Single Sign-on: How to deploy white-labeled MicroStrategy applications behind single sign-on solutions
Single Sign-on: How to deploy white-labeled MicroStrategy applications behind single sign-on solutions

Loïc Fabro
Director, Product Management

Carlos Ugarte Peyron
Manager, Professional Service

- What is Single Sign-On?
- Benefits of SSO
- How-to SSO with MicroStrategy
Copyright and Safe Harbor Notice

This presentation may include statements that constitute “forward-looking statements” for purposes of the safe harbor provisions under the Private Securities Litigation Reform Act of 1995, including descriptions of technology and product features that are under development and estimates of future business prospects. Forward-looking statements inherently involve risks and uncertainties that could cause actual results of MicroStrategy Incorporated and its subsidiaries (collectively, the “Company”) to differ materially from the forward-looking statements.

Factors that could contribute to such differences include: the Company’s ability to meet product development goals while aligning costs with anticipated revenues; the Company’s ability to develop, market and deliver on a timely and cost-effective basis new or enhanced offerings that respond to technological change or new customer requirements; the extent and timing of market acceptance of the Company’s new offerings; continued acceptance of the Company’s other products in the marketplace; the timing of significant orders; competitive factors; general economic conditions; and other risks detailed in the Company’s Form 10-K for the year ended December 31, 2016 and other periodic reports filed with the Securities and Exchange Commission. By making these forward-looking statements, the Company undertakes no obligation to update these statements for revisions or changes after the date of this presentation.
SSO in the three Key Target Scenarios for Embedded Analytics

Embed MicroStrategy content into custom applications and workflows

- Embed MicroStrategy content into a web page or application
- Embed data from MicroStrategy into an application
- Leverage MicroStrategy capabilities (SSO, Folders, …) in an application
- White label MicroStrategy functionalities

Integrate MicroStrategy platform into a custom product offering

- Automated deployment and upgrade of a MicroStrategy environment
- Programmatic user and security management
- Updating MicroStrategy cube data from 3rd party applications/workflows
- Programmatic object management

Extend MicroStrategy capabilities with 3rd party functionality (and vice versa)

- Connect new sources to MicroStrategy
- Add new visualizations to MicroStrategy
- Add new workflows to MicroStrategy
- Push new data and metadata to MicroStrategy
- Pull data from MicroStrategy and process in other systems (e.g. Machine Learning)
Single sign-on (SSO) provides the capability to authenticate once, and be subsequently and automatically authenticated when accessing various target systems. It eliminates the need to separately authenticate and sign on to individual applications and systems, essentially serving as a user surrogate between client workstations and target systems. Target applications and systems still maintain their own credential stores and present sign-on prompts to client devices. Behind the scenes, SSO responds to those prompts and maps the credentials to a single login/password pair. SSO is commonly deployed in enterprise, Web and federated models.

Source: Gartner https://www.gartner.com/it-glossary/sso-single-sign-on
SSO Demo Demo

Single Sign On -> I don't enter any password anywhere

mac-lfablo
Benefits of SSO for enterprises

It’s not always about the users!

---

**Reduced costs**
Less operational cost
Faster access to data

---

**Better user experience**
Less prompts = less interruption

---

**Better security**
Only one service to monitor and protect
Application (aka “Service Provider”) does not know/receive the user credentials
Enterprise SSO and derivatives
As the term evolved over time, so did the enterprise implementations

---

**Single credential**
The same credentials are used to access multiple applications:
- Single credential validation system
- Password synchronized across various systems

LDAP, etc.

