Single Sign-On Across Business Applications

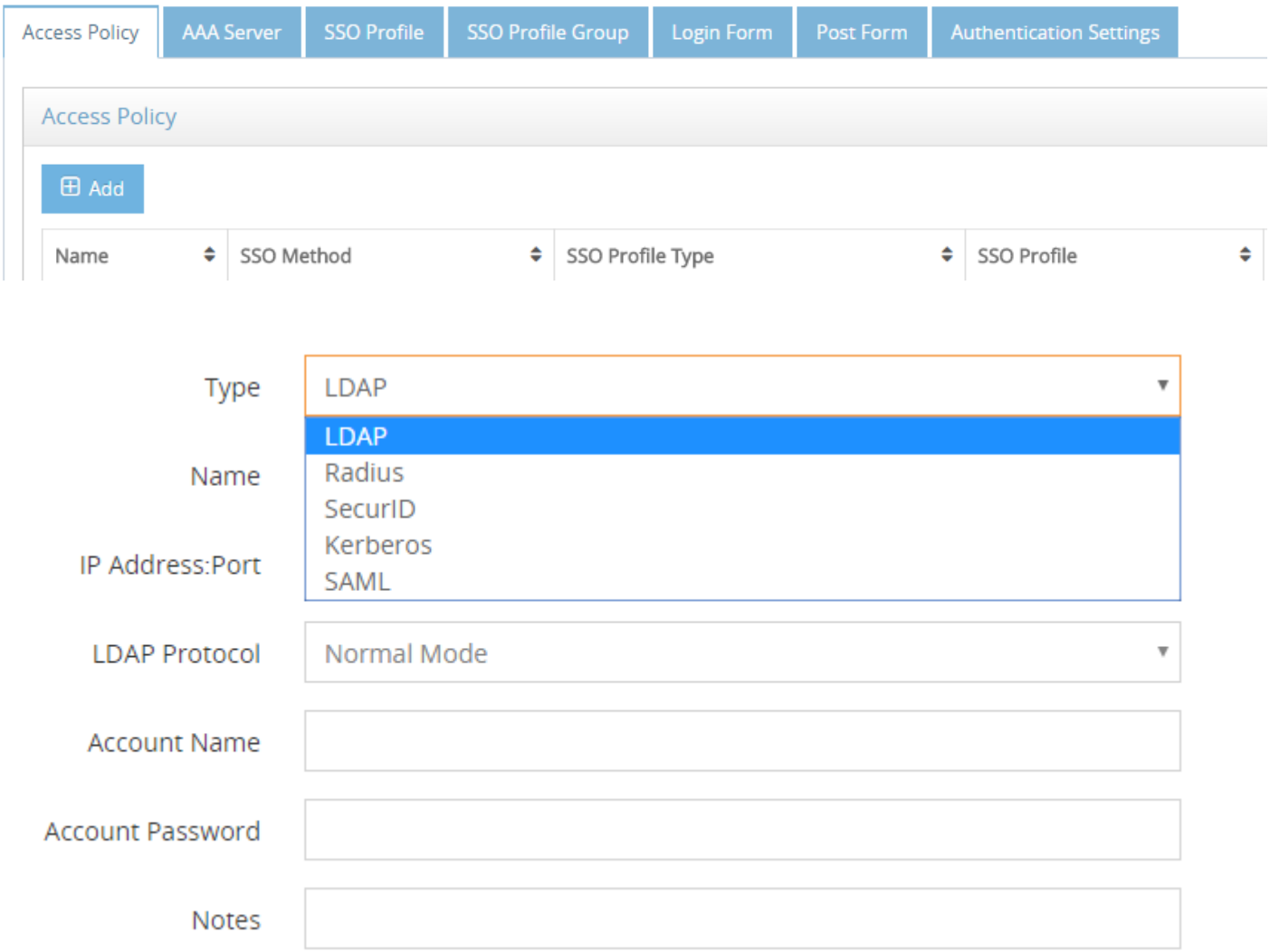
Enterprises need to allow client access to different business applications without data leakage. These applications might not use common authentication. Each application has its own user directory store. For instance, in an organization, Windows uses Active Directory service to authenticate users, and middleware applications integrate the front-end and back-end applications.

