follow. You can chain only one policy to a rule.

9.6. Example setup with conditional rules

In the setup described in this section, traffic from managed apps using AppTunnel (AppConnect apps using AppTunnel and managed apps using Ivanti Tunnel) on an iPhone or iPad, and all traffic from laptops, desktops, and Android and Windows 10 mobile devices flows through Ivanti Access.

- Setup with conditional
- Expected behavior with the example setup

Setup with conditional

The following outlines the example setup with conditional rules:

- Configure Salesforce service provider and related IdP in Federated Pairs.
- Apply Ivanti Tunnel VPN to the Salesforce app.
- Configure the following rules in Conditional Access:

Conditional rule name	Action
Trusted App and Device on iOS	Allow
Untrusted Apps on iPhone	Block
Untrusted Apps on iPad	Block
General Bypass	Allow

> The order of the rules matters. Rules are evaluated in the order they appear.

Expected behavior with the example setup

The following outlines the expected behavior with the example setup:

- Traffic from the managed Salesforce app on an iPhone and on an iPad will be allowed through Ivanti Access. This setup allows apps such as Web@Work that use AppTunnel to also authenticate to Salesforce.
- All other traffic from iPhone and iPad will not be allowed through Ivanti Access.
- Therefore, on an iPad or iPhone, only traffic from the managed Salesforce app and any apps that use AppTunnel will have access to Salesforce.
- This setup allows users on other devices to continue to access Salesforce. Other devices include desktops, laptops, and Windows 10 and Android mobile devices.

For additional examples, seeKB article.

9.7. Managing policies and rules

You can take the following actions on a conditional policy or rule:

- Disable: Disables the conditional rule. The rule is no longer applied.
- Delete: Deletes the conditional rule or policy. You cannot delete a policy that is applied to a federated pair, however you can delete conditional rules in that policy.
- Edit: Allows you to edit the settings in a policy or a rule.
- Reorder: Allows you to reorder the position of the conditional rule.

Applying a conditional policy to a federated pair

See **Assigning a policy to a federated pair**.

Editing a conditional policy

Procedure

1. In the Ivanti Access administrative portal, go to Profile > Conditional Access.
2. To edit the name of a conditional policy, click on the edit icon next to the policy name.
3. To edit the description for a policy, click on the edit icon next to the descriptive text.
4. To make changes to the conditional rules in a policy, click on the directional arrow to expand the policy.

See **Editing a rule**.

5. Click Publish to push the changes associated with the Profile.

Deleting a conditional policy

Procedure

1. In the Ivanti Access administrative portal, go to Profile > Conditional Access.
2. Click on the trash icon next to the policy name you want to delete.
3. In the pop up window, click Delete Policy.
4. Click Publish to update the changes associated with the Profile.

Editing a rule

Procedure

1. In the Ivanti Access administrative portal, go to Profile > Conditional Access.

2. Click on the directional arrow to expand the policy you want to edit.
3. Click on the Edit icon for the conditional rule you want to edit.

For a description of the fields, see **Customizable conditional rules**.

4. Click Done to save the changes.
5. Click Publish to update the changes associated with the Profile.

Disabling, enabling, or deleting a rule

Procedure

1. In the Ivanti Access administrative portal, go to Profile > Conditional Access.
2. Click on the directional arrow to expand the profile you want to edit.
3. For each conditional rule you can do the following:
   - Disable: The rule is no longer applied.
   - Enable: Enables the conditional rule. The rule is applied in the order in which it is listed.
   - Edit: Modifies the conditional rule.
   - Delete: Deletes the conditional rule.
   - Reorder: Move the conditional rule higher or lower in the list.
4. Click Publish to update the changes associated with the Profile.

9.8. Enabling the compliance remediation page

If a device is not in compliance, authentication traffic to Access is blocked and the user is presented with an Internet unavailable error. The error is logged in Access in Reports > Errors.

Enabling Compliance Remediation Page allows you to specify a customized remediation page to the device user.

- This feature is not available for Ivanti Access + Standalone Sentry deployments.
- If split tunneling is configured, only authentication traffic is blocked. All other traffic is allowed to destination.

Before you begin

Ensure that you have created a remediation page to present to users from non-compliant devices. For information on creating a custom remediation page, see **Adding a remediation page**.

Procedure

1. In Access, navigate to Profile > Conditional Access.
2. For Compliance Remediation Page, slide the toggle to ON.

3. From the drop-down list, select a remediation page.
   The remediation page is presented to users attempting to access a cloud service from a non-compliant device.
4. Click Save and publish the changes.

10. Configuring Mobile App Single Sign-on (SSO)

In an Ivanti Access deployment, single sign-on (SSO) allows users access to enterprise cloud services from the apps on their mobile devices without having to enter passwords. Single sign-on is available only for managed apps, including the Safari browser, on managed devices using Ivanti Tunnel. Access identifies the user based on the certificate used to establish the VPN tunnel. Based on the information provided in the certificate, Ivanti Access generates a federation response to the service provider (SP) without redirecting the user to the original identity provider (IdP). Access determines the contents of the federation response based on the Native Mobile Application Single Sign-On (SSO) configuration in Ivanti Access, which includes the user identifying information that the SP expects.

The user identifying information that the SP expects is typically available in the enterprise LDAP directory. The UEM SCEP that Ivanti Tunnel uses captures the user information from LDAP and makes the information available in the Ivanti Tunnel certificate. The Native Mobile Application Single Sign-On (SSO) configuration uses the information from the Ivanti Tunnel certificate in the federation response to the SP.

This feature is also referred to as certificate-based single sign-on.

Before you begin

- Ensure that the user identifying information that the service provider (SP) expects is available in the Ivanti Tunnel certificate.

The following are examples of user identifying information:

- Email address
- Immutable ID
- Configure the subject alternative names in the SCEP setting for the Ivanti Tunnel certificate in the UEM.

Example: If you are using the email address and immutable ID as the user identifying information, configure the following in the subject alternative name:

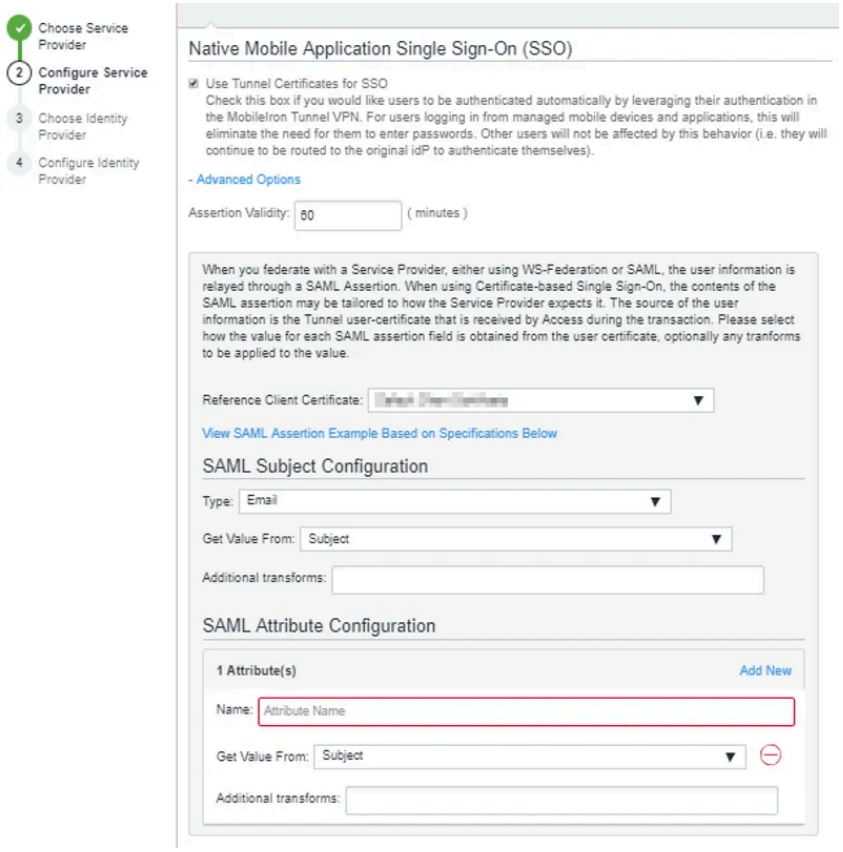
Type	Value
RFC 822 Name	$EMAIL$
NT Principal Name (Required only for Office 365, holds the unique immuatble ID)	$USER_CUSTOM1$

- SCEP obtains users information from LDAP. Therefore, ensure that the LDAP settings in UEM fetch the appropriate attributes from LDAP. If you are using email and immutable ID as the user identifying information, ensure that the following values are available in LDAP settings in UEM:
- Email: userPrincipalName
- Custom 1: ObjectGUID
- For more information, see **Configuring Ivanti EPMM for SSO certificates**, **Configuring Ivanti Neurons for MDM for SSO certificates**, and **Customizing certificates for single sign-on in Ivanti Access**.
- To make it easier to configure mobile application single sign-on, upload a sample Ivanti Tunnel certificate and assign user friendly names to each field in the certificate. For more information, see **User Certificates**.

Procedure

1. In Ivanti Access, go to Profile > Federated Pairs.

2. Click +Add New Pair or edit an existing pair.
3. In the service provider (SP) configuration page, scroll down to the Native Mobile Application single Sign-On (SSO) section.
   Figure 1. Application single sign-on advanced options



1. Select **Use Ivanti Tunnel Certificates for SSO**.
2. Expand Advanced Options.
3. From the **Reference Client Certificate** drop-down list, select the sample Ivanti Tunnel certificate.
4. In the SAML Subject Configuration section, for Type, select
   - Unspecified for SAML
   - the type the service provider expects for WS-Fed.
5. For Get Value From, select the certificate field from which to get the value.
   You created the user-friendly names when you added the sample Ivanti Tunnel certificate to Access in the User Certificates tab.
6. (Optional) For Additional Transforms: Enter the required transforms if the SP expects values that are derived from the value provided in the certificate.
7. (Optional) SAML Attribute Configuration. The SAML attribute configuration populates the Attribute and value section of the federation response from Access. Configure this if the SP expects such attributes. Click New to add each new attribute.
8. (Optional) For Encryption Algorithms, select the data encryption algorithm and the key transport algorithm.
   The encyrption options are available only if Encrypt SAML assertions is enabled.
9. (Optional) Click the View SAML Assertion Example Based on Specifications Below link to verify that the SAML assertion contains the required user-identifying information.

Related topics

- For information about configuring the assertion fields in a federation response, see **Customizing certificates for single sign-on in Ivanti Access**.
- For information about encrypting SAML assertions, see **Encrypting SAML assertions**

11. Split Tunneling

In an Ivanti Access deployment, all authentication traffic for the federated pairs configured in Access goes through Access using Tunnel VPN. Depending on the type of Ivanti Access deployment, all other traffic through Tunnel VPN goes directly to the destination server or through Standalone Sentry. Split tunneling allows you to control which traffic goes through Standalone Sentry to on-premise enterprise resources and which traffic goes directly to the destination.

For example, you may need to configure split tunneling if your deployment uses Ivanti Tunnel VPN:

- to authenticate to a service provider (SP), such as Salesforce, via Access.
- to access an internal SharePoint server such as sharepoint.mycompany.com via Standalone Sentry.

In the example, federated authentication traffic to Salesforce goes through Access, traffic to the SharePoint server goes through Standalone Sentry, and data traffic to Salesforce goes directly to the destination.

Split tunneling is supported for both Ivanti Access and Ivanti Access + Standalone Sentry deployments.

The following topics provide additional information about split tunneling:

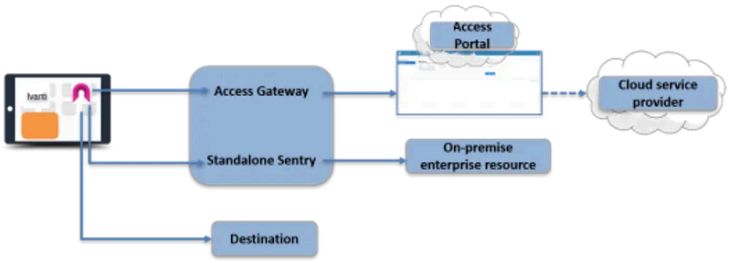
- **Split tunneling in an Ivanti Access + Standalone Sentry deployment**
- **Split tunneling in an Ivanti Access deployment**
- **Split tunneling for Android**
- **Split tunneling for iOS and macOS**
- **Overview of steps for configuring split tunneling in Ivanti Access**

Split tunneling in an Ivanti Access + Standalone Sentry deployment

In an Ivanti Access + Standalone Sentry deployment, all authentication traffic for the federated pairs configured in Access goes to Ivanti Access. All other Ivanti Tunnel VPN traffic goes through Standalone Sentry. Split tunneling allows you to specify how the traffic that is not federated through Ivanti Access is handled. You can specify whether the traffic goes through Standalone Sentry or directly to the destination.

> Split Tunneling is disabled if all the Sentry profiles from VPN are removed from all the registered EMMs.

Figure 1. Split tunneling in an Ivanti Access + Standalone Sentry deployment



Split tunneling in an Ivanti Access deployment

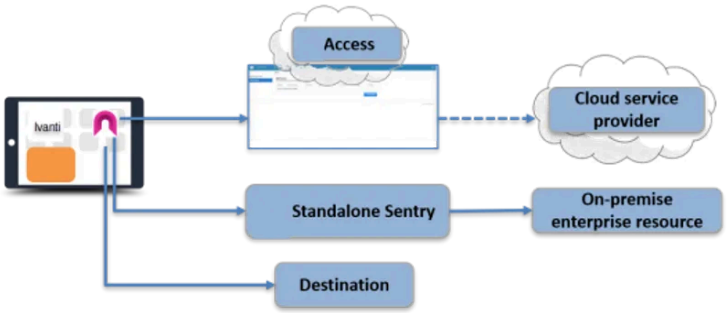
In an Ivanti Access deployment, by default, all authentication traffic for the federated pairs configured in Access goes to Access. All other traffic goes directly to the destination. However, you may require that some traffic go through Standalone Sentry to access on-premise enterprise resources. In such cases, you configure split tunneling to do the following:

- Authentication traffic for federated pairs configured in Ivanti Access goes through Access.
- Traffic to on-premise enterprise resources goes through Standalone Sentry.
- All other traffic goes directly to destination.

Figure 2. Default split tunneling in an Access (without Standalone Sentry) deployment



Figure 3. Split tunneling Access (without Standalone Sentry) and Standalone Sentry



Split tunneling for Android

For Android apps, split tunneling is configured in the Ivanti Tunnel VPN configuration for Android or in the Ivanti Tunnel for Android enterprise configuration. Split tunneling using Ivanti Tunnel for Android native and Android enterprise is handled in the Tunnel configuration for those devices. See the *Ivanti Tunnel for Android Guide* for information about setting up split domains and routes lists.

> In an Ivanti Access deployment, tunneling to both enterprise cloud services and to on-premise enterprise resources is not supported with Ivanti Tunnel for Samsung Knox Workspace.

Split tunneling for iOS and macOS

For iOS apps and macOS, split tunneling is configured in Ivanti Access in Profile > Split Tunneling. The split tunneling configuration in Ivanti Access is only applicable to Ivanti Tunnel for iOS and macOS.

Overview of steps for configuring split tunneling in Ivanti Access

The following is an oveview of steps for configuring split tunneling in Ivanti Access:

1. **Enabling split tunneling**
2. **Adding domains for split tunneling**

11.1. Enabling split tunneling

The split tunneling feature is disabled by default.

To configure split tunneling for iOS devices, enable split tunneling and configure the domains to go to Standalone Sentry or direct to destination.

Deleting a Standalone Sentry configuration from an UEM and performing a sync removes the Standalone Sentry data from Access. This also disables split tunneling. To stop traffic from being redirected, Publish the changes in Ivanti Access.

Before you begin

- To access on-premise enterprise resources through Standalone Sentry, ensure that you have deployed Standalone Sentry and that the Standalone Sentry is selected in the Ivanti Tunnel VPN configuration.
- In an Ivanti Access + Standalone Sentry deployment, ensure that you have an SP and IdP pair configured. An Access profile is created only if an SP-IdP pair is configured. Assign Standalone Sentry to the profile. Assigning the Standalone Sentry to an Access profile, allows Standalone Sentry to pull the Access configurations, which includes the split tunneling configuration. The SP-IdP pair can be an SP-IdP pair with dummy data.

Procedure

1. In Ivanti Access, go to Profile > Split Tunneling.

The Split Tunneling Configuration page displays.

2. For Enable Split Tunneling, move the toggle to On.

By default, traffic that does not go to Ivanti Access goes directly to destination.

3. To change the default behavior, click the link next to Default Action.

Related topics

For more information, see the **KB article**.

> When you enable split tunneling, the **Tunnel authentication traffic to Access** rule is added by default. This rule is the default domain to which traffic is sent. The rule cannot be edited.

11.2. Adding domains for split tunneling

Add destination domains to configure which domains go directly to the destination and which domains go via Standalone Sentry.

Before you begin

- Verify that the Ivanti Tunnel-enabled apps and Safari are tested before deploying to production. This is because enabling or disabling split tunneling in Ivanti Access impacts the traffic through Ivanti Tunnel .
- Verify that split tunneling is enabled in Ivanti Access. See **Enabling split tunneling** .

Procedure

1. In Ivanti Access, go to Profile > **Split Tunneling**.

The Split Tunneling Configuration page displays.

2. Click **Add Domain**.
3. In the **Add Split Tunneling Rule** pane, enter the name for the rule.
4. (Optional) Enter a description for the domain.
5. In the **Split Tunnel Config** section, enter the destination domain.

Examples: login.example.com or *.example.com

6. In the **Action** drop-down, select the appropriate action.

- **Send to destination via Sentry**: Traffic destined to the domain is sent to Standalone Sentry.
- Send directly to destination: Traffic destined to the domain goes directly to the destination.

7. Click **Done**. The domain rule is added to the table and is enabled by default.
8. Click Publish to make the changes available.

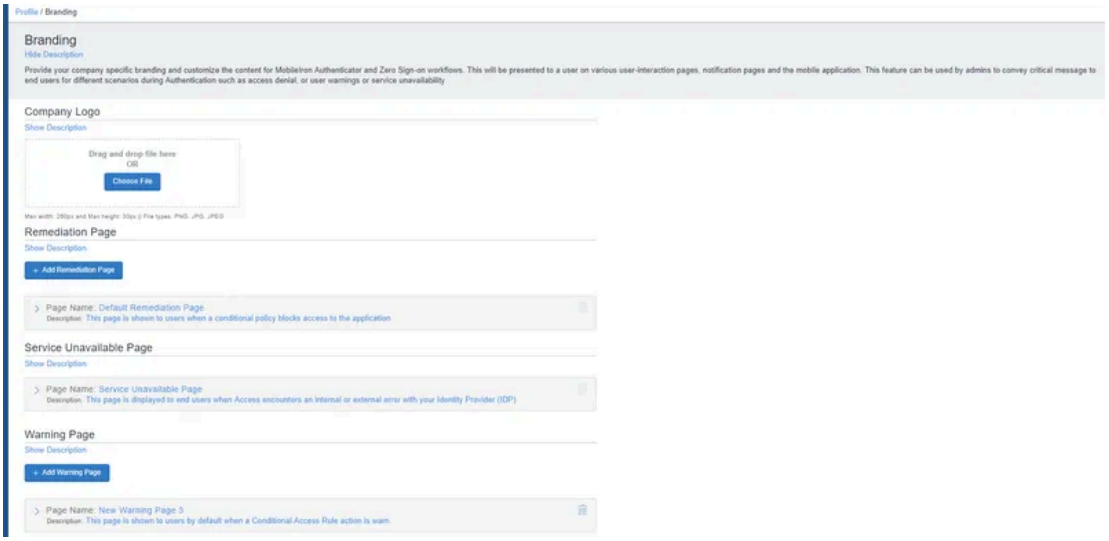
12. Branding

The Branding page allows you to customize what users see if an app on a device cannot access a cloud resource.

12.1. Branding overview

You configure branding in Profile > Branding. Ivanti Access provides the following options to customize the branding and messaging that users see in the interaction pages on their device.

Figure 1. Branding options



- Company Logo: Upload your company logo to customize what device users see in interaction pages for Zero Sign-on and Authenticator. See, **Configuring branding for Zero Sign-on**.
- Remediation Page: Use this page to customize the message that device users see if a conditional rule blocks access to an application. You can redirect device users to a URL or create a custom error page. You can add a different remediation page for each conditional rule to block access to an application. See, **Adding a remediation page**.
- Service Unavailable Page: Use this page to customize the message that the device users see if an application cannot access the cloud service or any other reason. For example, the service may not be available due to network issues. You can redirect device users to a URL or create a custom error page.
- Warning Page: Use this page to customize the message that device users see when conditional access rule has the action set to *warn*. You can allow users to continue through this warning.

The following default interaction pages are available:

- **Interaction page when access to ivanti neurons for mdm application is blocked on desktop and mobile**
- **Interaction page when the service is unavailable on desktop and mobile**
- **Interaction page when access to ivanti neurons for mdm application is blocked on desktop and mobile**

Figure 2. Interaction page when access to ivanti neurons for mdm application is blocked on desktop and mobile

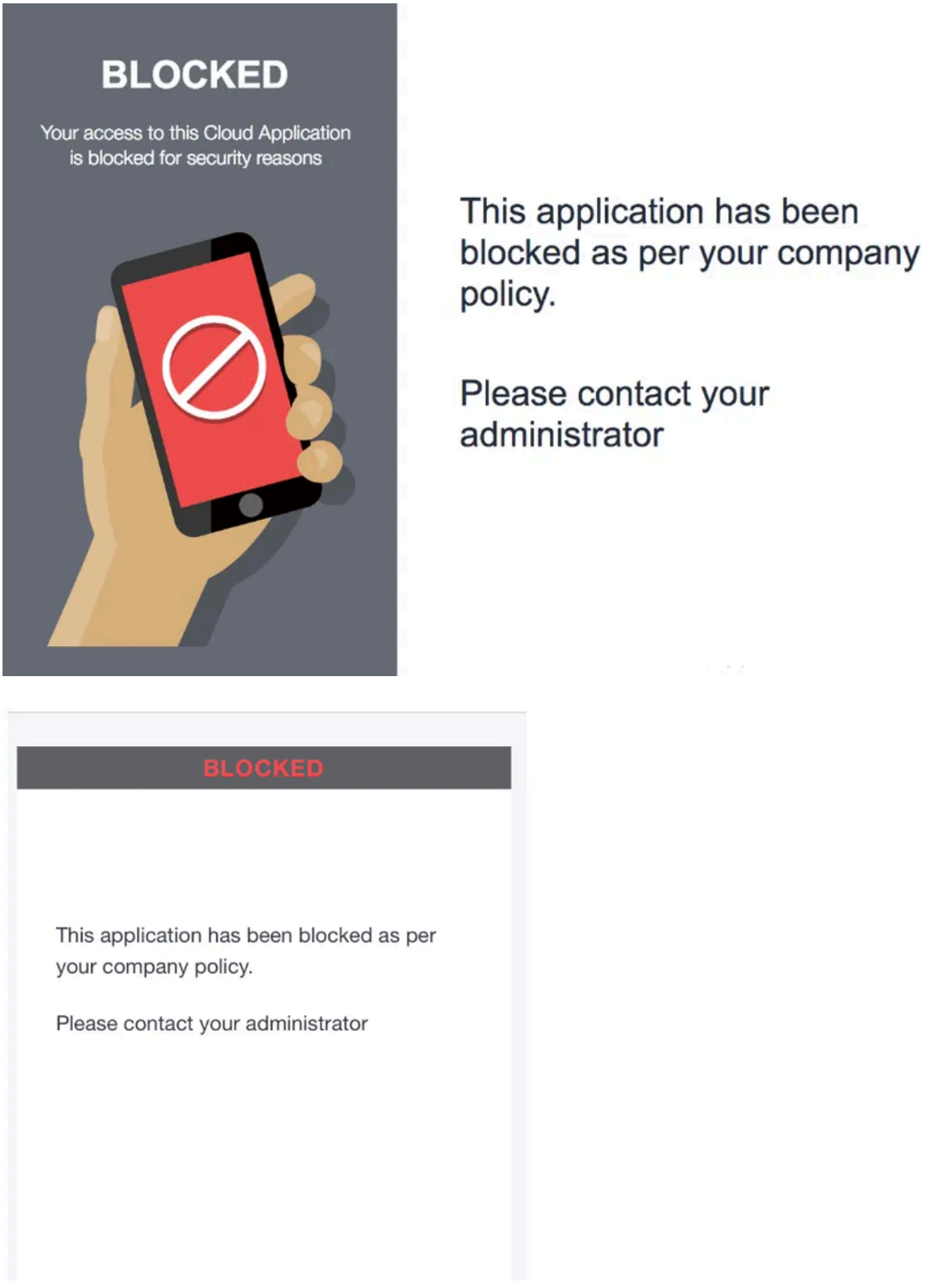


Figure 3. Interaction page when the service is unavailable on desktop and mobile

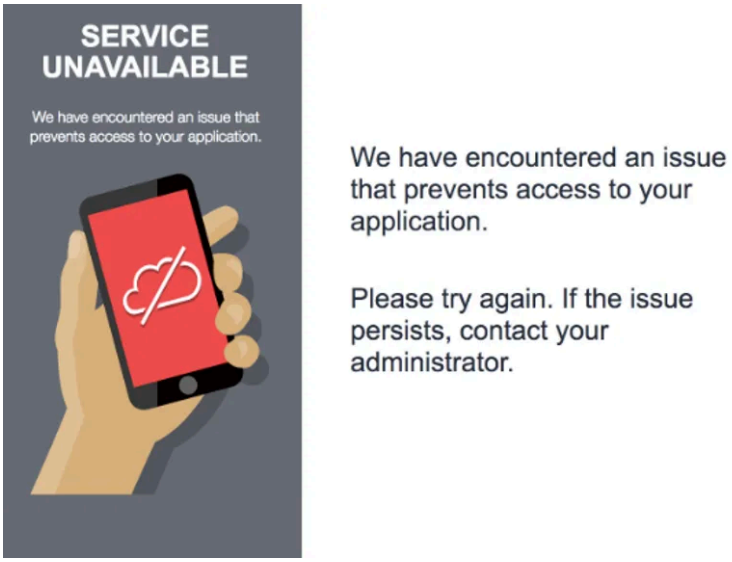
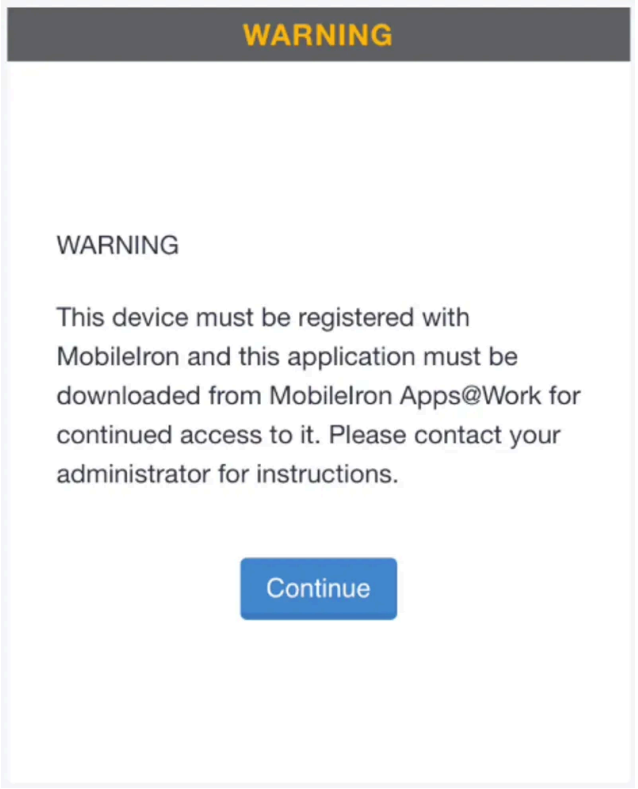


Figure 4. Interaction page with a warning for security reasons




WARNING
WARNING
This device must be registered with MobileIron and this application must be downloaded from MobileIron Apps@Work for continued access to it. Please contact your administrator for instructions.
Continue

12.2. Adding a remediation page

A remediation page is presented to device users if a conditional rule blocks access to a cloud service. You can customize the default remediation page that is provided or you can create a new remediation page. You can create separate remediation pages for each conditional rule to customize the remediation actions that device users see.

After you create a remediation page, navigate to Profile > Conditional Access to associate the remediation page with the conditional rule.

Before you begin

- If your deployment is Ivanti Access + Standalone Sentry, verify that you have installed Sentry 9.1.2 through the most recently released version as supported by Ivanti.
- Verify that you have a working federated pair before enabling this feature.

Procedure

1. Navigate to Profile >**Branding.**
2. Click **Add Remediation Page** in the Remediation Page Branding panel.
   The new Remediation page is added below the default remediation page.
3. Customize and preview the remediation page.
4. (Optional) The administrator can choose to associate an appropriate Remediation page with the rule.
5. Click **Publish** to apply the conditional rule with the profile.

In Ivanti Access + Standalone Sentry deployment, there is a delay of fifteen minutes for Sentry to be updated.

You can customize what the user sees in one of the following ways. If the branding is not customized, the default message is displayed to the device user.

- Redirecting device users to a URL
- Creating a customized message

12.3. Redirecting device users to a URL

If an application is blocked or the connection fails for any reason, you can redirect the device users to a specified URL.

Procedure

1. In Ivanti Access, go to Profile > Branding > Remediation Page or Service Unavailable Page.
2. In **Page Options**, select I want to redirect users to my website URL.
3. Enter the redirect URL in the text box for Redirect URL.

The redirect URL must include http:// or https://.

4. Click Save Changes to save the settings.

If a redirect URL is configured in the Remediation Page, device users are directed to the redirect URL if an application is blocked.

If a redirect URL is configured in the Service Unavailable Page, device users are directed to the redirect URL if the cloud service is unavailable. For example, a 503 error.

12.4. Creating a customized message

If an application is blocked or the connection fails for any other reason, you can customize the error message presented to the device user. You can customize the error message by adding your company logo, company name, custom text, and a Help link.

Procedure

1. In the Ivanti Access administrative portal, go to Profile > Branding > Remediation Page or Service Unavailable Page.
2. In **Page Options**, select I want to customize the page presented to users.
3. In **Customization Settings**, click Choose File to navigate to the location of your company logo.

The graphic must be no more than 300 pixels wide and 50 pixels high.

If you do not want to upload a graphic, select Remove logo.

4. Enter a Message describing why users have encountered the issue.

You can enter up to 255 characters.

5. Enter a Help message describing how users can access help or report the issue. You can enter up to 255 characters.
6. Enter the Help Link. Choose http:// or https://, and enter the URL in the text box.
7. Enter the Help Link Text that the device users see instead of the URL.
8. Click Save Changes to save the settings.

The Preview section displays the customized message.

Device users are now presented with the customized message.

> Use Reset to Default option, in the Remediation page or Service Unavailable page to restore the default values when the profile was created.

Creating a customized warning message

You can customize the warning messages to device users when a Conditional Access Rule is set to warn.

Procedure

1. In the Ivanti Access administrative portal, go to Profile > Branding > Warning Page.
2. In **Customization Settings**, click Choose File to navigate to the location of your company logo.

The graphic must be no more than 300 pixels wide and 50 pixels high.

If you do not want to upload a graphic, select Remove logo.

3. Enter a Warning Message about the issue.

You can enter up to 255 characters.

4. Enter a Help message describing how users can access help or report the issue. You can enter up to 255 characters.
5. Enter the Help Link. Choose http:// or https://, and enter the URL in the text box.
6. Enter the Help Link Text that device users see instead of the URL.
7. Enter the Continue Button Text that the users see to click and proceed.
8. Click Save Changes to save the settings.

The Preview section displays the customized message.

Device users are now presented with the customized message.

> Use the Reset to Default option, in the Warning page to restore the default values when the profile was created.

13. Session Revocation

Ivanti Access provides authentication assertions, based on the SAML or WS-Federation protocols, to cloud services. As a result of the authentication, the app gets a session token from the cloud service. This token is stored on the device and allows the app to access the cloud service without having to reenter user credentials. The session token expires after a certain length of time, after which the user is prompted to authenticate again.

> Session revocation is now triggered for multi-user sign-in applications. On a shared device, even if the user is signed-out , session revocation is still triggered.
> For example: On an iOS shared device, if the user uses Office 365 and later logs out of the device and when a new user logs into the device, the user is prompted for credentials again.

The following topics provide more information about session revocation:

- **About session revocation**
- **Configuring Session Revocation**
- **Session revocation report**
- **What users see if session revocation is configured**

13.1. About session revocation

Session revocation allows administrators to terminate or revoke the session token if a device is out of compliance and the UEM policy action is blocked or a device is retired. The revocation prevents out of compliance and retired devices from continuing to use a session token on the device to access the cloud service. Session revocation impacts the sessions of the managed applications (service provider) on all the devices that the user uses to access the cloud service. After a session token is revoked, the user has to re-authenticate with the service provider through Access to get a new session token. When the user tries to re-authenticate, Access enforces conditional policies and unblocks the app.

> You can update the compliance policies in Ivanti EPMM> Policies & Configs > Compliance Policies.

Compliance policy

- Support for policy action based Session revocation
- Ivanti Access Session revocation service (SRS) workflows are improved to consider UEM (Ivanti EPMM) policy action configurations
- Session revocation is triggered only for those devices which are non compliant and also have a blocking action setup against the corresponding policy
- Session revocation actions is also triggered for other device states such as quarantine, wipe, and retire
- For all other cases of violation, if there is a non blocking action (such as email, monitor, notify, etc) no action will be taken by Ivanti Access.

Session revocation is supported for Ivanti Access deployments for Office 365 using the Azure Graph API and G Suite using Google API console. However, the session revocation feature is not supported for Ivanti Access + Standalone Sentry deployments.

- To start session revocation, Ivanti Access verifies the compliance action configured on UEM when the device goes out of compliance and the actions configured against them. For Ivanti Neurons for MDM or Ivanti EPMM deployments, session revocation is triggered if the device is out of compliance and the compliance action is either block or quarantine. Session revocation is also triggered if the device is Wiped or Retired.
- To start session revocation, Ivanti Access verifies the compliance action configured on UEM when the device goes out of compliance and the actions configured against them. For Ivanti EPMM deployments, session revocation is triggered if the device is out of compliance and the compliance action is block. Session revocation is not triggered if the action is SendAlert.

13.2. Configuring Session Revocation

Session revocation is configured in Ivanti Access.

Before you begin

- Verify the following before configuring session revocation:
  - You have an Ivanti Access deployment with a UEM.
  - The Ivanti Access administrator has Common Platform Services (CPS) role in UEM.
    Ivanti Neurons for MDM: For information on assigning roles, see "Assigning Roles to Users" in the *Ivanti Neurons for MDM Guide* or click Help in the Ivanti Neurons for MDM administrative portal.
    Ivanti EPMM: For information on assigning roles, see the *Ivanti EPMM Delegated Administration Guide*.
  - Common Platform Services Notifications is enabled in UEM.
    Ivanti Neurons for MDM: Go to Admin > Common Platform Services Notifications, and enable Common Platform Services Notifications.
    Ivanti EPMM: From the Ivanti EPMM command line interface (CLI), enter the following command in CONFIG mode - activemq
  - Session tokens are revoked if the device state is retired or non-compliant as reported by the UEM to Ivanti Access.
    For information about configuring compliance polices, see your UEM documentation.
    Ivanti Neurons for MDM: See "Policies" in the *Ivanti Neurons for MDM Guide* or click Help in the Ivanti Neurons for MDM administrative portal.
    Ivanti EPMM: See the *Ivanti EPMM Device Management Guide*.
  - Users are registered LDAP users with custom attribute of userPrincipalName and objectGUID in a UEM.
    Ivanti Neurons for MDM: See **Configuring LDAP in Ivanti Neurons for MDM for session revocation**.
    Ivanti EPMM: See **Configuring LDAP in Ivanti EPMM for session revocation**.
  - Port 8883 in the firewall is open to allow Ivanti Access to pick up queued up events.
- For Office 365
  - A federated pair with Office 365 and ADFS configured in Ivanti Access
  - An app registration for the Ivanti Access revocation service in Microsoft Azure. This set up provides Access permission to revoke session tokens for Office 365.
    For information about creating an app registration for the Ivanti Access session revocation service, see the knowledge base article
    Configuring an application in Azure for the session revocation service (SRS) for Office 365 (Azure AD). Make a note of the Azure directory ID, application ID, and the secret key.
- For G Suite
  - A federated pair with G Suite and any appropriate IdP configured in Ivanti Access.
  - Generate a service account key file using Google API console. This set up provides Ivanti Access permission to revoke session tokens from G Suite.
    For more information about creating the service account key file, see the knowledge base article **Configuring G Suite for the session revocation service (SRS)**. Make a note of the G Suite service account key.

Procedure

1. In Ivanti Access, go to Profile > Session Revocation.
   The Service Provider Configuration page displays.

2. In the Service Provider Configuration page, click +Add Configuration.
3. For service provider, click Office 365 or G Suite appropriately.
4. Enter the following information.

Item	Description
Name	Enter a name for the configuration.
Add Description	Add a description for the configuration.
Configuration for Office 365	
Azure Directory ID	Enter the Azure directory ID.
Application ID	Enter the application ID from the app registration you created for the Ivanti Access session revocation service in Azure.
Secret key	Enter the Azure secret key from the app registration you created for the Ivanti Access session revocation service in Azure.
Configuration for G Suite	
G Suite Service Account Key	Service account key file in JSON format. To obtain this file, follow KB article:
G Suite administrator Email ID	Enter the Super Admin email ID.

5. Click Save.

13.3. Session revocation report

For information on which user and service provider (SP) a revocation action was performed, see Reports > Session Revocation in the Ivanti Access administrative portal.

The report provides status information on whether the revocation was successful or not and the context for the revocation.

13.4. What users see if session revocation is configured

If the session token is revoked, users are prompted to log in to the cloud service. Based on conditional policies, Ivanti Access evaluates whether the user on the device has access to the cloud service. If access is denied, a message is presented to the user stating that they are blocked by the administrator from accessing the service.

14. Zero Sign-on with Ivanti Access

With Fast Identity Online (FIDO2) or extended Zero Sign-on solution, Ivanti provides ease of access to enterprise resources within a highly secure framework. Users access enterprise cloud resources from either unmanaged or managed devices without the requirement of having to enter their username and password.

The following provides information about FIDO2 or extended Zero Sign-on with Ivanti Access:

- Overview
- Configuring Zero Sign-on in Ivanti Neurons for MDM
- Configuring Zero Sign-on in Ivanti EPMM
- Configuring Zero Sign-on in Ivanti Access
- Authenticate
- What users see for FIDO2
- Client Registration Settings

14.1. Overview

Using Fast Identity Online (FIDO2) secure authentication protocols, Ivanti extends the Zero Sign-on solution to third-party managed devices. FIDO2 is the industry standard that replaces passwords with a login experience that is passwordless, fast, and secure across websites and apps.

For information about the FIDO2 standard, see **https://fidoalliance.org**.

Key features

- FIDO2 standard provides Secure, Phishing-proof, and convenient methods of authentication.
- Users never need to enter username.
- Users never need to enter passwords.
- FIDO2 uses biometric authentication.
- FIDO2 has standard around no username authentication too.

Use cases

FIDO2 is supported on desktops managed by Ivanti Neurons for MDM, Jamf and SCCM.

> Zero Sign-on with FIDO2 solution is for managed desktops only and not for mobiles. Authenticate must be installed on your desktop for this solution to function.

Deployment use cases

The following use cases are supported for FIDO2 or Zero Sign-on solution:

Deployment Use cases	Notifications	Interaction Use case
Passwordless login to cloud services from cloud managed desktops	• Biometrics on the desktop, or • Push notifications to a managed device or a Auth-only device.	User verification (Step Up Authentication) is disabled for 3rd party managed UEM desktops along with device authentication • only device authentication is done using FIDO2 client on desktop Block unmanaged traffic from unmanaged devices which are not 3rd party UEM managed • block the access if FIDO2 authentication cannot be performed Block 3rd party UEM managed desktops which are non compliant where device posture is not correct
Passwordless login to cloud services from Jamf managed desktops	• Biometrics on the desktop, or • Push notifications to a managed device or a Auth-only device.	• Allow 3rd party UEM managed desktops which are non compliant where device posture is not correct • Allow 3rd party UEM managed desktops which are non compliant where device posture is not correct • User verification is enabled for 3rd party managed UEM desktops along with device authentication ◦ Along with device authentication, user verification mus be done which can be performed either using biometrics of desktops or mobile devices or using username or password authentication with original IdP.
Passwordless login to cloud services from SCCM managed desktops	• Biometrics on the desktop, or • Push notifications to a managed device or a Auth-only device.	• Allow 3rd party UEM managed desktops which are non compliant where device posture is not correct • Allow 3rd party UEM managed desktops which are non compliant where device posture is not correct
Passwordless login to a desktop	• Push notifications to a managed device or a Auth-only device	User verification is disabled for 3rd party managed UEM desktops along with device authentication • only device authentication is done using Authenticate on desktop
Passwordless login from unmanaged devices	• QR code • Push notifications to a managed device or a Auth-only device • administrator mandates compliance check to be performed for these devices and block if they are non compliant	• Allow unmanaged traffic from unmanaged devices which are not 3rd party UEM managed. • Block unmanaged traffic from unmanaged devices which are not 3rd party UEM managed

Required components

- Ivanti Access
- Ivanti Neurons for MDM deployment

- Authenticate for macOS and Windows 10
- If FIDO2 is not enabled, then the following components are required in an Ivanti Access deployment:
  - Ivanti Tunnel configuration with Ivanti Access enabled.
  - Ivanti Tunnel deployed to devices.