---

**Seamless Login (e.g. modern SSO)**
Login once, access all through:
- Portal (aka “Identity Provider initiated” login workflow)
- Direct Access to the application (aka “Identity Provider initiated” login workflow)

Windows authentication, Kerberos, SAML, OAuth, etc.
Protocols and technologies used for SSO
Most prevalent technologies in enterprise SSO deployments

---

Vendor-specific implementations
Microsoft Windows Authentication (NTLMv2)

---

Standard-based implementations
Kerberos (RFC4120 - 2005)
SAML 2.0 (RFC6749 - 2012)
OAuth 2.0 (RFC6749 - 2012)
OIDC (Open ID Connect, built on top of OAuth 2.0)
What do we always forget about?
User management challenges

Authentication is only the tip of the iceberg:

• Provisioning (i.e. user and group creation)
• Update (e.g. group membership, name update, etc.)
• Decommission (i.e. user and group deletion)

Key to success: Automation
When to use what authentication mode?
Remember, this is just a guideline! 😊

- **Username/Password**
  - Less than 20 users, pilot deployment

- **LDAP**
  - Enterprise or department deployment

- **Database**
  - Legacy system where security is all defined on the data source

- **Guest**
  - Public data or demo application

- **Windows NT**
  - Legacy deployments

- **Kerberos**
  - End-to-end user identity

- **Trusted Security Providers**
  - Legacy SSO deployments

- **SAML**
  - Enterprise standard

- **Mix & Match or custom authentication**
## Authentication mode security capabilities

<table>
<thead>
<tr>
<th></th>
<th>Password complexity check</th>
<th>Credential validation delegated to 3rd party system</th>
<th>Data security delegated to Data Source</th>
<th>Create user profile at logon</th>
<th>Sync user profile from AD/LDAP at logon</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard</td>
<td>Yes</td>
<td>No</td>
<td>No**</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Guest (aka Anonymous)</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Windows NT</td>
<td>N/A</td>
<td>Yes</td>
<td>No**</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>LDAP / AD</td>
<td>N/A</td>
<td>Yes</td>
<td>No**</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Integrated (aka Kerberos)</td>
<td>Possible</td>
<td>Yes</td>
<td>Possible</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Database</td>
<td>Possible</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>SAML</td>
<td>Possible</td>
<td>Yes</td>
<td>No**</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Trusted Provider</td>
<td>Possible</td>
<td>Yes</td>
<td>No**</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Custom</td>
<td>Possible</td>
<td>Possible</td>
<td>Possible**</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

* Possible using MicroStrategy Security (ACL, Privileges)
** Possible using MicroStrategy Database Connection Mapping
When to use what authentication mode?

Remember, this is just a guideline! 😊

- **Username/Password**
  - Less than 20 users, pilot deployment

- **LDAP**
  - Enterprise or department deployment

- **Database**
  - Legacy system where security is all defined on the data source

- **Guest**
  - Public data or demo application

- **Mix & Match or custom authentication**

---

### SSO Experience

- **Windows NT**
  - Legacy deployments

- **Kerberos**
  - End-to-end user identity

- **Trusted Security Providers**
  - Legacy SSO deployments

- **SAML**
  - Enterprise standard
Kerberos authentication

Authenticating to MicroStrategy with Kerberos
Integrated Authentication
How to leverage Kerberos Authentication

What is Kerberos?
- Open Standard for network authentication
- Published by the MIT to allow for secure network authentication in 1989
- Supports Authentication Delegation (aka authentication forwarding)

Enabling MicroStrategy to use Kerberos
- Use the documentation:
  https://www2.microstrategy.com/producthelp/10.10/SystemAdmin/WebHelp/Lang_1033/Content/Admin/Enabling_integrated_authentication.htm
- Enable web browsers to use Kerberos
  - Internet Explorer / Edge: automatic
  - Chrome, Safari, Firefox: manual steps
How does Kerberos work?
Hum…. This is very simplified, but good enough!