XPoint AppScaler provides centralized and flexible application access authentication to consolidate identity access management infrastructure and realize enhanced security at a reduced operational cost.

XPoint AppScaler leverages both advanced client authentication and access management, combined with the programmability of Post Form, it can offload authentication processing from business applications to make for a simpler, more flexible and secure environment.

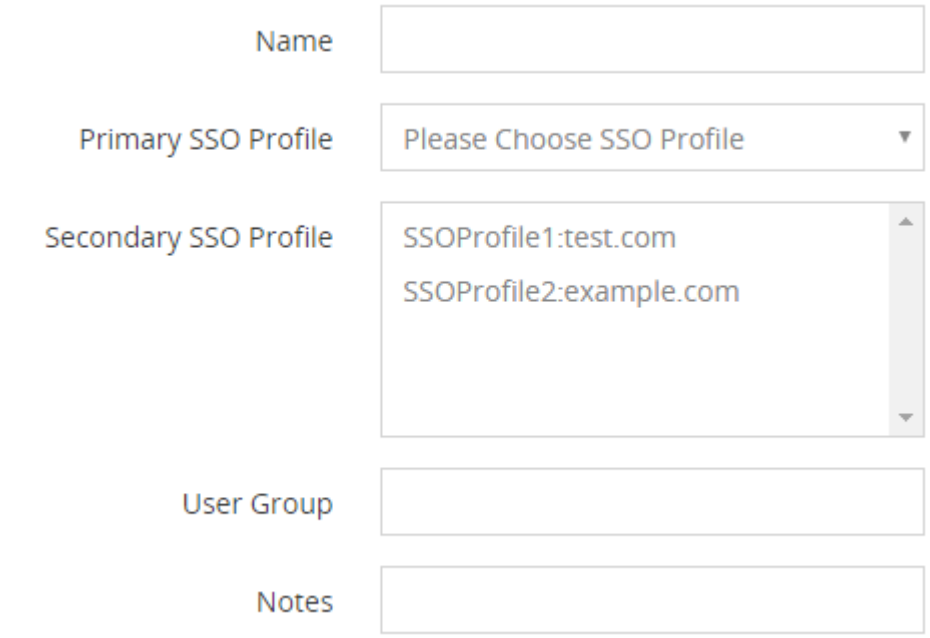
Seamless Integration with Access Management Infrastructure

Providing SSO across applications deployed on heterogeneous platforms requires standardization on a common identity and access management framework, XPoint AppScaler supports a wide range of authentication protocols including LDAP, Radius, RAS SecurID, Kerberos, SAML and NTLM.



Multiple LDAP Domains Authentication

You can set up one SSL Profile Group to consolidate multiple LDAP Servers as the SSO authentication relay and grant granular access control for expanded flexibility based on LDAP user groups.