Ivanti Tunnel only works with managed desktops and does not work for other 3rd party managed devices.

Supported devices

- macOS devices managed by Ivanti Neurons for MDM
- Windows 10 devices managed by Ivanti Neurons for MDM

Supported browsers

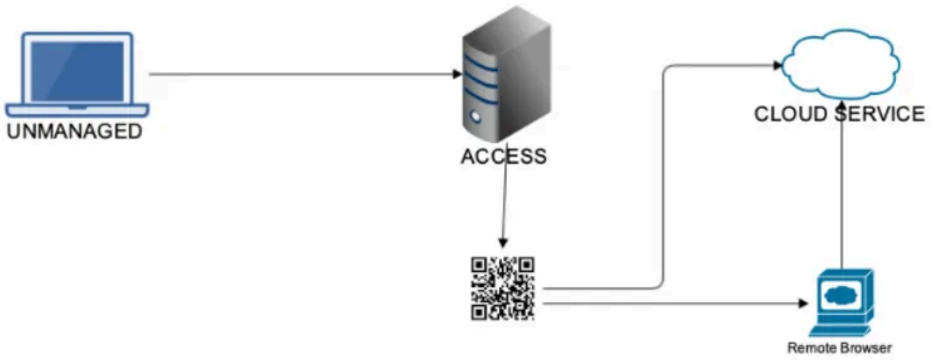
- macOS: Safari, Chrome
- Windows 10: Edge, Chrome, Firefox

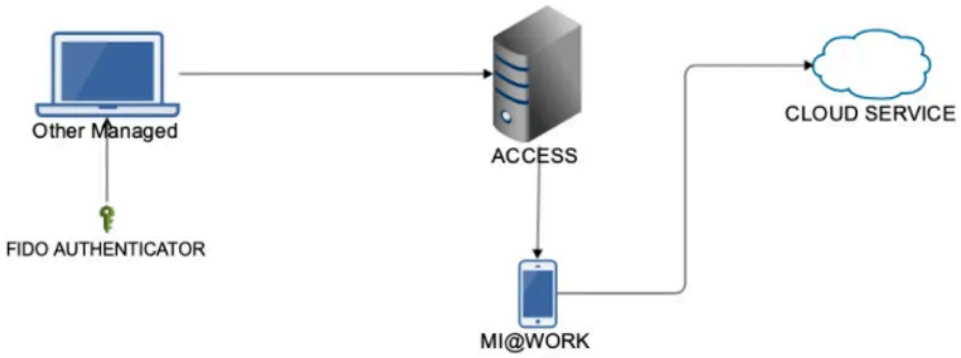
Authentication flow types

The following flow types lists the authentication workflow in a FIDO2 solution:

- Managed flow
- Unmanaged flow
- Other managed flow


TUNNEL
MI Managed
ACCESS
CLOUD SERVICE


UNMANAGED
ACCESS
CLOUD SERVICE
Remote Browser


Other Managed
FIDO AUTHENTICATOR
ACCESS
CLOUD SERVICE
MI@WORK

14.2. Configuring Zero Sign-on in Ivanti Neurons for MDM

Create a Zero Sign-on configuration in Ivanti Neurons for MDM and sync with Ivanti Access.

Before you begin

Ensure that you have set up Ivanti Access with Ivanti Neurons for MDM. See **Overview of configuration with Ivanti Neurons for MDM**.

Procedure: Overview of steps

1. **Creating a Zero Sign-On configuration in Ivanti Neurons for MDM**
2. **Syncing the Zero Sign-On configuration with Ivanti Access**

Creating a Zero Sign-On configuration in Ivanti Neurons for MDM

In Ivanti Neurons for MDM, create a Zero Sign-on configuration.

Before you begin

Ensure that you have configured Zero Sign-on in Ivanti Access.

Procedure

1. In Ivanti Neurons for MDM, go to Configurations > + Add > Saas Sign-On.
2. In the Name field, enter a name for the configuration.
3. (Optional) Expand + Add Description, to add a description for the configuration.
4. For SCEP Identity, select the identity certificate you created for Ivanti Tunnel.
   The Ivanti Tunnel certificate is the same certificate you used to set up mobile app single sign-on in Ivanti Access.
5. Turn on the Enable FIDOtoggle switch to enable FIDO 2 authentication.
6. Select a distribution option.
   The configuration is distributed to the devices in the selected option.
7. Click Done.

Related topics

- For more information about configuring mobile app single sign-on (SSO):
  - For a federated pair, see **Configuring Mobile App Single Sign-on (SSO)**.
  - For delegated IdP, see **Configuring Ivanti Access as the delegated IdP** .

Syncing the Zero Sign-On configuration with Ivanti Access

Sync with Ivanti Access to pull the Zero Sign-on configuration from the UEM.

Procedure

1. In Ivanti Access, navigate to the UEM tab.
2. Select the Ivanti Neurons for MDM UEM and click the Sync UEM icon.

3. Enter the UEM administrator credentials .
4. Enter the credentials and click Verify.
5. Click Done.
   The SaaS Sign-on configuration and Authenticate configuration is now synced with Ivanti Access.

14.3. Configuring Zero Sign-on in Ivanti EPMM

Create a Zero Sign-on configuration in Ivanti EPMM and sync with Ivanti Access.

Before you begin

You have set up Ivanti Access with Ivanti EPMM. See **Overview of configuration with Ivanti EPMM**.

Procedure: Overview of steps

1. **Creating a Zero Sign-on policy in Ivanti EPMM**
2. **Syncing the Zero Sign-on policy with Ivanti Access**

Creating a Zero Sign-on policy in Ivanti EPMM

In Ivanti EPMM, create a Zero Sign-on policy.

Before you begin

Ensure that you have configured Zero Sign-on in Ivanti Access.

Procedure

1. In Ivanti EPMM, go to Policies & Configs > Policies > Add New > SaaS Sign-on.
2. In the Name field, enter a name for the configuration.
3. For Status, select Active.
   Active is default status.
4. (Optional) Add a description for the policy.
5. For Identity Certificate, select the certificate enrollment setting you created for Ivanti Tunnel.
   The Ivanti Tunnel certificate is the same certificate you used to set up mobile app single sign-on in Ivanti Access.
6. Turn on the Enable FIDOtoggle switch to enable FIDO authentication.
7. Click Save.
8. Apply the policy to a label.
   1. Select the SaaS sign-on policy.
   2. Click Actions > Apply To Label.
   3. Select the labels to apply and click Apply.

Related topics

- For more information about configuring mobile app single sign-on (SSO):
  - For a federated pair, see **Configuring Mobile App Single Sign-on (SSO)**.
  - For delegated IdP, see **Configuring Ivanti Access as the delegated IdP** .

Syncing the Zero Sign-on policy with Ivanti Access

Sync with Ivanti Access to pull the Zero Sign-on configuration from the UEM.

Procedure

1. In Ivanti Access, navigate to the UEM tab.
2. Select the Ivanti EPMM UEM and click the Sync UEM icon.
3. Enter the credentials and click Verify.
4. Click Done.

14.4. Configuring Zero Sign-on in Ivanti Access

This section provides information for the following scenarios:

- Setting Zero Sign-on security and user experience
- Passwordless authentication to service providers on unmanaged devices
- Password less login to cloud services for managed desktops
- Zero Sign-on from desktops managed by Jamf and SCCM

14.4.1. Setting Zero Sign-on security and user experience

Users can customize the security and user experience of Zero Sign-on. You can find the settings in Profile > Zero Sign-on > Zero Sign-on Settings. It lists the following configuration options:

- General: **Setting the session timeout duration**
- Authenticate: **Registering with Authenticate**
- FIDO Key: **FIDO Key**
- Security Key and Biometrics: **Security Key and Biometrics**
- QR Code: **QR Code**
- Password: **Password**

Setting the session timeout duration

Use the Zero Sign-on configuration, Profile >Zero Sign-on, to do the following:

- Set the session timeout duration after users authenticate using Zero Sign-on.
  Once user authenticates on their managed or personal device, they don't have to sign-in next time while they are within the signed-in session duration. Except if the policy associated to the Service Provider requires Step-Up Authentication, then user would be prompted for it. Session is terminated by closing the browser.

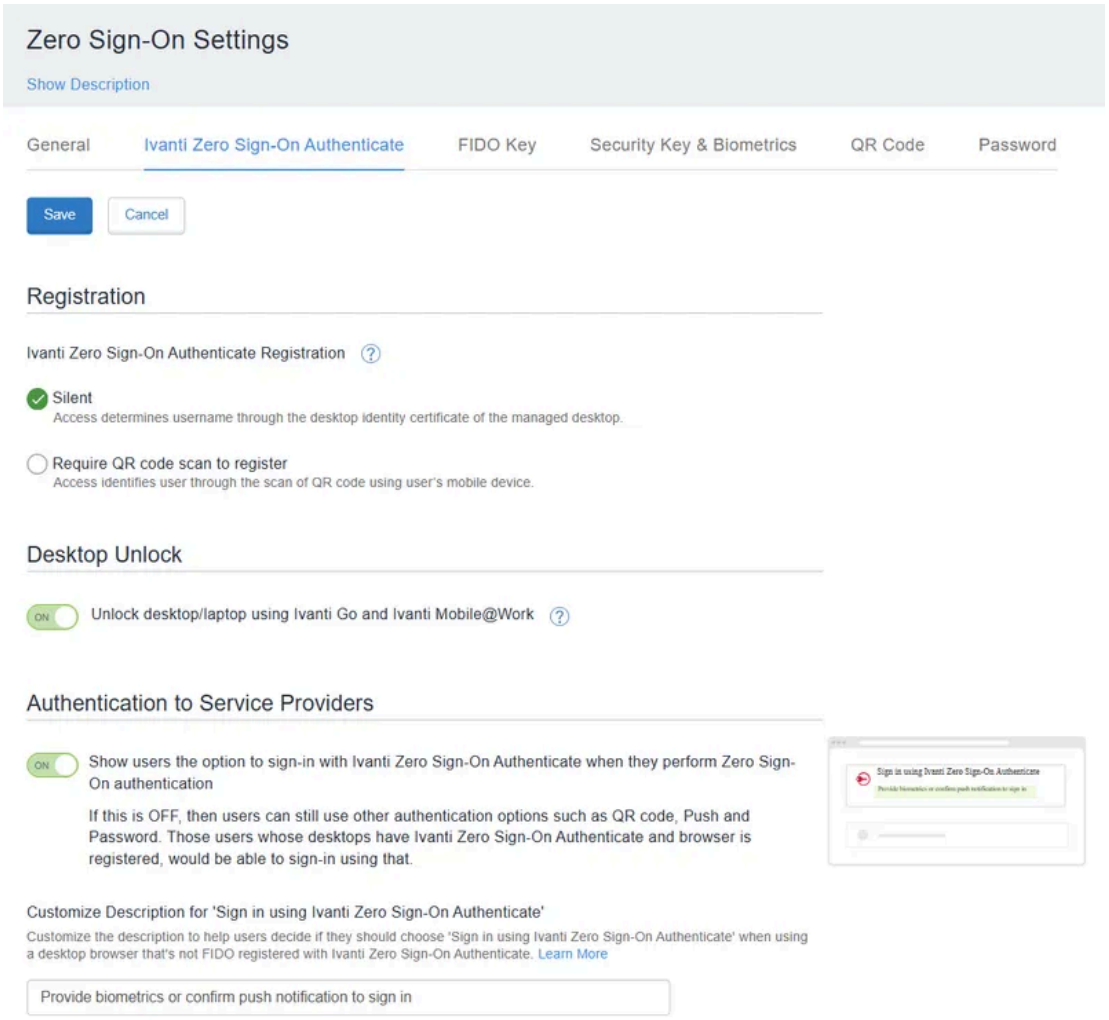
Procedure

1. In Ivanti Access, go to Profile > Zero Sign-on.
2. Click **Zero Sign-on Settings**> **General** to update the number of hours, if needed, for Enable Signed In Session.

3. By default, the option is enabled and the number of hours is set at 12. The option sets the session timeout that is applied when users select the Yes, this is my personal computer option in the Zero Sign-on interaction page.
4. Click Save .

Registering with Authenticate

After an automatic installation , Authenticate connects with Ivanti Access to register to the desktop to the appropriate user.



You can register in one of the following methods:

- **Silent**: Registration is done by fetching the username from the desktop identity certificate.
- **Require QR code scan to register**: User must open Authenticate application and scan the QR code using Go app. The username is then obtained from the mobile device identity certificate.

Unlocking the desktop

Desktop unlock is a secure and convenient method of unlocking user's desktop using a phone. The Authenticate application on the desktop works in conjunction with Ivanti Access to send a push notification to the user's activated mobile phone to authenticate and unlock the desktop. Keep the toggle on in **Profile** > **Zero Sign-on** > **Zero Sign-on Settings** > **Zero Sign-on Authenticate** to enable the feature.

Authentication for service providers

The toggle switch "Show users the option to sign-in with Authenticate when they perform Zero Sign-On authentication" is disabled by default. When this option is enabled, this option lets the users sign-in to Authenticate on the desktops.

Even with this option disabled, users can use the other authentication options such as QR code, Push and Password.

Provide a customized description for *Sign-in using Zero Sign-on Authenticate*. This description helps the users decide to select the "Sign-in using Zero Sign-on Authenticate " when using a desktop browser that is not FIDO registered with Authenticate.

FIDO Key

FIDO keys are used for stronger authentication. During registration with an online service, the user's client device creates a new key pair. The client's private keys can be used only after they are unlocked locally on the device by the user. The user can manage the settings of the FIDO key in Ivanti Access after registering.

> Ivanti recommends that the admin does not need to change the settings. However, the admin should discuss before enabling or disabling the settings.

Procedure

1. In Ivanti Access, go to Profile > Zero Sign-on.
2. Click **Zero Sign-on Settings**> **FIDO Key**.

3. Update the following fields to enhance the feature as required:
   - **Rotation Period for FIDO Key**: Specify the duration required to generate a new FIDO key.
   - **Grace period to rotate the FIDO Key before expiry**: Specify the grace period to generate a FIDO key if it was not during the Rotation period.
   - **FIDO key storage**: Specify the Trusted Platform Module version supported to store the FIDO key.
   - **Allow storing in iOS keychain**: Turn on option iOS user.
   - **Allow storing in Windows Certificate Store**: Specify if the FIDO key can be stored in Certificate Store.
   - **Allow storing in MacOS keychain**: Turn on the option for MacOS user.
   - **Allow storing in Android key store**: Turn on the option for Android user.
   - **Desktop Password Encryption**: Specify the RSA key size for Mobile devices or for desktops.
   - **Public Key Algorithms**: Select the public key algorithms and specify the order that they must be applied.
   - **Authenticate as a FIDO key**: Select the option to authenticate with FIDO key on the website. Authenticate is automatically invoked and prompts the user to authenticate with a push notification.
4. Click **Add New** to add the relying parties that accept FIDO keys to use Authenticate to sign-in.
5. Click **Save**.

Security Key and Biometrics

The **Security Key and Biometrics** lets you enable the feature for end users to see an option to sign in using Security Key & Biometrics.

Procedure

1. In Ivanti Access, go to Profile > Zero Sign-on.
2. Click **Zero Sign-on Settings**> Security Key & Biometrics.



3. Enable the toggle switch for Enable sign in via Security Key & Biometric.
4. Click Save.

QR Code

The **QR Code** provides a convenient and secure way for users to authenticate by scanning a QR code with their mobile device, typically using an authentication app or camera.

Procedure

1. In Ivanti Access, go to Profile > Zero Sign-on.
2. Click **Zero Sign-on Settings**> QR Code.



3. Enable the toggle switch for Enable sign in via QR Code.
4. Click Save.

Password

The **Password** provides a secure way to authenticate users by verifying their identity through a password.

Procedure

1. In Ivanti Access, go to Profile > Zero Sign-on.
2. Click **Zero Sign-on Settings**> Password.

3. Enable the toggle switch for Enable sign in via Password.
4. Click Save.

14.4.2. Passwordless authentication to service providers on unmanaged devices

This section contains the following sections:

- Password-less login from unmanaged devices

14.4.2.1. Password-less login from unmanaged devices

The following describes the configuration in Ivanti Access for Zero Sign-on.

Before you begin

- Ensure that you have an Ivanti Access deployment with UEM.
  See **Overview of configuration with Ivanti Neurons for MDM**.
  OR
  See **Overview of configuration with Ivanti EPMM**
- Ensure that mobile app single sign-on (SSO) is configured for the service provider (SP).
  For a federated pair, see **Configuring Mobile App Single Sign-on (SSO)**.
  For delegated IdP, see **Configuring Ivanti Access as the delegated IdP** .

Procedure: Overview of steps

- **Enabling Password-less Authentication on Go and Mobile@Work**
- **Adding a Zero Sign-on Rule in the Policies**

> A green tick displays when these steps are configured correctly. This shows that the authentication is configured correctly.

Enabling Password-less Authentication on Go and Mobile@Work

Before you begin

- Configure the user information for Zero Sign-on.
  - To configure the user information, map the fields in the certificate from which Ivanti Access gets user identifying information. This is the identity certificate used for setting up the configuration. Configuring the user information enables password-less authentication.

Procedure

1. In Ivanti Access, go to Profile > Zero Sign-on.
2. Under Steps to deploy, expand **Enable Password-less Authentication on Go and Mobile@Work**.
3. Click **See Details** to view the existing configuration details for the devices.

4. To enable more devices follow the steps i) and ii) as shown above.
   1. Deploy SaaS Sign-On on managed mobile devices.
   2. Sync UEM.

Adding a Zero Sign-on Rule in the Policies

In the policy associated with the SAML pair for which Zero Sign-on is required, add a Zero Sign-on Rule conditional rule. If the rule is added, users accessing the cloud service from an unmanaged device see an interaction page. The interaction page contains a

QR code, which device users can scan from a managed device to authenticate to the cloud service. Alternately, the interaction page also contains a link to authenticate with username and password.

Before you begin

- Ensure that mobile app single sign-on is configured for the federated pair or delegated IdP to which you want to assign the Zero Sign-on Rule. If mobile app single sign-on is not configured, you will see errors when creating or assigning the Zero Sign-on Rule.

Procedure

1. In Ivanti Access, go to Profile > Zero Sign-on.
2. Under Steps to deploy, expand **Add Zero Sign-On Rule in the Policies**.

3. Click See Details to view the existing UEMs with SaaS on configuration created and synced with Ivanti Access.
4. Verify that the rule is configured.
   Else add a rule in **Profile** > **Conditional Policies**.
5. In Ivanti Access, go to Profile > Conditional Access.
6. Expand Default Policy.
   If you want Zero Sign-on only for some federated pairs or delegated IdP, create a new policy.
   The Zero Sign-on rule can be added to any policy. Adding the Zero Sign-on rule to the default policy makes it available to all pairs to which the default policy is applied. Add the Zero Sign-on rule to another policy if you want to apply the rule to only some federated pairs or delegated IdP.
7. Click +Add Rule > Zero Sign-on Rule to add the conditional rule for Zero Sign-on.
8. Enter a name and description for the rule.

9. Configure the rule for one of the following devices.
   1. For unmanaged devices: Enable the toggle switch to allow admins to independently manage the authentication methods. Users are authenticated with one of the following methods: **Password**, **Security Key & Biometrics**, **QR code**, **Push notification** and **One Time Password (OTP)**.

      The following are the granular authentication control criteria.
      - The global (tenant-wide) settings must be enabled to enable the granular (per-federation) settings.
      - At least one authentication method must be enabled.

      > Disabled options are clearly indicated in the UI with explanatory tooltips.

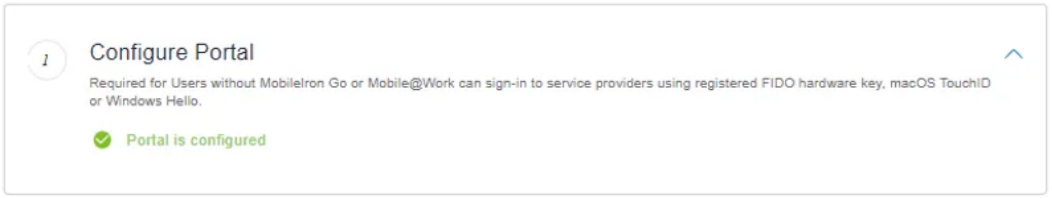
   2. Step-Up Authentication: Enable the toggle switch to step-up authentication such as Push notifications or biometric for managed desktops.
10. For Rule Action, select Allow.
11. Click Done to save the policy and rule.

The order of the conditional rules matters. When you create a Zero Sign-on Rule, Ivanti Access automatically orders the rules such that the Zero Sign-on Rule follows the Trusted App and Device rule. The order of rules, if they are configured, is as follows: Trusted App and Device rule, Zero Sign-on Rule, Multi-Factor Authentication rule. However, the rules can be manually reordered. Ensure that the order of the rules matches the order stated in this note.

Configuring portal for FIDO security

The Configure Portal section is required for users without MobileIron Go or Mobile@Work to sign-in to service providers using registered FIDO hardware key, macOS TouchID or Windows Hello.

The section provides information if the portal is configured. Else it provides a link to configure the portal.



Configuring branding for Zero Sign-on

Customize the user experience for your enterprise users by uploading your company logo to Ivanti Access. The user notification screen as well as the interaction page with the QR code are customized to display your company logo.

Ensure that your company logo is no more than 260 pixels wide by 30 pixels high. Supported file types are: PNG, JPG, JPEG, and SVG.

Procedure

1. In Ivanti Access, go to Profile > Branding.
2. In the Company Logo section, drag and drop your company logo or click Choose to navigate to the location of the file and add.

Next steps

Publish the updates. See **Publishing the changes**.

Publishing the changes

Publish the changes to make the updates available. In the Ivanti Access administrative portal, a publish banner appears in any of the Profile tabs when there are configuration changes.

Procedure

1. In the Ivanti Access, go to Profile > Overview.
2. Click Publish.
3. Click OK.

14.4.3. Password less login to cloud services for managed desktops

This chapter contains the following sections:

- Password-less log in to cloud services from managed desktops
- Password-less login from managed devices

14.4.3.1. Password-less log in to desktops

- Passwordless login to desktops with push notifications to a managed device.
- Users signing into their desktops get push notification to their managed device. Users do not need to enter their username and password.

Required components

- Ivanti Neurons for MDM deployment
- Authenticate for Windows 10
- FIDO2 cloud instance

Supported devices

- macOS devices managed by Ivanti Neurons for MDM
- Windows 10 devices managed by Ivanti Neurons for MDM

Supported browsers

- macOS: Safari, Chrome
- Windows 10: Edge, Chrome, Firefox

14.4.3.2. Password-less log in to cloud services from managed desktops

The FIDO2 solution is based on FIDO2 standards and extends the passwordless experience to desktops with TouchID.

Use cases

The following use cases are supported for passwordless log in:

- Log in to cloud services from managed desktops.
  Users are automatically authenticated using macOS TouchID if the device supports TouchID. Entering their username and password is not required. The biometric option is also available and is turned off by default.
- Log in to cloud services from unmanaged desktops using push notifications.
  Users are prompted to allow the access from a push notification sent to a managed or Auth-only mobile device. Entering their username and password is not required.
- Log in to a desktop using push notifications.
  Users are prompted to allow the access from a push notification sent to a managed or Auth-only mobile device. Entering their username and password is not required.
  This use case requires that you also have Ivanti Neurons for MDM deployment.

Required components

- Ivanti Neurons for MDM deployment
- Authenticate for macOS
- Authenticate for Windows 10
- FIDO2 Ivanti Neurons for MDM instance

Supported devices

- macOS devices managed by Ivanti Neurons for MDM
- Windows 10 devices managed by Ivanti Neurons for MDM

Supported browsers

- macOS: Safari, Chrome
- Windows 10: Edge, Chrome, Firefox

14.4.3.3. Password-less login from managed devices

The following describes the configuration in Ivanti Access for Zero Sign-on.

- Deploying Authenticate using UEM
- Review Registration Settings
- Enabling Password-less Authentication on Go and Mobile@Work
- Adding a Zero Sign-on Rule in the Policies

Deploying Authenticate using UEM

You can connect UEM with Ivanti Access and distribute Authenticate to user desktops.

Procedure

1. In Ivanti Access, go to Profile > Zero Sign-on.
2. Under Steps for deploy, expand Deploy Authenticate using UEM.

3. For desktops managed by :
4. **3rd Party UEM**: In Ivanti Access, go to **UEM** > **3rd Party UEMs**tab. Click **Connect UEM** and follow steps.
5. **Ivanti Neurons for MDM**: Go to UEM. Select the Ivanti Neurons for MDM UEM and follow steps in the Authenticate section.

Review Registration Settings

The Registration settings are used by clients such as Go to register user's device with Ivanti Access.

Procedure

1. In Ivanti Access, go to Profile > Zero Sign-on.
2. Under Steps to deploy, expand **Review Registration Settings**.
   Verify the certificate mapping.

3. Click View Template to view the default client certificate.
4. Click **Edit** to modify the registration.

5. Select the username mapping in the certificate appropriately and click Save. For more information, see Client Registration Settings.

Related topics

For information about MiTra expressions, see Language to generate values from certificate fields.

Enabling Password-less Authentication on Go and Mobile@Work

Before you begin

- Configure the user information for Zero Sign-on.

- To configure the user information, map the fields in the certificate from which Access gets user identifying information. This is the identity certificate used for setting up configuration. Configuring the user information enables passwordless authentication.

Procedure

1. In Ivanti Access, go to Profile > Zero Sign-on.
2. Under Steps to deploy, expand **Enable Password-less Authentication on Go and Mobile@Work**.

3. Click **See Details** to view the existing configuration details for the devices.
4. To enable more devices follow the steps i) and ii) as shown above.
    1. Deploy SaaS Sign-On on managed mobile devices.
    2. Sync UEM.

Adding a Zero Sign-on Rule in the Policies

In the policy associated with the saml pair for which Zero Sign-on is required, add a Zero Sign-on Rule conditional rule. If the rule is added, users accessing the cloud service from an unmanaged device see an interaction page. The interaction page contains a QR code, which device users can scan from a managed device to authenticate to the cloud service. Alternately, the interaction page also contains a link to authenticate with username and password.

Before you begin

- Ensure that mobile app single sign-on is configured for the federated pair or delegated IdP to which you want to assign the Zero Sign-on Rule. If mobile app single sign-on is not configured, you will see errors when creating or assigning the Zero Sign-on Rule.

Procedure

1. In Ivanti Access, go to Profile > Zero Sign-on.
2. Under Steps to deploy, expand **Add Zero Sign-On Rule in the Policies**.



3. Verify that the rule is configured.
   Else add a rule in **Profile** > **Conditional Policies**.
4. In Ivanti Access, go to Profile > Conditional Access.
5. Expand Default Policy.
   If you want Zero Sign-on only for some federated pairs or delegated IdP, create a new policy.
   The Zero Sign-on rule can be added to any policy. Adding the Zero Sign-on rule to the default policy makes it available to all pairs to which the default policy is applied. Add the Zero Sign-on rule to another policy if you want to apply the rule to only some federated pairs or delegated IdP.
6. Click +Add Rule > Zero Sign-on Rule to add the conditional rule for Zero Sign-on.

7. Enter a Name and Description for the rule.
8. Configure the rule for one of the following devices.
    1. For managed desktops: Users device is automatically authenticated using Authenticate and FIDO2 protocol. Enable the toggle switch to select this configuration.



2. For unmanaged devices: Enable the toggle switch to allow access on unmanaged devices. Users are authenticated with one of the following methods: QR code, Push notification, One Time Password (OTP), and FIDO Authenticator.

3. Step-Up Authentication: Enable the toggle switch to step-up authentication such as Push notifications or biometric for managed desktops.

9. For Rule Action, select Allow.
10. Click Done to save the policy and rule.

: The order of the conditional rules matters. When you create a Zero Sign-on Rule, Ivanti Access automatically orders the rules such that the Zero Sign-on Rule follows the Trusted App and Device rule. The order of rules, if they are configured, is as follows: Trusted App and Device rule, Zero Sign-on Rule, Multi-Factor Authentication rule. However, the rules can be manually reordered. Ensure that the order of the rules matches the order stated in this note.

Configuring branding for Zero Sign-on

Customize the user experience for your enterprise users by uploading your company logo to Ivanti Access. The user notification screen as well as the interaction page with the QR code are customized to display your company logo.

Ensure that your company logo is no more than 260 pixels wide by 30 pixels high. Supported file types are: PNG, JPG, JPEG, and SVG.

Procedure

1. In Ivanti Access, go to Profile > Branding.
2. In the Company Logo section, drag and drop your company logo or click Choose to navigate to the location of the file and add.

Next steps

Publish the updates. See **Publishing the changes**.

Publishing the changes

Publish the changes to make the updates available. In the Ivanti Access administrative portal, a publish banner appears in any of the Profile tabs when there are configuration changes.

Procedure

1. In Ivanti Access, go to Profile > Overview.
2. Click Publish.
3. Click OK.

14.4.4. Zero Sign-on from desktops managed by Jamf and SCCM

The FIDO2 Zero Sign-on solution allows you to provide a password less log in experience from your Jamf/SCCM managed desktops.

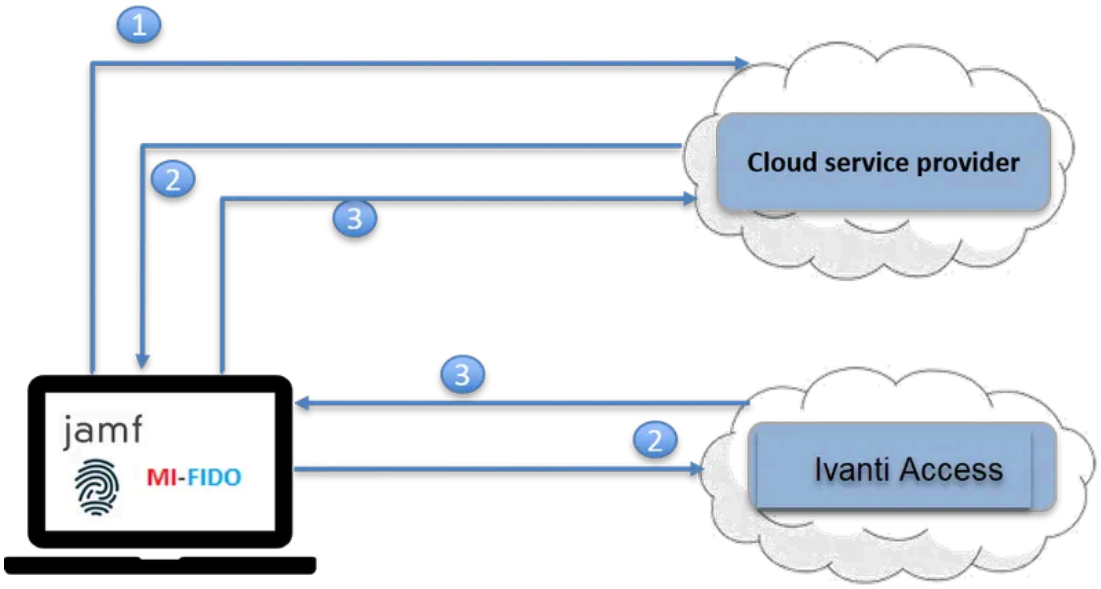
Use cases

The following use cases are supported for passwordless log in:

- Log in to cloud services from desktops managed by Jamf/SCCM on the desktop.
  Users are automatically authenticated using macOS TouchID if the device supports TouchID. Entering their username and password is not required.
  This use case does not require that you also have Ivanti Neurons for MDM deployment.
  This configuration is optional and if turned off by default.
- Log in to cloud services from desktops managed by Jamf/SCCM using push notifications.
  Users are prompted to allow the access from a push notification sent to a managed or Auth-only mobile device. Entering their username and password is not required.
  This use case requires that you also have Ivanti Neurons for MDM deployment.
- Log in to a desktop using push notifications.
  Users are prompted to allow the access from a push notification sent to a managed or Auth-only mobile device. Entering their username and password is not required.
  This use case requires that you also have Ivanti Neurons for MDM deployment.

Authentication flow from desktops

Figure 1. Authentication flow from managed desktops



1. User requests access to a cloud service from a Jamf /SCCM desktop.
2. The cloud service redirects user to the configured identity provider (IdP)to authenticate. Since Ivanti Access is the configured IdP, the request is redirected to Ivanti Access.
3. Ivanti Access generates a new SAML response to redirect to the original SP. The original SP obtains the user identity from the SAML response and presents the personalized screen to the user.

Required components

- Authenticate for macOS
- FIDO2 Ivanti Neurons for MDM instance (Access in the EAP cluster with configured SP+IdP federated pairs)
- Ivanti Neurons for MDM deployment if push notifications to Ivanti managed device is needed.

Supported devices

- macOS devices managed by Jamf/SCCM

Supported browsers

- macOS: Safari, Chrome

14.4.4.1. Configuring UEM with Jamf in Ivanti Access

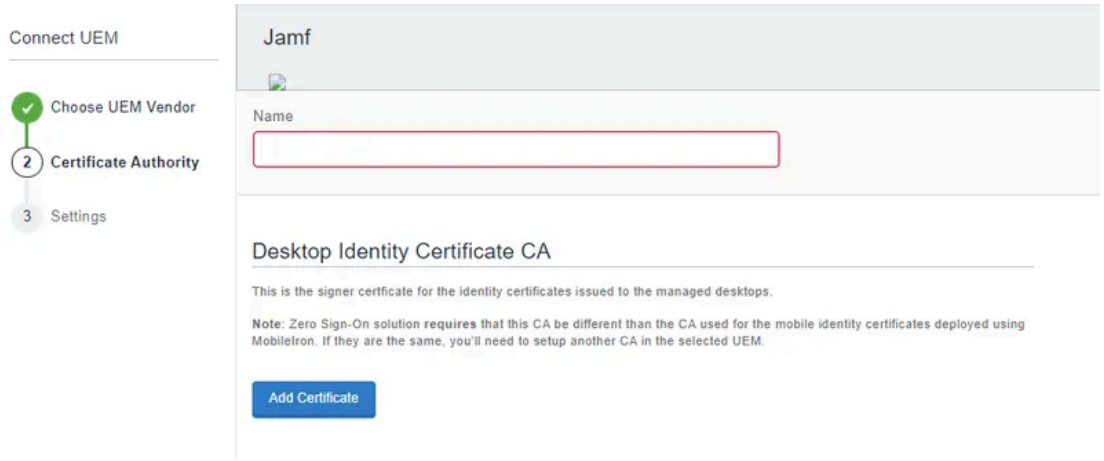
Ivanti Access integrates with Jamf (UEM vendor) to provide Zero Sign-on capability for desktops or laptops managed by them.

Before you begin

- Verify that you provide the CA signer certificate from the 3rd party UEM used for the identity certificate in the managed desktops.
- Verify that you have the Desktop Identity Certificate CA referenced in Certificate based Single Sign On (Profile >Federation).
- Download the PKG file from Ivanti support site.

Procedure

1. Login to Access > UEM > 3rd Party UEMs.
2. Click Connect UEM.
3. Select Jamf.



1. Enter the following details:
    1. Enter a Name.
    2. Click Add Certificate under Desktop Identity Certificate CA.
2. Enter the Certificate Name and add the certificate.
   Or
   Paste the certificate.
   Only PEM and CER file types are allowed.
3. Click Done.
4. Click Next.
5. (Optional) Enter the Management Check details.
   Check whether desktop is registered to Jamf and check compliance if smart group is provided.
    - Enable to toggle for "Verify desktop is managed by Jamf and limit access to only managed desktops".
      Enabling this option performs a check during Authenticate registration and authentication to service providers.
    - Enter the Tenant URL.

- Username
- Password

6. (Optional) Enter the compliance criteria using Smart Group to enable restricted access to service providers.
   Use the Zero Sign-on rule to enforce that only desktops compliant with this criteria are able to access the service providers governed by the policy.
7. Click Done.
8. Under UEM > 3rd Party UEMs, the Jamf instance is created.
9. Click **Download Plist** and save the XML as a .plist file to upload in Jamf.



Next steps

- **Configuring Authenticate on Jamf**

14.4.4.2. Configuring UEM with SCCM in Ivanti Access

Ivanti Access integrates with SCCM (UEM vendor) to provide Zero Sign-on capability for desktops or laptops managed by them.

Before you begin

- Verify that you provide the CA signer certificate from the 3rd party UEM used for the identity certificate in the managed desktops.
- Verify that you have the Desktop Identity Certificate CA. See Desktop Identity Certificate.
- Download the msi file from support site.

Procedure

1. Login to Access > UEM > 3rd Party UEMs.
2. Click Connect UEM.
3. Select SCCM.



4. Click Add Certificate and enter the certificate name.
5. Click Browse to add the certificate.
   To download the certificate, run the command `certutil -ca.cert ca_name.cer` on the same machine where the AD CS service is running.
   For more information, see **How to export Root Certification Authority Certificate**.
6. Click Done > Next.
7. (Optional) Enter the SCCM details. For more information, see **Configuring certificate authority for SCCM** and **Configuring CMG application for compliance check**.

Creating desktop identity certificate

1. On the AD CS machine, for the desktop identity certificate, click certificate templates.
2. Create a new template for provisioning certificates.
3. On the Subject Name tab, select Build from Active Directory information.
4. On the Request Handling tab, select Enroll subject without requiring any user input.
5. Add custom SAN attributes to Desktop Identity Certificate.
   For more information, see **Microsoft Certificate Authority Template**.

Next steps

Configuring certificate authority for SCCM

Configuring certificate authority for SCCM

Before you begin

- Ensure that you have ve set up Certificate Authority (AD CS) running on Microsoft Server.
- Ensure to export the **Root certification authority certificate**.

Procedure

1. On Certificate Authority, run `adsiedit.msc`.
2. Click Configuration > Services > Public Key Services > Certificate Templates.

3. Select the template and enter the value of msPKI-Certificate-Name-Flag field after converting hexadecimal to decimal and adding the value.
   For more information, see **Certificate Name Flag Attribute.**

   For example: To add the following names to the Subject Alternative Name extension in certificates: DS Object Guid, Email, and UPN.

   - Domain Names (DNS and NETBIOS): 4194304
   - UPN: 33554432
   - Email: 67108864
   - DS Guid: 285212672
   - SPN: 8388608

   Add all the numbers together and replace the *msPKI-Certificate-Name-Flag* with that value. To include UPN, Email, and DS Guide, replace the value with 385875968.

4. Request Certificate on Client using the template.

Configuring CMG application for compliance check

In SCCM, you can configure the CMG application that allows to access SCCM services from the internet.

For more information on how to set up CMG application for SCCM, see **Microsoft docs.**

Before you begin

To enable Ivanti Access CMG communication, in the Advanced Settings, set the option *Allow public client flow* to yes for compliance check by Ivanti Access to SCCM.

Procedure

1. In Configuration Manager, click Compliance Settings.

2. To fetch the Baseline XML files, right-click and select View XML definition.

3. Note the LogicalName and AuthoringScopeID from the XML.
   Copy the XML or download and save the XML.

4. To fetch the CMG URL for admin service.
   1. Click Start > Run > Regedit to open the registry editor.
   2. Expand to open HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SMS\SMS_CLOUD_PROXYCONNECTOR\UrlMappings.

   3. Copy the text to notepad and locate the URL for AdminService.
      Append '/wmi/SMS_G_System_DCMDeploymentState' to the URL. So the final URL is HTTPS://MICMGBNG.MIFIDOLAB.COM/CCM_Proxy_ServerAuth/72057594037927941/AdminService/wmi/SMS_G_System_DCMDeploymentState.

      For example: https://micmgbng.mifidolab.com/CCM_Proxy_ServerAuth/72057594037927941/AdminService



5. To fetch credentials to authenticate to CMG, open Configuration Manager.
   1. In Configuration Manager, add a user from the domain with Read-Only access.

6. Fetch the Client ID, Secret ID, and Tenant ID from Azure portal.
   1. Login to Azure Portal > App Registration.
   2. Click the CMG application created.
   3. Copy the Client ID, Tenant ID, and the Application ID URI.

   4. (Optional) Click Certificates & secrets and add a new Client secret.
      Note the ID and Value of this secret.



Configuring SCCM to distribute Authenticate and user environment variable

Before you begin

- Download the MSI file for Authenticate from Ivanti support site.
- Copy the values of command line from Ivanti Access.
- Configure the client for user environment variable to use in command line.
  - On your client, create a new GPO or edit the existing user setting.
  - Click User config > Preferences > Windows Settings > Environment.