Key Distribution Center (KDC)
- Authentication Service (AS)
- Ticket Granting Service (TGS)

I am Sue and need a Ticket to Get a Ticket (TGT)
- Here is your TGT if you can decrypt this response with your password hash

Here is my TGT, give me a Service Ticket
- Here is your Service Ticket
- Here is my Service Ticket, authenticate me
- Here is your session identifier
Benefits of Kerberos authentication
Appealing for enterprise deployments

Why use Kerberos?
- Mutual Authentication
- Open standard
- Authentication Delegation (aka authentication forwarding)
- Standard for Authentication since Windows 2000 for Microsoft Operating Systems

Challenges deploying Kerberos?
- Complex initial setup
  - Initial Server-level setup is fairly straight forward
  - Non-Microsoft browsers require managed configuration
- Not designed with Cloud-based SaaS
  - the “Cloud” did not exist when v5 was released at the beginning of the century
Demo: MicroStrategy Web Login with Kerberos

SSO implemented with Kerberos
Trusted authentication providers

Authenticating to MicroStrategy leveraging 3rd party authentication providers
Trusted Authentication Providers
Already deployed in many enterprises

Why use a 3rd party Authentication Provider?
- Support for multiple authentication protocols
- Cloud and on premise support
- Ease the deployment of multi-factor authentication

Setup steps
- Install the Authentication Provider junction/web agent/webgate on the web server
- Configuration MicroStrategy to use trusted authentication

Tested providers
- IBM Security Access Manager (f.k.a. IBM Tivoli Access Manager)
- CA Single Sign-On (f.k.a. CA SiteMinder)
- Oracle Access Manager (f.k.a. Oblix CoreID)
- Ping Identity PingFederate
Demo: MicroStrategy Web Login with CA SiteMinder

Trusted Authentication Provider for SSO
Trusted Provider authentication experience using CA SiteMinder
SAML authentication
Authenticating to MicroStrategy leveraging a SAML Identity Provider (IdP)
SAML Authentication
SAML (Security Assertion Markup Language) is available in many enterprises already

Why use SAML 2.0?
- Industry standard (all SSO providers support SAML)
- Cloud and on premise support
- Client-side workflow (i.e. easy to deploy)

Setup steps
- Register MicroStrategy Web/Mobile/Library as an application on SAML Identity Provider
- Configure MicroStrategy Web, Mobile and Library to use trusted authentication and SAML

Tested IdPs
- MicroStrategy Usher
- Microsoft ADFS
- Shibboleth
- Ping Identity PingFederate
Demo: MicroStrategy Web Login with SAML
SAML Authentication using Trustelem
SAML Authentication

Demo

Client → MicroStrategy Web → Identity Provider

User access to MicroStrategy URL
- Not valid session or SAML token found
  - Redirect user to IDP for authentication
    - Redirect to Authorization Server Login page
  - User logs in
    - Redirect to MicroStrategy and add SAML token
      - Access to MicroStrategy with SAML token in the request
        - Redirect user to MicroStrategy Web page with established session.
SAML Authentication
Demo

Environment:
• Service Provider (SP): MicroStrategy Web 10.9 running on a JSP server.
• Identity provider (IdP): Trustelem.

Steps for Configuring SAML support for MicroStrategy Web
1. Generate configuration files.
2. Register MicroStrategy Web with your identity provider.
4. Configure logging.
5. Configure the Intelligence Server connection.
SAML Authentication

Demo

Enabling single sign-on with SAML authentication for JSP Web and Mobile

- Starting in v10.9, dashboards will be referred to as dashlets. Please keep this in mind as you review documentation that may still reference dashboards.

You can configure MicroStrategy Web and MicroStrategy Mobile to work with SAML-compliant single sign-on (SSO).

- Though the following prerequisites and procedures refer to MicroStrategy Web, the same information applies to MicroStrategy Mobile, except where noted.

Prerequisites

Before you begin configuring MicroStrategy Web to support single sign-on, make sure you have done the following:

- Deployed a SAML-enabled identity provider (IdP) infrastructure
- Verified that MicroStrategy Web is run on a JSP server.
- Deployed MicroStrategy Web on this application server

Deploy the MicroStrategy Web WAR file on the application server in accordance with your application server documentation.