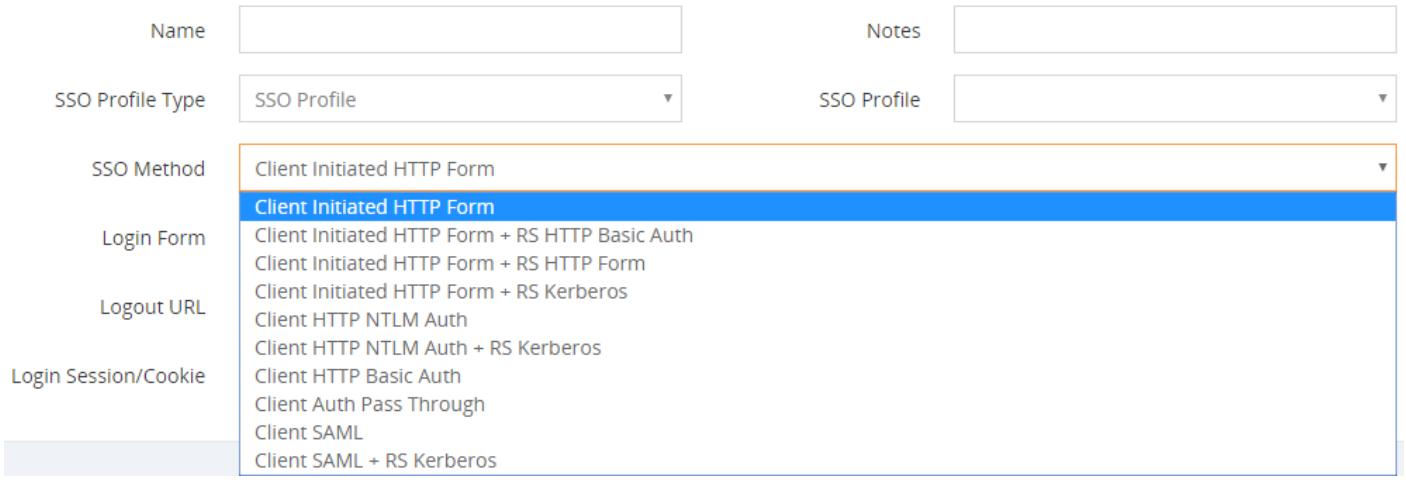
Comprehensive Authentication Methods

The wide range of authentication methods supported including:

HTTP Authentication (Basic, NTLM/Kerberos)

HTTP Form

Client Authentication Pass Through



Health Monitoring

Health checking against the authentication servers includes:

LDAP

Radius

RSA SecurID

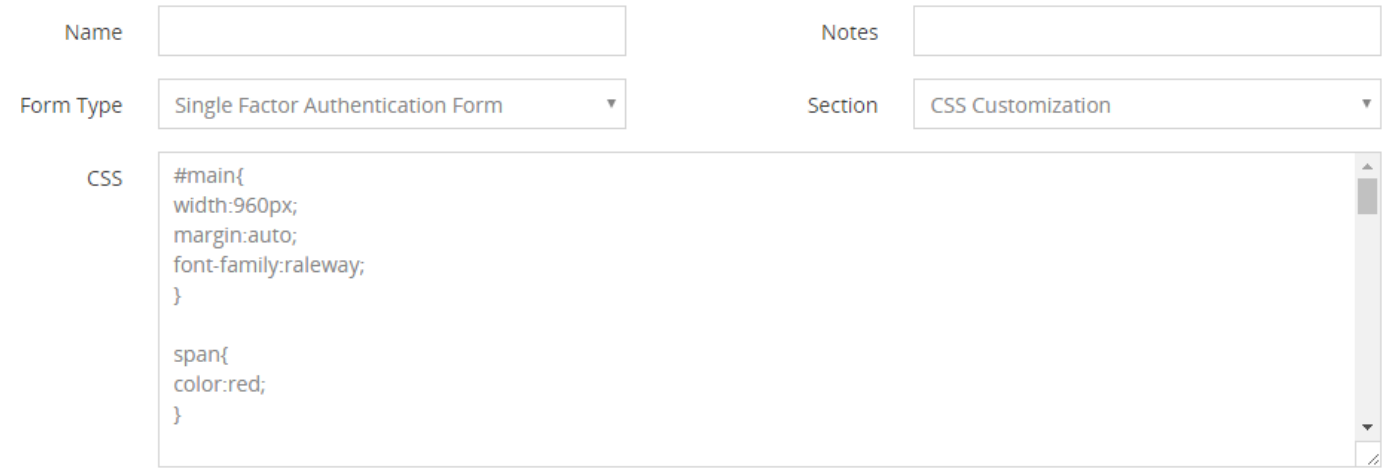
Kerberos

Fully Customized Login Form

The custom login form includes:

1 Factor Authentication Login Form

2 Factor Authentication Login Form

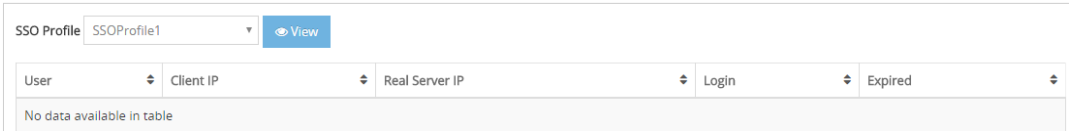


Fully Programmed Post Form

When using Client Form Based and Server Form Based method, you can program the attributes to be sent to backend applications through POST method. It can make the integration between common authentication services with specific backend application servers. For instance, when the client logins the built-in HTML form, XPoint AppScaler will store its credentials and other attributes to the backend application.