- Create a new environment variable:
  1. Action: Update
  2. Select: User Variable
  3. Name: UPN
  4. Value: %UPN%
- Click the Common tab.
- Enter a description: Create an environment variable called UPN and populate it with the UserPrincipalName attribute for the user, as held in Active Directory.
- Tick "Item-level Targeting" and click Targeting.
- Select New Item > LDAP Query.
  - Filter: (&(objectClass=user)(sAMAccountName=%USERNAME%))
  - Binding: LDAP:
  - Attribute: userPrincipalName
  - Environment variable name: _UPN
- Click Ok.

Procedure

1. Admin must update DESKTOP_IDENTITY_CERTIFICATE_CN and DESKTOP_IDENTITY_CERTIFICATE_ISSUER_CN based on their environment DESKTOP_IDENTITY_CERTIFICATE_ISSUER_CN = the subject of the CA used. This is used to upload to SCCM configuration in Ivanti Access.

   DESKTOP_IDENTITY_CERTIFICATE_CN

   1. If it is a static, then use the string.
   2. If it is an environment variable as defined, use %env_var%

      DESKTOP_IDENTITY_CERTIFICATE_CN=DesktopIdentity
      DESKTOP_IDENTITY_CERTIFICATE_ISSUER_CN=DesktopIdentityCA

      ACCESS_URL=https://16188152107641848098929.miaccessqa.com/MobileIron WEBSOCKET_API_URL=wss://ws-access.miaccessqa.com/ws BOOTSTRAP_URL=https://access.miaccessqa.com/MobileIron/efa/api/v1/setManaged
2. Create Application on SCCM
   1. On the Configuration Manager, click Software Library> Overview > Application Management > Applications > Create Application.
      The Create Application Wizard opens.
   2. On the General tab, select "Automatically detect information about this application from installation files".
   3. Click Browse in the Location filed and share the file on the appropriate SCCM network.
   4. Click Next > Next.
   5. On the General Information tab, enter the Name.
   6. In the Installation program path, paste the Access URL after the existing path /q.
   7. On the Install behavior drop down, select Install for user as enviroment user variable is used.

8. Click Next > Next.
9. Right-click the Authenticate application > Properties.
10. On Content tab, select Download content from distribution point and run locally.

3. Deploy the application to preferred user or device collection.
    1. Right-click the application in the Applications folder and click Deploy.
    2. On the Deploy Software Wizard General tab, click Browse to select the Collection.
    3. Select User Collections or Device Collections appropriately and click Ok.

14.4.5. What users see for FIDO2

FIDO2 is a feature available with the UEM client. The UEM clients are: Go or Mobile@Work, and Authenticate.

If FIDO2 solution is configured, users can authenticate and access enterprise cloud services from third party managed devices with Authenticate installed.

When a user tries to log in, a push notification is sent to all active devices. When the user allows push notification on any appropriate device, access is granted for the session. However, on all other devices, the sessions become invalid and deactivating on this device does not deactivate on other devices.

The following provide information about the user experience with FIDO2:

- **Workflow for registered browsers**
- **Workflow for non-registered browsers**
- **Workflow on Android devices**
- **Workflow on iOS devices**
- **Workflow for Desktop login**

Workflow for registered browsers

A browser that launches after a successful Authenticate registration, is a registered browser.

For a registered browser, when user tries to open the service provider, Ivanti Access automatically invokes Authenticate and authenticates the user using FIDO2.

If step up authentication is configured, user is prompted to either present biometrics or approve a push notification sent to registered mobile device.

The following provides an example of the authentication workflow with a registered browser:



Workflow for non-registered browsers

Non-registered browser are browsers that are not default browsers and other browsers that are not registered with Authenticate.

The non-registered browsers must authenticate using either Authenticate, QR Code, or with Passwords.

The following provides an example to login using Authenticate:



The following provides an example to login using QR Code:



The following provides an example to login using username and password credentials:



Workflow on Android devices

This section provides information for the various end user interactions on Android devices.

- Unlocking a desktop on Android devices
- Activating a password-less sign-in on Android device
- Deactivating a password-less sign-in on Android device
- Ending a browser session

Unlocking a desktop on Android devices

To unlock a FIDO2 windows or mac desktop, you must authenticate from your device.

Unlocking a Windows desktop

The following provides an example to authenticate on a device using Go, when a user tries to unlock his FIDO2 enabled Windows desktop:



Unlocking a Mac desktop

The following provides an example to authenticate on a device using Go, when a user tries to unlock his FIDO2 enabled Mac desktop:



Activating a password-less sign-in on Android device

To activate a FIDO2 Android device, (If it is not already done during enrollment) go to Go > Menu > Settings > Authenticate and turn on the toggle button. Follow authentication as shown below:

Deactivating a password-less sign-in on Android device

To deactivate an Android FIDO2 device, turn off the toggle button in Go > Menu > Settings > Authenticate.

Ending a browser session

You can end a browser session from Go > Menu > Settings > Authenticate > End Browser Session. Ending a browser session automatically signs you out of the company websites on the browsers.

> This option is available only if the user has active browser sessions running.



Workflow on iOS devices

This section provides information for the various end user interactions on iOS devices.

- Unlocking a desktop on iOS devices

- Activating password-less sign-in on iOS device
- Deactivating password-less sign-in on iOS device
- Ending a browser session on an iOS device

Unlocking a desktop on iOS devices

To unlock a desktop on an unlocked mobile , go to Go > Menu> Settings > Authenticate.



To unlock a desktop on a locked mobile, go to Go > Menu > Settings > Authenticate.



Activating password-less sign-in on iOS device

To activate a FIDO2 iOS device, go to Go > Menu> Settings > Authenticate and turn on the toggle button. Follow authentication as shown below:



Deactivating password-less sign-in on iOS device

To deactivate an iOS FIDO2 device, turn off the toggle button in Go > Menu > Settings > Authenticate.



Ending a browser session on an iOS device

You can end a browser session from Go > Menu > Settings > Authenticate > End Browser Session. Ending a browser session automatically signs you out of the company websites on the browsers.



Workflow for Desktop login

You must login to a desktop and approve the push notification on your mobile device.



14.5. Authenticate

Authenticate is a Fast Identity Online (FIDO2) solution that simplifies the user experience while reducing the risk of data breaches. Authenticate ensures that only verified users can access business applications and it prevents the misuse of an employee's corporate credentials in case they are stolen.

Authenticate eliminates risky password-based security on desktop endpoints by providing a trust model for Ivanti-secured devices.

This authentication is done by requesting the user to present multiple factors to confirm their identity. Users gain instant approval through mobile push. Intelligent authentication flows adapt to the type of device, app, network, user location, and more.

Authenticate leverages a user’s smartphone so the user no longer have to carry (and potentially misplace) cumbersome key fobs. Authenticate sends push notifications that enable quick access for convenient authentication based on the user’s needs.

14.5.1. Configuring Authenticate on Ivanti Neurons for MDM

Configure the FIDO2 Desktop Agent to provide password less authentication for cloud services and desktop login.

Before you begin

- Verify that you have configured Ivanti Neurons for MDM.
- Verify that you have uploaded the desktop identity certificate in Access > UEM.
  - Download the certificate from Ivanti Neurons for MDM > Admin > Infrastructure > Certificate Management.

Procedure

1. On Ivanti Neurons for MDM, click Configurations > Add.
2. In the Search Configurations field, enter Authenticate.
3. Select Authenticate.
   The Create Zero Sign-on Authenticate Configuration page opens.
4. Enter the following details:
   1. Name
   2. Description
5. Under Configuration Setup, select the following:
   1. Select the Desktop Identity Certificate from the drop-down.
   2. Select the Operating System, macOS or Windows or both.
6. Select Windows and click Done to complete the Authentication.
   Windows does not require distribution.
   OR
7. Select macOS and enter the Key and Value for Custom Data. Click Next.
   1. Select the devices to which the configuration is applied and click Done to complete the authentication.
8. Under Configurations, select the Authenticate configuration created and click Details.
9. Click Copy Command Line Text to distribute the app.

Next steps

Adding and distributing a macOS application for Authenticate

14.5.1.1. Configuring macOS for Authenticate

You must configure macOS for Authenticate.

Procedure

1. On Ivanti Neurons for MDM, click Configurations > Add.
2. In the Search Configurations field, enter macOS Kernel Extension Policy.
3. Select the policy.
   The Create macOS Kernel Extension Policy Configuration window opens.
   
4. Enter a Name for the policy.
5. Under Configuration Setup, click Add.

6. Enter 2P68G9Z44L as the Team Identifier.
7. Click Next.
8. Select the devices to which the configuration is applied and click Done to complete the configuration.

Next steps

Configure the **Configuring privacy preference for accessibility permission**.

14.5.1.2. Configuring privacy preference for accessibility permission

1. On Ivanti Neurons for MDM, click Configurations > Add.
2. In the Search Configurations field, enter Privacy Preference.
3. Select the configuration.
   The Create Privacy Preference Configuration window opens.
4. Enter the name: Accessibility Permission.
5. In Accessibility, create an Identity Dictionary Key.
    1. Click Add. The Identity Dictionary Keys window opens.
    2. Enter the identifier: co.gotrustid.fidovhid
    3. **Identifier Type**: Bundle ID
    4. **Code Requirement**: anchor apple generic and identifier "com.gotrustid.fidovhid" and (certificate leaf[field.1.2.840.113635.100.6.1.9] /* exists */ or certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = "2P68G9Z44L")
    5. Select Allowed.
    6. **Comment**: Allow fidovhid
    7. Click Save.
6. Add another Identity Dictionay Key.
    1. Click Add. The Identity Dictionary Keys window opens.
    2. Enter the identifier: com.mobileiron.authenticator.MiMacApp
    3. **Identifier Type**: Bundle ID
    4. **Code Requirement**: identifier "com.mobileiron.authenticator.MiMacApp" and anchor apple generic and certificate leaf[subject.CN] = "3rd Party Mac Developer Application: MobileIron (CVC9UUN572)" and certificate 1[field.1.2.840.113635.100.6.2.1] /* exists */
    5. Select Allowed.
    6. **Comment**: Allow MiMacApp
    7. Click Save.
7. Click Next.
8. Select the macOS devices to which the configuration is applied and click Done to complete the configuration.

14.5.1.3. Adding and distributing a macOS application for Authenticate

After configuring Authenticate for an appropriate operating system , the user adds the Authenticate application in Ivanti Neurons for MDM.

Before you begin

- Download the PKG file for Authenticate from the Ivanti support site.

Procedure

1. In Ivanti Neurons for MDM, click Apps > App Catalog > Add.
2. Select In-House from the drop-down.

3. Click Choose File and upload the PKG file appropriately. Click Next.

4. Enter the appropriate Category in the description page.

5. (Optional) Add Screenshots appropriately.

6. (Optional) Delegate this application if it should be inherited by newly created spaces.

7. Choose any option to distribute the app between the appropriate users and click Next.
    1. Everyone
    2. No One
    3. Custom: Select Users or User Groups, Distribution Filter and view the App Distribution Summary.

8. In App Configurations, configure the application as desired.
    1. Install on device: Allows specifying install settings for an application.
    2. Promotion: Defines how the app gets promoted and appears in the app catalog for specific groups or individuals.
    3. Per App VPN: Enables Per App VPN for the application such that it connects to enterprise services through native iOS/macOS capabilities or using Ivanti Tunnel app.

9. Click Done.

14.5.1.4. Adding and distributing a Windows application for Authenticate

After configuring Authenticate for an appropriate operating system , the user adds the Windows Authenticate application in Ivanti Neurons for MDM.

Before you begin

- Download the MSI file for Authenticate from the Ivanti support site.

Procedure

1. In Ivanti Neurons for MDM, click Apps > App Catalog > Add.
2. Select In-House from the drop-down.
3. Click Choose File and upload the MSI file appropriately. Click Next.
4. Enter the appropriate Category in the description page.

5. Under App Installer - Settings, enter the Command Line Text copied when configuring MI Authenticator. See **Configuring Authenticate on Ivanti Neurons for MDM**.
6. (Optional) Add Screenshots appropriately.



7. (Optional) Delegate this application if it should be inherited by newly created spaces.



8. Choose any option to distribute the app between the appropriate users and click Next.
    1. Everyone
    2. No One
    3. Custom: Select Users or User Groups, Distribution Filter and view the App Distribution Summary.

9. In App Configurations, configure the application as desired.
    1. Install on device: Allows specifying install settings for an application.
    2. Promotion: Defines how the app gets promoted and appears in the app catalog for specific groups or individuals.
    3. Per App VPN: Enables Per App VPN for the application such that it connects to enterprise services through native iOS/macOS capabilities or using Ivanti Tunnel app.



10. Click Done.

14.5.2. Configuring Authenticate on Jamf

Ivanti Access integrates with Jamf (UEM vendors) to provide Zero Sign-On capability for desktops or laptops managed by them.

Before you begin

- Verify that you have the Jamf credentials and account to log in.
- Verify that you have downloaded the PKG package file from Ivanti Support site.
- Verify that you have configured Jamf in Ivanti Access. See **Configuring UEM with Jamf in Ivanti Access**.
- Verify that you have the .plist file that you saved when configuring Jamf in Ivanti Access. See **Configuring UEM with Jamf in Ivanti Access**.

Procedure

1. Login to Jamf account with admin credentials.
2. Click Computers> Configuration Profiles.

3. Click Upload > Choose File > Upload.
4. Click Management Settings > Packages > New.

5. Enter the Display Name and select the Category to add the package to.

6. Click Upload Package File to upload the PKG package file downloaded from the Ivanti Support site.
7. Click Save.
8. Click Policies > New > Display Name.

9. Click Packages > Configure.
10. Add the PKG package file that was uploaded in Management Settings.
11. Click Save.

14.5.3. What users see for Authenticate

After configuring Authenticate on UEM, Windows or macOS desktops get notification to authenticate and register Authenticate.

A silent registration is enabled by default for Authenticate.

The following provide information about the user experience with Authenticate:

- Workflow on Windows desktop
- Workflow on macOS desktop
- FIDO Key Rotation Details and Required Actions

Workflow on Windows desktop

Workflow for Silent Registration



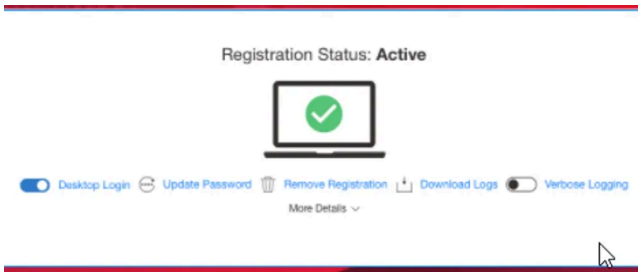
Workflow for QR Code



Workflow for QR Code and password



Registration Status



Lock pass initiated on a Windows lock screen



Workflow on macOS desktop

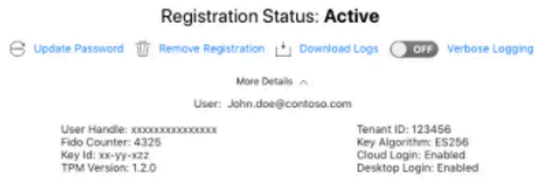
Silent Registration



Workflow on a macOs light mode



Registration Status



FIDO Key Rotation Details and Required Actions

Key Generation

During registration, two asymmetric key pairs are generated:

- Desktop Signing Key (DSK) – used to perform FIDO Authentication
- Desktop Encryption Key (DEK) – used to encrypt any data, needs to be sent to the Desktop Trust Agent.

These keys are governed by:

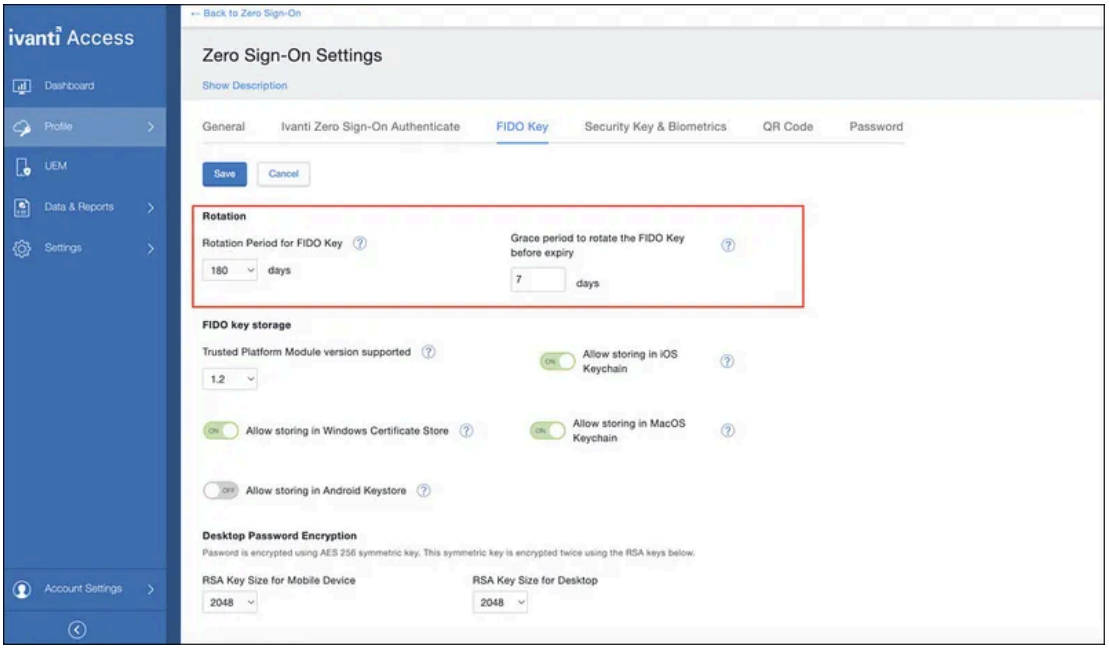
- **Rotation Period for FIDO Key** (default: 180 days)

> Increasing Rotation Period does not apply retroactively to already-registered agent. It takes effect only if the user updates keys during grace period or upon agent re-registration.

- **Grace period to rotate the FIDO Key before expiry** (e.g., 7 or 15 days)

> Increasing Grace Period enables the notifications to appear earlier than before.
> Example: With a 15-day grace period, the warning starts on Day 165 (for a 180-day rotation).

This doesn't have any negative impact on the functionality.



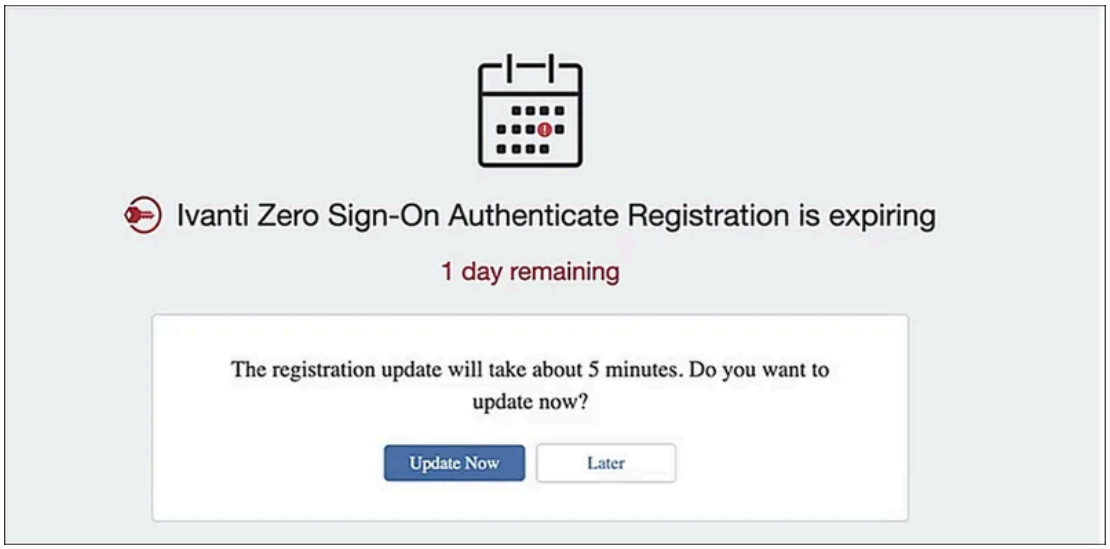
Configurations are managed in the Zero Sign-On settings in the Access console.

User Access – Normal Flow

1. Select **Sign in using Ivanti Zero Sign-On Authenticate** option.
2. Authentication succeeds if keys are valid.

Pre-Expiry Notification Flow

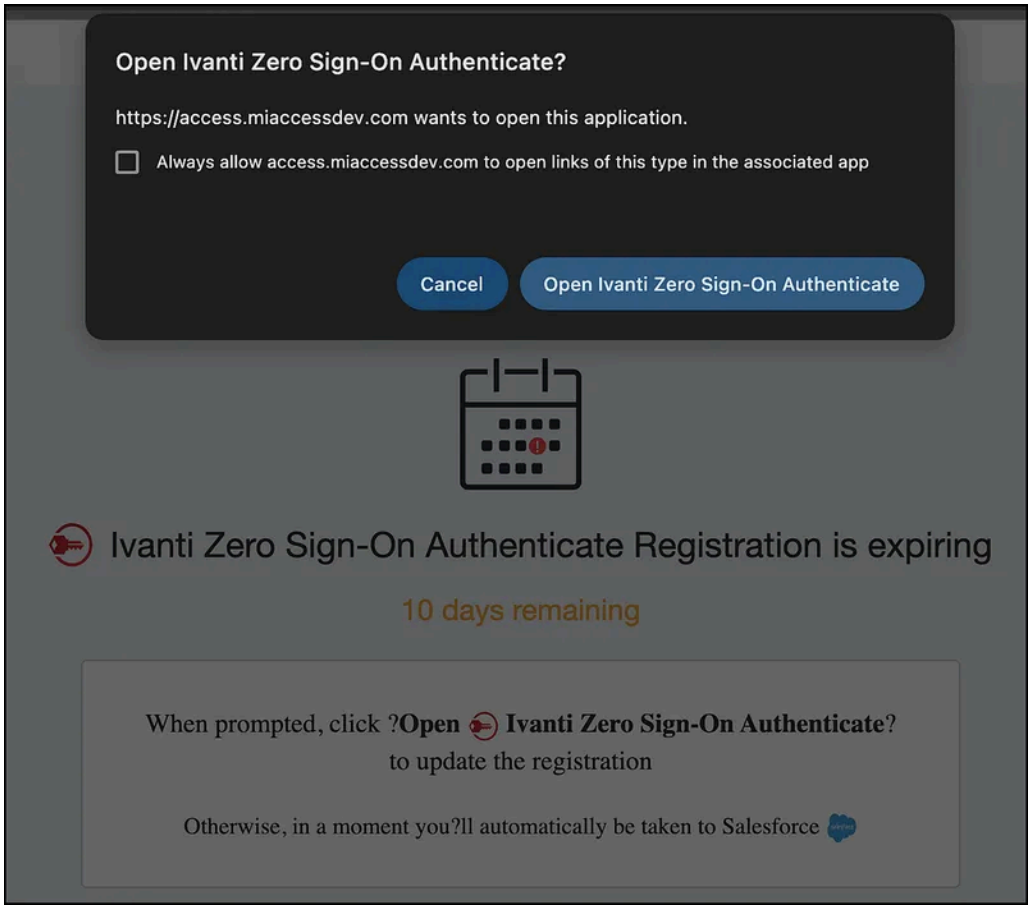
Within the configured grace period before key expiry (e.g., Day 179 of a 180-day rotation): A popup notification appears informing the user about upcoming key expiry.



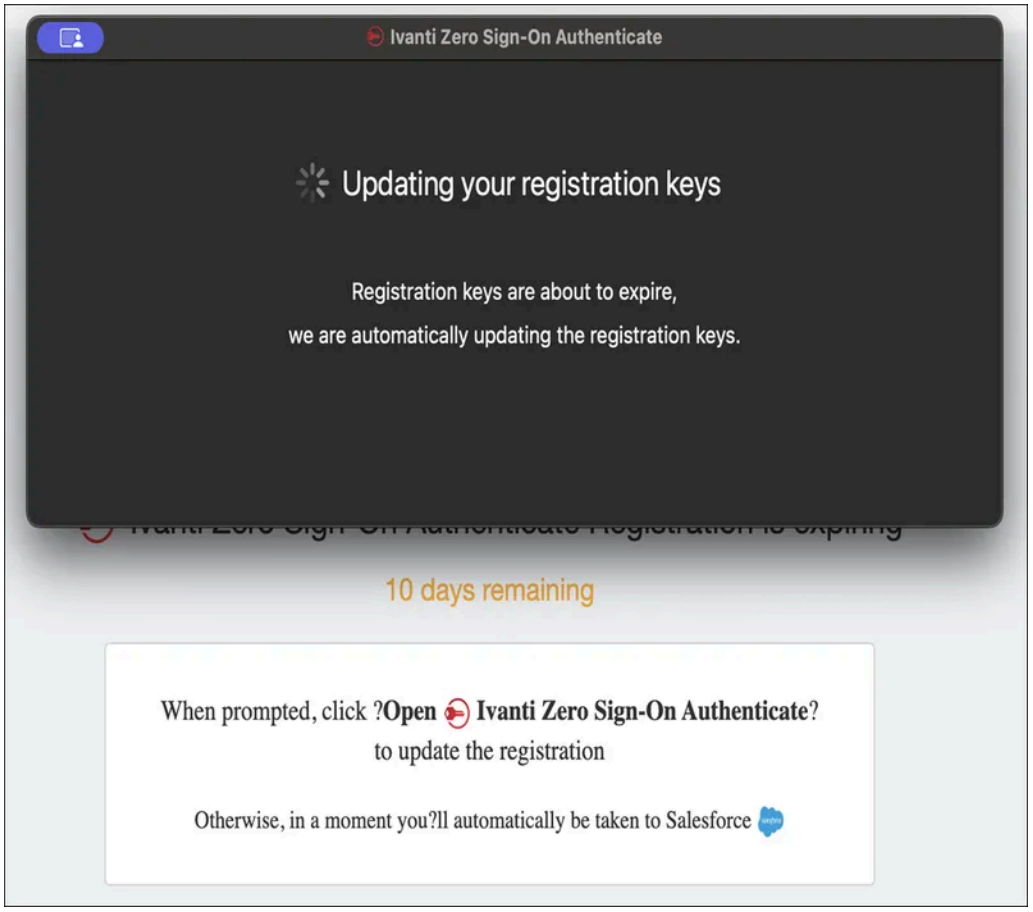
> Users cannot check the key expiry status ahead of time. Notification appears only during the configured grace period.

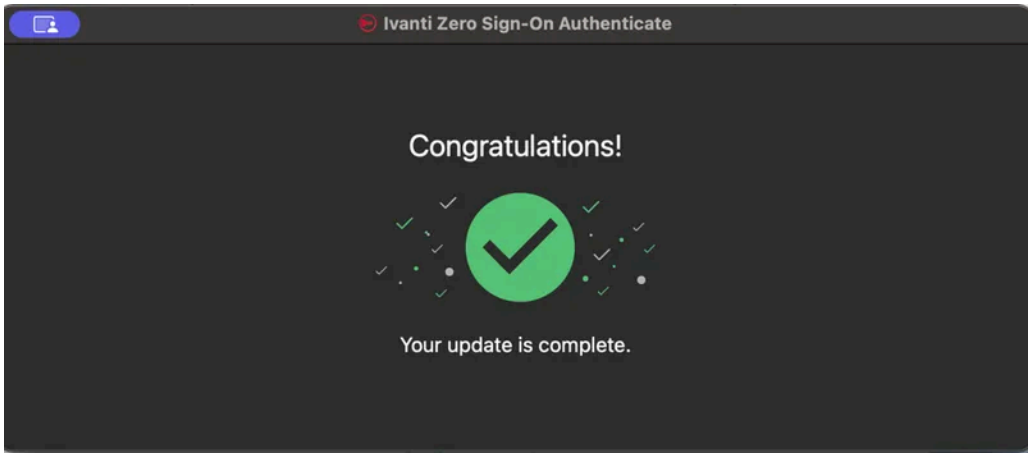
Two options are presented:

1. **Update Now**: Triggers regeneration of keys via Ivanti FIDO Authenticator.
    1. Click **Open Ivanti Zero Sign-On Authenticate**.



2. Registration is updated automatically.



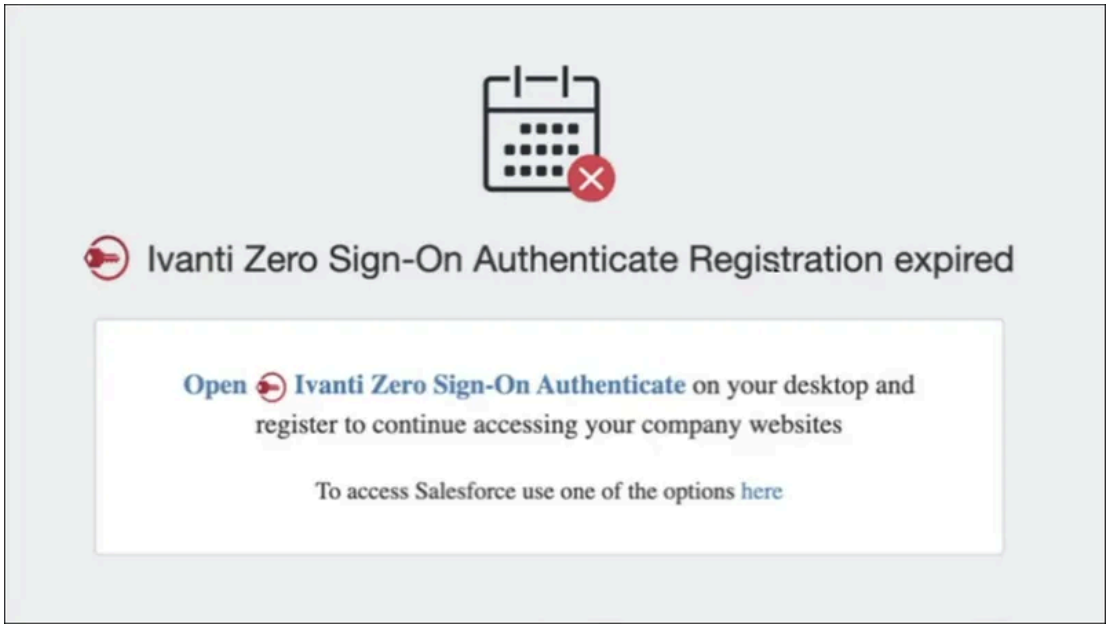


2. **Later**: Dismisses the warning. You can continue to log in if keys are still within valid period.

Post-Expiry Behavior

Once the rotation + grace period expires: Keys become invalid.

1. You will get an "expired" screen when selecting ZSO Authenticate.



1. ZSO authentication is blocked. The following user alternatives are available:
    1. Choose another login method (if enabled by admin):
        - Sign in using QR Code
        - Sign in using Password
        - Sign in using Security key or Biometric
    2. Re-register the ZSO Authenticate Agent:
        - Relaunch the Desktop Trust Agent.
        - Follow the registration flow again.

        > Device does not need to be re-enrolled. Only the ZSO Authenticate Agent is re-registered.

14.6. Client Registration Settings

The Client Registration Settings is used to register Zero Sign-on clients such as Go and Authenticate with Access. The clients send the device identity certificate to Access for Zero Sign-on registration.

The device identity certificates used by clients must follow the same schema as the certificate used in Certificate SSO, under Federation. Use the following setting to determine the username from the certificate and register.

Procedure

1. In Ivanti Access, go to Profile > Client Registration Settings.
2. For User Certificate, select the user certificate from which to get the user identification information such as the username. The user certificate is the Ivanti Tunnel sample certificate you uploaded to Ivanti Access.

3. For Field Name, select the field from which the UEM client gets user identifying information.
4. (Optional) For Additional transforms, enter a MiTra expression.
   Configure a MiTra expression if the value in the certificate does not map directly to the user identifying information.
   Example: select:X509:SubjectAltName:rfc822Name
5. Click Save Registration.

Next steps

- **Configuring Zero Sign-on in Ivanti Access**
- **Configuring multi-factor authentication in Ivanti Access**

Related topics

For information about MiTra expressions, see **Language to generate values from certificate fields**.

15. Zero sign-on support in Ivanti Access using FIDO hardware keys for unmanaged desktops

For unmanaged desktops, users can now use their FIDO enabled hardware keys to access the service provider with zero sign-on.

When the user is authenticated using certificate-based SSO, attribute mappings in Ivanti Access federated pair configuration are required to populate the attributes to be sent to Service Provider (SP) in SAML assertion. The attribute mappings and transformation configured in Federated pair is used to extract and transform the user attributes in Identity certificate to service provider specific attributes when constructing SAML assertion.

With FIDO hardware security key, identity certificate is not available to Ivanti Access or used to authenticate the user. Consequently, there is no option available to obtain user attributes from certificate to generate SAML assertion after FIDO authentication.

The following procedure must be completed to configure hardware keys:

- Admin Configures Ivanti Access to use Access Attributes
- Admin Configures a User Portal (to register and manage keys)
- User logon to User Portal and register hardware key
- User logon to SP using "Sign in using Register Key" option on ZSO interaction page.

Use case

- Allow users to sign-in to the federated service without password from an unmanaged desktop.

> For managed desktops, use Ivanti Tunnel or Authenticate.

15.1. Configuring attribute mapping and migration in federation

Before you begin

- Verify that you have enabled the access attributes and hardware key.

Procedure

1. Login to Ivanti Access administration portal with admin credentials.
   Click Profile to view new links such as User Home, Users, and User Certificates.
2. Click User Certificates to import a new certificate and map the user attributes to control the user information exchanged between Identity Providers and Service Providers.
   If the Certificate based Single Sign-on (SSO) attributes are updated in the federated pair and if the attributes are migrated into User Certificates, then an error displays. Click Copy to migrate the changes to User attributes.
3. Click Save to import and copy the changes to User Certificates.
   This option is irreversible.
4. Click Profile > Federation and publish the changes.
   Ivanti Access Attribute mapping is now available in the federated pair and the User Certificates attributes are now mapped to Access Attributes.

Verifying the SAML pair for attributes

Procedure

1. Login to any application to validate authentication.
2. After authentication, login to Access
3. Click Data & Reports > Access.
4. Ensure that the Assertion Attributes are validated appropriately.

15.2. Configuring user portal

This topic lets you configure portal URL and authentication process to the portal.

Before you begin

- Verify that you have the SAML metadata of the identity provider.
- Verify that you have set up the attribute mapping of certificate attributes to access attributes in User Certificate tab. For more information, see **Configuring attribute mapping and migration in federation**.

Procedure

1. Login to Ivanti Access with admin credentials.
2. Click Profile > User home.
3. Click Configure Portal.
   The Portal Settings window opens.
4. Enter the following details:
   1. **Name**
   2. **Enter the Portal URL**: https://<tenant name>.miaccessdev.com
      After the setup is complete, the company name cannot be changed.
   3. The Access attribute mapping is complete.
5. Click Next.
6. Select the appropriate identity provider from the list.
7. Select the signing certificate from the drop-down list.
8. Select Metadata URL and enter the metadata for the identity provider.
9. Click Done > Ok.
10. Click Publish > Ok.
    The User portal is now configured.
11. Click Actions > Assign Policy to assign a ZSO policy or a default policy.
    If the user now tries to access a federated pair, sign-in using hardware key option is not available.
    The configuration is now complete.
12. On the User Home portal, click Edit on the pair .
13. In Ivanti Access attribute mapping, select rfc822name1.
14. Click Add New to add a new attribute.
    1. Type: UserDomain
    2. Access attribute mapping: directoryName
15. Click Next > Done.
16. Click Publish.
    You can now distribute the Portal URL to the users and it can be used to sign-in to the portal.

15.3. Logging into user portal

Before you begin

- Verify that you have configured the User Portal. For more information, see **Configuring attribute mapping and migration in federation**.

Procedure

1. Login to Ivanti Access with admin credentials.
2. Click Profile> User Home.
3. Copy the Portal URL that is available through an email communication.
4. Paste the Portal URL in a new browser.
   The IdP login window displays.
5. Login with the credentials.
   The Ivanti User Home portal opens. The biometric and security keys available are listed on this page.

Next Steps

Register security key or biometric for FIDO authentication appropriately.

> On macOS earlier than v11, when Mac Touch ID and security key are registered and security key is inserted into the laptop during authentication, browser gives preference to security key and does not allow to select Mac Touch ID. In such a scenario, unplug the security key to use Mac Touch ID as the authenticator.
>
> On macOS later than v11, the browser gives preference to Mac Touch ID. However, user can click Cancel to change the authentication method.

15.3.1. Registering the security key for FIDO authentication

You must register the security key to use the key for FIDO authentication. With security key, you can securely sign-in to your work websites from any device.

Before you begin

- Verify that you have configured the user portal. For more information, see **Configuring attribute mapping and migration in federation**.
- Verify that you are logged into the user portal. For more information, see **Logging into user portal**

Procedure

1. Login to the Ivanti User Home portal.
2. In the Security Key section, click Register to register the security keys.
   The Register Key window opens.

3. Enter the name of the key.

   The name of the key must contain alpha numeric, hyphen and underscore. A space is not allowed in the key name.
4. Continue with the process to complete the registration.
   You can now use this key to to sign-in to user portal and service providers.

15.3.2. Registering the biometric for Zero Sign-on authentication

You must register the biometric to use your fingerprint for Zero Sign-on authentication. Registering the biometric lets you securely sign-in to your work websites on registered devices using biometric.

Before you begin

- Verify that you have configured the user portal. For more information, see **Configuring attribute mapping and migration in federation**.
- Verify that you are logged into the user portal. For more information, see **Logging into user portal**

Procedure

1. Login to the Ivanti User Home portal using Sign in using Password option for first time log in or with a Sign in using Security key or Biometric option if security key is registered.
2. In the Biometrics section, click Register to register the biometrics for Windows Hello, MacTouch ID, or other mobile devices. The Register Biometrics window for Windows Hello or MacTouch ID or for devices opens based on the device that you are using.

3. Windows Hello
    1. Enter a name that is already not in use and click Next.
    The Windows security wizard displays for security PIN.
    2. Enter the security PIN and click OK.
    
    3. Click Done to complete the Windows Hello ID registration.
    
4. MacTouch ID
    1. Enter a name that is already not in use and click Next.
    2. The security wizard opens to use Touch ID or password.
    
    3. Click Done to complete the Mac Touch ID registration.
5. Mobile devices
    1. Enter a name that is not in use.

    2. Click Done to Register your Biometric Device.

    3. The registration is complete.

6. Verify that the biometrics are registered by signing out and signing in again from the User Home portal using biometrics.

15.4. Accessing service provider using security key or biometric

You can access the service provider using the security key that was created.

Before you begin

- Verify that you have enabled Security Key and Biometric authentication in **Access** > **Zero Sign-On** > **Zero Sign-On Settings** > **Security Key and Biometrics**.
  For more information, see **Setting Zero Sign-on security and user experience**.

Procedure

1. Open the appropriate service provider from your browser.
   The authentication window opens.

2. Click Sign in using Registered Security key or Biometric.
3. Click Continue and follow the instructions
4. **For Security key**: Touch the Key and enter the Security Pin.
   For Biometric: Touch the pad to authenticate using fingerprint.
   Only fingerprint biometric is supported for 2FA authentication.
5. The authentication completes and user is successfully logged in to the service provider.



Biometric authentication is now available on iOS and Android devices for registration.

16. Authenticator Only with Ivanti Access

Authenticator Only allows employees to use their unmanaged mobile device as their identity and authentication factor. Using their mobile device as their identity allows employees to take advantage of Zero Sign-on features, which allow passwordless access to SaaS applications and other business services.

- About Authenticator Only with Ivanti Access
- Configuring Authenticator Only on Ivanti Neurons for MDM
- Viewing Authenticator Only on Ivanti Neurons for MDM
- Configuring Authenticator Only on Ivanti EPMM
- Viewing Authenticator Only on Ivanti EPMM
- What users see for Authenticator Only

16.1. About Authenticator Only with Ivanti Access

In an Authenticator Only deployment, employees register their device with a unified endpoint management (UEM) platform in Authenticator Only mode. A device that is registered with in Authenticator Only mode is not managed. This means that mobile device management policies and configurations such as mobile threat defense, password requirements, Wi-Fi, VPN are not applied to the device. However, the Authenticator Only device checks in with the UEM periodically and registers the posture of the device. If the Authenticator Only device is in compliance, users can continue to use it as their identity and authentication factor.

The following provides additional information about Authenticator Only with Ivanti Access:

- **Required components for Authenticator Only**
- **Use cases for Authenticator Only**
- **Authentication flow for Authenticator Only**
- **Device actions and policies for Authenticator Only**
- **Android enterprise and Authenticator Only**

Required components for Authenticator Only

Deploying Authenticator Only requires that the following components are set up:

- Ivanti Access deployment with a Unified Endpoint Management (UEM) platform. The UEM platforms are:
  - Ivanti Neurons for MDM
  - Ivanti EPMM
- UEM client. The UEM clients are:
  - Go for Ivanti Neurons for MDM
  - Mobile@Work for Ivanti EPMM.