The following procedures describe how to configure and integrate SAML support for MicroStrategy Web to implement single sign-on.

- Configuring SAML support for MicroStrategy Web
- Disabling SAML support for MicroStrategy Web
- Integrating SAML support with Usher
- Integrating SAML support with ADFS

Configuring SAML support for MicroStrategy Web
Custom authentication
Extending MicroStrategy authentication methods
Custom Authentication
When the out-of-the-box options don’t meet your needs

Why go the custom route?
- Enterprise uses a non-supported SSO authentication method
- Some of the login workflow steps can’t be achieved out-of-the-box

What option do I have to customize the authentication?
- MicroStrategy Web External Security Module
- Custom Login Task
- Web Server filter (ISAPI filter/HTTP module for Microsoft IIS or Filters for J2EE application servers)
- Custom SAML Provider
API-level SSO Support: Dynamic Group Membership and System Prompt Answer

Delegate security to a 3rd party authentication provider

Extension to the Session Creation

• Easy-to-use XML based definition for security and personalization extension to the Java session creation API.
• Leverages the same infrastructure the native LDAP and SSO Provider supports
• Available in any MicroStrategy 10 deployment

What can you do with the APIs:

• Set Answers for System Prompts at session creation time
• Specify user group membership at login time

Why is this enhancement relevant?

• Session creation performance is much higher and security much higher since no separate administrative session is required
• No need for “synchronization” and no lag between system and security update (i.e. “real-time” security and personalization)
• Designed for MicroStrategy Web (External Security Module) and MicroStrategy Mobile (Login Task)

Custom Authentication – MicroStrategy Web ESM
MicroStrategy Web External Security Module

What is it?
- A component written in Java that will be used by MicroStrategy Web

How to build it?
- Use the MicroStrategy Web Customization Editor to create a new ESM.
- Configure MicroStrategy Web to use that ESM

Custom Authentication – MicroStrategy Login Task
MicroStrategy Web External Security Module

What is it?
- A component written in Java that will replace the MicroStrategy mobile MobileAppLoginTask task

How to customize?
- Use the MicroStrategy Web Customization Editor to overwrite the MobileAppLoginTask task.

Custom Authentication – Web Application Filter
MicroStrategy Web External Security Module

What is it?
- A component written in Java (as a Filter for J2EE app servers) or c,c#,vb.net, etc. (HTTP module or ISAPI filter for IIS) that will intercept any incoming request and, in case of lack of valid application session, can redirect the client to an external login page.

How to customize?
- Use your preferred IDE to write the code specific to your application server.

Can leverage the same workflows Trusted Authentication providers are using that MicroStrategy Web/Mobile already supports.
Custom Authentication – Custom SAML Provider

Security Assertion interface

What is it?
- A component written in Java (for J2EE app servers) or c/c#/etc (for IIS) that will "speak" SAML and that MicroStrategy will use when the user's identity is needed.

How to customize?
- Use your preferred IDE to write the code.
- Register your SAML provider with MicroStrategy Server
- This is a way to leverage the same workflow than the standard SAML integration supports for all end-user MicroStrategy interfaces (Web, Mobile, Library, Desktop and Workstation)

SAML 2.0 Protocol

Identity Provider

Browser

Service Provider

GET
http://idp.example.com/realms/realms/realms

HTTP/1.1 302 Found
Location: http://idp.example.com/realms/realms

POST
SAML: Assertion

HTTP/1.1 302 Found
Location: http://idp.example.com/realms/realms

SAML: Assertion in HTML FORM

Digital Signature
Custom authentication support across user interfaces

<table>
<thead>
<tr>
<th></th>
<th>External Security Module</th>
<th>Custom Login Task</th>
<th>Web Server Filter</th>
<th>Custom SAML Provider</th>
</tr>
</thead>
<tbody>
<tr>
<td>MicroStrategy Web</td>
<td>Yes</td>
<td></td>
<td>Yes</td>
<td>Yes*</td>
</tr>
<tr>
<td>MicroStrategy Mobile</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>MicroStrategy Library</td>
<td></td>
<td></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>MicroStrategy Desktop</td>
<td></td>
<td></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>MicroStrategy Workstation</td>
<td></td>
<td></td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

