

salesforce

Identity and Access Management Designer

Virtual Fast Path

Ahmed Saad
Senior Manager, Partner Practice Development, APAC
ahmed.saad@salesforce.com



Forward-Looking Statement



Statement under the Private Securities Litigation Reform Act of 1995:

This presentation contains forward-looking statements about the company's financial and operating results, which may include expected GAAP and non-GAAP financial and other operating and non-operating results, including revenue, net income, diluted earnings per share, operating cash flow growth, operating margin improvement, expected revenue growth, expected current remaining performance obligation growth, expected tax rates, the one-time accounting non-cash charge that was incurred in connection with the Salesforce.org combination; stock-based compensation expenses, amortization of purchased intangibles, shares outstanding, market growth and sustainability goals. The achievement or success of the matters covered by such forward-looking statements involves risks, uncertainties and assumptions. If any such risks or uncertainties materialize or if any of the assumptions prove incorrect, the company's results could differ materially from the results expressed or implied by the forward-looking statements we make.

The risks and uncertainties referred to above include -- but are not limited to -- risks associated with the effect of general economic and market conditions; the impact of geopolitical events; the impact of foreign currency exchange rate and interest rate fluctuations on our results; our business strategy and our plan to build our business, including our strategy to be the leading provider of enterprise cloud computing applications and platforms; the pace of change and innovation in enterprise cloud computing services; the seasonal nature of our sales cycles; the competitive nature of the market in which we participate; our international expansion strategy; the demands on our personnel and infrastructure resulting from significant growth in our customer base and operations, including as a result of acquisitions; our service performance and security, including the resources and costs required to avoid unanticipated downtime and prevent, detect and remediate potential security breaches; the expenses associated with new data centers and third-party infrastructure providers; additional data center capacity; real estate and office facilities space; our operating results and cash flows; new services and product features, including any efforts to expand our services beyond the CRM market; our strategy of acquiring or making investments in complementary businesses, joint ventures, services, technologies and intellectual property rights; the performance and fair value of our investments in complementary businesses through our strategic investment portfolio; our ability to realize the benefits from strategic partnerships, joint ventures and investments; the impact of future gains or losses from our strategic investment portfolio, including gains or losses from overall market conditions that may affect the publicly traded companies within the company's strategic investment portfolio; our ability to execute our business plans; our ability to successfully integrate acquired businesses and technologies, including delays related to the integration of Tableau due to regulatory review by the United Kingdom Competition and Markets Authority; our ability to continue to grow unearned revenue and remaining performance obligation; our ability to protect our intellectual property rights; our ability to develop our brands; our reliance on third-party hardware, software and platform providers; our dependency on the development and maintenance of the infrastructure of the Internet; the effect of evolving domestic and foreign government regulations, including those related to the provision of services on the Internet, those related to accessing the Internet, and those addressing data privacy, cross-border data transfers and import and export controls; the valuation of our deferred tax assets and the release of related valuation allowances; the potential availability of additional tax assets in the future; the impact of new accounting pronouncements and tax laws; uncertainties affecting our ability to estimate our tax rate; the impact of expensing stock options and other equity awards; the sufficiency of our capital resources; factors related to our outstanding debt, revolving credit facility, term loan and loan associated with 50 Fremont; compliance with our debt covenants and lease obligations; current and potential litigation involving us; and the impact of climate change.

Further information on these and other factors that could affect the company's financial results is included in the reports on Forms 10-K, 10-Q and 8-K and in other filings it makes with the Securities and Exchange Commission from time to time. These documents are available on the SEC Filings section of the Investor Information section of the company's website at www.salesforce.com/investor.

Salesforce.com, inc. assumes no obligation and does not intend to update these forward-looking statements, except as required by law.