See the Release notes for Ivanti Neurons for MDM or Ivanti EPMM for supported client versions.

Use cases for Authenticator Only

The following describes the authentication use case enabled with Authenticator Only devices:

- Password less access from unmanaged devices: Users accessing an enterprise cloud service provider (SP) from an unmanaged device are presented with a QR code. Scanning the QR code with their Authenticator Only device authenticates the user and allows access from the unmanaged device. Users scan the QR code using the client and the native camera on the Authenticator Only device. Users do not need to enter their username and password. Users have the following additional options for subsequent log in:
  - Enable push notifications. If enabled, a push notification is sent to the managed device on subsequent log in from the unmanaged device.
  - Alternately, users can use the client on their managed device to generate a one-time passcode (OTP). OTP allows users to access cloud services from the unmanaged device even when the client does not have access to the Internet.

The following table describes the passwordless features with Authenticator Only devices:

UEM	Client	Feature supported
Ivanti Neurons for MDM	Go for iOS	QR code, push notifications, OTP
	Go for Android and Android enterprise	QR code, push notifications, OTP
Ivanti EPMM	Mobile@Work for iOS	QR code, push notifications, OTP
	Mobile@Work for Android and Android enterprise	QR code, push notifications, OTP

Authentication flow for Authenticator Only

The following describes the authentication flow from an Authenticator Only device using passwordless authentication.

Figure 1. Authenticator Only authentication flow



1. User requests access to a cloud service from an unmanaged device, such as a desktop.
2. The cloud service redirects user to the configured identity provider (IdP)to authenticate. Since Ivanti Access is the configured IdP, the request is redirected to Ivanti Access.
3. Ivanti Access generates and presents a QR code to the user.
4. The user scans the QR code with the mobile device in Authenticator Only mode to approve the login.
5. Access generates a new SAML response to redirect to the original SP. The original SP obtains the user identity from the SAML response and presents the personalized screen to the user.

Device actions and policies for Authenticator Only

A device in Authenticator Only mode is not managed by UEM. Device and app management policies and features are not available on a device in Authenticator Only mode. To view the device's security posture, the following devices actions and policies are available and applied to Authenticator Only devices.

- **Administrator actions (Ivanti Neurons for MDM)**
- **Administrator actions (Ivanti EPMM)**
- **Device user actions**
- **Compliance polices and actions (Ivanti Nerons for MDM)**
- **Polices and actions (Ivanti EPMM)**

Administrator actions (Ivanti Neurons for MDM)

Administrators can take the following actions on Authenticator Only devices on Ivanti Neurons for MDM:

- Retire: The Retire action removes the SaaS configuration (Ivanti Nerons for MDM) or policy (Ivanti EPMM) from the device and retires the device.
- Add to Group: Select or change the device group.
- Assign Custom Attributes

- Remove Custom Attributes
- Assign to user
- Force Check-in
- Set Ownership

Administrator actions (Ivanti EPMM)

Administrators can take the following actions on Authenticator Only devices on Ivanti EPMM:

- Retire: The Retire action removes the SaaS policy from the device and retires the device.
- Apply to Label
- Remove from Label
- Set Custom Attributes: Set or clear custom attributes.

Device user actions

The following lists the actions device users can take on the User portal:

- Retire Device
- Send invitation

Compliance polices and actions (Ivanti Nerons for MDM)

The following compliance policy is applied to Authenticator Only devices on Ivanti Nerons for MDM:

- Compromised Devices policy: Go checks in with the Ivanti Nerons for MDM and reports if the device is compromised. The device status is displayed in the listing for the device in Device > Device on Ivanti Nerons for MDM. The following compliance actions are applied on Authenticator Only devices:
  - Retire: Removes the SaaS configuration from the device and retires the device.
  - Quarantine: Uninstalls the SaaS only configuration and associated certificates.

Polices and actions (Ivanti EPMM)

The following policies and compliance actions are applied to Authenticator Only devices on Ivanti EPMM:

- Security policy: The default policy is applied.
- Sync policy: The default policy is applied.
- Privacy policy: The default policy applied.
- Compliance actions:
  - Quarantine: The SaaS policy is removed.

See "Managing Compliance" in the Ivanti EPMM Device Management Guide

Android enterprise and Authenticator Only

If the UEM supports both Work Profile for device management (MDM), as well as Authenticator Only, the Work Profile policies and configurations take priority.

Therefore, Ivanti recommends creating separate user groups for Android enterprise and for Authenticator Only. Do the following:

- Apply the Authenticator Only devices to the Authenticator Only user group.
- Do not apply Android enterprise devices, polices, and configurations, to the Authenticator Only user group. The Android enterprise configurations are:
  - Android enterprise: Work Profile (Android for Work)
  - Android enterprise: Work Managed Device (Android for Work)
  - Android enterprise: Managed Device with Work Profile

16.2. Configuring Authenticator Only on Ivanti Neurons for MDM

An Authenticator Only deployment requires an Ivanti Access deployment with UEM, as well as additional configurations for Zero Sign-on in Ivanti Access and in the UEM. The configurations for Authenticator Only are done in UEM. The following steps provide an overview of the configuration steps for deploying Authenticator Only and pointers to the relevant content in the *Ivanti Neurons for MDM Guide*.

Before you begin

- Ensure that you have an Ivanti Access deployment with UEM.
  See **Overview of configuration with Ivanti Neurons for MDM**.
- Ensure that Zero Sign-on is configured.
  See "Zero Sign-on" in the Ivanti Access Guide.

Procedure: Overview of steps

1. Create a user group to deploy Authenticator Only and manually add users to the group.
   See "Creating a manually managed user group" in the ***Ivanti Neurons for MDM Guide***.
2. Create a dynamically managed device group with the rule "user group," which equals to the user group created for Authenticator Only.
   See "Adding a device group" in the ***Ivanti Neurons for MDM Guide***.
   If devices had been previously enrolled in an Ivanti Neurons for MDM tenant, users will not be able to register with the same Ivanti Neurons for MDM tenant using Authenticator Only. Delete the devices from the Ivanti Neurons for MDM tenant, then register again with the same Ivanti Neurons for MDM tenant using Authenticator Only.
3. Create an Authenticator Only configuration and assign it to the dynamically managed device group created for Authenticator Only.
   See **Adding an Authenticator Only configuration on Ivanti Neurons for MDM**.
4. Sync with Ivanti Access.
   See **Syncing with Ivanti Access**
5. Download and register Go.
   If Always require client registration is enabled in Users > User Settings > Device Registration Setting in Ivanti Neurons for MDM, users automatically get emails for registering their device using Go. Device users download Go to their device directly from the Apple App Store or from Google Play Store.
   See **What users see for Authenticator Only** for information about how device users can register their devices to your Ivanti Neurons for MDM instance.

Related topics

- **About Authenticator Only with Ivanti Access**
- **What users see for Authenticator Only**

Adding an Authenticator Only configuration on Ivanti Neurons for MDM

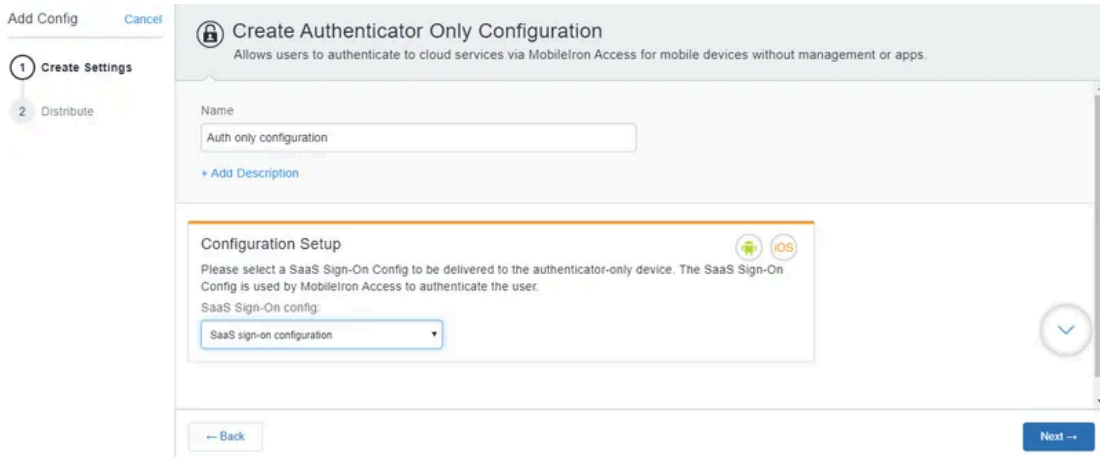
Create an Authenticator Only configuration on Ivanti Neurons for MDM.

Before you begin

You can create the Authenticator Only configuration only if a SaaS Sign on configuration is available. Therefore, verify that a SaaS Sign on configuration has been created. The SaaS Sign on configuration is created for a Zero Sign-on deployment. See "Zero Sign-on" in the Ivanti Access Guide.

Procedure

1. In Ivanti Neurons for MDM, go to Configurations > + Add > Authenticator Only.
   Figure 1. Authenticatory only configuration



1. In the Name field, enter a name for the configuration.
2. (Optional) Expand + Add Description, to add a description for the configuration.
3. For SaaS Sign-On config, select a SaaS sign on configuration.
   The selected SaaS Sign-On configuration is pushed to the device. Ivanti Access uses the SaaS sign-on configuration to authenticate the device.
4. Click Next.
5. Verify that the the check box for Enable this configuration is selected.
   The option is selected by default.
6. Select the distribution group created for Authenticator Only.
   The configuration is distributed to the devices in the selected option.
7. Click Done.

Next steps

Syncing with Ivanti Access

Syncing with Ivanti Access

Sync with Ivanti Access to pull the UEM configurations.

Procedure

1. In Ivanti Access, navigate to the UEM tab.
2. Select the Ivanti Neurons for MDM UEM and click the Sync UEM icon.
3. Enter the UEM administrator credentials and click Verify.
4. Click Done.

Next steps

See **Registration workflow for Authenticator Only devices**

16.3. Viewing Authenticator Only on Ivanti Neurons for MDM

After a device registers with Ivanti Neurons for MDM in Authenticator Only mode, device information and status is available on Ivanti Neurons for MDM.

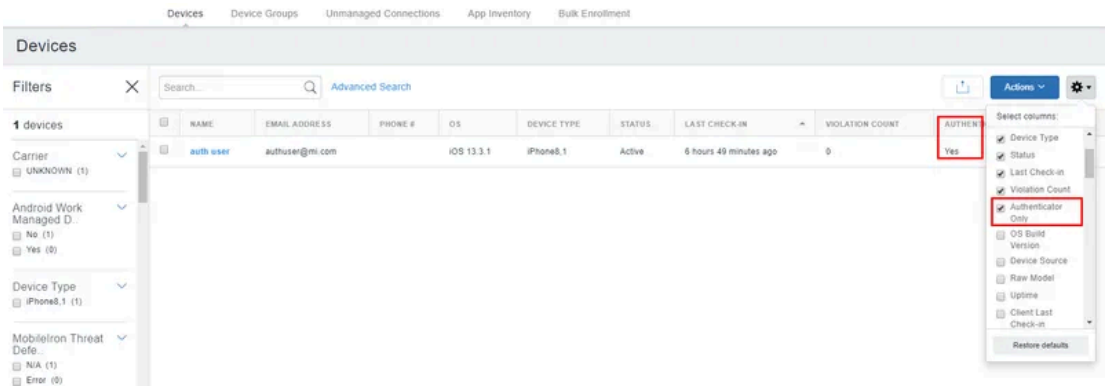
- Devices list
- Device details

Devices list

A device in Authenticator Only mode is listed with all other devices registered with Ivanti Neurons for MDM. To view device listings, on Ivanti Neurons for MDM, go to Devices > Devices. Go to the Settings icon and select the check box for Authenticator Only. Selecting the option makes the Authenticator Only column visible in Devices > Devices. The Settings icon is visible on the top right corner of Devices listing page.

The value for Authenticator Only displays as Yes if the device is registered as an Authenticator Only device.

Figure 1. Authenticator only column in devices list

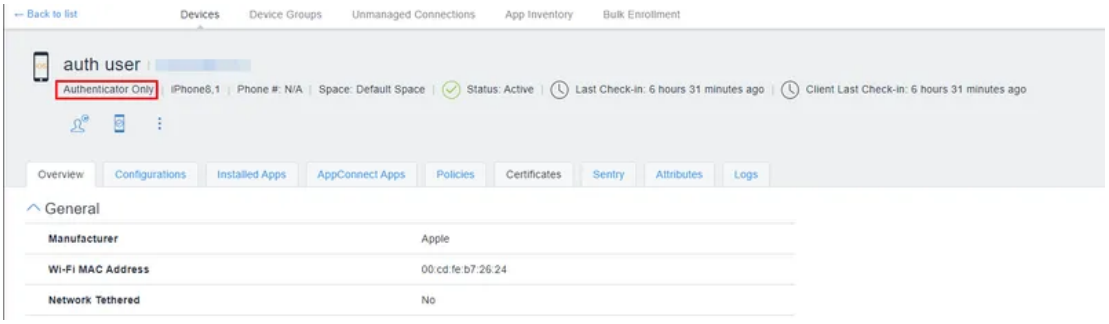


Device details

The Authenticator Only device label is seen for devices when you click on the device listing for more details.

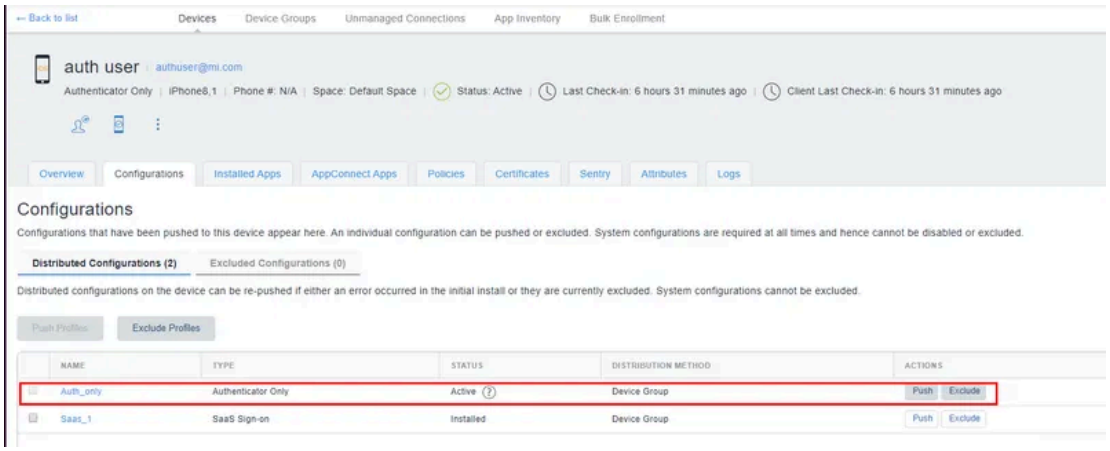
> The label is also visible in the user portal for an Authenticator Only device.

Figure 2. Authenticator only label in device details



The Configuration tab in device details also displays the Authenticator Only configuration applied to the device.

Figure 3. Authenticator Only configuration in device details



16.4. Configuring Authenticator Only on Ivanti EPMM

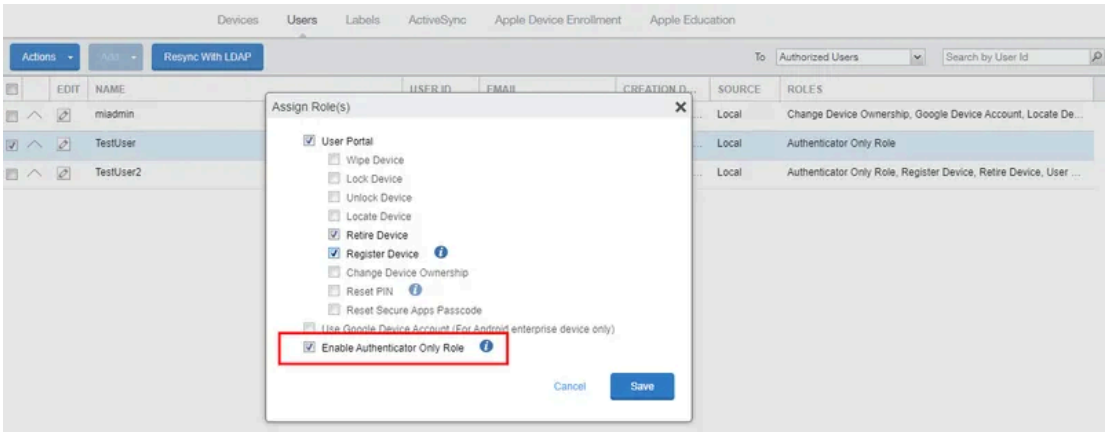
An Authenticator Only deployment requires an Ivanti Access deployment with UEM, as well as additional configurations for Zero Sign-on in Ivanti Access and in the UEM. The configurations for Authenticator Only are done in UEM. The following steps provide an overview of the configuration steps for deploying Authenticator Only and pointers to the relevant content in the Getting Started with Ivanti EPMM guide.

Before you begin

- You have set up Ivanti Access with Ivanti EPMM.
  See **Overview of configuration with Ivanti EPMM**.
- Ensure that Zero Sign-on is configured.
  See "Zero Sign-on" in the Ivanti Access Guide.

Procedure: Overview of steps

1. Create an LDAP group for Authenticator Only deployment and configure the group in Ivanti EPMM.
   See "Managing LDAP users" in the Getting Started with Ivanti EPMM guide.
   Alternately, you can add local users.
   See "Adding local users" in the Getting Started with Ivanti EPMM guide.
2. Assign the Enable Authenticator Only Role user role to the Authenticator Only LDAP group or local user in Ivanti EPMM.
   When you assign the Enable Authenticator Only Role to a user, the Retire Device and Register Device User Portal roles are selected by default. The Retire Device and Register Device roles are the only User Portal roles available for Authenticator Only users. All other User Portal roles are grayed out.
   See "Assigning and removing device user roles" in the Getting Started with Ivanti EPMM guide.
   If a user is assigned the Enable Authenticator Only Role, then the user can register their device in Authenticator Only mode. This does not impact any devices that the user has already registered.
   Figure 1. enable authenticator only role on ivanti epmm



1. Sync with Ivanti Access.
2. Download and register Mobile@Work.
   In-app registration is supported. Users will need to use their enterprise credentials and know the Ivanti EPMM server address to register. Device users download Mobile@Work to their device directly from the Apple App Store or from Google Play. See "In-app registration for iOS and Android" in the Ivanti EPMM Device Management Guide

n from the UEM.

Procedure

1. In Ivanti Access, navigate to the UEM tab.
2. Select the Ivanti EPMM UEM and click the Sync UEM icon.
3. Enter the UEM administrator credentials and click Verify.
4. Click Done.

Next steps

See **Registration workflow for Authenticator Only devices**

16.5. Viewing Authenticator Only on Ivanti EPMM

After a device registers with Ivanti EPMM in Authenticator Only mode, device information and status is available on Ivanti EPMM.

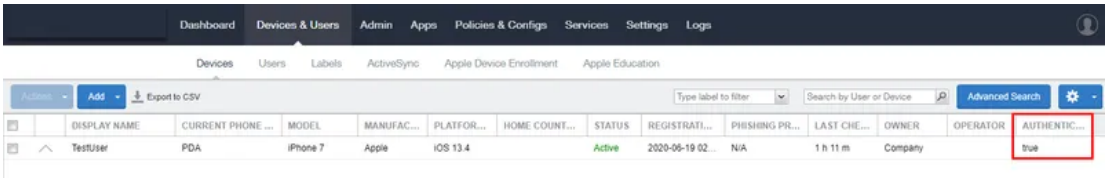
- Devices list
- Device details

Devices list

A device in Authenticator Only mode is listed with all other devices registered with Ivanti EPMM. To view device listings, on Ivanti EPMM Admin Portal, go to Devices & Users > Devices.

The value for Authenticator Only displays as Yes if the device is registered as an Authenticator Only device.

Figure 1. Authenticator only column in devices list

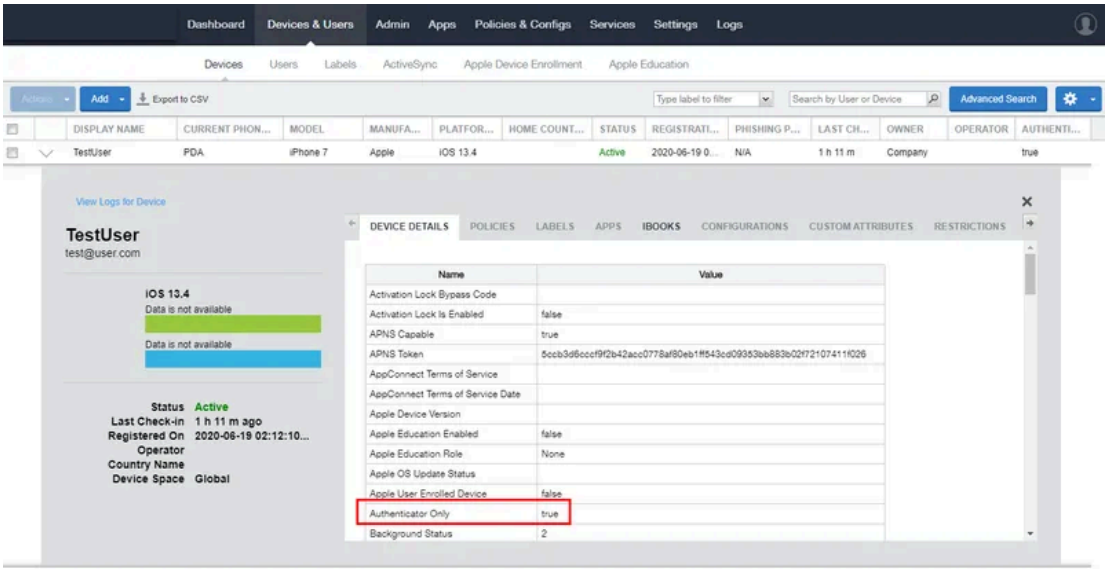


Device details

The Authenticator Only device label is seen for devices when you click on the device listing for more details.

> The label is also visible in the user portal for an Authenticator Only device.

Figure 2. Authenticator only label in device details



16.6. What users see for Authenticator Only

Authenticator Only is a feature available with the UEM client. If Authenticator Only is configured, users can register their unmanaged device in Authenticator Only mode. The device can now serve as the user's identity and authentication factor, allowing users to authenticate and access enterprise cloud services from an unmanaged device without having to use their user name and password.

The following provide information about the user experience with Authenticator Only:

- Registration workflow for Authenticator Only devices
- Log in to cloud services
- Zero Sign-on with QR code - Android Authenticator Only devices
- Zero Sign-on with QR code - iOS Authenticator Only devices
- Zero Sign-on with push notifications or OTP
- Device out of compliance
- Deactivate Authenticator Only on the device

Registration workflow for Authenticator Only devices

To register their devices with UEM in Authenticator Only mode, users can download the UEM client (Go or Mobile@Work) from the Apple App Store or from Google Play Store.

Only in-app registration is supported.

- Authenticator Only registration workflow on Android devices
- Authenticator Only registration workflow on iOS devices

Authenticator Only registration workflow on Android devices

To register their unmanaged device in Authenticator Only mode, users download the UEM client from the Google Play Store. The following picture illustrates the Authenticator Only registration workflow using Go on Android devices.

Users are prompted to grant permission for Go to access the camera. Ivanti Access to the camera is needed to scan the QR code for passwordless authentication. If biometrics is configured on the UEM, device users are prompted to set up biometrics after they have registered.

Authenticator Only registration workflow on iOS devices

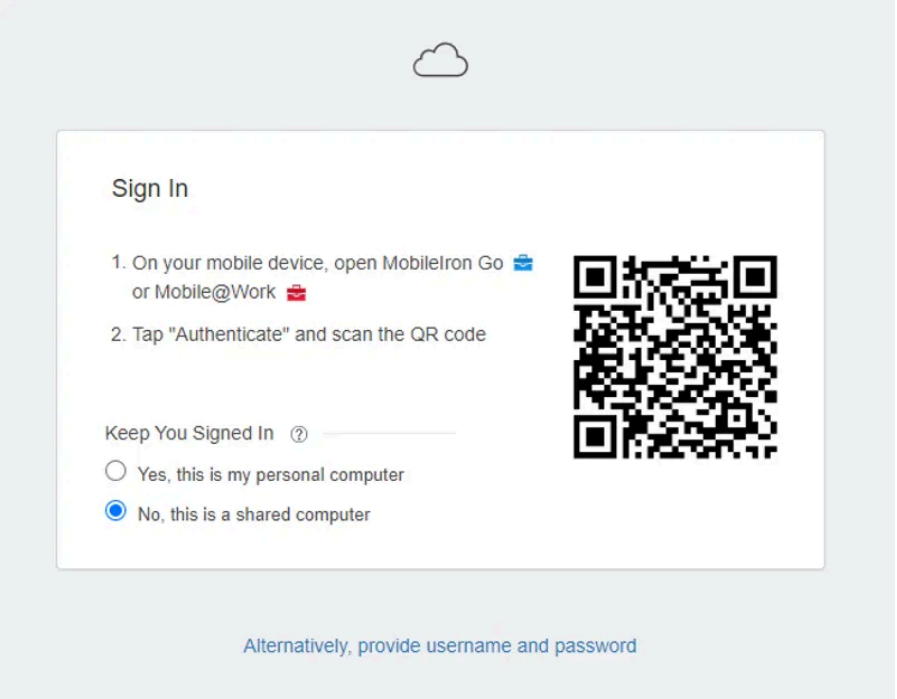
To register their unmanaged device in Authenticator Only mode, users download the UEM client from the Apple App Store. The following picture illustrates the Authenticator Only registration workflow using Go on iOS devices.

If biometrics is configured on the UEM, device users are prompted to set up biometrics after they have registered.

Log in to cloud services

When users attempt to access an enterprise cloud service on an unmanaged device, such as their desktop, they are presented with an interaction page.

Figure 1. QR code presented on an unmanged device



The interaction page contains a QR code and the following options, which are provided for additional security and ease of use:

- Yes, this is my personal computer
  By selecting this option, users indicate that the device is trusted.
- No, this is a shared computer
  By selecting this option, users indicate that the device is publicly available.

Users scan the QR code with the UEM client, Go or Mobile@Work, on their mobile device to sign on to the enterprise cloud service. To scan the QR code, device users,

1. Tap the UEM client on their mobile device.
2. Tap Authenticate.
3. Authenticate with pass code or biometrics.
   The authentication method depends on the setup of the device and the UEM client.

> The Authenticator Only device used to scan the QR code automatically becomes the primary device for passwordless authentication. Push notifications are sent to the primary device.

Subsequent login attempts

If users select the Yes, this is my personal computer option on the interaction page when scanning the QR code, the user ID is remembered on the browser for 30 days. For subsequent login attempts to the enterprise cloud services set up on Ivanti Access:

- Login is seamless. Users are not prompted to sign in for the session timeout duration set by the administrator in Profile > SaaS Sign on.
- For login attempts after the session timeout duration, a push notification is automatically sent to their managed device. Users have the option to either enter an OTP or scan a QR code.

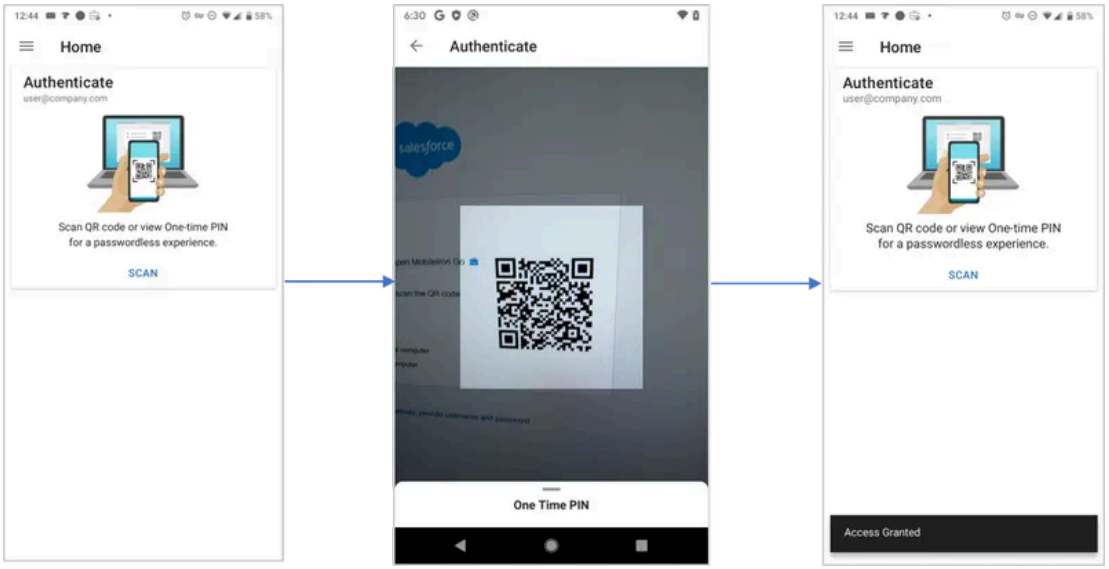
- At the end of 30 days, the user ID is no longer remembered in the browser, and users are once again prompted to scan a QR code.

If users select No, this is a shared computer the session management settings in the cloud service are applied.

Zero Sign-on with QR code - Android Authenticator Only devices

The following figure provides an example of the workflow on an Android Authenticator Only device when using passwordless authentication.

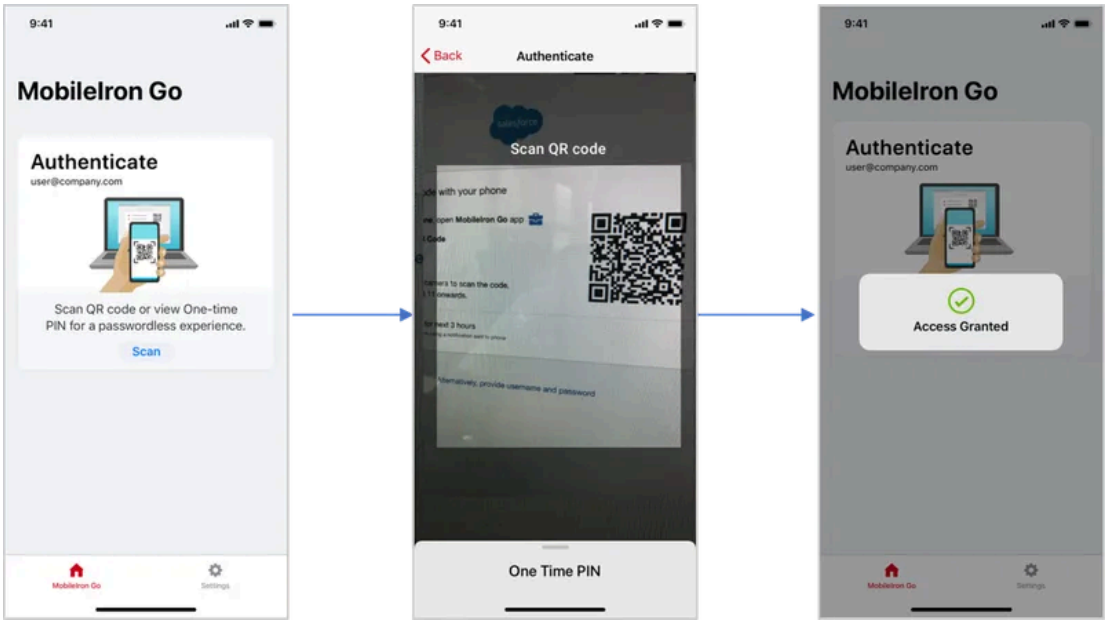
Figure 2. Scanning the QR code - workflow on Anddroid Authenticator Only device



Zero Sign-on with QR code - iOS Authenticator Only devices

The following figure provides an example of the workflow on an iOS Authenticator Only device when using passwordless authentication.

Figure 3. Scanning the QR code - workflow on iOS Authenticator Only device

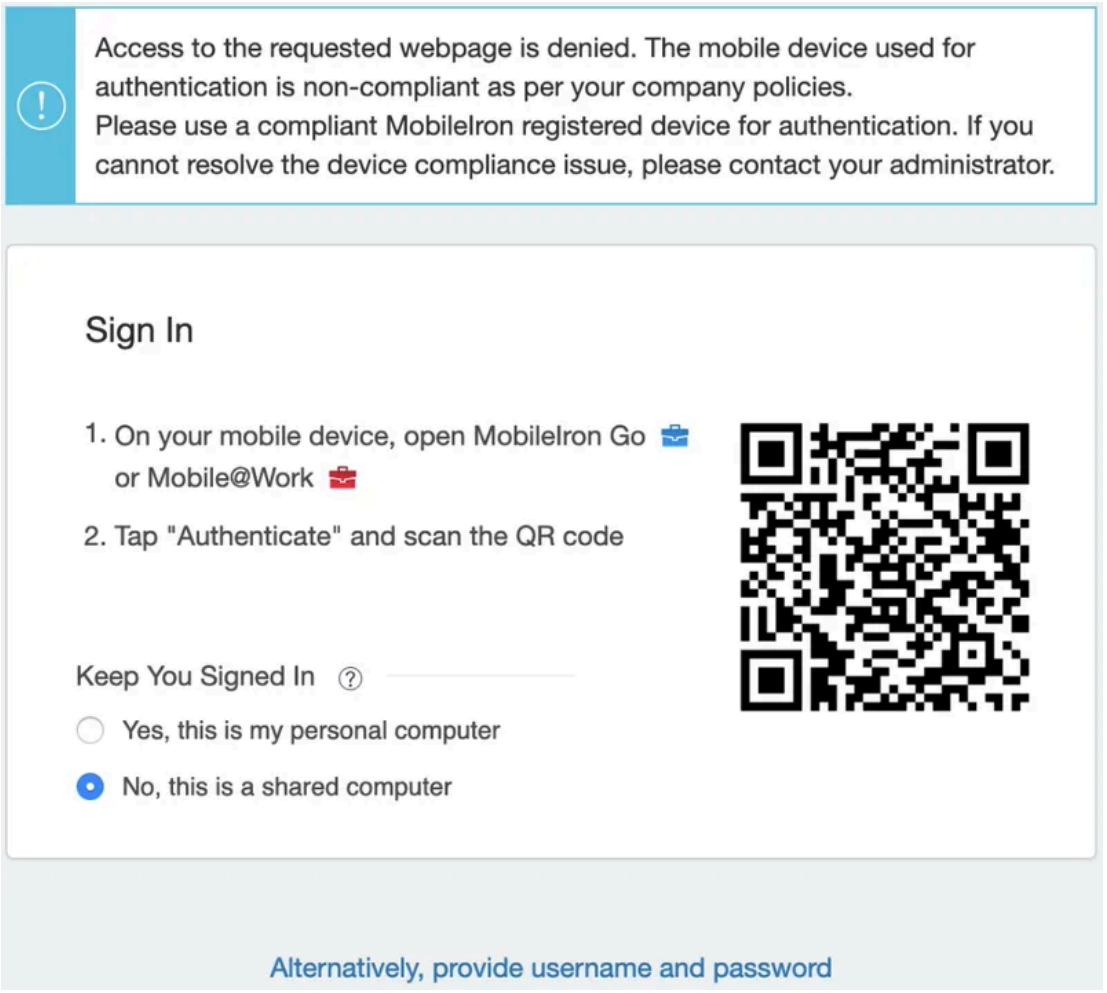


Zero Sign-on with push notifications or OTP

Push notifications are sent to the Authenticator Only device that was used to scan the QR code. . Accepting the push notification on the Authenticator Only device completes the sign-on to the enterprise cloud service.

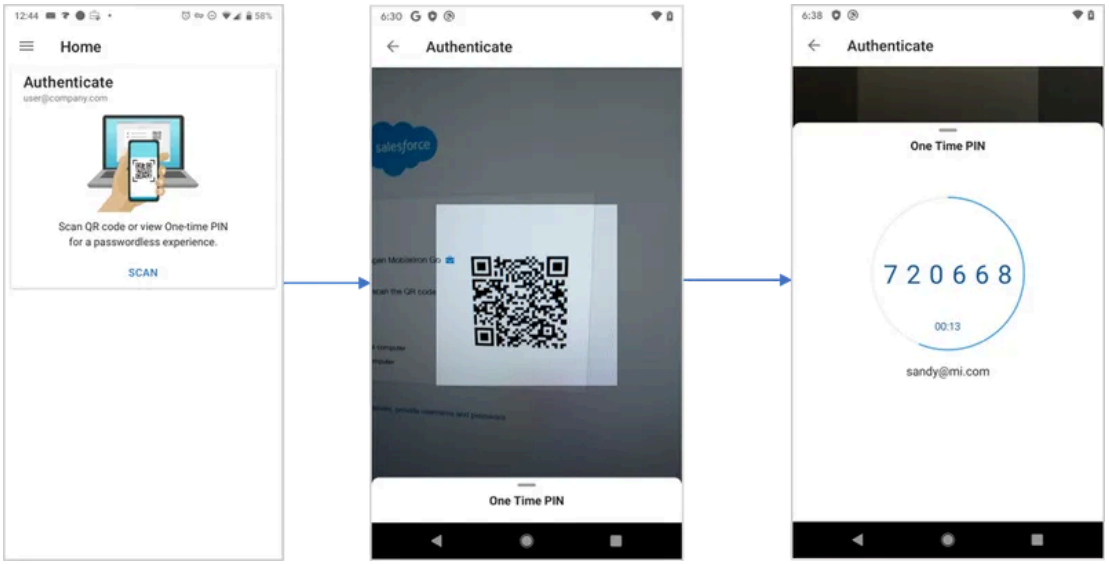
Users also have the option to generate and use a one-time passcode (OTP) instead of using a push notification. Generate the OTP on the Authenticator Only device, then click the OTP option on the unmanaged device to enter the passcode.

Figure 4. Login message if a push notification is sent



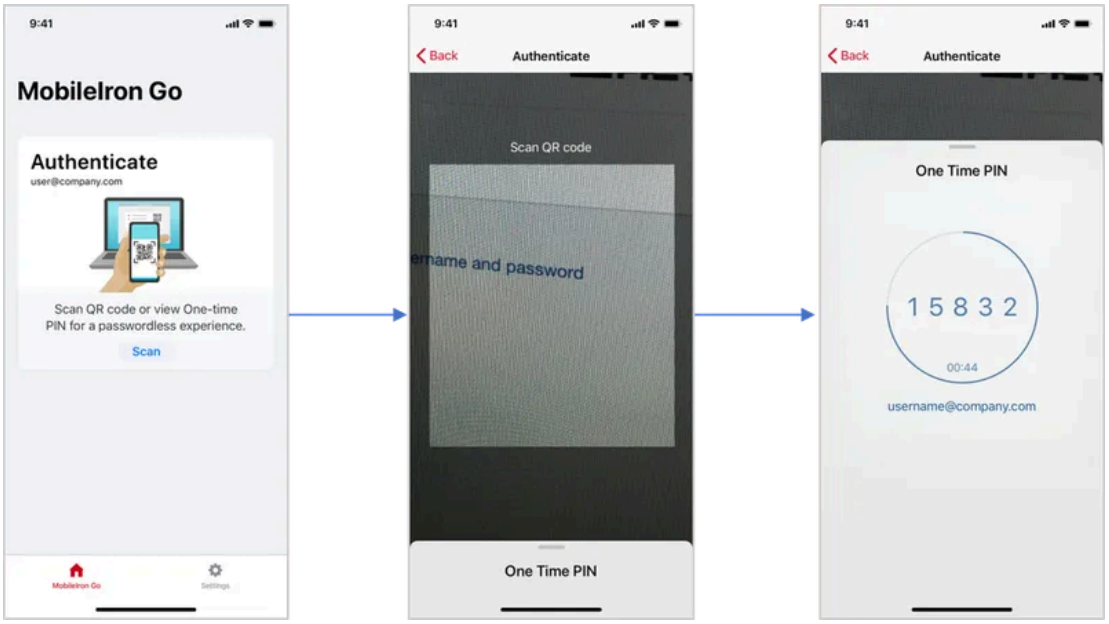
The following illustrates an example of the OTP workflow on an Android device using Go.

Figure 5. OTP option on an Android Authenticator Only device



The following illustrates an example of the OTP workflow on an iOS device using Go.