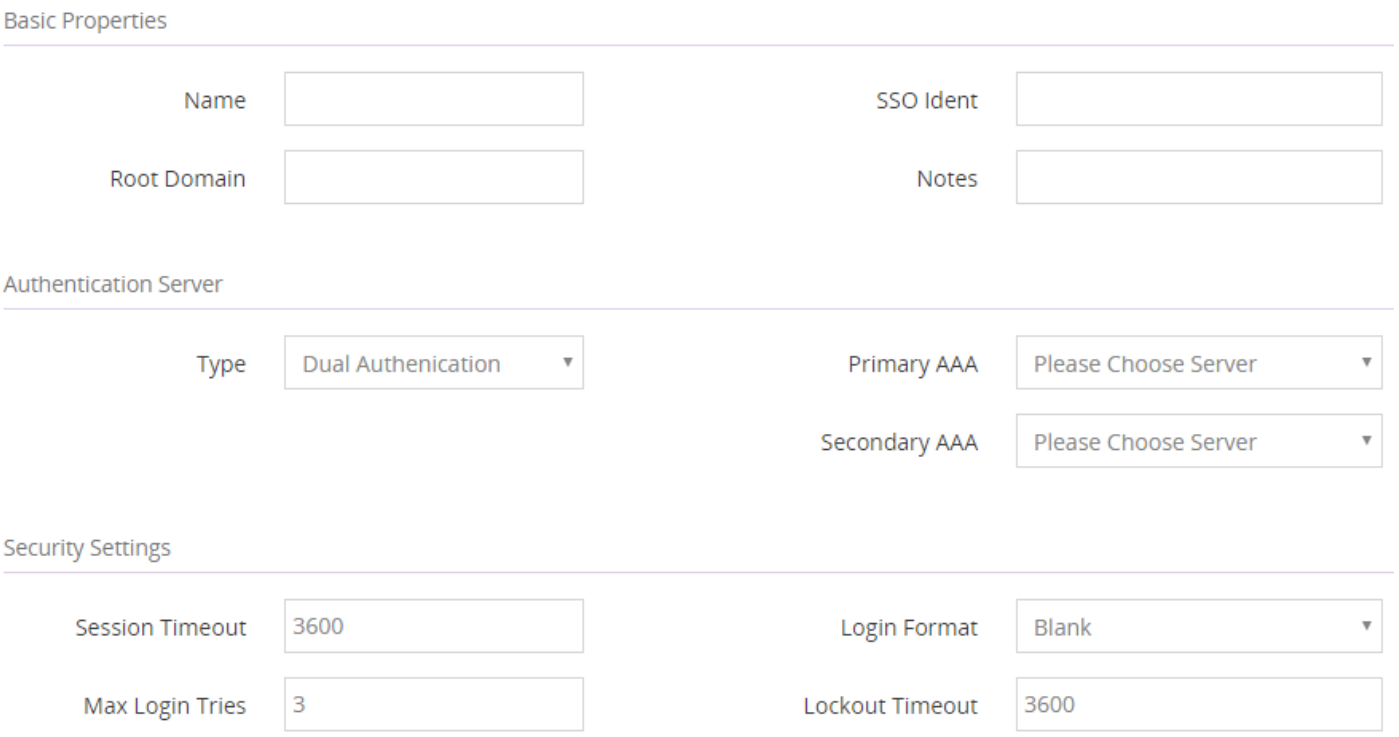
Authentication Logs

All the access events records can be stored for audit purpose.



2 Factor Authentication

The 2 factor authentication is fully supported.



Unified Access Policy

XPoint AppScaler provides unified access policies to enforce access across different business applications. It enables organizations to seamlessly identify users and apply access policies at strategic point of control which decreases the effect of access-related attacks and improve application performance by saving unnecessarily consumed resources.

Some SSO Use Cases

1. With SSO features on XPoint AppScaler you can replace discontinued Microsoft Forefront TMG (Threat Management Gateway) solution.

2. Integrate with Microsoft Applications like Outlook as a reliable authentication mechanism.

3. SSO provides a generic single sign-on solution. Middleware applications and custom adapters can take advantage of SSO to securely store and transmit user credentials across the environment. End users do not have to remember different credentials for different applications.

Summary

XPoint AppScaler consolidates and streamlines web application access management and authentication services, offloads authentication processes from servers and realize a more cohesive, integrated identity and access management infrastructure.