* 10.6 or higher (J2EE; w/ 3rd party adapter for IIS)
Demo: MicroStrategy Web Login with a custom ESM
Custom External Security Module to interface with OAuth Identity Provider
Custom Authentication – Custom OAuth Provider
Demo implemented by MicroStrategy Professional Services Team

Environment:
• Service Provider (SP): MicroStrategy Web 10.4 running on a JSP server.
• Identity provider (IdP): Auth0.

Steps for creating a custom OAuth support for MicroStrategy Web:
1. Create a new plugin to extend MicroStrategy Web ESM.
2. Register MicroStrategy Web with your identity provider (Auth0).
3. Configure properties files with endpoints, application details, attributes.
Custom Authentication – Custom OAuth Provider

Demo implemented by MicroStrategy Professional Services Team
Custom Authentication – Custom OAuth Provider

Demo implemented by MicroStrategy Professional Services Team

1. Web Browser
2. MicroStrategy Web
   - Request the access token with the authorization code: /token POST
   - Response JSON with Bearer token
   - Extract the Bearer token from the JSON response: access_token
   - Retrieve the user information with Bearer access_token from profile endpoint
   - Response JSON with user info
   - Extract the trusted id from the JSON response: name
3. Auth0
4. MicroStrategy Intelligence Server
   - Establish Trusted Session with identified User
5. Session
   - Display requested MicroStrategy content
Custom Authentication – Custom OAuth Provider

Demo implemented by MicroStrategy Professional Services Team
What do we always forget about?
User management challenges

Authentication is only the tip of the iceberg:

- Provisioning (i.e. user and group creation)
- Update (e.g. group membership, name update, etc.)
- Decommission (i.e. user and group deletion)

Key to success: Automation
SSO in the three Key Target Scenarios for Embedded Analytics

Embed MicroStrategy content into custom applications and workflows

- Embed MicroStrategy content into a web page or application
- Embed data from MicroStrategy into an application
- Leverage MicroStrategy capabilities (SSO, Folders, …) in an application
- White label MicroStrategy functionalities

Integrate MicroStrategy platform into a custom product offering

- Automated deployment and upgrade of a MicroStrategy environment
- Programmatic user and security management
- Updating MicroStrategy cube data from 3rd party applications/workflows
- Programmatic object management

Extend MicroStrategy capabilities with 3rd party functionality (and vice versa)

- Connect new sources to MicroStrategy
- Add new visualizations to MicroStrategy
- Add new workflows to MicroStrategy
- Push new data and metadata to MicroStrategy
- Pull data from MicroStrategy and process in other systems (e.g. Machine Learning)
MicroStrategy 10 is Built as an **Open Architecture**

A comprehensive set of APIs allows you to integrate, embed, and extend the functionality of your existing investments.

---

**MicroStrategy Community for documentation, samples, etc.:** [https://community.microstrategy.com/s/topic/0TO44000000FliLGAS](https://community.microstrategy.com/s/topic/0TO44000000FliLGAS)
Where should you go next?
Remember, this is just a guideline! 😊

Today: Embedded Analytics track
Workshop: Embedding a dossier using REST and Embedding APIs

MicroStrategy Product Documentation for 3rd party authentication
https://www2.microstrategy.com/producthelp/10.10/WebAdmin/WebHelp/Lang_1033/Content/Enable_third-party_auth.htm

MicroStrategy API Documentation for custom authentication and every other API-related topic:  https://developer.microstrategy.com/