Figure 6. OTP option on an iOSauth-only device



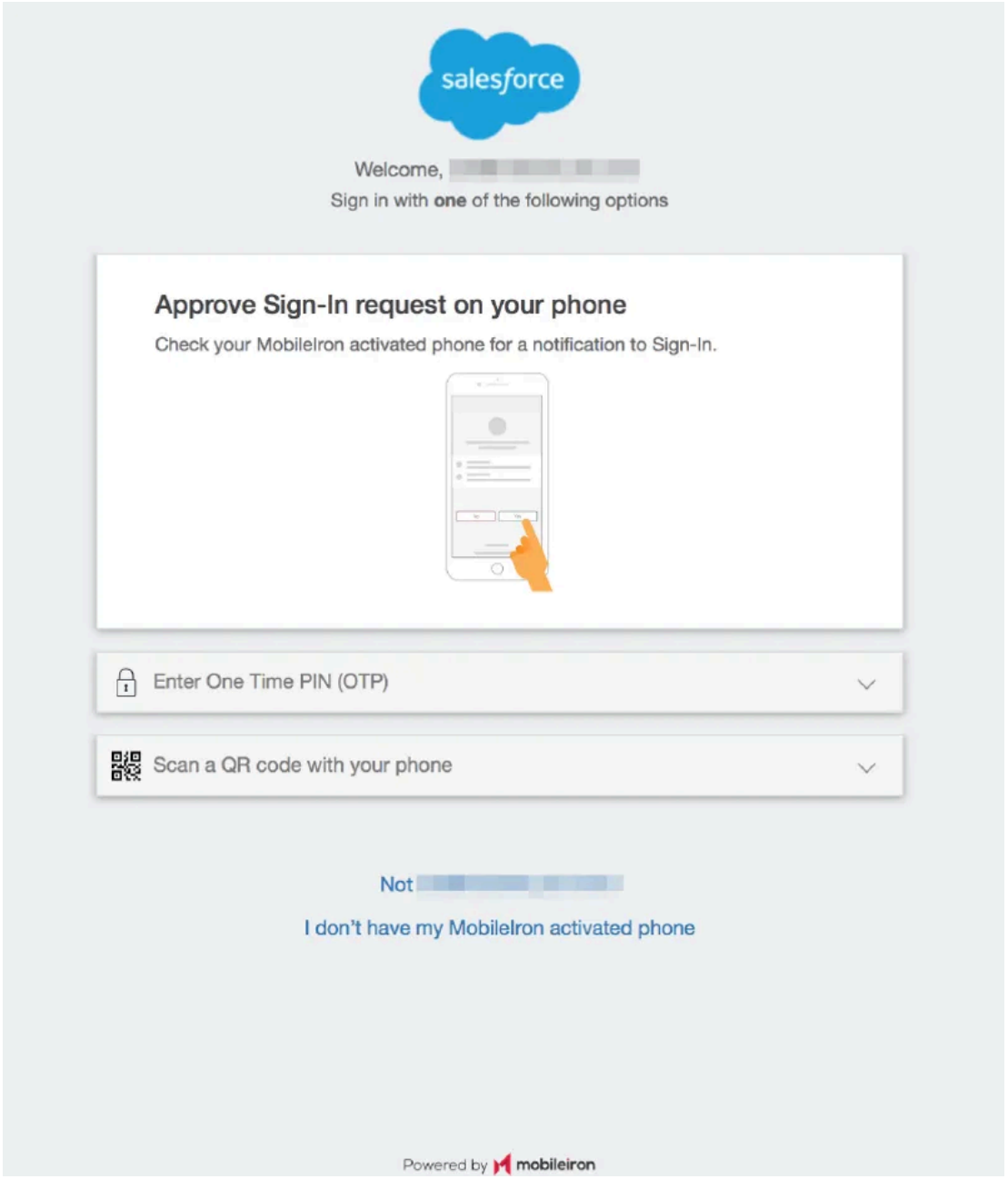
Device out of compliance

In a Authenticator Only deployment, if users scan the QR code with a Authenticator Only device that is out of compliance, an out of compliance message is presented. Ivanti Access to the enterprise cloud service is not granted. A new QR code is presented to the user. Users can switch to a compliant Authenticator Only device to authenticate.

Users see the non-compliance message in the following cases:

- Initial login by user, however the Authenticator Only device is not in compliance.
- Subsequent login by user, however the push notification sent to the Authenticator Only device is not in compliance.

Figure 7. Out of compliance message for devices

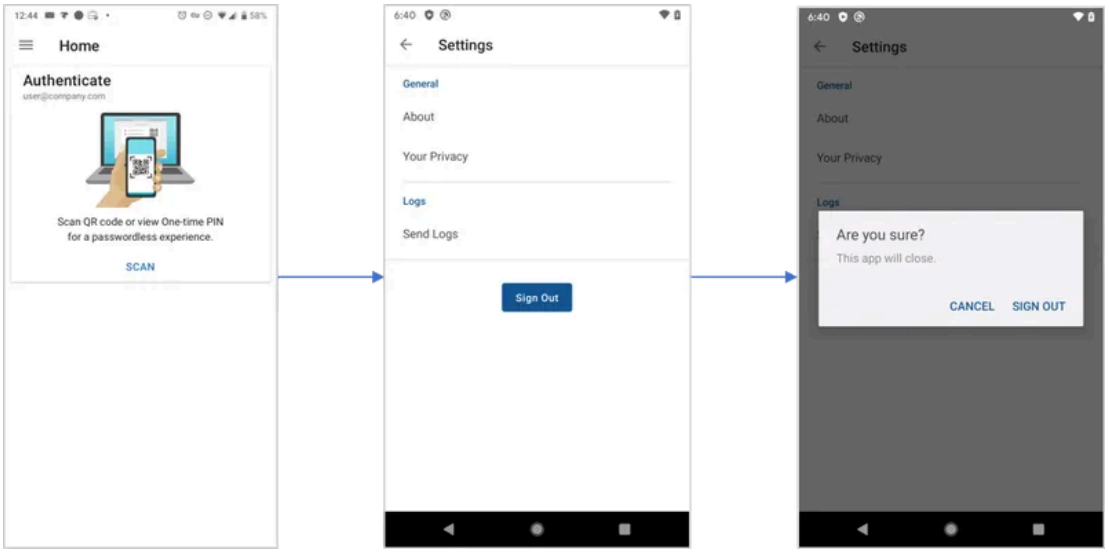


Deactivate Authenticator Only on the device

Users can deactivate Authenticator Only on their device. Users may want to deactivate Authenticator Only on a device if they want to use another Authenticator Only device to scan the QR code and receive push notifications on the new device. The device used to scan the QR code automatically becomes the primary device for Authenticator Only and receives push notifications if the user enabled the feature when scanning the QR code. Deactivating Authenticator Only on the device stops the device from receiving push notifications.

To deactivate Authenticator Only in the UEM client for Android,open the menu and tap Settings > Sign Out.

Figure 8. Deactivate Authenticator Only on Android devices



When users sign out, the device is unregistered from the UEM. However, the UEM client app remains on the device. To register once again, launch the UEM client app on the device and enter the username and password.

On iOS devices, users deactivate Authenticator Only by removing the UEM client from the device. To use the device as user's identity and authentication factor, device users can install and register the UEM client for iOS in Authenticator Only mode.

17. Multi-factor Authentication with UEM Client

Multi-factor authentication with the UEM client allows device users to use their managed mobile device for second-factor authentication.

The reference to multi-factor authentication in device settings is removed from Access user interface. Use the **Client Registration Settings** to register clients such as Go and Authenticate with Access. For more information about configuring, see **Configuring multi-factor authentication in Ivanti Access**.

The multi-factor authentication feature is not supported with Access + Standalone Sentry deployments.

The following provide more information about multi-factor authentication:

- **About multi-factor authentication with UEM client**
- **Overview of configuring multi-factor authentication with UEM client**
- **Configuring multi-factor authentication in Ivanti Access**
- **What users see for multi-factor authentication in UEM client**

17.1. About multi-factor authentication with UEM client

All approval notifications are sent to the primary device. Users also have the option to generate one-time passcode (OTP).

- Required components for multi-factor authentication with UEM client
- Use cases for multi-factor authentication
- One-time passcode (OTP)
- Multi-factor authentication flow
- One-time passcode workflow

Required components for multi-factor authentication with UEM client

Deploying multi-factor authentication with Ivanti Access requires that the following components are set up:

- Ivanti Access deployment.
- UEM client.

See the *Ivanti Access Release Notes* for supported versions.

Use cases for multi-factor authentication

- Two-factor authentication to enterprise cloud services with push notification. Users accessing an enterprise cloud service confirm their identity by:
  - Providing their user credentials, typically the name and password, to the identity provider.
  - Accepting the push notification on their managed device.
- Two-factor authentication to enterprise cloud services with one-time passcode (OTP). Users accessing an enterprise cloud service confirm their identity by:
  - Providing their user credentials, typically the name and password, to the identity provider.
  - Generating a one-time passcode (OTP) using their UEM client, and entering the OTP in addition to their user credentials.
- In addition, administrators can configure conditional rules to define when multi-factor authentication is triggered.
  Example: Create a User Info Rule to trigger multi-factor authentication for only a certain set of users or groups, a Network Rule to trigger multi-factor authentication if the user is outside the enterprise IP range.

One-time passcode (OTP)

Device users have the option of generating a one-time passcode (OTP) in the UEM client, which they can use instead of using push notification. OTP provides users another option to control access to enterprise cloud services from another managed device. It also provides an option to control access to enterprise cloud services even when the client does not have access to the Internet.

The OTP for multi-factor authentication is displayed when the UEM client is launched.

Multi-factor authentication flow

The following describes the authentication flow with multi-factor authentication.

Figure 1. Multi-factor authentication flow



1. User requests access to a cloud service.
2. The cloud service redirects user to the configured identity provider (IdP)to authenticate. Since Ivanti Access is the configured IdP, the request is redirected to Ivanti Access.
3. Ivanti Access redirects the request to the original IdP.
4. The original IdP challenges the user for a user name and password.
5. The user enters the user name and password and posts to the IdP.
6. Ivanti Access obtains the user identity from the SAML response, and sends a push notification to the managed device registered to receive authentication push notifications for that user.

If one-time passcode (OTP) is enabled, users have the option to generate an OTP in the UEM client. See **One-time passcode workflow**

7. The user receives the push notification and launches the UEM client to respond. If the user approves the transaction, the UEM client authenticates to Ivanti Access.
8. If Ivanti Access verifies the user identity received from the UEM client to be the same as the user identity received in the SAML response, Ivanti Access generates a new SAML response to redirect to the original SP
9. The original SP obtains the user identity from the SAML response and presents the personalized screen to the user.

One-time passcode workflow

Device users can generate a one-time passcode (OTP) in the UEM client. A progress value indicates for how long the OTP is valid.

The following describes the OTP workflow when users access a cloud service provider (SP) from a browser or an unmanaged app or device:

1. Users are redirected to an interaction page to enter their credentials. They have the option to click on the Enter one-time password link to enter the OTP obtained from the UEM client.
2. Ivanti Access validates the passcode entered by the user against the passcode generated by the UEM client. A match completes the second-factor authentication of the user.
3. Ivanti Access verifies and retrieves the user identity from the activated device and generates a new SAML response to redirect to the original SP.
4. The original SP obtains the user identity from the SAML response and presents the personalized screen to the user.

17.2. Overview of configuring multi-factor authentication with UEM client

Multi-factor authentication requires configurations in Ivanti Access as well as in the UEM.

Before you begin

- Ensure that you have an Ivanti Access deployment.

See **Set up Ivanti Access with UEM**.

Procedure: Overview of steps

1. Configure multi-factor authentication in Ivanti Access
   See **Configuring multi-factor authentication in Ivanti Access**
2. Configure SasS sign-on in UEM.
   See **Configuring Zero Sign-on in Ivanti Neurons for MDM**.
   OR
   See **Configuring Zero Sign-on in Ivanti EPMM**

Related topics

- **About multi-factor authentication with UEM client**

17.3. Configuring multi-factor authentication in Ivanti Access

The following describes the multi-factor authentication configuration in Ivanti Access.

Procedure: Overview of steps

1. Configuring multi-factor authentication.
   See **Configuring user ID for multi-factor authentication**.
2. Add a conditional rule in Ivanti Access for enabling multi-factor authentication, which triggers authentication using the UEM client.
   See **Adding a conditional rule for multi-factor authentication**.
3. Configure your company branding. Users see the branding on the messages on the device from which they attempt to access cloud services.
   See **Configuring branding for multi-factor authentication in Ivanti Access**.
4. Publish the changes.
   See **Publishing the changes**.

Configuring user ID for multi-factor authentication

Enable multi-factor authentication in Ivanti Access in Profile > Client Registration Settings. You will also map the fields from which the UEM client gets user identifying information.

Before you begin

Upload a sample Ivanti Tunnel certificate in Profile > User Certificates. For more information, see **User Certificates**.

Procedure

1. In Ivanti Access, go to Profile > Client Registration Settings.
2. For User Certificate, select the user certificate from which to get the user identification information.
   The user certificate is the Ivanti Tunnel sample certificate you uploaded to Ivanti Access.

3. For Field Name, select the field from which the UEM client gets user identifying information.
4. (Optional) For Additional transforms, enter a MiTra expression.
   Configure a MiTra expression if the value in the certificate does not map directly to the user identifying information.
   Example: select:X509:SubjectAltName:rfc822Name
5. Click Save.

> One time pass code (OTP) is enabled by default.

Next steps

Add a conditional rule for multi-factor authentication. See **Adding a conditional rule for multi-factor authentication**.

Related topics

For information about MiTra expressions, see **Language to generate values from certificate fields**.

Adding a conditional rule for multi-factor authentication

In the default policy in Ivanti Access, add a Multi-Factor Authentication conditional rule. The rule triggers multi-factor authentication.

Procedure

1. In Ivanti Access, go to Profile > Conditional Access.
2. Expand Default Policy.
3. Click +Add Rule > Multi-Factor Authentication to add the conditional rule.
4. Complete the requested fields.

Item	Description
Name	Enter a name for the multi-factor authentication rule.
Description	Enter a descriptive text for the rule.
Map the Identity Provider (IDP) user ID to Authenticator user ID	Select one of the following: • SAML Subject (Default) • SAML Attribute
Additional transforms	(Optional) Enter a MiTra expression. Configure a MiTra expression, if the value in the federation response does not map directly to the user identifying information. Example: The certificate contains the base-64 representation of the user ID, however you need the hex representation. Enter the following: decode:Base64
Rule Action	From the drop down menu, select Allow.

5. Click Done to save the policy and rule.
   The rule appears at top of the list in the policy.
6. Ensure that the Trusted App and Device rule is enabled and the rule is moved to the top of the list.
7. Edit the General Bypass rule, and set the Action for the rule to Block.

> You can create additional conditional rules to further define how multi-factor authentication is triggered. For example, you can create an User Info Rule to trigger multi-factor authentication for only a certain set of users or groups

Next steps

Configure branding. See **Configuring branding for multi-factor authentication in Ivanti Access**.

Related topics

For information about MiTra expressions, see **Language to generate values from certificate fields**.

Configuring branding for multi-factor authentication in Ivanti Access

Customize the user experience for your enterprise users by uploading your company logo to Access. The user notification screens are customized to display your company logo.

Ensure that your company logo is no more than 260 pixels wide by 30 pixels high. Supported file types are: PNG, JPG, JPEG, and SVG.

Procedure

1. In Ivanti Access, go to Profile > Branding.
2. In the Company Logo section, drag and drop your company logo or click Choose to navigate to the location of the file and add.

Next steps

Publish the updates. See **Publishing the changes**.

Publishing the changes

Publish the changes to make the updates available.

Procedure

1. In the Ivanti Access administrative portal, go to Profile > Overview.
2. Click Publish.

Publish is only available if a federated pair has been created.

3. Click OK.

Next steps

Configure SasS sign-on in UEM.

- See **Configuring Zero Sign-on in Ivanti Neurons for MDM**.
  OR
- See **Configuring Zero Sign-on in Ivanti EPMM**

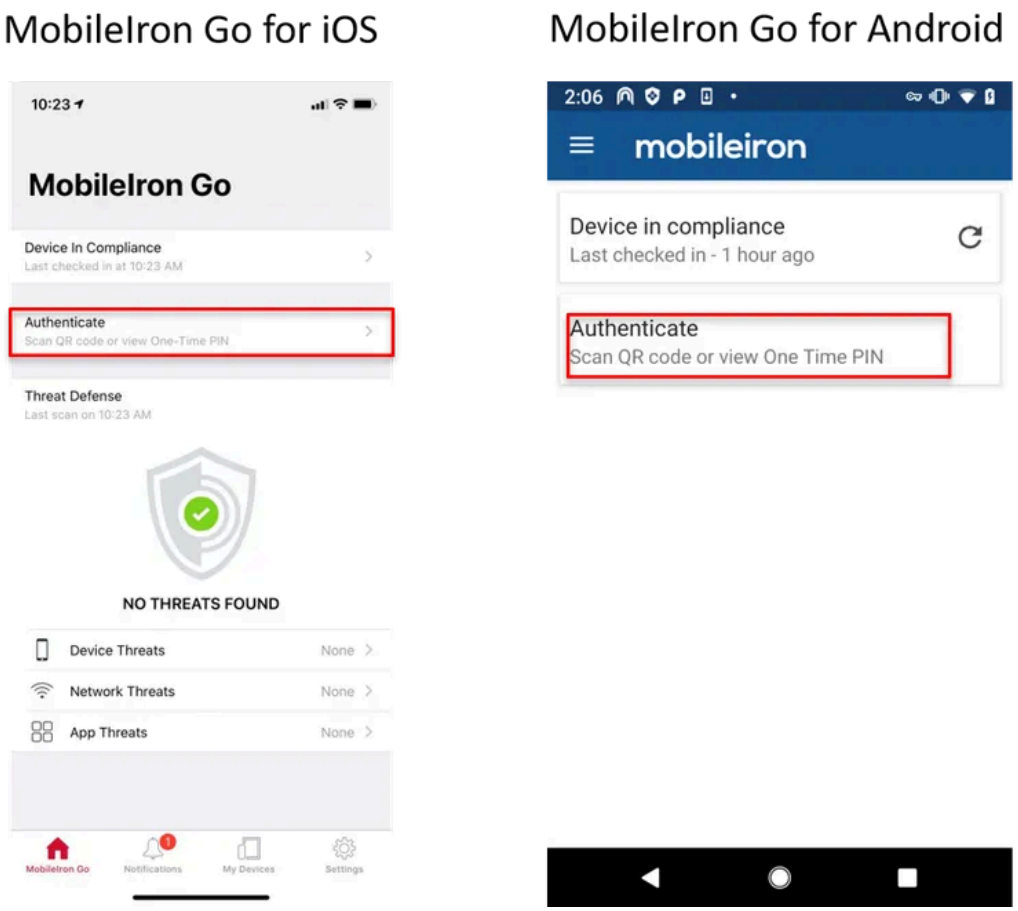
Related topics

Publishing a profile

17.4. What users see for multi-factor authentication in UEM client

If multi-factor authentication is configured, device users can authenticate and access enterprise cloud services from an unmanaged device. Users see the Authenticate option in the UEM client on their managed device.

Figure 1. Authenticate option in Go



The following topics provide information about multi-factor authentication on the UEM client:

- Ivanti Access cloud services
- Custom service provider
- Generating one-time passcode (OTP)

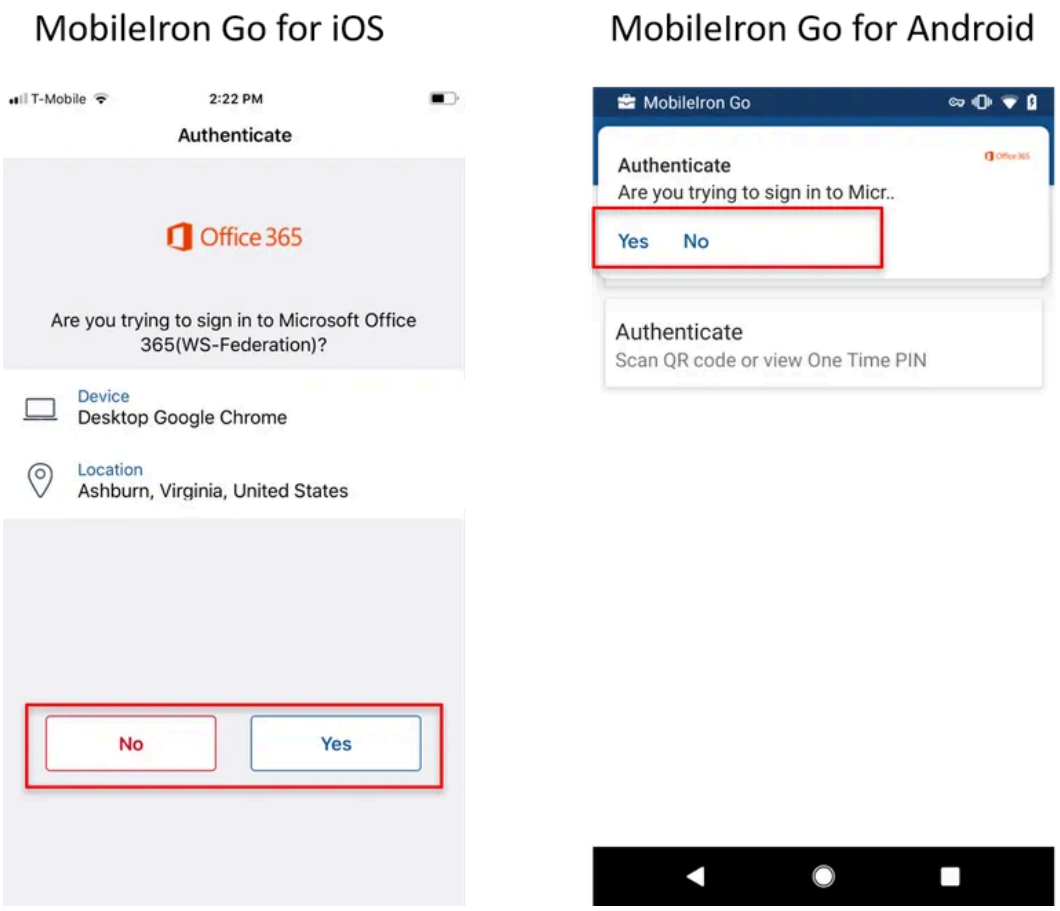
Ivanti Access cloud services

When users attempt to access an enterprise cloud service from an unmanaged device, they are prompted to enter their user name and then prompted to confirm the request on the managed device that has the UEM client.

> The configured IdP challenges users for their credentials. Access does not ask users for their credentials.

A prompt appears on the managed device alerting the user to the access request. If users accept the prompt, they are allowed access from the unmanaged device. If users decline the prompt, they see an authentication failed message on the device and the authentication request from the device is blocked.

Figure 2. prompt to allow Ivanti access from unmanaged device



Custom service provider

The interaction pages and push notification for two-factor authentication display the service provider (SP) name and logo. For a custom service provider, if a name is not configured, the interaction pages and push notifications display Custom Service Provider for the SP name. If a logo is not configured for the custom SP, the name of SP is seen where the logo would have been displayed.

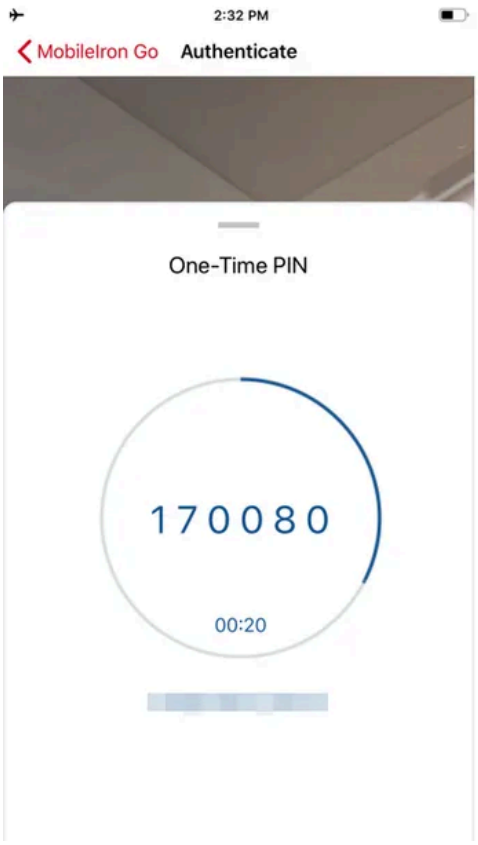
Generating one-time passcode (OTP)

Device users can generate a one-time passcode in the UEM client. Users may want to generate an OTP if the managed device does not have access to the Internet.

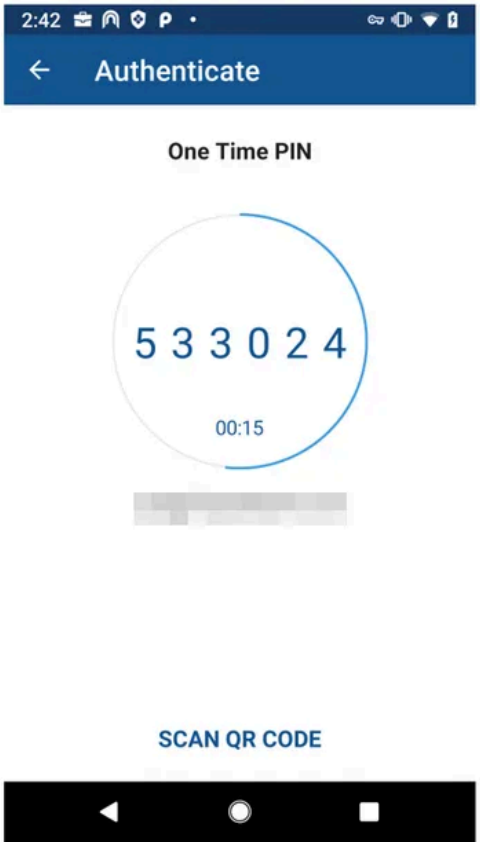
Procedure

1. Launch the UEM client.
2. Tap Authenticate > One-Time PIN.
   Figure 3. One-time pin

MobileIron Go for iOS



MobileIron Go for Android



18. Multi-factor Authentication with Authenticator

Multi-factor authentication with Authenticator allows device users to use their managed mobile device, which has the Authenticator app, for second-factor authentication. The managed device on which the Authenticator app is installed is the primary device.

The multi-factor authentication feature is not supported with Ivanti Access + Standalone Sentry deployments.

The following provide more information about multi-factor authentication:

- **About multi-factor authentication with Authenticator**
- **Configuring multi-factor authentication in Ivanti Access for Authenticator**
- **What users see for multi-factor authentication**
- **Lost Device Access Procedure**

18.1. About multi-factor authentication with Authenticator

For multi-factor authentication, there can be only one primary device. The managed device on which the Authenticator app is installed is the primary device. All approval notifications are sent to the primary device. If multiple managed devices have Authenticator installed, the latest managed device on which Authenticator is activated is considered the primary device. If enabled, users also have the option to generate one-time passcode (OTP).

- Required components for multi-factor authentication with Authenticator
- Use cases for multi-factor authentication with Authenticator
- One-time passcode (OTP) with Authenticator
- Multi-factor authentication flow
- One-time passcode workflow
- Authenticator app features

Required components for multi-factor authentication with Authenticator

Deploying multi-factor authentication with Ivanti Access requires that the following components are set up:

- Ivanti Access deployment
- Ivanti Tunnel
- Authenticator app on a managed mobile device.
  The managed device can be either an iOS, Android, or Android enterprise device.

See the *Ivanti Access Release Notes* for supported versions.

Use cases for multi-factor authentication with Authenticator

- Authenticator provides two-factor authentication to enterprise cloud services. Users accessing an enterprise cloud service confirm their identity by:
  - Providing their user credentials, typically the name and password, to the identity provider.
  - Accepting the Authenticator notification on their managed device.
- In addition, administrators can configure conditional rules to define when multi-factor authentication with the Authenticator app is triggered. Example: Create a User Info Rule to trigger multi-factor authentication for only a certain set of users or groups, a Network Rule to trigger multi-factor authentication if the user is outside the enterprise IP range.

One-time passcode (OTP) with Authenticator

Device users have the option of generating a one-time passcode (OTP) in Authenticator, which they can use instead of using push notification. OTP provides users another option to control access to enterprise cloud services from another managed device. It also provides an option to control access to enterprise cloud services even when Authenticator does not have access to the Internet.

The OTP for multi-factor authentication is displayed when the application is launched.

Multi-factor authentication flow

The following describes the authentication flow with multi-factor authentication.

Figure 1. Multi-factor authentication flow



1. User requests access to a cloud service.
2. The cloud service redirects user to the configured identity provider (IdP)to authenticate. Since Ivanti Access is the configured IdP, the request is redirected to Ivanti Access.
3. Ivanti Access redirects the request to the original IdP.
4. The original IdP challenges the user for a user name and password.
5. The user enters the user name and password and posts to the IdP.
6. The IdP verifies the user identity, generates a SAML Response containing the user identity and sends it to the configured service provider (SP) via a redirect. Since Ivanti Access is the configured SP in the IdP, Ivanti Access receives the redirect.
7. Ivanti Access obtains the user identity from the SAML response, and sends a push notification to the managed device registered to receive authentication push notifications for that user.

If one-time passcode (OTP) is enabled, users have the option to generate an OTP in Authenticator. See **One-time passcode workflow**

8. The user receives the push notification and launches the Authenticator to respond. If the user approves the transaction, the Authenticator authenticates to Ivanti Access using Ivanti Tunnel.
9. If Ivanti Access verifies the user identity received from Authenticator to be the same as the user identity received in the SAML response, Ivanti Access generates a new SAML response to redirect to the original SP
10. The original SP obtains the user identity from the SAML response and presents the personalized screen to the user.

One-time passcode workflow

The Authenticator app automatically generates and displays a one-time passcode (OTP) when device users launch the app. A progress value indicates for how long the OTP is valid.

The following describes the OTP workflow when users access a cloud service provider (SP) from a browser or an unmanaged app or device:

1. Users are redirected to an interaction page to enter their credentials. They have the option to click on the Enter one-time password link to enter the OTP obtained from Authenticator.
2. Ivanti Access validates the OTP entered by the user against the OTP generated by Ivanti Access for the activated device for that user. A match completes the second-factor authentication of the user.
3. Ivanti Access verifies and retrieves the user identity from the activated device and generates a new SAML response to redirect to the original SP.

4. The original SP obtains the user identity from the SAML response and presents the personalized screen to the user.

Authenticator app features

The Authenticator app provides the following features:

- The Authenticator app is easy to activate or deactivate on users' managed devices.
- Device users can either allow or block access to requests. They may want to deny access if an unknown user attempts to access an enterprise cloud service.
- If a request is not allowed or blocked within 5 minutes, the request expires and the authentication attempt from the device is blocked.
- Device users have the option to generate a one-time passcode (OTP) instead of using push notifications.
- If the managed device is locked, a notification is presented. Users unlock the device to view the request in Authenticator.
- Authenticator provides information about the service being accessed and device information and location.
- Administrators can add their company branding to the Authenticator app.

18.2. Configuring multi-factor authentication in Ivanti Access for Authenticator

Multi-factor authentication requires an Ivanti Access deployment, as well as additional configurations for multi-factor authentication in Ivanti Access.

Before you begin

- Ensure that you have an Ivanti Access deployment.

See **Set up Ivanti Access with UEM**.

Procedure: Overview of steps

1. Configure multi-factor authentication in Ivanti Access.
   See **Configuring user ID for multi-factor authentication**
2. Add a conditional rule in Ivanti Access for enabling multi-factor authentication, which triggers authentication using the Authenticator app.
   See **Adding a conditional rule for the Authenticator app**.
3. Configure the user identifying information to use with the Authenticator app. Authenticator extracts the user identifying information from the certificate associated with Ivanti Tunnel.
   See **Configuring multi-factor authentication in Ivanti Access for Authenticator**.
4. Configure your company branding. Users see the branding on the messages on the device from which they attempt to access cloud services and on the Authenticator app.
   See **Configuring branding for multi-factor authentication in Ivanti Access**.
5. Publish the changes.
   See **Publishing the changes**.
6. Add the Authenticator app to EMM for distribution to managed devices.
   See the following:
   - **Adding the Authenticator app to Ivanti Neurons for MDM**
   - **Adding the Authenticator app to Ivanti EPMM**.

Configuring user ID for multi-factor authentication

Enable multi-factor authentication in Ivanti Access in Profile > SaaS Sign-on. You will also map the fields from which Authenticator gets user identifying information.

Before you begin

Upload a sample Ivanti Tunnel certificate in Profile > User Certificates. For more information, see **User Certificates**.

Procedure

1. In Ivanti Access, go to Profile > Client Registration Settings.
2. For User Certificate, select the user certificate from which to get the user identification information.
   The user certificate is the Ivanti Tunnel sample certificate you uploaded to Ivanti Access.
3. For Field Name, select the field from which Authenticator gets user identifying information.

4. (Optional) For Additional transforms, enter a MiTra expression.
   Configure a MiTra expression if the value in the certificate does not map directly to the user identifying information.
   Example: select:X509:SubjectAltName:rfc822Name
5. Click Save Registration.

> One time pass code (OTP) is enabled by default.

Next steps

Add a conditional rule for the Authenticator app. See **Adding a conditional rule for the Authenticator app**.

Related topics

For information about MiTra expressions, see **Language to generate values from certificate fields**.

Adding a conditional rule for the Authenticator app

In the default policy in Ivanti Access, add a Multi-Factor Authentication conditional rule. The rule triggers multi-factor authentication using the Authenticator app.

Procedure

1. In Ivanti Access, go to Profile > Conditional Access.
2. Expand Default Policy.
3. Click +Add Rule > Multi-Factor Authentication to add the conditional rule for the Authenticator app.
4. Complete the requested fields.

Item	Description
Name	Enter a name for the multi-factor authentication rule.
Description	Enter a descriptive text for the rule.
Map the Identity Provider (IDP) user ID to Authenticator user ID	Select one of the following: • SAML Subject (Default) • SAML Attribute
Additional transforms	(Optional) Enter a MiTra expression. Configure a MiTra expression, if the value in the federation response does not map directly to the user identifying information. Example: The certificate contains the base-64 representation of the user ID, however you need the hex representation. Enter the following: decode:Base64
Rule Action	From the drop down menu, select Allow.

5. Click Done to save the policy and rule.
   The rule appears at top of the list in the policy.
6. Ensure that the Trusted App and Device rule is enabled and move the Trusted App and Device rule to the top of the list.
7. Edit the General Bypass rule, and set the Action for the rule to Block.

> You can create additional conditional rules to further define how the Authenticator app is triggered. For example, you can create an User Info Rule to trigger multi-factor authentication for only a certain set of users or groups

Next steps

Configure branding. See **Configuring branding for multi-factor authentication in Ivanti Access**.

Related topics

For information about MiTra expressions, see **Language to generate values from certificate fields**.

Configuring branding for multi-factor authentication in Ivanti Access

Customize the user experience for your enterprise users by uploading your company logo to Ivanti Access. The user notification screen as well as the Authenticator app are customized to display your company logo.

Ensure that your company logo is no more than 260 pixels wide by 30 pixels high. Supported file types are: PNG, JPG, JPEG, and SVG.

Procedure

1. In Ivanti Access, go to Profile > Branding.
2. In the Authenticator section, drag and drop your company logo or click Choose to navigate to the location of the file and add.

Next steps

Publish the updates. See **Publishing the changes**.

Publishing the changes

Publish the changes to make the updates available.

Procedure

1. In the Ivanti Access administrative portal, go to Profile > Overview.
2. Click Publish.

Publish is only available if a federated pair has been created.

3. Click OK.

Next steps

Add the Authenticator app to Ivanti Neurons for MDM for distribution to managed devices. See the following:

- **Adding the Authenticator app to Ivanti Neurons for MDM**
- **Adding the Authenticator app to Ivanti EPMM**

Related topics

Publishing a profile

18.3. Adding the Authenticator app to Ivanti EPMM

Adding the Authenticator app to Ivanti EPMM makes the app available to distribute to managed devices.

- Adding the Authenticator app for iOS to Ivanti EPMM
- Adding Authenticator for Android AppConnect to Ivanti EPMM
- Adding Authenticator for Android enterprise to Ivanti EPMM

Adding the Authenticator app for iOS to Ivanti EPMM

Device users can download Authenticator for iOS directly from the Apple App Store. You can also distribute the app as a recommended app through Apps@Work.

Procedure

1. In Ivanti EPMM, go to Apps > App Catalog.
2. From the Quick Import drop-down list, select iOS.
3. Enter Authenticator in the Application Name text box.
4. Click Search.
5. Select the app from the list that is displayed.
6. For Authenticator, click Import.
7. Click OK on the pop-up message, and close the Quick Import dialog.
   Authenticator is now listed in the App Catalog. Information included in the app, such as the name, is automatically configured. All other settings, such as the App Category and whether the app is a free app, are set to default settings.
   To view and edit the settings for the app, click on the app name in the App Catalog.
8. Apply the Ivanti Tunnel VPN configuration to the app:
   1. Click on the app name in the App Catalog to edit the app settings.
   2. In the Per App VPN Settings, apply the Ivanti Tunnel VPN setting to the app.
   3. Click Save.
9. Select the app to and apply to a label:
   1. Click Actions > Apply to Label.
   2. Select the label that represents the iOS devices for which you want the selected app to be displayed.
   3. Click Apply

Next steps

Create a managed app setting for the Authenticator app. See Creating a managed app setting for the Authenticator app for iOS.

Related topics

For more information about adding iOS apps to Ivanti EPMM for distribution, see the *Ivanti EPMM Apps@Work Guide*.

Creating a managed app setting for the Authenticator app for iOS

Create a managed app configuration for the Authenticator app to provide additional configurations for the device.

Before you begin

- Make a note of the bundle ID for Authenticator. The bundle ID is com.mobileiron.efa.distribution.mica
- Create a plist file with the following content:

<?xml version="1.0" ?>

<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDsPropertyList-1.0.dtd">

<plist version="1.0">

<dict>

<key>ACC_URL</key>

<string>https://ACC_URL_HERE</string>

</dict>

</plist>

Replace https://ACC_URL_HERE with one of the following:

- If your Ivanti Access URL is access-na1.mobileiron.com, replace with

https://access.access-na1.mobileiron.com

OR

- If your Ivanti Access URL is access-eu1.mobileiron.com, replace with

https://access.access-eu1.mobileiron.com

Procedure

1. In the Ivanti EPMM Admin Portal, go to Policies & Configs > Configurations.
2. Click Add New > iOS And macOS > Managed App Config.
3. Enter the requested information.
4. Click Save.
5. Apply to the configuration to the same label to which you applied the Authenticator app.

Related topics

For more information about creating a managed app configuration in Ivanti EPMM, see the "Managed App Config settings that use plists" section in the *Ivanti EPMM Device Management Guide* for iOS.

Adding Authenticator for Android AppConnect to Ivanti EPMM

Upload the Authenticator app to Ivanti EPMM as an in-house app and configure the app to make it available to Android devices.

Before you begin

- Ensure that Secure Apps Manager is also installed on Ivanti EPMM. For the supported Secure Apps Manager (SAM) version for Authenticator, see the *Ivanti Access Release Notes*.

- Download the Authenticator for Android AppConnect from the software download site at https://www.ivanti.com/support/product-documentation.
- This section provides basic information about how to add and configure the Authenticator app for Android AppConnect. For information about AppConnect apps, see the *Ivanti EPMM AppConnect and AppTunnel Guide*.

Procedure

1. In the Ivanti EPMM Admin Portal, go to Apps > App Catalog > Add+ > In-House. (Prior to Ivanti EPMM 8.0 go to Apps > App Distribution Library, and select Add App).
2. Add the apps just as you would any in-house app.
3. Add Secure Apps Manager (SAM) if you have not already uploaded it to support other secure apps.
4. After adding the apps, apply the apps to appropriate labels so that they are available to the required devices.

Next steps

Edit the AppConnect app configuration for Authenticator. See **Configuring an AppConnect app configuration for Email+ in Ivanti EPMM**.

Related topics

- For information on adding in-house apps for Android, see "Working with Apps for Android devices" in the *Ivanti EPMM Apps@Work Guide*.

Configuring an AppConnect app configuration for Email+ in Ivanti EPMM

When you add Authenticator for Android AppConnect, an AppConnect app configuration is automatically created for Authenticator. Edit the automatically-created AppConnect app configuration to add app specific configurations.

Make sure only one AppConnect app configuration for Authenticator is applied to each device.

Procedure

1. In the Ivanti EPMM Admin Portal, go to Policy & Configs > Configurations.
2. Select the automatically-created AppConnect app configuration for Authenticator for Android, and click Edit.
3. Select Enable Access.
4. In App-specific Configurations, add the following key-value pairs:

Key: ACC_URL

Value: https://access.YourAccessCluster.ivanti.com.

YourAccessCluster is either access-na1 or access-eu1.

Example: https://access.access-na1.ivanti.com

5. Click Save.

The automatically-created app configuration has the same labels you applied to the app. You do not need to apply the automatically-created app configuration to a label.

Adding Authenticator for Android enterprise to Ivanti EPMM

Upload the Authenticator app to Ivanti Neurons for MDM from the Google Play Store and configure the app to make it available to Android enterprise devices.

Before you begin

Ensure that your Unified Endpoint Management (UEM) platform is set up for Android enterprise. Your UEM is either Ivanti Neurons for MDM or Ivanti EPMM.

- Ivanti EPMM: See the *Ivanti EPMM Device Management Guide for Android for Work*.
- Ivanti Neurons for MDM: See the Ivanti Neurons for MDM online help documentation.