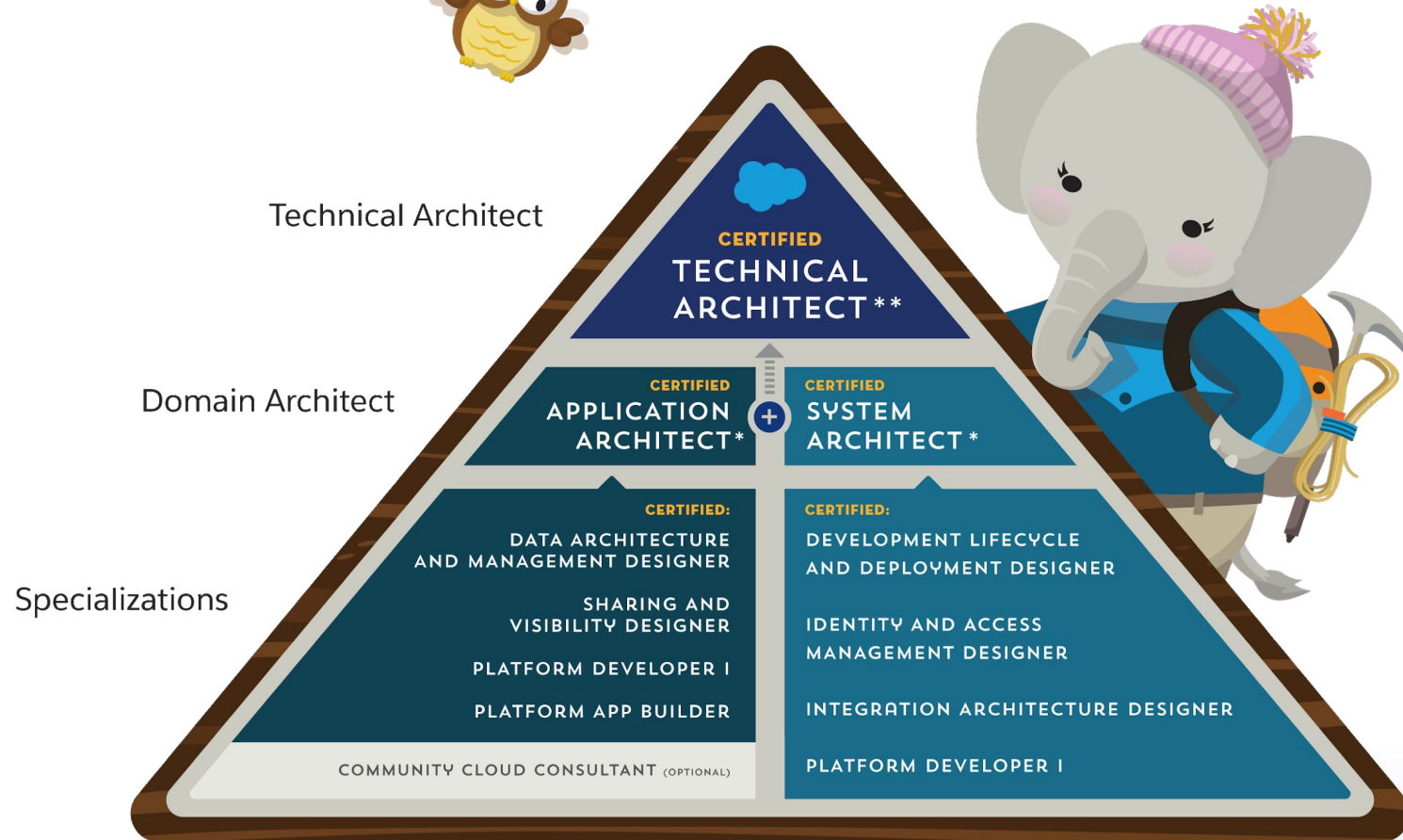
The Salesforce logo, which consists of a blue cloud-like shape with the word "salesforce" in white lowercase letters inside it.

salesforce

Introduction & Overview

A stylized illustration of a forest scene. On the right side, there are several tall, dark brown tree trunks. In the center, there are two green, triangular evergreen trees. The foreground features dark green bushes and small orange flowers. The background is a light blue sky with soft, white clouds.

The Road to the CTA Certification



Related Certification: Certified Administrator (optional)

* Credential earned upon completion of exams within the specializations tier, no additional exam requirements.