Procedure

1. In Ivanti EPMM, go to Apps >App Catalog > +Add.
2. Select Google Play from the drop-down menu next to the search box.
3. In the search box, enter Authenticator.
4. Click Authenticator to select the app.
5. Click Next and then Next .
6. Choose a distribution option for the app and click Next.
7. Update the settings in App Configurations as follows:

In Install on device, enable Install on Device.

This is the recommended setup. Install on Device silently installs the app on the devices in the selected distribution option.

In Promotion, update the promotion settings as needed.

For Managed Configurations for Android, click +.

Enter a name for the configuration.

In the Managed Configurations section:

For ACC_URL, enter https://access.YourAccessCluster.ivanti.com.

YourAccessCluster is either access-na1 or access-eu1.

Example: https://access.access-na1.ivanti.com

8. Click Done.

9. If necessary, update the Ivanti Tunnel VPN configuration for Android to tunnel authentication traffic from Authenticator to Ivanti Access.

The Ivanti Tunnel VPN configuration for Android is listed in Ivanti Neurons for MDM in Configurations.

Related topics

- See the *Ivanti EPMM Apps@Work Guide* for more information about adding Android enterprise apps to the Ivanti EPMM app catalog.

18.4. Adding the Authenticator app to Ivanti Neurons for MDM

Adding the Authenticator app to Ivanti Neurons for MDM makes the app available to distribute to managed devices.

- Adding the Authenticator app for iOS to Ivanti Neurons for MDM
- Adding Authenticator for Android AppConnect to Ivanti Neurons for MDM
- Adding Authenticator for Android enterprise to Ivanti Neurons for MDM

Adding the Authenticator app for iOS to Ivanti Neurons for MDM

Upload the Authenticator app to Ivanti Neurons for MDM from the Apple AppStore and configure the app to make it available to iOS devices.

Procedure

1. In Ivanti Neurons for MDM, go to Apps >App Catalog > +Add.
2. Select the icon for AppStore from the drop down list.
3. Enter Authenticator in the search text box.
4. Select Authenticator from the search results and click Next.
5. Make updates as necessary and click Next

You can change the category and add a description.

6. Choose a distribution option for the app and click Next.
7. Update the settings in App Configurations as follows:

In Install on device, enable Install on Device.

This is the recommended setup. Install on Device silently installs the app on the devices in the selected distribution option.

In iOS Managed App Configuration, click +Add.

For Key, enter ACC_URL.

For Value, enter https://access.YourAccessCluster.ivanti.com.

YourAccessCluster is either access-na1 or access-eu1.

Example: https://access.access-na1.ivanti.com

In Per App VPN, click + to add a per app VPN configuration.

Select Enable Per-App VPN for this app.

From the drop-down list, select the Per-App VPN configuration for Ivanti Tunnel.

	8.	Click Done.

Related topics

See the *Ivanti Neurons for MDM Guide* or Help for more information on adding apps to the Ivanti Neurons for MDM app catalog.

Adding Authenticator for Android AppConnect to Ivanti Neurons for MDM

Upload the Authenticator app to Ivanti Neurons for MDM as an in-house app and configure the app to make it available to Android devices.

Before you begin

- Ensure that Secure Apps Manager is also installed on Ivanti Neurons for MDM. For the supported Secure Apps Manager version for Authenticator, see the *Ivanti Access Release Notes*.
- Download the Authenticator for Android AppConnect from the Ivanti software download site at **https://www.ivanti.com/support/product-documentation**.

Procedure

	1.	In Ivanti Neurons for MDM, go to Apps >App Catalog > +Add > In-House

Add the app just as would any in-house app.

	2.	Choose a distribution option for the app and click Next.

	3.	Update the settings in App Configurations as follows:

In Install on device, enable Install on Device.

This is the recommended setup. Install on Device silently installs the app on the devices in the selected distribution option.

In Promotion, update the promotion settings as needed.

In App Configurations, for AppConnect Custom Configuration, click +.

Enter a name for the configuration.

In the AppConnect Custom Configuration section:

For Key, enter ACC_URL.

For Value, enter https://access.YourAccessCluster.ivanti.com.

YourAccessCluster is either access-na1 or access-eu1.

Example: https://access.access-na1.ivanti.com

	4.	Click Done.

5.	If necessary, update the Ivanti Tunnel VPN configuration for Android to tunnel authentication traffic from Authenticator to Ivanti Access.

The Ivanti Tunnel VPN configuration for Android is listed in Ivanti Neurons for MDM in Configurations.

Related topics

- See the *Ivanti Neurons for MDM Guide* or Ivanti Neurons for MDM Helpfor more information on adding Android AppConnect apps to the Ivanti Neurons for MDM app catalog.
- See the *Ivanti Tunnel for Android Guide*for information on configuring the Ivanti Tunnel VPN configuration for Android.

Adding Authenticator for Android enterprise to Ivanti Neurons for MDM

Upload the Authenticator app to Ivanti Neurons for MDM from the Google Play Store and configure the app to make it available to Android enterprise devices.

Procedure

1. In Ivanti Neurons for MDM, go to Apps >App Catalog > +Add.
2. Select Google Play from the drop-down menu next to the search box.
3. In the search box, enter Authenticator. <is this what we are calling the app in Google play?>
4. Click Authenticator to select the app.
5. Click Next and then Next .
6. Choose a distribution option for the app and click Next.
7. Update the settings in App Configurations as follows:

In Install on device, enable Install on Device.

This is the recommended setup. Install on Device silently installs the app on the devices in the selected distribution option.

In Promotion, update the promotion settings as needed.

For Managed Configurations for Android, click +.

Enter a name for the configuration.

In the Managed Configurations section:

For ACC_URL, enter https://access.YourAccessCluster.ivanti.com.

YourAccessCluster is either access-na1 or access-eu1.

Example: https://access.access-na1.ivanti.com

8. Click Done.
9. If necessary, update the Ivanti Tunnel VPN configuration for Android to tunnel authentication traffic from Authenticator to Ivanti Access.

The Ivanti Tunnel VPN configuration for Android is listed in Ivanti Neurons for MDM in Configurations.

Related topics

- See the *Ivanti Neurons for MDM Guide* or Ivanti Neurons for MDM Help for more information on adding Android enterprise apps to the Ivanti Neurons for MDM app catalog.
- See the *Ivanti Tunnel for Android Guide*for information on configuring the Ivanti Tunnel VPN configuration for Android.

18.5. What users see for multi-factor authentication

Authenticator provides secure login to your enterprise cloud services. If you have configured the app to be installed silently, which is recommended for a seamless user experience, the app is installed on managed devices when the device checks in with Ivanti Neurons for MDM.

> If a device user has already launched Authenticator for iOS as a standalone trial app, the device user must uninstall and reinstall the app to use it as a managed app.

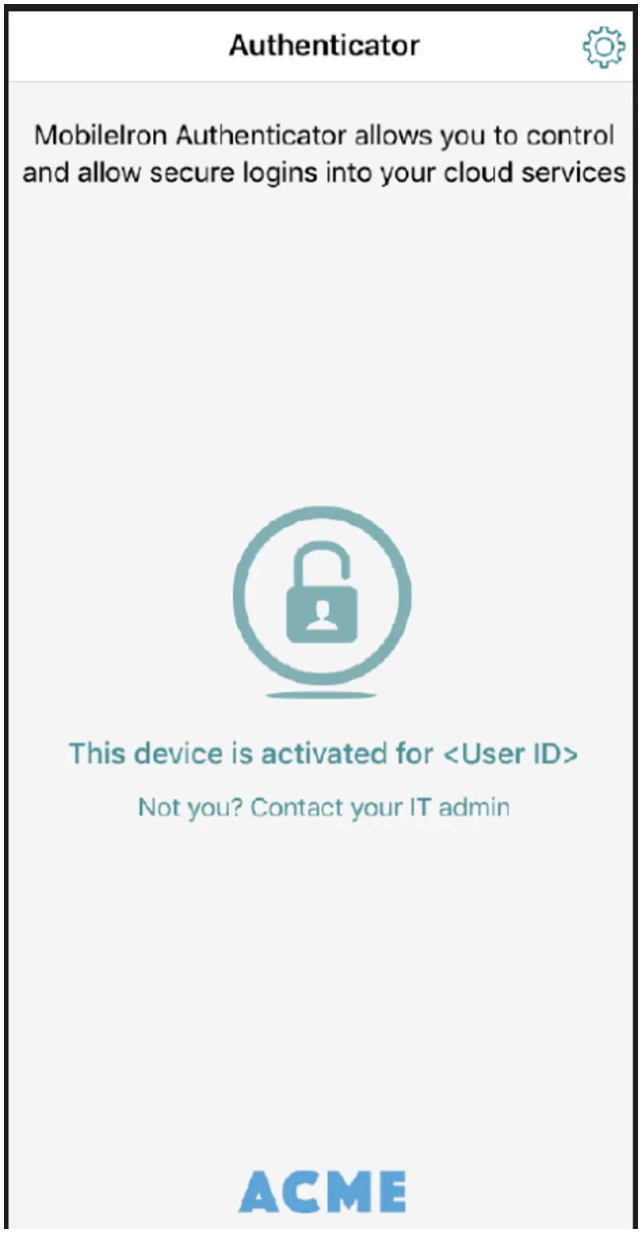
The following topics provide information about multi-factor authentication:

- **Activate Authenticator**
- **Ivanti Access cloud services**
- **Custom service provider**
- **Authenticator settings**

Activate Authenticator

To activate Authenticator, users simply launch the app after it is installed.

Figure 1. Launch Authenticator



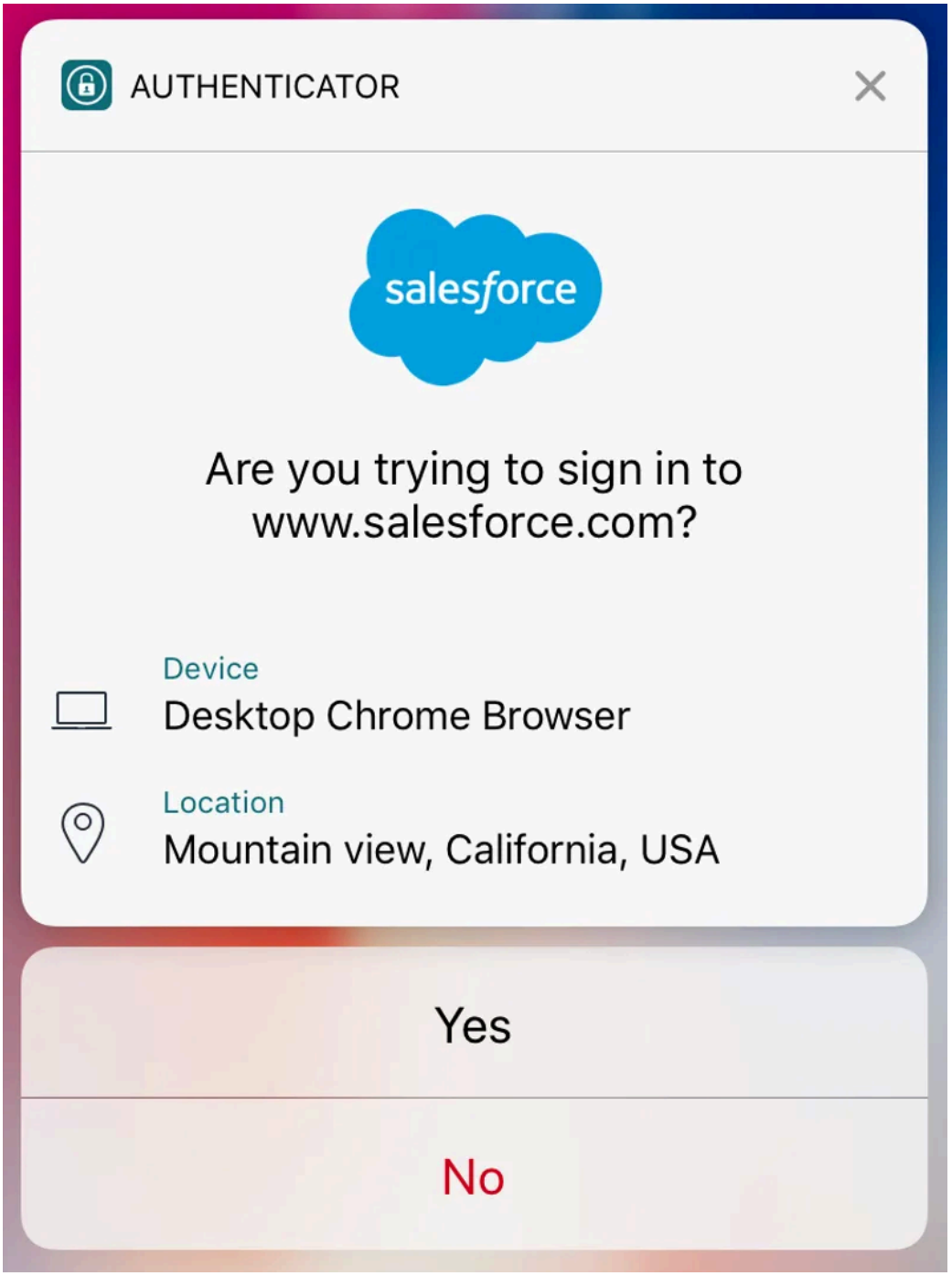
Ivanti Access cloud services

When users attempt to access an enterprise cloud service, they are prompted to enter their user name and then prompted to confirm the request on the managed device that has the activated Authenticator app.

A prompt appears from the Authenticator app on the managed device alerting the user to the access request. If users accept the prompt, they are allowed access. If users decline the Authenticator prompt, they see an authentication failed message on the device and the authentication request from the device is blocked.

> The configured IdP challenges users for their credentials. Ivanti Access does not ask users for their credentials.

Figure 2. Authenticator prompt on managed device



Custom service provider

The interaction pages and push notification for two-factor authentication display the service provider (SP) name and logo. For a custom service provider, if a name is not configured, the interaction pages and push notifications display Custom Service Provider for the SP name. If a logo is not configured for the custom SP, the name of SP is seen where the logo would have been displayed.

Authenticator settings

The following table describes the information available in Settings in the Authenticator app.

Setting	Description
About	Tap to view version and license information.
Debug Logging	Disabled by default. Device users can enable debug logging if necessary.
Email Debug Log	Tap to enter an email address to send the debug logs.
Deactivate	Tap to deactivate the Authenticator app.

18.6. Lost Device Access Procedure



Ivanti Access has an email-based One-Time Password (OTP) recovery option for users who lose access to their Two-Factor Authentication (2FA) device. This feature provides a secure and convenient way to regain account access without administrative intervention. Users can request an OTP via email to authenticate and reset their 2FA settings.

Procedure

1. Enter your username and password on the login screen.
2. Click **Sign In** to proceed.
3. On the next screen, enter the 2FA code from your authenticator app (e.g., Ivanti Authenticator, Microsoft Authenticator).
4. If you cannot access your 2FA device, click **Can't access 2FA device?**
   This triggers an OTP email to your registered email address.
5. On the next screen, enter the OTP received via email.

> The OTP expires in 5 minutes.

1. If you enter the correct OTP:
   1. 2FA is turned off for your account.
   2. You are redirected to the 2FA setup screen to reconfigure your authentication method.
2. If you enter an incorrect OTP five times, you will be blocked for 1 hour and redirected to the login screen.
3. Click **Resend OTP** if needed:
   1. You can resend OTP up to four times within 10 minutes.
   2. After the fourth request, the **Resend OTP** option is disabled for 1 hour.

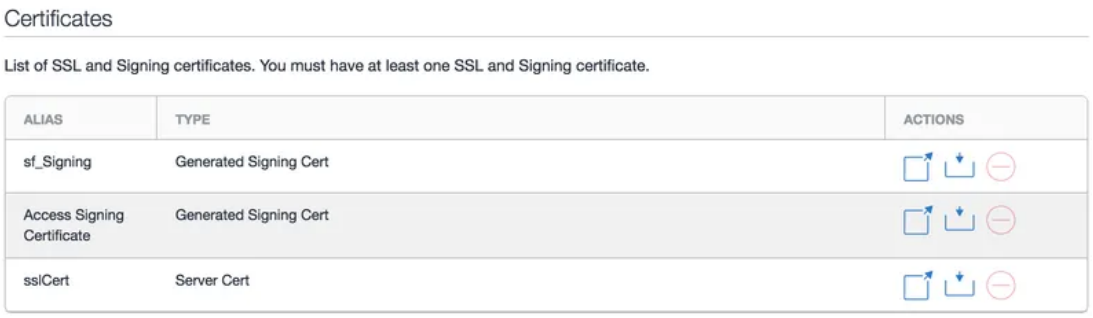
19. Access Certificates

The Certificates page lists the SSL certificates and signing certificates that have been uploaded to the Ivanti Access administrative portal.

19.1. Certificates

By default at least one SSL certificate and an Ivanti Access Signing Certificate are always available. These certificates are not editable.

Figure 1. SSL and signing certificates



Actions you can take

You can take the following actions on a certificate:

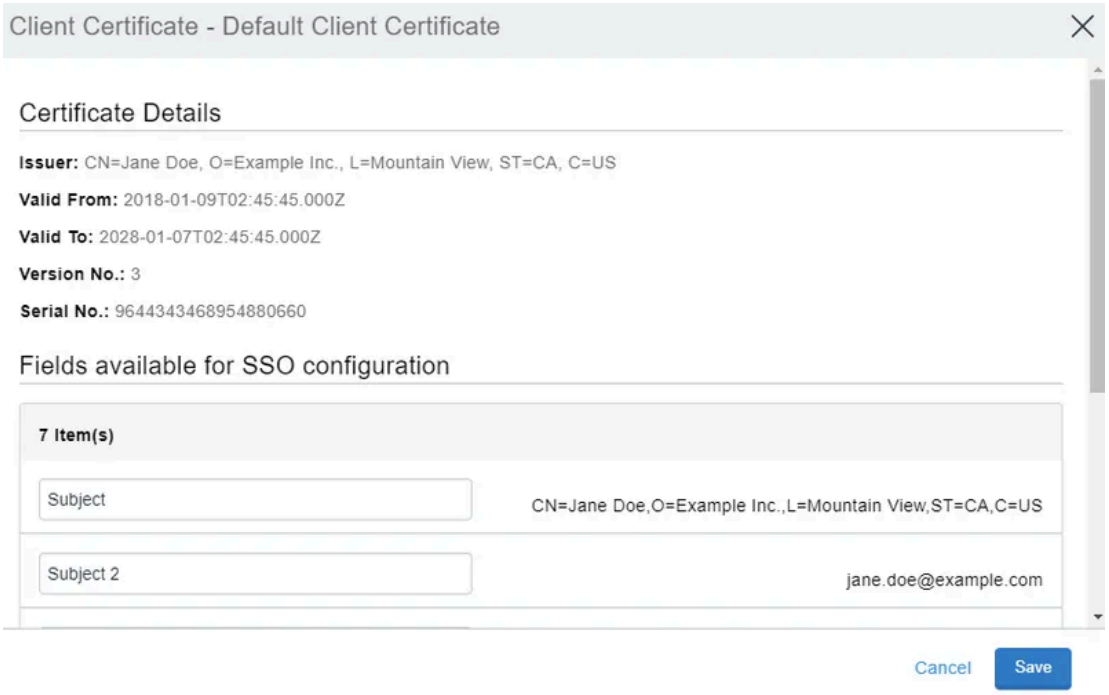
- : Click to view certificate details.
- : Click to download the certificate.
- : Click to delete the certificate.

> Only the X509 certificate is available for viewing or downloading. Private keys are not available for viewing or downloading.

19.2. User Certificates

The User Certificates page lists the client certificates that are uploaded to the Ivanti Access administrative portal. The **Default Client Certificate** is created by default. The Default Client Certificate can be used as a reference certificate and cannot be deleted.

Figure 1. default Client certificate



Adding a certificate

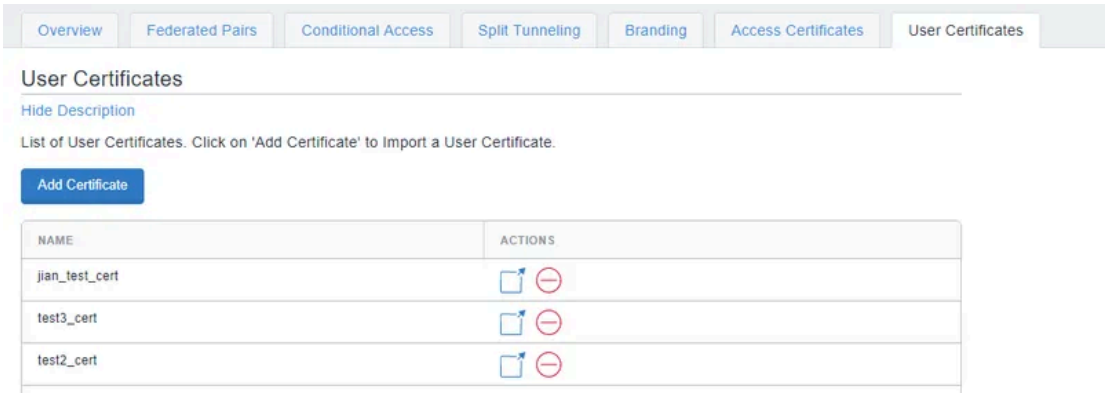
Adding your own user certificate enables you to easily map fields from the certificate into federation responses generated by Ivanti Access in Certificate based Single Sign-on. You can add a sample certificate used by your Ivanti Tunnel VPN profile that is assigned to mobile applications that use cloud services federated with Ivanti Access.

Before you begin

Verify that you have created a certificate of your choice using the default certificate as a reference.

Procedure

1. In Ivanti Access, go to Profile > **User Certificates**, click **Add Certificate** to import a User Certificate.
2. Enter a **Certificate Name**.
3. Under **Upload Certificate**, click **Choose File** and browse to select the appropriate PEM certificate.
4. Click **Add Certificate**.
   The user certificate is added.
   Figure 2. user certificate



Actions you can take

You can take the following actions on a certificate:

- : Click to view certificate details.
- : Click to delete the certificate.

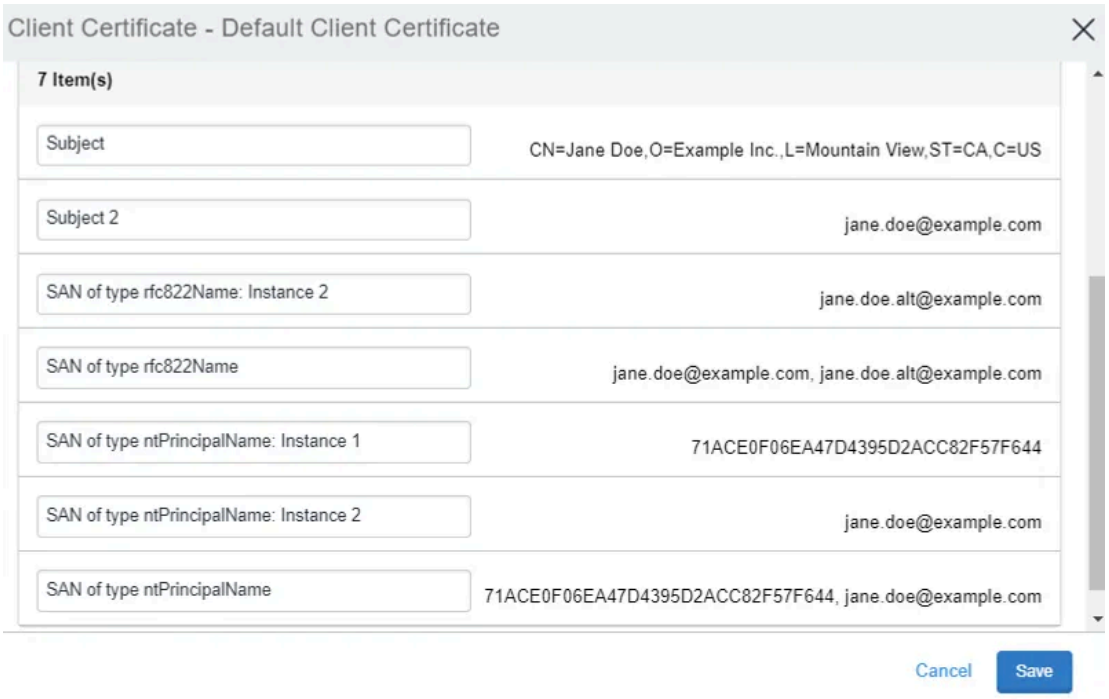
> You cannot delete a certificate that is configured in a federated pair for single sign-on. In order to remove a certificate, you must first edit and associate the certificate with another certificate (during enabling cert SSO). This disassociates the older certificate. You can then remove the older certificate.

User Certificate Details

The Client Certificate consists of **Certificate Details** and **Fields available for SSO configuration.** The Certificate Details lists the Issuer, Serial No, Validity and Version of the Certificate.

The **Fields available for SSO configuration** enable you to view and provide friendly names to fields populated in the User Certificate that you uploaded. These friendly names match the MiTra expression for a field used for SSO configuration.

Figure 3. client certificate


Client Certificate - Default Client Certificate
7 Item(s)
Subject
CN=Jane Doe,O=Example Inc.,L=Mountain View,ST=CA,C=US
Subject 2
jane.doe@example.com
SAN of type rfc822Name: Instance 2
jane.doe.alt@example.com
SAN of type rfc822Name
jane.doe@example.com, jane.doe.alt@example.com
SAN of type ntPrincipalName: Instance 1
71ACE0F06EA47D4395D2ACC82F57F644
SAN of type ntPrincipalName: Instance 2
jane.doe@example.com
SAN of type ntPrincipalName
71ACE0F06EA47D4395D2ACC82F57F644, jane.doe@example.com
Cancel
Save

19.3. Certificate expiry notifications

Ivanti Access periodically verifies the validity of the metadata for a service provider (SP) and identity provider (IdP) federated pair. A scheduled job runs every 24 hours to check the federated pairs metadata files. Any issues found during the scheduled job display as notifications in the administration portal in Profile > Federated Pair.

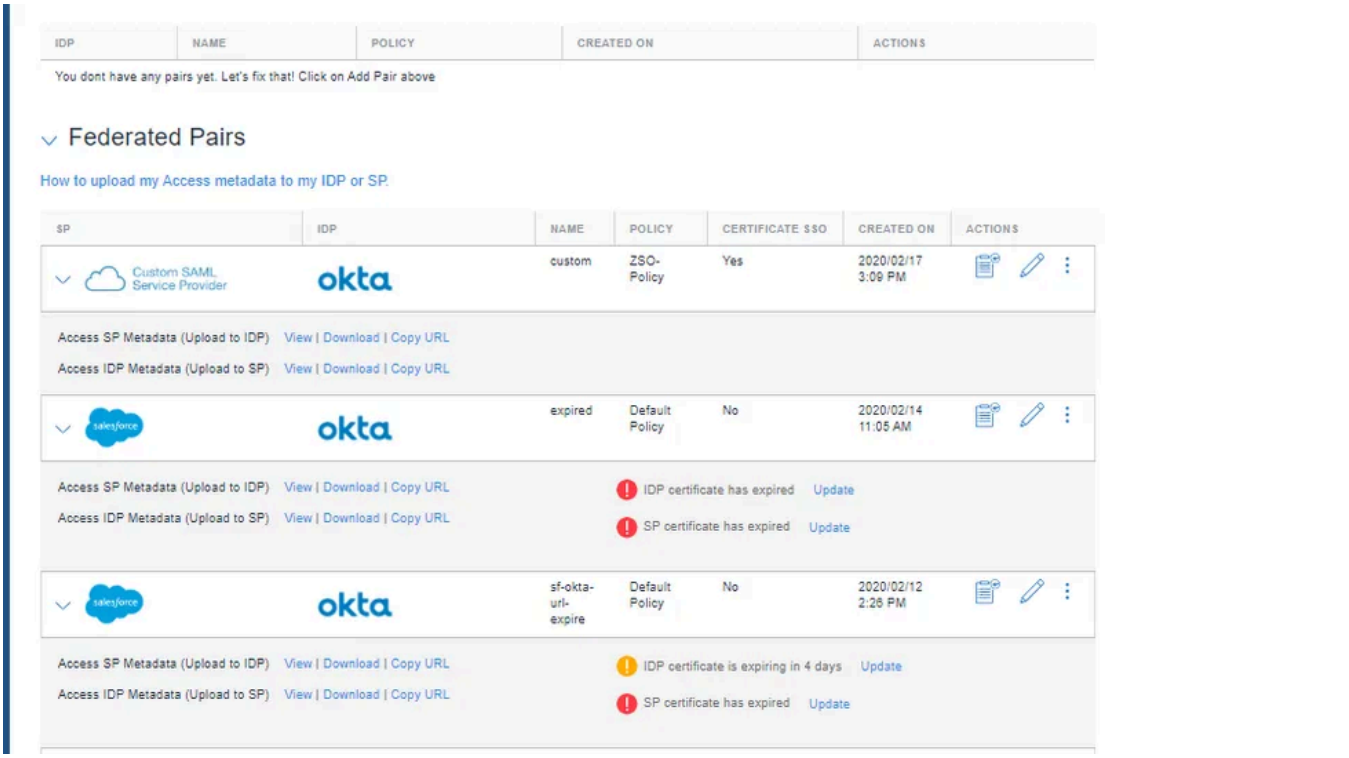
The verification includes checking the expiration date of the certificate embedded in the metadata. Ivanti Access sends email notifications to Ivanti Access administrators on the 30th, 15th, and 7th day before the expiry of the certificate. Starting on the 7th day before the certificate is set to expire, an email notification is sent every day till the expiration date. Once the certificate expires, an email is sent to confirm that the certificate has expired.

> Update the certificate before expiry to ensure that the most current certificates are available in Ivanti Access. If the certificate in Ivanti Access does not match the certificate in the SP or IdP, authentication will fail for device users accessing the federated cloud service through Ivanti Access. Authentication will continue to work as expected if the certificate in Ivanti Access and in the SP or IdP are the same, irrespective of whether the certificates are expired or not.

In addition to email notifications, the following notifications are also provided in the Ivanti Access user interface:

Notification in Profile > Federation

A notification displays in Profile > Federation. The notification includes the number of days remaining before the certificate expires. The row for the delegated IdP or federated pair with certificates that have warnings expands by default.



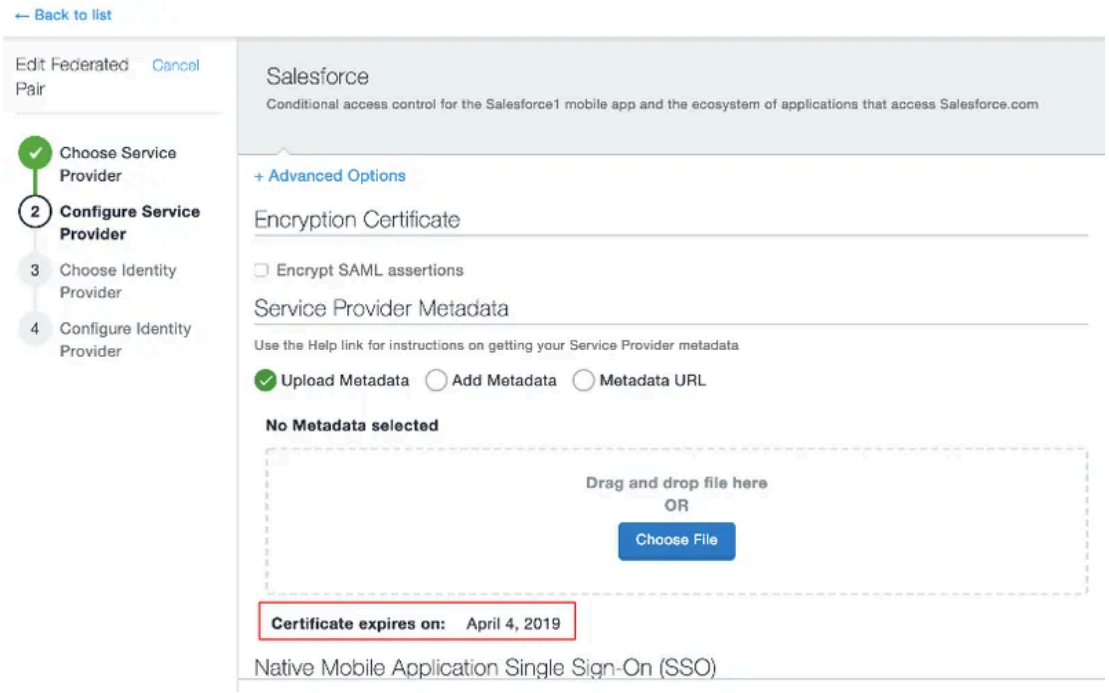
Notifications after a certificate expires

The following figure shows the notifications after the certificate expires for the delegated IdP or federated pair.



Notification when you edit a federated pair or delegated IdP

A notification displays when you edit the federated pair or delegated IdP. The notification includes the number of days remaining before the certificate expires. The following figures show notifications 30 days and one day prior to certificate expiration.



19.4. Updating certificates for an SP or IdP

Occasionally, you may need to update the service provider (SP) or identity provider (IdP) certificates for the federated pairs configured in Ivanti Access. You must update the certificates if the service provider or identity provider certificate is about to expire or has expired. Ivanti Access then provides notifications if the certificate expiration date is upcoming. The administrator can then update the certificate by providing the updated metadata. For information about certificate expiration notifications, see **Certificate expiry notifications**.

> Ivanti recommends to update certificates for uninterrupted services.

Certificate information is available in the service provider or identity provider metadata you upload to Ivanti Access. Depending on whether you uploaded metadata, added metadata, or entered a metadata URL when configuring the federated pair, do one of the following to update the certificate:

- **Certificate update if you uploaded metadata**
- **Certificate update if you entered a metadata URL**
- **Certificate update if you entered a metadata URL**

> Ivanti Access only consumes the information in the metadata. If the metadata references an expired certificate or soon-to-expire certificate, Ivanti Access continues to show the certificate expiration notifications.

Certificate update if you uploaded metadata

Do the following if you uploaded metadata from the service provider (SP) or identity provider (IdP) when configuring the federated pair.

Procedure

1. Get the metadata from the affected SP or IdP.
   See Ivanti Access Cookbooks for more details.
2. Go to Profile > Federation.

3. Click Update beside the warning message to update the certificate for the SP or IdP. The Update IDP metadata screen displays.



   1. (Optional) Click Edit to provide an URL or to add metadata instead of Upload Metadata. OR
   2. Click Choose File to upload the metadata data for the SP or the IdP as appropriate.
   3. Click Upload Metadata.
   4. Click Done.

Related topics

- For information about getting metadata from the SP or IdP, see "Before you begin" in **Configuring federated pairs**.
- For information about editing a federated pair, see **Editing a federated pair**.

- For information about downloading the Ivanti Access proxy metadata and uploading the proxy metadata to the SP or IdP, see Uploading proxy metadata.

Certificate update if you added metadata

Do the following if you added a metadata when configuring the federated pair.

Procedure

1. Go to Profile > Federation.
2. Click Update beside the warning message to update the certificate for the SP or IdP. The Update IDP metadata screen displays.

   1. Update the certificate.
      If a valid certificate is updated, a confirmation message displays that the update is successful.



   2. (Optional) Click Edit to change metadata to provide URL or Upload Metadata instead of Add Metadata.

Certificate update if you entered a metadata URL

Do the following if you entered a metadata URL when configuring the federated pair.

Procedure

1. Go to Profile > Federation.

2. Perform one of the following actions based on the changes:
   1. **Update link for Metadata expired or expiring** : The Update IDP metadata window opens sync option is available. Click Sync metadata to complete the update. However, the modified attributes are not listed.
   2. **Update link for change in metadata**: The Update IDP metadata window opens and the modified attributes are listed along with a sync button. Click Sync metadata to complete the update.



   3. **Update SP or IDP metadata via menu option** : This is a one-click sync operation link. Clicking on the menu option syncs the metadata automatically and the quick update window displays the attributes that are modified.

3. (Optional) Click Edit to Upload or Add Metadata instead of Metadata URL.
4. Click Sync metadata > Close.
   A sync completed successfully confirmation message displays.

For Office 365 and Microsoft ADFS, when the Office 365 domain is federated with Ivanti Access and Ivanti Access is federated with ADFS, ADFS metadata is uploaded in Ivanti Access or it can provided using metadata URL.

ADFS has certificate rollover functionality where it provides both primary and secondary signing certificates in the metadata. When the primary is about to expire, ADFS switches to secondary certificate. Ivanti Access also uses the certificate which has later expiry date and monitors that certificate. This does not break the authentication.

However whenever the certificate is updated on ADFS side, it must either be uploaded in Ivanti Access by providing new ADFS metadata or can also be synced using "Sync IdP Metadata" if ADFS metadata is provided using url.
For more information, see **https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-fed-o365-certs**.

Related topics

- **View federated pairs**
- **Service provider (SP) metadata**
- **Identity provider (IdP) metadata**

20. Reports

You can generate reports in the Ivanti Access administrative portal that provide information about authentication, errors, and certain audit actions.

The following topics provide more information about reports:

20.1. About reports

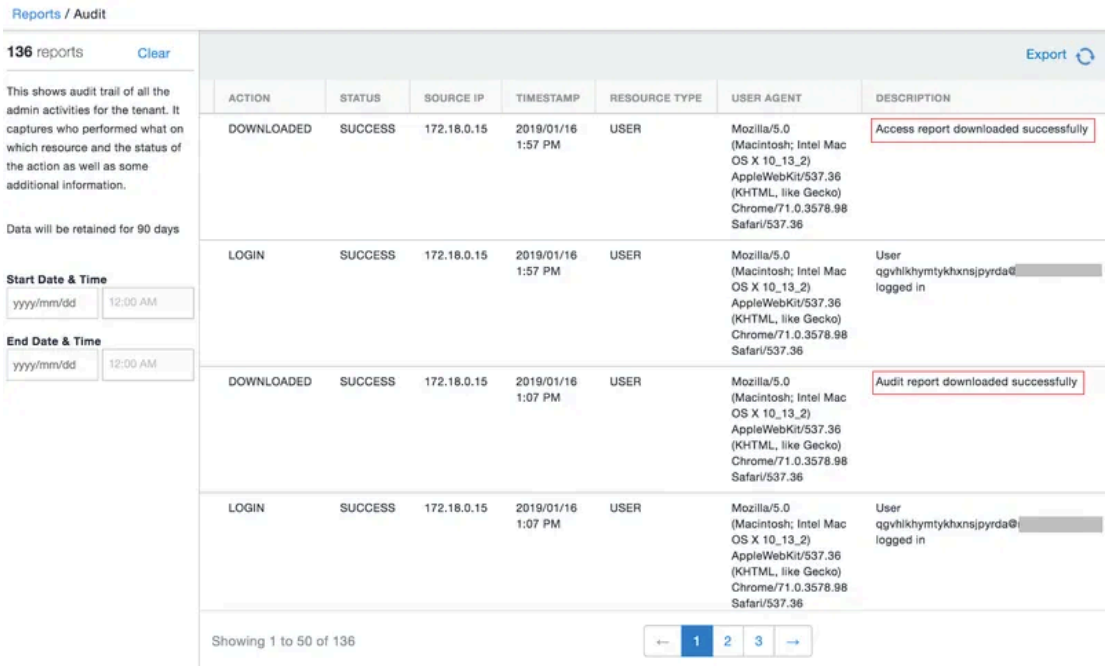
The following types of reports are available in the Ivanti Access administrative portal:

- Ivanti Access Reports: Authentication traffic that goes through Ivanti Access is captured and displayed in Reports > Access.
- Session Revocation: Session revocation report provides status information whether the user and service provider (SP) revocation action was successful or not and the context for the revocation. The report is displayed in Reports > Session Revocation. For more information, see **Session Revocation**.
- Error Reports: Whenever a device connection to gateway fails, an error report is generated and displayed in Reports > Errors.
- Audit Log: Actions taken by the Ivanti Access local administrator in the Ivanti Access administrative portal are displayed in Reports > Audit.
- Authenticator: The Authenticator report provides debugging and activity tracking logs for the multi-factor authentication activity from the Authenticator app in Reports > SaaS Sign-on.

Reports data is retained for 90 days.

You can download a report by clicking on Export. The report is downloaded as a CSV file. The export action is captured in the Audit log. If the download fails, a failure message is also captured in the Audit log.

Figure 1. ivanti Access reports



20.2. Ivanti Access reports

Authentication traffic that goes through Ivanti Access is captured and displayed in Access Reports. Each IdP or SP proxy request to Ivanti Access is logged and displayed as a separate row. For a single authentication instance, there may be up to two log entries.

Each row provides visibility into users, devices, and apps accessing cloud services.

You can do the following with the report data displayed in Access Reports:

- Filter the reported instances to view a subset.
- View details for the reported instances.
- Export the reported instances that are displayed.
- Search for reports in the search bar with advanced and flexible query search to filter desired report data.
- Ivanti Access Report now displays the Client IP or the Device IP in the Access Reports.

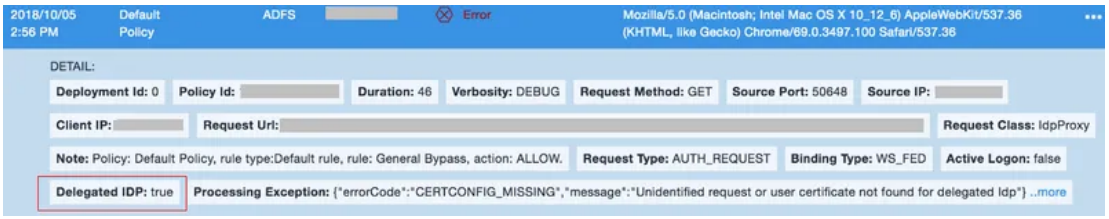
Figure 1. Ivanti Access report



Delegated IdP field in Ivanti Access reports

Ivanti Access displays the persisting Delegated IDP field in Ivanti Access reports that help users identify the log entries for delegated IdP.

Figure 2. Delegated IdP field in Ivanti Access report



authnRequestID field in Ivanti Access reports

The authrequestID field for SP proxy and IdP proxy in Ivanti Access Reports allows administrators to correlate entries for the IdP proxy and SP proxy that are part of the same pair. The authrequestID for SpProxy and IDpProxy is now visible in Ivanti Access Reports which lets you relate between the two entries. Export the report to a .csv file to do the correlation.

> The authnrequestId is not searchable through flexible search.

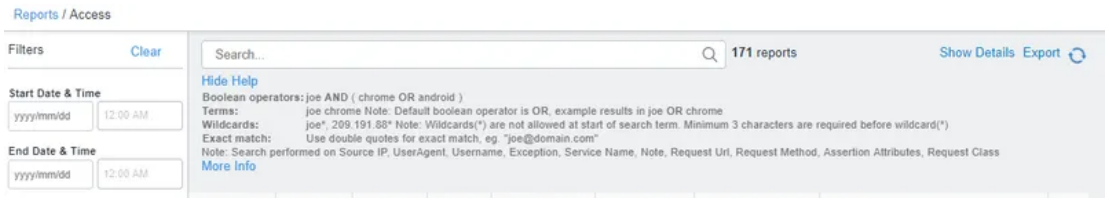
Figure 3. authnrequestid in Ivanti access report



Search Ivanti Access reports

Ivanti Access reports includes a search option that allows you to do advanced and flexible queries to filter the desired data and customize the report in Reports > Access.

Figure 4. reports search bar



The screen displays the advanced query that you can use to search the report. A maximum or 1024 characters is supported in a query.

The following query words are searched in the Search bar:

- Source IP
- UserAgent
- Username
- Exception
- Service Name
- Request Class
- Assertion Attributes
- Request Method
- Note
- Request Url

Flexible Query

The following flexible query types are supported. If more than one word (except boolean operators) is specified, the select condition is composed by operators.

- An exception is thrown for any word (except boolean operators) with wildcard (*,?) having length less than three characters. For example: ab*, a?b, etc results in an exception, while abc*, abc? will not result in exception.
- Searching is not case sensitive.

Type	Supported Values
Operators	AND | OR | NOT
Unsupported characters	All characters except the invisible control characters and unused code points are supported.
Wildcards	* and ?

Query Examples

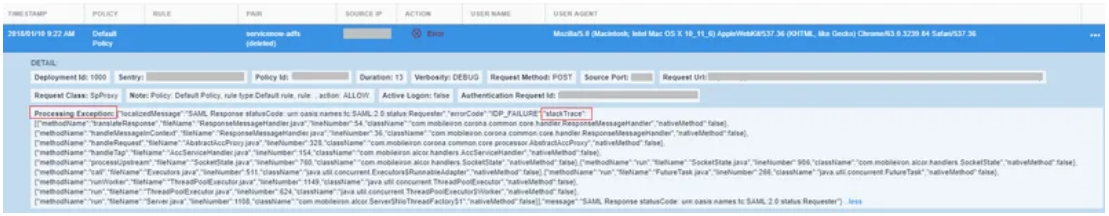
The following table provides examples of search queries.

Type	Example
AND Operator	To search for records having IP Address as 10.11.12.13 and Chrome as the User agent: • 10.11.12.13 AND chrome
OR Operator	To search for records having IP Address as 10.11.12.13 or chrome: • 10.11.12.13 OR chrome
Difference between AND and OR. A *AND* B means both A and B must be present in the record. A *OR* B means either A or B should be present in the record.	
NOT Operator	NOT operator is used to exclude certain terms from the result. For example, the below query returns all records that do not contain chrome and 10.11.12.13 • NOT chrome AND NOT 10.11.12.13
Wildcard	If the details are partially unknown, use wildcards to fetch the results: • 10.11.1* AND chro*
Using Quotes (")	1. Double quotes are used around search words to get the exact match. 2. If two words are separated by a space, then by default OR operator is used. 3. To search for space separated words as an exact string, apply double quotes around the whole string. For example: To fetch the results with chrome version, use the below query: • "Chrome/60.0.3112.113" This query returns the records that have chrome version, 60.0.3112.113 For example, a search query, *Intel Mac os x* is interpreted as *Intel OR Mac OR os OR x*. For example: "Intel Mac os x" This query returns the records with complete string *Intel Mac os x.*
Grouping	Multiple Operators along with parenthesis can be used for searching. For example, (chrome AND (10.11.12.13 OR 10.11.12.14)) This query returns all the records with chrome and IP Address as either 10.11.12.13 or 10.11.12.14. It is recommended to include parenthesis in the query as it provides grouping. For example, the above example without parenthesis might be interpreted differently by the system and desired results might not be obtained.
Best Practice: If the search word contains a special character, Ivanti recommends to use double quotes around the searched word. For example: While searching for username *joe@domain.com*, it is recommended to use quotes around the username for better results - "joe@domain.com".	

Display exceptions in reports

When there is an Ivanti Access Report with error, by expanding Report Details an exception message is displayed. When you click **More**, stack trace is also displayed. Also, the default message has the error code and message.

Figure 5. exceptions in reports



Filtering report data

To filter report data, do one or a combination of the following in the left panel:

- Enter a Start Date & Time and End Date & Time.
- Select the data type to view a subset of the reported data.

> The report data is always sorted by timestamp in descending order. By default, the filter for time is set from 12 AM to 12 AM.

Data available for filtering

The following fields are available to filter the report data. When you run a report, the active federated pairs, policies, and rules are listed on top of the list. The deleted items are structured at the bottom of the list.

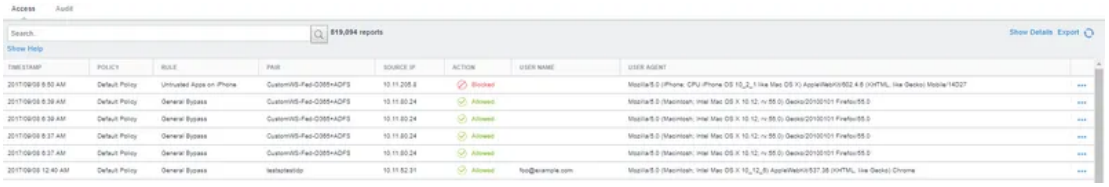
Item	Description
Start Date & Time	Enter a start date and time to filter the data.
End Date & Time	Enter an end date and time to filter the data.
Federated Pair	Select the federated pair for which you want to see data.
Action	Select one of the following: • Allow • Block • Error • Warn
Policy	Select the conditional access policy for which you want to see data.
Rule	Select the conditional access rule for which you want to see data. Only the rules in the selected policy are available for selection. If a policy is not selected, rules will not be available for selection.

Viewing details

To view additional details for a report entry, click on one of the following options:

- Show Detail: Click on Show Detail to see the details for all rows.
- Click on the three dots (...) adjacent to each row to view details for that log entry.

Figure 6. report details



Exporting report data

The Export feature allows you to download Ivanti Access report data as a CSV file. You can then import the .csv file to a reporting tool and generate custom views and reports.

When you export report data, only the rows in the Reports > Access view will be downloaded. You cannot customize the fields for exporting.

Procedure

1. In the Ivanti Access administrative portal, go to Reports > Access.
2. Click on Export. The Export Reports window appears that displays the size of the report file.

Figure 7. Export reports



3. Click Export if the size is appropriate.

A CSV file containing the report data is downloaded.

- When a report is exported, there is an appropriate entry in the Audit reports.
- Use the left navigation filter to select appropriate records such as files that are larger in size. Only the filtered records are then exported in the file and can help in reducing file sizes.

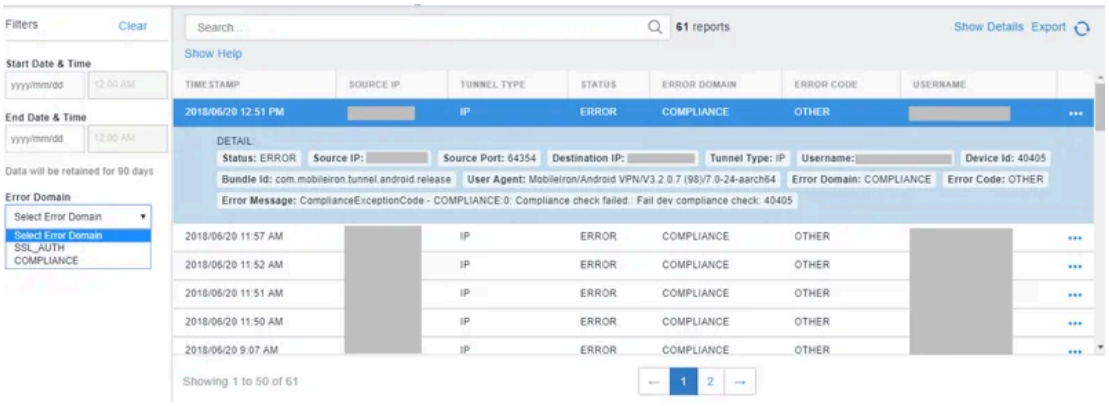
20.3. Errors Report

Whenever a device connection to Ivanti Access fails, an error report is generated and displayed in Ivanti Access. Each row provides visibility into Source IP, Ivanti Tunnel Type, Error Domain, and Error Code.

To view the Errors report in Ivanti Access, click Reports > Errors. Reports are generated for the following error domains :

- SSL_AUTH: Errors related to authentication. For example, an invalid certificate.
- COMPLIANCE: Errors related to device reported in a non compliant state.
- CONFIGURATION: Error in reading or processing tenant configuration update from Ivanti Access, or issues with local configuration of UEM.
- CONNECTION: Errors while attempting to connect to Ivanti Access.

Figure 1. Error Report



You can filter the Error report data displayed in Ivanti Access Reports based on the following error domain:

- SSL_AUTH
- COMPLIANCE

For more information on search field, see *Search* in **Ivanti Access reports**.

Export error report

Export the error report to a .csv file for correlation.

Procedure

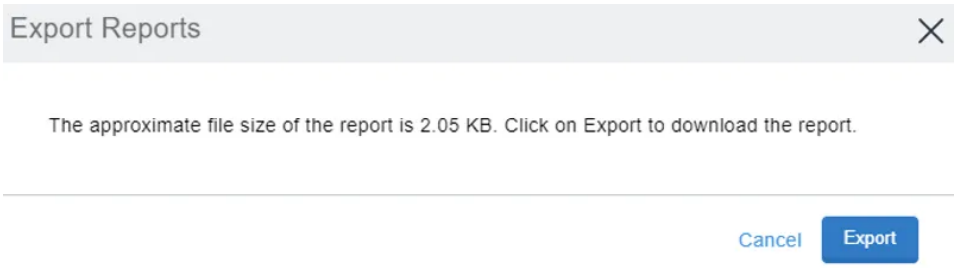
1. In Ivanti Access, navigate to Reports > Errors.

The Error report displays.

2. Click Export at the right hand top corner.

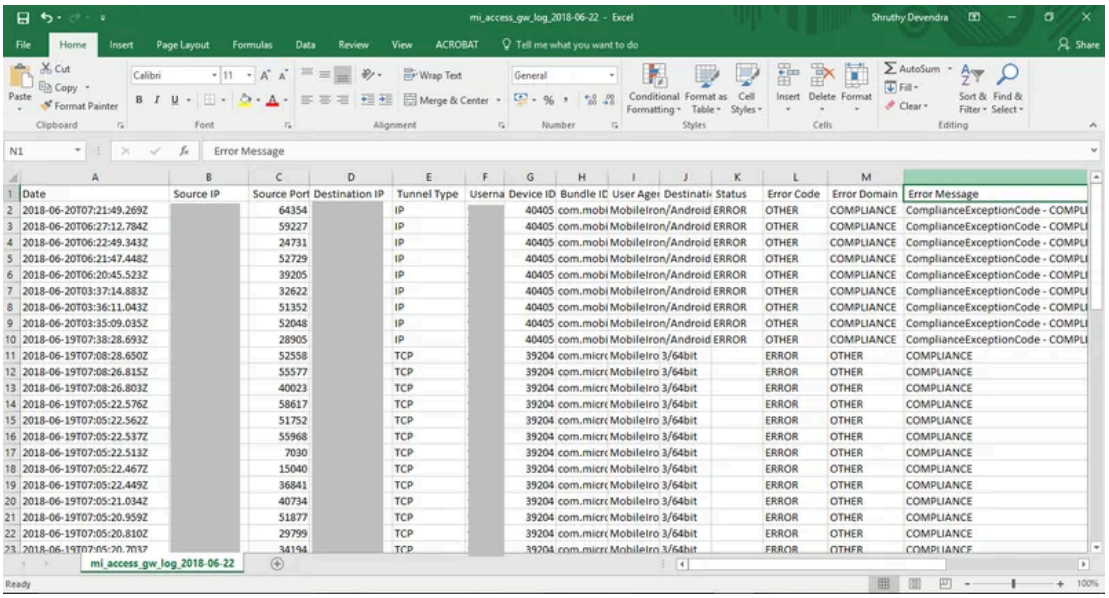
The Export Reports window appears.

Figure 2. Export Reports



	3.	Click Export to confirm.

The report is exported to your local drive.

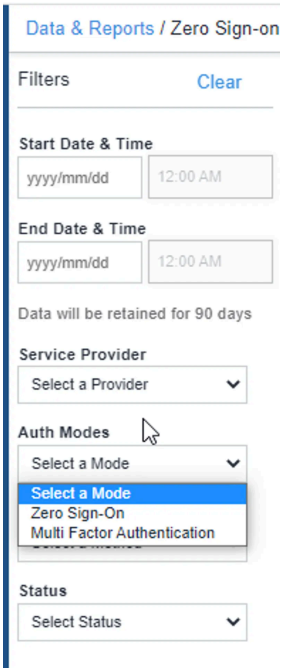


20.4. Zero Sign-on Reports

The Zero sign-on reports provide information about the service provider such as Time Stamp, User ID, Auth Mode, Auth Method and Status.

Auth Modes

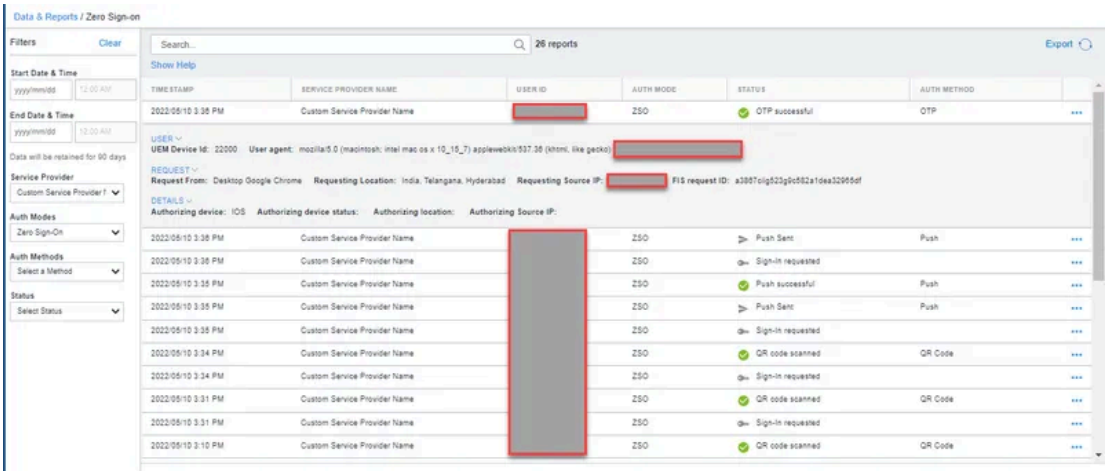
You can select an authentication mode to get information about the service provider. They include Zero Sign-on and Multi Factor Authentication.



Auth methods

The Auth methods filter lets you select the athentication method such as Push, Zero Sign-on Authenticate, QR Code, OTP, IDP Login, Security Key, Windows Hello and Mac Touch ID.

The report is now updated to provide information



20.5. Audit Log

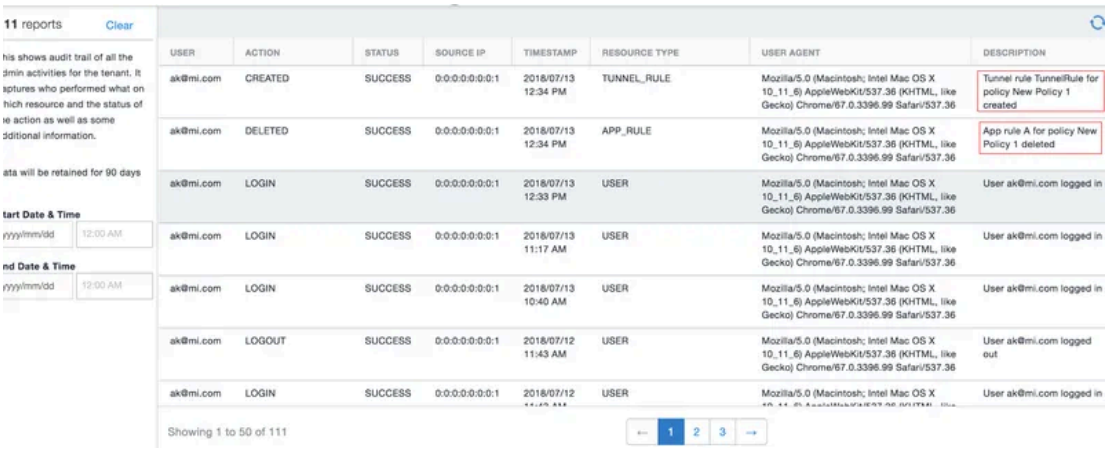
Actions taken by the Ivanti Access local administrator are captured in logs and displayed in Reports > Audit.

The Audit log displays audit trail information such as Actions, Status, SourceIP, Timestamp and so on.

The Description field now provides the following information about

- The policy update that displays the federated pair it belongs to.
- The rule update that displays the policy it belongs to.

Figure 1. audit log



You can do the following with the audit report data:

- Filter the reported instances to view a subset.

Filtering audit report data

To filter audit report data, do the following the following in the left panel:

- Enter a Start Date and End Date.

Audit report data available for filtering

The following fields are available to filter the report data:

Item	Description
Start Date	Enter a start date to filter the data.
End Date	Enter an end date to filter the data.

Actions

Local administrator actions logged and reported in Reports > Audit include:

Action	Description
Login	Local administrator signs in to the Ivanti Access administrative portal (User).
Logout	Local administrator sings out of the Ivanti Access administrative portal (User).
Password Changed	The local administrator password is changed (User).
Password Reset	Password recovery key is reset.
Created	The following are created or added: • Profile. • Certificate. • Service provider (SP) and identity provider (IdP) pair (SAML_Pair). • Policy. A policy is automatically created when you click Continue in the App and Device Identity Trust screen in the Getting Started Wizard. • Conditional rule for a IP address range (Source_IP_Rule). • Conditional rule for an app or device platform (User_Agent_Rule).
Updated	The following are edited and saved: • Profile is edited and saved. • Service provider (SP) and identity provider (IdP) pair. • Profile details are updated. (Policy). • Conditional rule for a IP address range (Source_IP_Rule). • Conditional rule for an app or device platform (User_Agent_Rule). • Remediation page.
Deleted	The following are deleted: • Service provider (SP) and identity provider (IdP) pair. • Conditional rule for a IP address range (Source_IP_Rule). • Conditional rule for an app or device platform (User_Agent_Rule). • Standalone Sentry is deleted (CRT).
Rules_Reordered	Conditional rules are reordered (Policy).
Registered	A Standalone Sentry is registered to Ivanti Access (CRT).
Assigned	Standalone Sentry is assigned to the profile (CRT).
Unassigned	Standalone Sentry is unassigned from the profile (CRT).
Recovery Key Generated	A Recovery Key is generated for the Ivanti Access administrator account.
EmailId	An Email ID is associated with Ivanti Access.

Status provided for an action include:

- Success: The action was successful.
- Failure: The action was unsuccessful.

The description column provides a description of the action taken.

- Successful example: Saml pair SP-Box-IDP-PingIdentity created
- Failed example: Saml pair SP-Box-IDP-PingIdentity updated (failed)

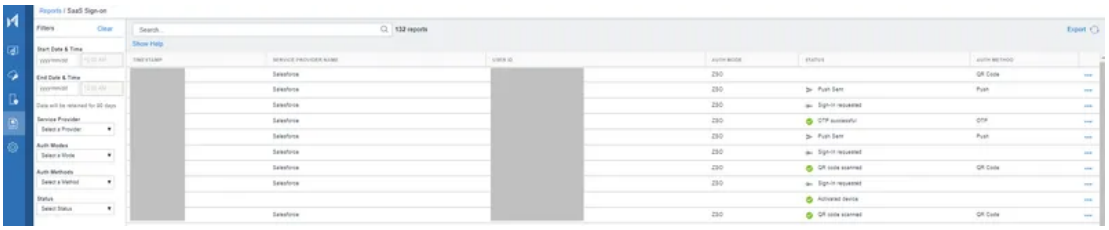
20.6. SaaS Sign-on

The SaaS Sign-on report provides debugging and activity tracking logs for the multi-factor authentication and single sign-on activity. The Export feature allows you to download SaaS sign-on report data as a CSV file. The SaaS sign-on reports have a retention period of 90 days.

Select the Service Provider, Auth Modes (Zero Sign-on or Multi Factor Authentication), Auth Methods (OTP, Push, QR Code, IDP Login), and the Status appropriately to fetch the desired report. The Auth Method that you select displays the appropriate Status for that method. Select the Status that is applicable to the method from the list.

> For UserID, enter a partial or complete UserID in the query search bar.

Figure 1. SaaS sign-on report



The following table provides the multi-factor authentication actions logged and reported in Reports > SaaS Sign-on.

Status	Description
Device Status	
Activated device	User activates the client app. The client app is either Go or Authenticator.
Deactivated device	User deactivates the client app. The client app is either Go or Authenticator.
No activated device	User tries to log in through the client app but has not activated the client app on a device.
Non Compliant Device	The users device does not meet the compliance policy.
Authentication Status	
Error	Push notification could not be sent.
IDP Login Attempted	User logs in using identity provider instead of SaaS Sign-on.
OTP incorrect	User uses an incorrect one-time passcode (OTP).
OTP successful	User uses one-time passcode (OTP) to approve the transaction and is successful.
Push rejected	Firebase or APNS returned an error, therefore a push notification was not sent.
Push successful	Push is successfully sent to the Firebase or APNS service.
QR code scanned	Allows the user to view only logs for authentication to the service provider done using QR code.
Sign-In requested	A sign-in request is received by notification or QR scan.
Saas Sign-on Configuration	
Invalid transforms	Configuration for SaaS sign-on in Ivanti Access in Profile > SaaS Sign-on is incorrect. An incorrect configuration results in an exception during evaluation of the MiTra against the Ivanti Tunnel certificate.

21. Settings

Use the **Settings** tab to perform the following tasks:

- Create administrators from the Admins tab. See **Admins**.
- Create Test IDPs from the Test IDP tab. See **Working with Test IDP**
- Create Test SPs from the Test SP tab. See **Working with Test SP**.
- Enable or disable account-level features, such as delegated IdP, from the Tenant Settings tab.

See **Delegated IdP**.

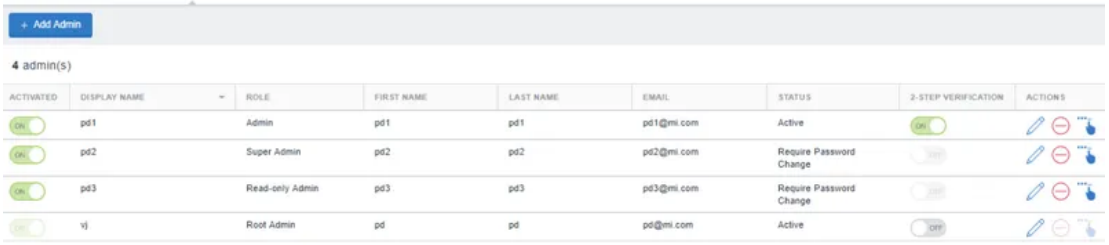
21.1. Admins

The **Admins**tab lets you create, delete, reset password, and manage 2-Step Verification for administrators to manage the Access portal. It also lets you activate and deactivate (enable or disable) the administrators.

> The Reset Password and 2-Step verification is not available with Ivanti Access and Ivanti Neurons for MDM portal.

Admins added in the Ivanti Access tab will not have any Cloud role. They will only see the Ivanti Access tab. Admins added in the Ivanti Neurons for MDM tab may have Ivanti Access roles as well as Cloud roles depending on what they are assigned.

Figure 1. admins tab



An administrator can perform tasks such as reset password, create Federated Pairs, create rules with conditional policies, and so on based on his role. These tasks are grouped as Configuration, Self Service, User Management, and viewing Analytics and Dashboard only tasks.

Dashboard and Reports	Configuration	User Management
Viewing Dashboard and Reports only.	• Create a new profile • Create, Edit, and Delete federated pairs • Create, Edit, and Delete conditional access policies • Configure split tunneling • Manage branding • Manage certificates	• Create admin • Delete admin • Reset admin (not Applicable for Access Ivanti Neurons for MDM portal) • Enable and Disable administrators • Change administrator role • Disable 2-Step Verification (not Applicable for Access Ivanti Neurons for MDM portal)

The administrator task details are provided in the following table:

Role	Tasks based on Roles
Root Admin	A Root Admin is created by the tenant provisioning process. A Root Admin has all the permissions and can perform all the tasks as mentioned in the above table. The Root Admin cannot be disabled or deleted.
Super Admin	A Super Admin can perform Read-only, Configuration, and User Management tasks. A Super Admin can delete all other admins, except Root Admin.
Admin	An Admin can perform Read-only and Configuration tasks. An Admin cannot delete any other admins.
Read-only Admin	A Read-only Admin can perform Read-only tasks only. A read-only Admin cannot delete any other admins.

Adding an administrator

A Root Admin and a Super Admin can add multiple role-based administrators.

> When adding an Admin, do not use ivanti.com as the domain.

Before you begin

- Verify that you have understood the various Admin Roles available in Ivanti Access. See **Admins**.
- Verify that you have the correct password to authorize the Admin creation.

Procedure

1. Navigate to Settings > Admins and click **+ Add Admin**.

The **Add New Admin** window opens.

2. In the **Admin details** panel, enter the following information in appropriate fields:
   - First name
   - Last name
   - Email
   - Display name
3. In the **Admin Roles** panel, select one of the following roles for the administrator:
   - Super Admin
   - Admin
   - Read-only Admin

	4.	Click **Save**.

The new **Admin** is created.

Deleting an administrator

You can delete an admin based on your role.

- A Root Admin cannot be deleted.
- A Root Admin can delete other administrators.
- A Super Admin can delete all other administrators, except administrators with Root Admin role.
- The Admin and Read-only Admin cannot delete any administrators.
- The Admin role cannot delete their own account.

Before you begin

- Verify that you have understood the various Admin Roles available in Access. See **Admins**.
- Verify that you have the correct password to authorize the Admin deletion.

Procedure

	1.	Navigate to Settings > Admins. All the available administrators are displayed.
	2.	Click ⊖ in the **Actions** column of the admin you wish to delete.
	3.	The admin is deleted successfully.

> You must always provide your login password to manage the administrators created.

Resetting password for an Access administrator

> Resetting the password for an Ivanti Access administrator is not applicable for Ivanti Access and Ivanti Neurons for MDM portal.

Administrators can reset the password of another administrator based on their role. The Audit log captures who reset the password. Self-reset password is not allowed as 'Change Password' is the specified option. Password reset is not allowed on a deactivated account.

The permission matrix for the roles to reset the password is as below:

Performs Action	Root Admin	Super Admin	Admin	Read-only Admin
Root Admin	x	yes	yes	yes
Super Admin	yes	yes	yes	yes
Admin	x	x	x	x
Read-only Admin	x	x	x	x

Before you begin

- Verify that you have understood the various Admin Roles available in Ivanti Access. See **Admins**.
- Verify that you have the correct password to authorize the password reset.

Procedure

1. Navigate to Settings > Admins.
   All the available administrators are displayed.
2. Click in the **Actions** column for the administrator you wish to reset the password.
   The password is reset and the affected administrator is emailed with the details to reset the password.

21.2. Working with Test IDP

The Test IDP tab lets you test IdP's in your environment before using the identity provider in your production deployment. It is provided only for testing purposes. You must use only commercial IdPs such as Microsoft ADFS, Okta, OneLogin, or PingIdentity. You can add up to 5 test IdP users in your environment.

Before you begin

- Verify that you have downloaded the metadata file available on Settings > Test IDP > Applications > Download Test IDP Metadata file.
- Create a federated pair with your service provider metadata file and the Test IDP metadata file that you downloaded. For example, Salesforce metadata and Test IDP metadata.

Procedure

1. Navigate to Settings > Test IDP and click Add Test IDP User. The Add Test IDP User window opens.
2. Enter the First name, Last name, Username, Email and New Password for the IDP user.
3. Click **Done**. The IdP user is created.
4. On the Applications tab, click Add Application and enter the **App Name**.
5. Select **Add Metadata** or **Upload Metadata** to upload the Ivanti Access SP Metadata file that you downloaded when creating a Federated Pair OR or select **Metadata URL** and enter the URL for metadata details.

For example, the Salesforce metadata file used to create the test federated pair.

6. Click Done.
7. The Test IDP Reports tab displays the report after being authenticated by test IdP, success or failure.

Use this report to assess the IdP use in your deployment.

21.3. Working with Test SP

The Test SP tab lets you test SP's in your environment before using the service provider in your production deployment. You can add up to 5 test SP users in your environment.

Before you begin

- Verify that you have the metadata (Entity ID) details for the test SP.

Procedure

1. Navigate to Settings > Test SP Users and click + Add Test SP User. The **Add Test SP User** window opens.
2. Enter the First name, Last name, Username, and Email for the SP user.
3. Click **Done**. The SP user is created.
4. On the Linked IDP tab, click + Add IDP Details and enter the **IDP Name**. Choose from one of the following options to login to the service provider:

- **Login to SP**: Click this link to log in to the service provider.
- **Copy Login URL**: Click this link to copy the SP login URL to use on a different browser.

5. Select **Upload Metadata** and upload the metadata file that you downloaded OR select **Add Metadata** and enter the details in the following table OR select **Metadata URL** and enter the URL for metadata details.

> When you upload the IDP metadata file, the details are populated by default.

Field	Values
IDP Name	Test IDP name.
Entity ID	Entity ID from the metadata file.
NameId Format	Supported values: • EMAIL • PERSISTENT • TRANSIENT • ENTITY
Auth Request Signed	Yes or No
Assertion Signed	Yes or No
Response Signed	Yes or No
Default IDP	Yes or No If the default IDP value is set to True,
Binding Type	• REDIRECT • POST
Redirect Location	Enter the data from the metadata file.
Post Location	Enter the data from the metadata file.
Signature Algorithm	RSA_SHA1 RSA_SHA256

6. Click **Done**. The IDP details are added.

7. Click **Login to SP** to verify redirection.

Login to SP redirects to Test IDP and after providing credentials and successful authentication, it redirects to Test SP.

22. Troubleshooting

The following topics help you troubleshoot:

- Password is not prompted by Email+ application when using Ivanti Access for Office 365
- Salesforce from Web@Work does not display authentication page
- Salesforce produces incorrect metadata with invalid Entity ID

22.1. Password is not prompted by Email+ application when using Ivanti Access for Office 365

Problem: Password does not prompt for Email+ configuration before using Ivanti Access for Office 365.

Cause: The prompt for email password option is not set to true in the Email+ configuration.

Solution:

- For Ivanti Neurons for MDM, in App Configuration setup, set the *Prompt for Password Before Connecting to Server* to true in Email+ configuration.
- For Ivanti EPMM, in AppConnect App Configuration, add *prompt_email_password* property and set the value to true.

22.2. Salesforce from Web@Work does not display authentication page

Problem: If your setup uses Ivanti EPMM, and you are using Okta as the IdP to access Salesforce, accessing Salesforce from Web@Work does not display the authentication page.

Solution: In the Standalone Sentry System Manager, in **Settings** > **Services** > **Sentry** > **Outgoing SSL Configuration**: check **Enable SNI** and remove **SSLv2Hello** from Selected protocols.

22.3. Salesforce produces incorrect metadata with invalid Entity ID

Problem: Sometimes Salesforce produces metadata incorrectly with the EntityID *https://saml.salesforce.com* instead of *https://customdomain.my.salesforce.com*.

Solution: Ivanti Access displays a warning message as follows:

You might have uploaded incorrect metadata. The EntityID in the uploaded metadata is saml.salesforce.com. However, it must be customdomain.my.salesforce.com.

When you upload the Ivanti Access metadata to Salesforce, download the Salesforce metadata again for the Ivanti Access IDP and upload it again. Alternatively, edit the Salesforce metadata file and provide the correct Entity ID. Upload the modified metadata file again to Ivanti Access.

23. Appendix

23.1. Configuring Ivanti Neurons for MDM for SSO certificates

Simple Certificate Enrollment Protocol (SCEP) must be configured in Ivanti Neurons for MDM to generate certificates from CAs configured within Ivanti Neurons for MDM. To create the fields in user or device certificates, you must define SCEP. In order to define SCEP, it must obtain information from LDAP source.

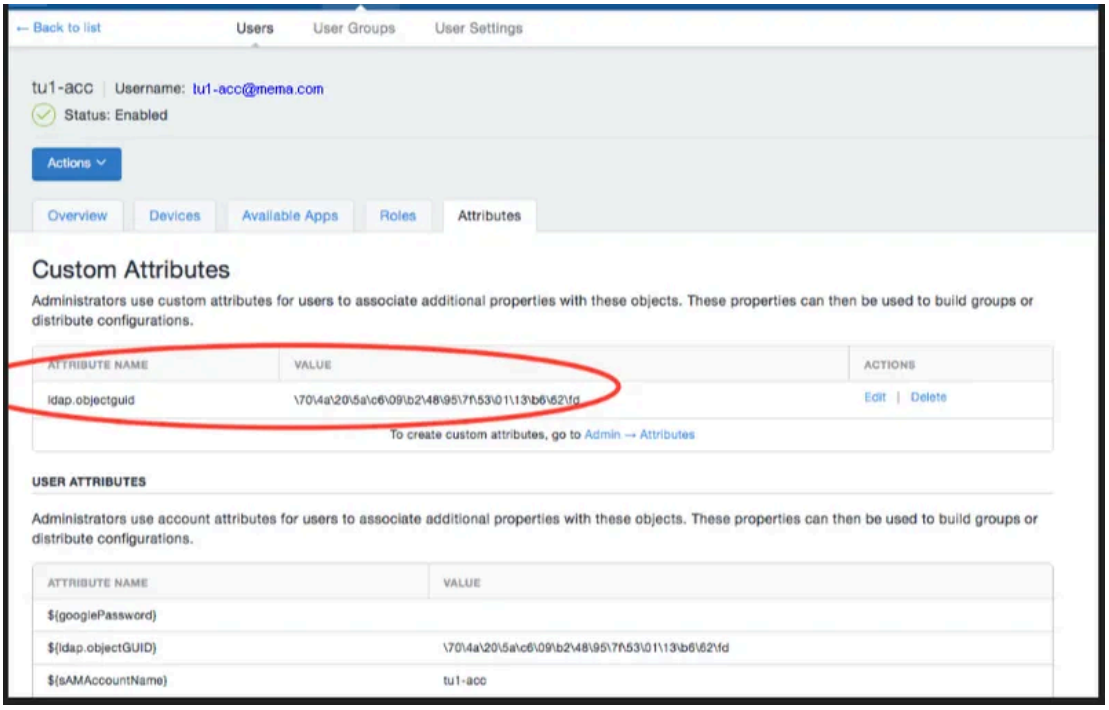
LDAP source configuration

For the SCEP to request user certificates from CA, it must obtain the user information from the LDAP source. For example, Active Directory as an LDAP Source. You must configure two important attributes:

- User's email address obtained from Active Directory. *userPrincipalName* is the LDAP attribute populated in the email field.
- User's unique ID in the Active Directory. *ObjectGUID* is obtained and set as the attribute Custom 1.

After updating LDAP, you must sync LDAP. On the User's tab, value of the custom attribute objectGUID is as below:

Figure 1. ldap source configuration



SCEP configuration

The SCEP configuration must be updated in two locations in Ivanti Neurons for MDM:

- Admin > Certificate Authority
- Configurations > Add > Identity Certificate

After the LDAP configuration, to obtain the fields for certificates, define the SCEP. Add two sub-fields in the Subject Alternative Name field of the certificate.

- The sub-field of type *RFC 822 Name* holds the email address. As shown in the LDAP configuration, this corresponds to the $EMAIL$ directory attribute.
- The sub-field of type *NT Principal Name* (required only for Office 365) holds the unique immutable Id. This configuration corresponds to the *objectGUID* custom attribute.

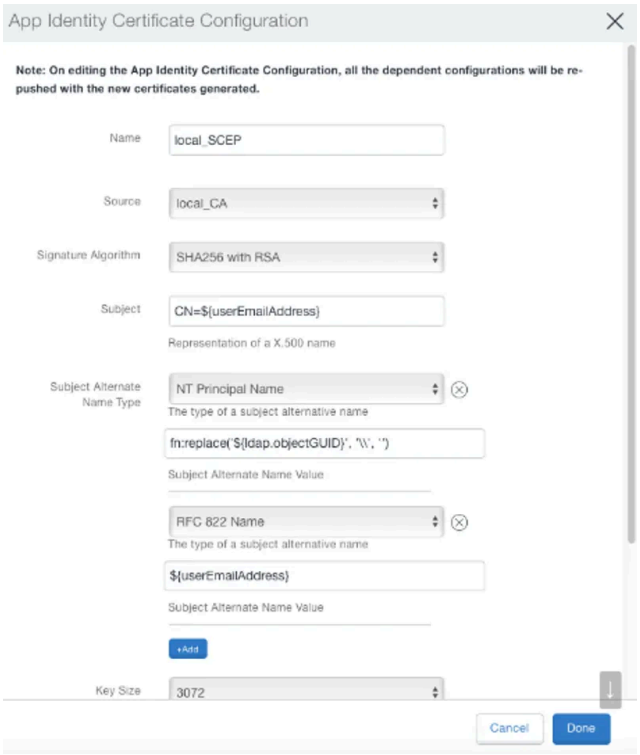
You must enter "fn:replace('$', '\\', '')" manually in this field value.

If you are using a local user instead of LDAP, then you can hardcore the value of RFC 822 name to EmailID of the user.
For Office 365, you can get the immutable ID by following the steps below:

1. Open the Azure Portal at https://portal.azure.com.
2. Search for "Users".
3. Select the user from the list.
4. Open the Properties tab for the user and get On-Premises Immutable ID field.

> Convert Immutable Id value from Base64 to Hex and then add it in the SCEP profile. Both the *Subject Alt Names* must be present in the SCEP profile for SSO to work.

Figure 2. identity certificate configuration



23.2. Configuring Ivanti EPMM for SSO certificates

Simple Certificate Enrollment Protocol (SCEP) must be configured in Ivanti EPMM to generate certificates from CAs configured in Ivanti EPMM. To create the fields in user or device certificates, you must define SCEP.

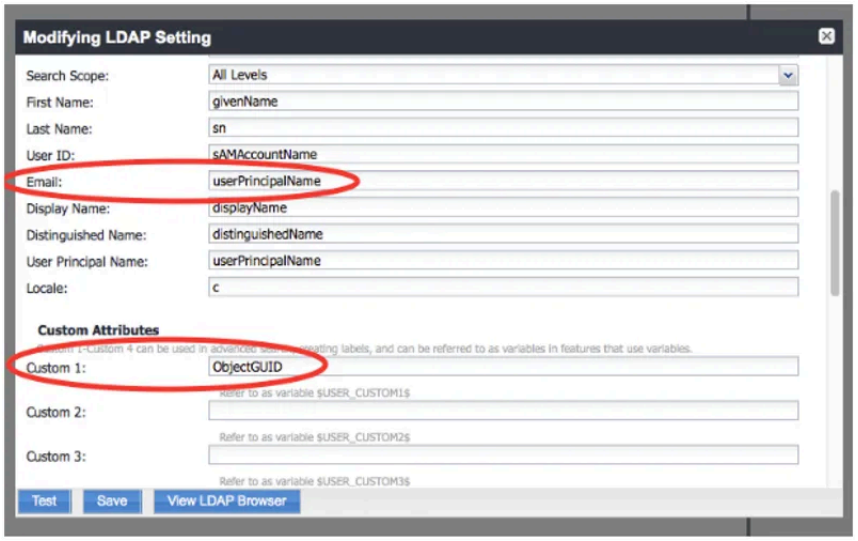
- LDAP source configuration
- SCEP configuration

LDAP source configuration

For the SCEP to request user certificates from CA, it must obtain the user information from the LDAP source. For example, Active Directory as an LDAP Source. You must configure two important attributes:

- User's email address obtained from Active Directory. *userPrincipalName* is the LDAP attribute populated in the email field.
- User's unique ID in the Active Directory. *ObjectGUID* is obtained and set as the attribute Custom 1.

Figure 1. LDAP source configuration



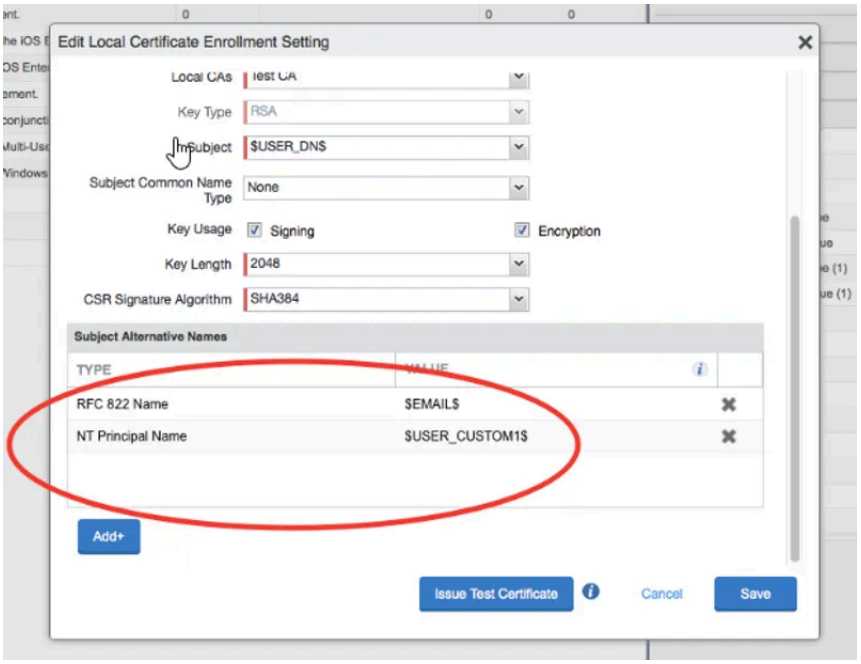
SCEP configuration

After the LDAP configuration to obtain the fields for certificates, you must define the SCEP. Add two sub-fields in the Subject Alternative Name field of the certificate.

- The sub-field of type *RFC 822 Name* holds the email address. As shown in the LDAP configuration, this corresponds to the $EMAIL$ directory attribute.
- The sub-field of type *NT Principal Name* (required only for Office 365) holds the unique immutable Id. As shown in the LDAP configuration, this corresponds to the *User Custom 1* attribute.

UI displays a drop-down list of values for this attribute that does not contain the *User Custom 1* option. You must enter *$USER_CUSTOM1$* manually in this field value.

Figure 2. scep configuration


Edit Local Certificate Enrollment Setting
Local CAs
Test CA
Key Type
RSA
Subject
$USER_DN$
Subject Common Name Type
None
Key Usage
Signing
Encryption
Key Length
2048
CSR Signature Algorithm
SHA384
Subject Alternative Names
TYPE
VALUE
RFC 822 Name
$EMAIL$
NT Principal Name
$USER_CUSTOM1$
Add+
Issue Test Certificate
Cancel
Save

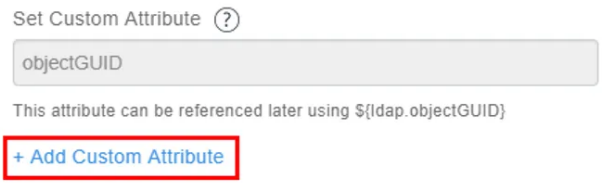
23.3. Configuring LDAP in Ivanti Neurons for MDM for session revocation

Configure one or all of the following custom attributes in the LDAP configuration in Ivanti EPMM:

- userPrincipalName
- objectGUID

Procedure

1. In the Ivanti Neurons for MDM, go to Admin > LDAP.
2. Select an LDAP server and click the Edit icon.
3. Click Test Connection and Continue.
4. In the Configure LDAP Server page, scroll down to Set Custom Attribute.
   Figure 1. Edit LDAP server



1. Click + Add Custom Attribute.
2. Enter one or both of the following custom attributes:
   - userPrincipalName
   - objectGUID
3. Click Done.

Related topics

- For information about configuring LDAP in Ivanti Neurons for MDM, see "Admin > LDAP" in the *Ivanti Neurons for MDM Guide* or click Help in the Ivanti Neurons for MDM portal.
- **Configuring Session Revocation**

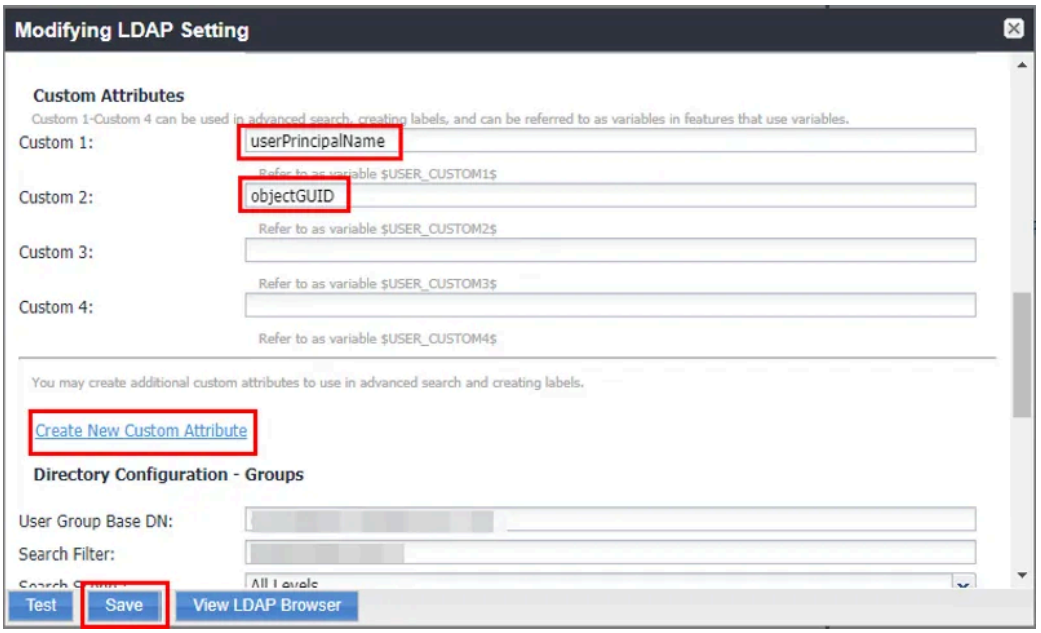
23.4. Configuring LDAP in Ivanti EPMM for session revocation

Configure one or all of the following custom attributes in the LDAP configuration in Ivanti EPMM:

- userPrincipalName
- objectGUID

Procedure

1. In the Ivanti EPMM Admin Portal, go to Services > LDAP.
2. Select an LDAP server and click the Edit icon.
   Figure 1. Edit LDAP server



1. In the Modifying LDAP Setting page, scroll down to Custom Attributes.
2. Enter one or both of the following custom attributes:
   - userPrincipalName
   - objectGUID

Use an available custom field or click Create New Custom Attribute to add a new custom field.

5. Click Save.

Related topics

- For information about configuring LDAP in Ivanti EPMM, see "Configuring LDAP servers" in theGetting Started with Ivanti EPMM Guide.
- **Configuring Session Revocation**

23.5. Customizing certificates for single sign-on in Ivanti Access

Certificate single sign-on lets you login to cloud services from managed apps on their devices without passwords. You can customize the certificates for single sign-on by selecting SAML Assertions with your SP. The SP requires additional information other than the email address in SAML Assertion's Subject field.

If you are authenticating an original Identity Provider, the SAML message that Ivanti Access obtains from the original IdP is relayed to the SP with minimal modifications. However, when the user is being authenticated using the Cert SSO, Ivanti Access must construct the SAML message, and put the appropriate user identifying values from the certificate into the SAML assertion in that message. To provide flexibility in choosing and transforming values from the certificate and putting them in the SAML, Ivanti Access provides a flexible customization capability. Currently, this capability is offered only when you choose the Custom SP.

- Configuring SAML assertion fields
- Language to generate values from certificate fields

Configuring SAML assertion fields

The Ivanti Access UI enabled you to choose the Certificate SAN rfc822Name and NTPrincipalName type values and add them into the SAML Subject or in SAML attributes. However, this might not be sufficient for all issues. For advanced configuration, select Custom and enter the values.

For more information, see Configuring Mobile App Single Sign-on (SSO).

Language to generate values from certificate fields

The values for either the subject or the attributes can be defined using *Ivanti Transform* expressions or *MiTra expressions*. The MiTra expressions are a comma-separated list of double-quoted strings. Each String in this list is called a specification. Each specification has a verb, a format and a format-specific pattern. The verb, format, and pattern are all separated by the ":" character. Evaluation of MiTra expressions is left-to-right, with the output of the preceding expression on the left is used as the input to the expression on the right. The first specification must be either a X509 format expression or a Literal format expression, so that values are either derived from the Tunnel certificate or a constant string.

The grammar for MiTra expressions is as follows:

specs = (X509spec / LiteralSpec) [*(", " spec)]

X509spec = "select:X509:" pattern

LiteralSpec = "select:Literal:" pattern

spec = ("select" / "encode" / "decode") ":" ("HTTP" / "HTML" / "URL" / "Base64" / "CompressedBase64" / "Deflate" / "XML" / "Hex" / "X509" / "RFC2253" / "Literal") [":" pattern]

The verb is a general description of the operation to be performed. The *encode* and *decode* verbs do not take any arguments. The *select* verb takes the *pattern* argument. The pattern specifies the selector within the format. For example, in X509, the pattern can be *Subject* or *SubjectAltName:rfc822Name*.

An example of a multi-expression specification is as follows:

select:X509:SubjectAltName:ntPrincipalName,decode:Hex,encode:Base64

The above expression sequence is used in constructing a SAML Subject for Office 365 from a cert that contains an ObjectGUID from an Active Directory. The following formats are supported by MiTra expressions:

Format	Description	Operations Supported	Notes
X509	X.509 Certificates	select	
Literal	Constants	select	Selection pattern is output verbatim.
RFC2253	LDAP name simple text representation	select	
URL	URL-encoded data	select, encode, decode	Selection pattern is parameter name.
Hex	Hex-encoded data	encode, decode	
HTML	HTML format string	select	Selection pattern is in CSS syntax.
HTTP	HTTP request stream	select	Selection pattern is either header name or *Content* to select the content.
Base64	Base64 encoded data	encode, decode	
CompressedBase64	Deflate encoded Base64	encode, decode	
Deflate	Deflate encoded data	encode, decode	
XML	XML-encoded data	select, decode	Selection pattern is XPath spec. Decode results in pretty-printed XML.

Selection pattern description

The selection pattern that appears in a MiTra expression after the second ":", is dependent on the format on which that expression applies. The following is the syntax of the pattern for each format:

- X509 Pattern Syntax

X509pattern = ("Subject" / sanPattern)

sanPattern = "SubjectAltName:" sub-type [":" occurence]

sub-type = ("otherName"/ "ntPrincipalName" / "rfc822Name" / "dnsName" / "x400Address" / "directoryName" / "ediPartyName" / "uniformResourceIdentifier" / "ipAddress" / "registeredId")

occurence = *DIGIT ; ordinal number starting with 1 for the first occurrence.

To select the second SAN extension of type rfc822Name, you must specify the following string:

select:X509:SubjectAltName:rfc822Name:2

- Literal

The pattern is any string that is selected in its entirety.

- RFC 2253

RFC2253 is the string representation of LDAP names. A certificate's subject or subjectAltName:directoryName might result in a value of type RFC2253 name. To choose a specific value from an RFC2253 name, the pattern specifies the DN component name and optionally its occurrence from the right. For example, a MiTra expression of the form

select:RFC2253:DC:2

from the string

"CN=testuser2521, OU=contacts, DC=ivanti, DC=com"

results in getting the value *ivanti*.

23.6. Back up and restore Office 365 settings

Back up Office 365 settings

- Open the PowerShell command window and enter the following command to connect to the Office 365 tenant:

PS C:\Connect-MgGraph -Scopes "Domain.ReadWrite.All Directory.AccessAsUser.All"

- Enter the following command to back up the current domain federation settings into a file:

PS C:\Get-MgDomainFederationConfiguration -DomainId <federated-domain> | Export-Clixml <xml-file-path>

For example:

Enter the following command to back up the current domain federation setting for the federated domain *orange.com* to an xml file *c:|orange.com-original-settings.xml.*

PS C:\Get-MgDomainFederationConfiguration -DomainId orange.com | Export-Clixml orange.com-original-settings.xml

Restore Office 365 settings

Perform the following tasks to restore Office 365 settings from an existing saved file:

1. Load the configuration into a variable.

PS C:\$original = Import-Clixml <xml-file-path>

For example:

load config from file *c:|orange.com-original-settings.xml* into variable $original

PS C:\$original = Import-Clixml orange.com-original-settings.xml

2. Enter the following command to unfederate the domain if the domain is federated.

PS C:\Update-MgDomain -DomainId <federated-domain> -AuthenticationType "Managed"

For example:

unfederate the *orange.com* domain

PS C:\Update-MgDomain -DomainId orange.com -AuthenticationType "Managed"

> Please wait for 1 minute after this command before proceeding to the next step.

3. Enter the following command to restore the configuration from the variable.

Please check if the values used in this command are present in the xml file. Values which are not present in the xml file can be removed from the command.

FederatedIdpMfaBehavior argument is mandatory, so if it is not present in the xml file, you can use the value "acceptIfMfaDoneByFederatedIdp" for this argument.

PS C:\New-MgDomainFederationConfiguration -DomainId <federated-domain> -DisplayName $original.DisplayName -IssuerUri $original.IssuerUri -PassiveSignInUri $original.PassiveSignInUri -ActiveSignInUri $original.ActiveSignInUri -SignOutUri $original.SignOutUri -SigningCertificate $original.SigningCertificate -PreferredAuthenticationProtocol $original.PreferredAuthenticationProtocol -FederatedIdpMfaBehavior $original.FederatedIdpMfaBehavior -MetadataExchangeUri $original.MetadataExchangeUri

23.7. Configuring Ivanti Access Splunk application

Splunk fetches Audit logs and Ivanti Access reports for a tenant everyday from Ivanti Access. You must configure Ivanti Access Splunk application for this activity. Splunk v8.0.1 and Ivanti Access Splunk app v5.0 is now supported.

Before you begin

- Verify that you have installed Java 8 (JRE and JDK).
- Verify that before you upgrade, delete the configured data input for Ivanti Access if any.

Procedure

1. Copy the app distribution .spl file (miaccess_splunk_ap.spl) to the Splunk machine.
   The **.spl file** is available at **Product Documentation Page.**
2. Login to **Splunk** > **Apps**.

Click **Install app from file** and select **miaccess_splunk_app.spl** file. The **Upload an app** window opens.

Figure 1. splunk app

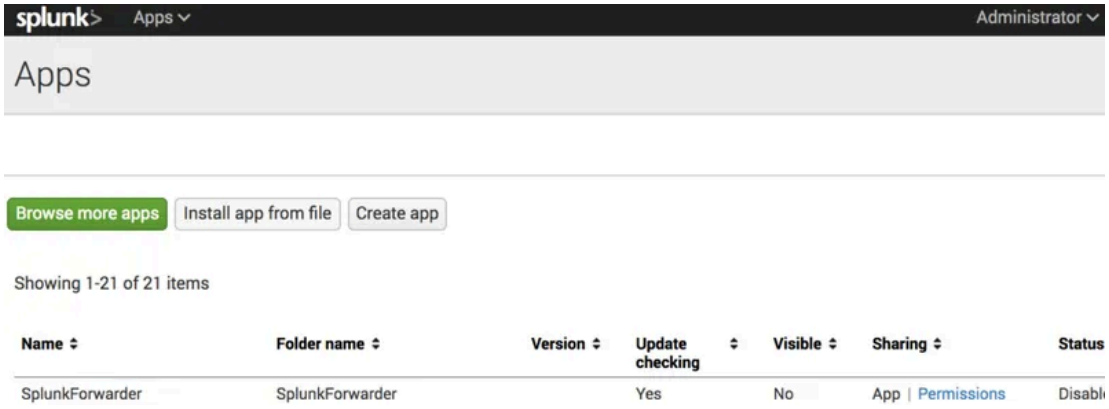
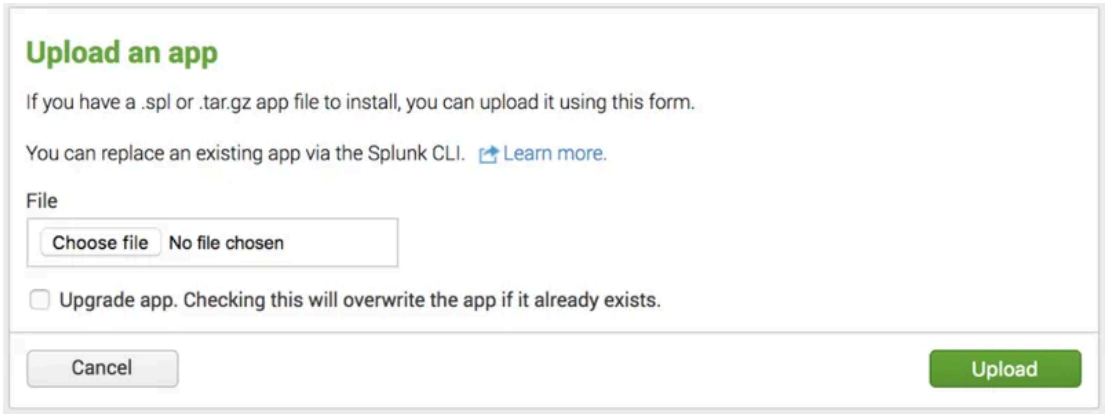


Figure 2. upload an app



3. Click **Choose file** and select **miaccess_splunk_app.spl**.

4. Select **Upgrade app. Check this will overwrite the app if it already exists**.

If you do not have the miaccess-splunk app already installed, then deselect this box.

5. Click **Upload**.

Once the upload completes, configure the data inputs.

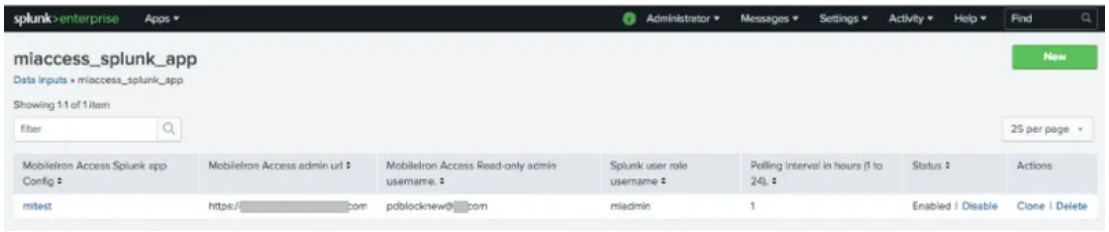
6. Click **Settings** > **Data inputs**.

Figure 3. Settings > Data inputs



The miaccess_splunk_app entry is now listed in local **Data inputs**.

Figure 4. ivanti access in data inputs



If you do not see the app listed in local Data inputs, then restart Splunk.

7. Click **New** in miaccess_splunk_app to configure the file.

The data input screen appears.

8. Enter the following details:

You must not modify the data inputs when the job is running. However, you can modify the data inputs when the job is not running.

- **Ivanti Access Splunk app Configuration**: Enter any name for the input configuration.
- **Ivanti Access Read-only admin username** and **Ivanti Access Read-only admin password**: Enter the Ivanti Access username and password.

Use Ivanti Access read-only user.

- **Ivanti Access admin url**: Enter the Ivanti Access admin URL such as https://access-na1.ivanti.com or https://access-eu1.ivanti.com.
- Ivanti Access Read-only admin username: Enter the Ivanti Access username.
- Ivanti Access Read-only admin password: Enter the password for Ivanti Access. The password is now masked.
- **Splunk user role username**: Enter the Splunk username with minimum user having *edit_tcp* role.

- **Splunk user role password**: Enter the Splunk user role password.
- Splunk management port: Enter the management port such as 8089.
- **Polling interval in hours**: Enter the frequency in number of hours to pull data from Ivanti Access.
- Click **Save**.

You can now monitor the fetching of audit logs and access reports in **splunkd.log** file. Use the following indexes to search for the reports after the Ivanti Access Reports are available in Splunk:

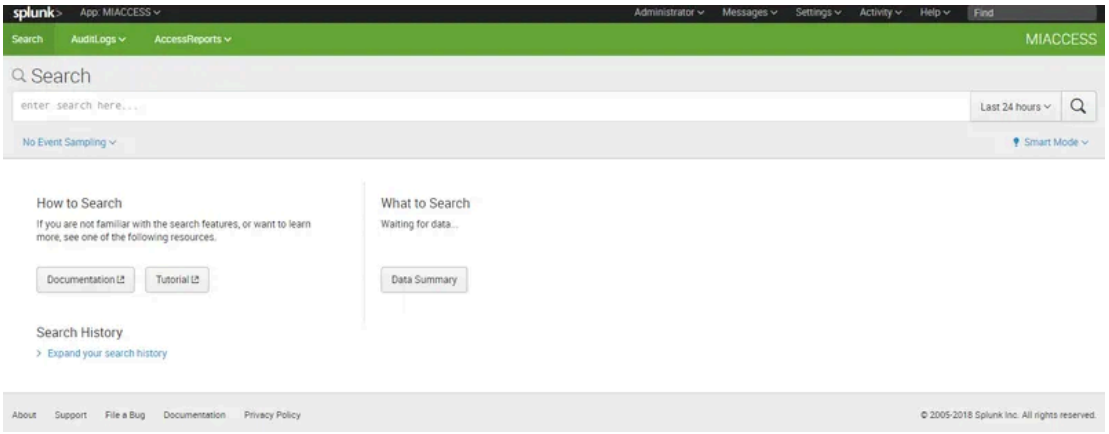
- index="miaccess_report_index"
- index="miaccess_audit_log_index"

- After importing the .spl file, if the app is not visible, then restart Splunk.
- When you configure Splunk for the first time, it pulls data for past 90 days which can take a few minutes.

Splunk dashboard

After adding and configuring the .spl file, the Ivanti Access application is available on the homepage. Click the application to view the dashboards for the application.

Figure 5. Splunk dashboard



The graphs are prepopulated for AuditLogs and Ivanti AccessReports. There is one graph for AuditLogs and four graphs for Ivanti Access Reports.

Figure 6. Audit Logs

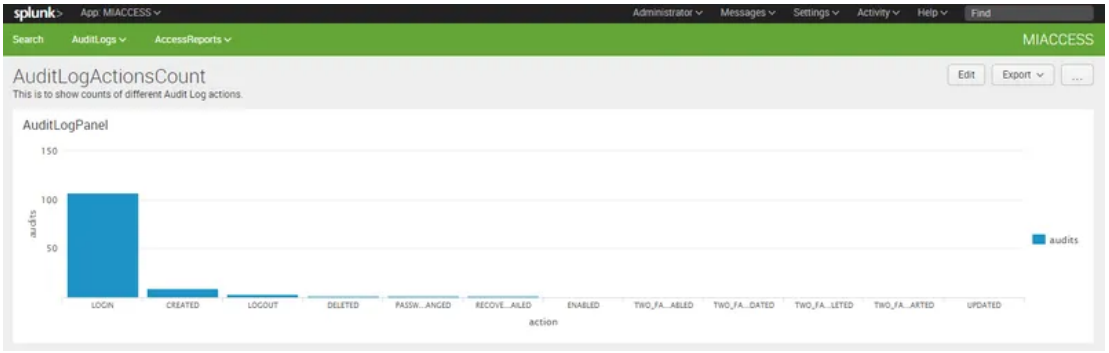


Figure 7. ivanti Access Reports Platforms

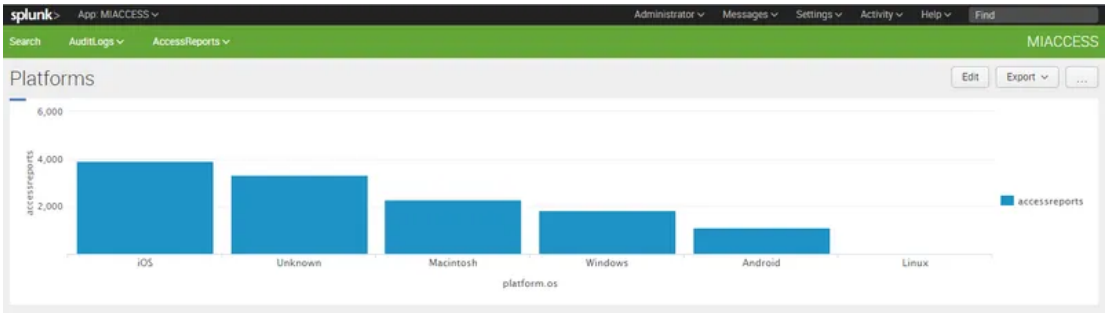


Figure 8. ivanti AccessReports Actions

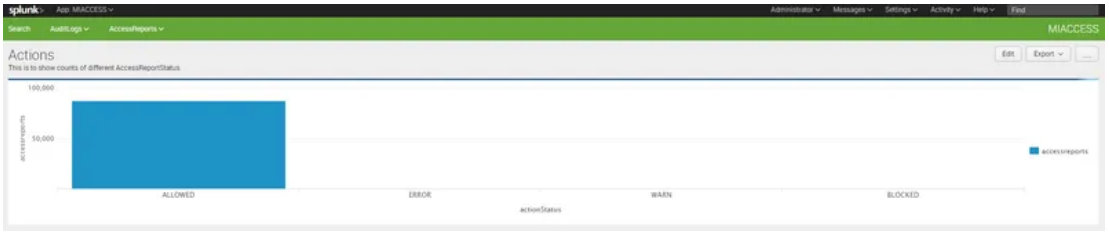


Figure 9. ivanti Access reports Geodata

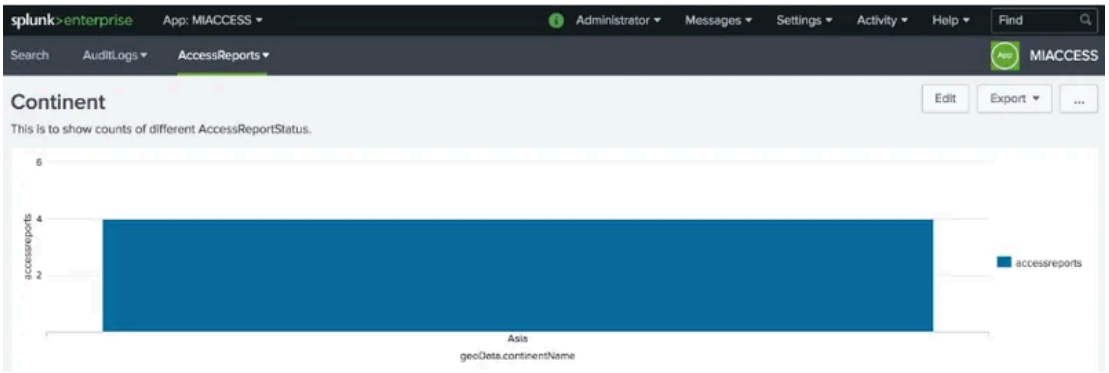


Figure 10. ivanti Access reports Country name

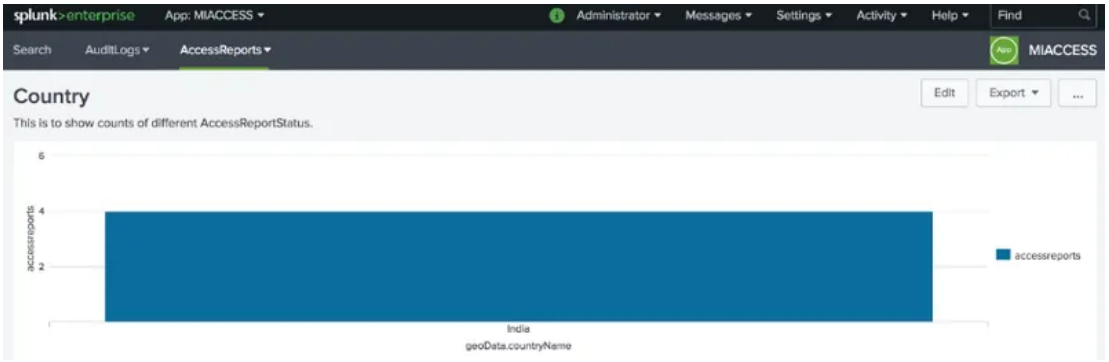


Figure 11. ivanti Access reports derived useragents



24. Third-Party Attributes

Ivanti Access includes components developed by third parties. You can view the list **here**.

25. About Zero Sign-on with MobileIron Access

Zero Sign-on provides secure passwordless access to enterprise cloud resources.

The following provides additional information about Zero Sign-on with MobileIron Access:

- Required components for Zero Sign-on
- Use cases for Zero Sign-on
- Considerations for Zero Sign-on
- Zero Sign-on authentication flow

Required components for Zero Sign-on

Deploying Zero Sign-on with MobileIron Access requires that the following components are set up:

- MobileIron Access deployment with a MobileIron unified endpoint management (UEM) platform. The MobileIron UEM platforms are: MobileIron Cloud, MobileIron Core, or MobileIron Connected Cloud.
  An Access deployment includes the following:
  - MobileIron Tunnel configuration with Access enabled.
  - MobileIron Tunnel deployed to devices.
- iOS, Android, Windows 10, or macOS devices devices managed by MobileIron UEM.
- MobileIron UEM client. The MobileIron UEM clients are: MobileIron Go for Cloud or Mobile@Work for Core.

See the MobileIron Access Release Notes for supported versions.

Use cases for Zero Sign-on

Zero Sign-on allows users password less access to enterprise cloud services. The following describes the use cases that are enabled when you configure Zero Sign-on:

- **Password less access from managed devices**: Users accessing an enterprise cloud service provider (SP) from a managed device are automatically authenticated using certificate-based single sign-on. Users do not need to enter their username and password.
- Password less access from unmanaged devices: Users accessing an enterprise cloud service provider (SP) from an unmanaged device are presented with a QR code. Scanning the QR code with their managed device authenticates the user and allows access from the unmanaged device. Users scan the QR code using the MobileIron client and the native camera on the managed device. Users do not need to enter their username and password. Users have the following additional options for subsequent log in:
  - Enable push notifications. A push notification is sent to the managed device on subsequent log in from the unmanaged device if the "remember me" option is selected.
    When a user tries to log in from the desktop browser, a push notification is sent to all the active devices. When the user allows push notification on any one of the appropriate device, access is granted to the user. However, on all other devices, the push notifications become invalid.
  - Alternately, users can use the MobileIron client on their managed device to generate a one-time passcode (OTP). OTP allows users to access cloud services from the unmanaged device even when the MobileIron client does not have access to the Internet.

Considerations for Zero Sign-on

Consider the UEM and client support described in the following table:

MobileIron UEM	MobileIron Client	Feature supported
MobileIron Cloud	MobileIron Go for iOS	QR code, push notifications, OTP
	MobileIron Go for Android and Android enterprise	QR code, push notifications, OTP
MobileIron Core	Mobile@Work for iOS	QR code, push notifications, OTP
	Mobile@Work for Android and Android enterprise	QR code, push notifications, OTP

Zero Sign-on authentication flow

The following describes the authentication flow from an unmanaged device using Zero Sign-on.

Figure 1. Zero Sign-on authentication flow



1. User requests access to a cloud service from an unmanaged device, such as a desktop.
2. The cloud service redirects user to the configured identity provider (IdP)to authenticate. Since Access is the configured IdP, the request is redirected to Access.
3. Access generates and presents a QR code to the user.
4. The user scans the QR code with a MobileIron managed mobile device to approve the login.
5. Access generates a new SAML response to redirect to the original SP. The original SP obtains the user identity from the SAML response and presents the personalized screen to the user.

26. Configuring Zero Sign-on

A Zero Sign-on setup requires an Access deployment with MobileIron UEM, as well as additional configurations forZero Sign-on in Access and in the MobileIron UEM. A Zero Sign-on configuration enables passwordless access to cloud resources by using the user identifying information in the Tunnel certificate for authentication.Zero Sign-on is part of a MobileIron Access deployment. Therefore, before configuring Zero Sign-on ensure that you have an Access deployment and that single sign-on is configured for cloud service providers.

Before you begin

- Ensure that you have an Access deployment with MobileIron UEM.
  See **Overview of configuration with Ivanti Neurons for MDM**.
  OR
  See **Overview of configuration with Ivanti EPMM**
  A Tunnel setup is part of deploying Access with MobileIron UEM. Detailed steps and references for setting up Tunnel and required certificates for Tunnel are included in the instructions for deploying Access with MobileIron UEM.
- Ensure that mobile app single sign-on (SSO) is configured for the service provider (SP).
  For a federated pair, see **Configuring Mobile App Single Sign-on (SSO)**.
  For delegated IdP, see **Configuring Ivanti Access as the delegated IdP** .
- MobileIron recommends, where available, that managed app configurations are deployed in MobileIron UEM for your cloud service provider apps, such as for Salesforce, Concur, Box, or Outlook. For a seamless end-user experience, deploy a managed app configuration to streamline the user and organization information input. For information about how to set up a managed app configuration, see the following:
  - For MobileIron Core: See "iOS managed app configuration" or "App configuration for Android enterprise apps" in the Ivanti EPMM Apps@Work Guide.
  - For MobileIron Cloud: See "Using iOS Managed App Configuration" or "Managed Configurations for Android" in the Ivanti Neurons for MDM Administrator Guide.

Procedure: Overview of steps

1. Configure Zero Sign-on in MobileIron Access.
   See **Configuring Zero Sign-on in Ivanti Access**.
   1. Enable Zero Sign-on and configure the user identifying information to use for authentication.
      See **Step 1: Enabling Password-less Authentication on MobileIron Go and Mobile@Work**
   2. Review or modify the registration settings used by clients to register users device with Access.
      see **Step 2: Review Registration Settings**
   3. Add a conditional rule in Access for enabling Zero Sign-on.
      See **Step 3: Adding a Zero Sign-on Rule in the Policies**.
   4. Configure your company branding. Users see the branding on the messages on the device from which they attempt to access cloud services and on MobileIron Go.
      See **Configuring branding for Zero Sign-on**.
   5. Publish the changes.
      See **Publishing the changes**.
2. Configure Zero Sign-on in MobileIron UEM.
   See **Configuring Zero Sign-on in Ivanti Neurons for MDM**.

OR

See **Configuring Zero Sign-on in Ivanti EPMM**

Related topics

- **About Zero Sign-on with MobileIron Access**
- **What users see for FIDO2**

27. Configuring Zero Sign-on in Ivanti Access

The following describes the configuration Ivanti Access for Zero Sign-on.

Before you begin

See **Configuring Zero Sign-on**.

1. **Step 1: Enabling Password-less Authentication on MobileIron Go and Mobile@Work**
2. **Step 2: Review Registration Settings**
3. **Step 3: Adding a Zero Sign-on Rule in the Policies**
4. **Setting the session timeout duration**
5. **Configuring branding for Zero Sign-on**
6. **Publishing the changes**

Step 1: Enabling Password-less Authentication on MobileIron Go and Mobile@Work

Before you begin

- Upload a sample Tunnel certificate in Profile > User Certificates. For more information about adding a certificate, see **User Certificates**.
- Configure the user information for Zero Sign-on.
    - To configure the user information, map the fields in the certificate from which Access gets user identifying information. This is the identity certificate used for setting up Tunnel. Configuring the user information enables passwordless authentication.

Procedure

1. In MobileIron Access, go to Profile > Zero Sign-on.
2. Under Steps to deploy, expand **Enable Password-less Authentication on MobileIron Go and Mobile@Work**.

3. Click **See Details** to view the existing configuration details for the devices.
4. To enable more devices follow the steps i) and ii) as shown above.
    1. Deploy SaaS Sign-On on managed mobile devices.
    2. Sync UEM.

Next steps

Step 2: Review Registration Settings.

Step 2: Review Registration Settings

The Registration settings are used by clients such as MobileIron Go to register user's device with Access.

Procedure

1. In MobileIron Access, go to Profile > Zero Sign-on.

2. Under Steps to deploy, expand **Step 2: Review Registration Settings**.
   Verify the certificate mapping.

3. Click **Edit** to modify the registration.

4. Select the username mapping in the certificate appropriately and click Save. For more information, see **Client Registration Settings**.

Next steps

Add a **Step 3: Adding a Zero Sign-on Rule in the Policies**.

Related topics

For information about MiTra expressions, see **Language to generate values from certificate fields**.

Step 3: Adding a Zero Sign-on Rule in the Policies

In the policy associated with the saml pair for which Zero Sign-on is required, add a Zero Sign-on Rule conditional rule. If the rule is added, users accessing the cloud service from an unmanaged device see an interaction page. The interaction page contains a QR code, which device users can scan from a managed device to authenticate to the cloud service. Alternately, the interaction page also contains a link to authenticate with username and password.

Before you begin

- Ensure that mobile app single sign-on is configured for the federated pair or delegated IdP to which you want to assign the Zero Sign-on Rule. If mobile app single sign-on is not configured, you will see errors when creating or assigning the Zero Sign-on Rule.

Procedure

1. In MobileIron Access, go to Profile > Zero Sign-on.
2. Under Steps to deploy, expand **Add Zero Sign-On Rule in the Policies**.
   
3. Verify that the rule is configured.
   Else add a rule in **Profile** > **Conditional Policies**.
4. In Access, go to Profile > Conditional Access.
5. Expand Default Policy.
   If you want Zero Sign-on only for some federated pairs or delegated IdP, create a new policy.
   The Zero Sign-on rule can be added to any policy. Adding the Zero Sign-on rule to the default policy makes it available to all pairs to which the default policy is applied. Add the Zero Sign-on rule to another policy if you want to apply the rule to only some federated pairs or delegated IdP.
6. Click +Add Rule > Zero Sign-on Rule to add the conditional rule for Zero Sign-on.
7. Enter a name and description for the rule.
8. For Rule Action, select Allow.
9. Click Done to save the policy and rule.

The order of the conditional rules matters. When you create a Zero Sign-on Rule, Access automatically orders the rules such that the Zero Sign-on Rule follows the Trusted App and Device rule. The order of rules, if they are configured, is as follows: Trusted App and Device rule, Zero Sign-on Rule, Multi-Factor Authentication rule. However, the rules can be manually reordered. Ensure that the order of the rules matches the order stated in this note.

Next steps

Configure branding. See **Configuring branding for Zero Sign-on**.

Setting the session timeout duration

Use the Zero Sign-on configuration, Profile >Zero Sign-on, to do the following:

- Set the session timeout duration after users authenticate using Zero Sign-on.
  If device users select the Yes, this is my personal computer option in the QR interaction page when they attempt to log in to the cloud service, they are not prompted to sign in for subsequent login attempts for the duration set in Profile > Zero Sign-on > Zero Sign-on Settings and their user ID is remembered on the browser for 30 days. For login attempts after the session timeout duration, a push notification is automatically sent to their managed device. Users have the option to either enter an OTP or scan a QR code. At the end of 30 days, the user ID is no longer remembered in the browser, and users are once again prompted to scan a QR code.

Procedure

1. In MobileIron Access, go to Profile > Zero Sign-on.
2. Click **Zero Sign-on Settings** to update the number of hours, if needed, for Enable Signed In Session.
3. By default, the option is enabled and the number of hours is set at 12. The option sets the session timeout that is applied when users select the Yes, this is my personal computer option in the Zero Sign-on interaction page.
4. Click Save Settings.

Configuring branding for Zero Sign-on

Customize the user experience for your enterprise users by uploading your company logo to Access. The user notification screen as well as the interaction page with the QR code are customized to display your company logo.

Ensure that your company logo is no more than 260 pixels wide by 30 pixels high. Supported file types are: PNG, JPG, JPEG, and SVG.

Procedure

1. In Access, go to Profile > Branding.
2. In the Company Logo section, drag and drop your company logo or click Choose to navigate to the location of the file and add.

Next steps

Publish the updates. See **Publishing the changes**.

Publishing the changes

Publish the changes to make the updates available. In the Access administrative portal, a publish banner appears in any of the Profile tabs when there are configuration changes.

Procedure

1. In the Access, go to Profile > Overview.
2. Click Publish.
3. Click OK.

Next steps

Configure Zero Sign-on in MobileIron UEM. See,

- **Configuring Zero Sign-on in Ivanti Neurons for MDM**
  OR
- **Configuring Zero Sign-on in Ivanti EPMM**

Related topics

Publishing a profile