** Credential earned upon successful completion of the Domain Architect tier and Review Board.

Identity and Access Management Exam Overview



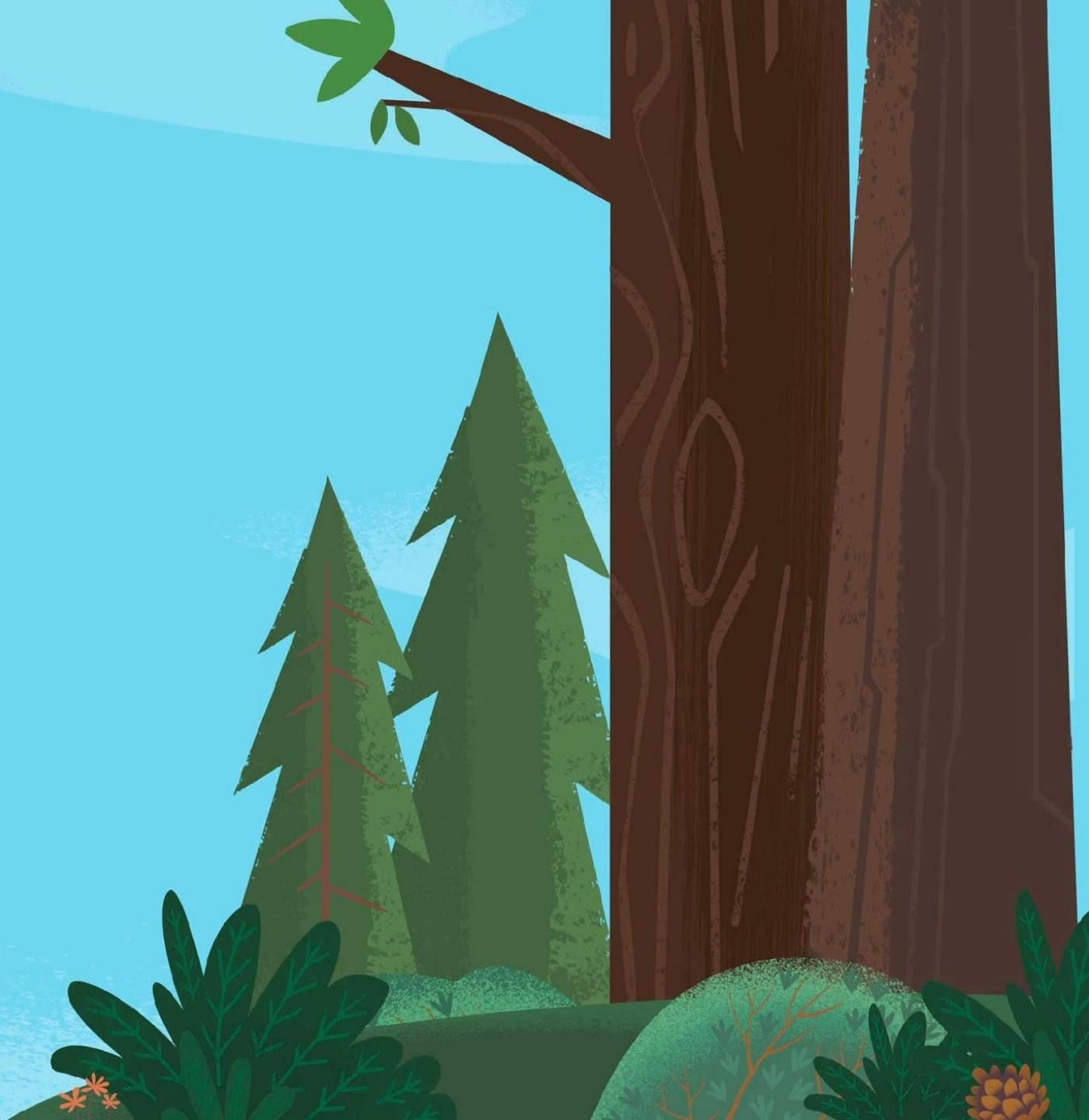
- Questions : 60
- Passing Score : 65%
- Duration 120 mins
- Trailmix: [Architect Journey: Identity and Access Management](#)



The Salesforce logo, which consists of a blue cloud-like shape with the word "salesforce" in white lowercase letters inside it.

salesforce

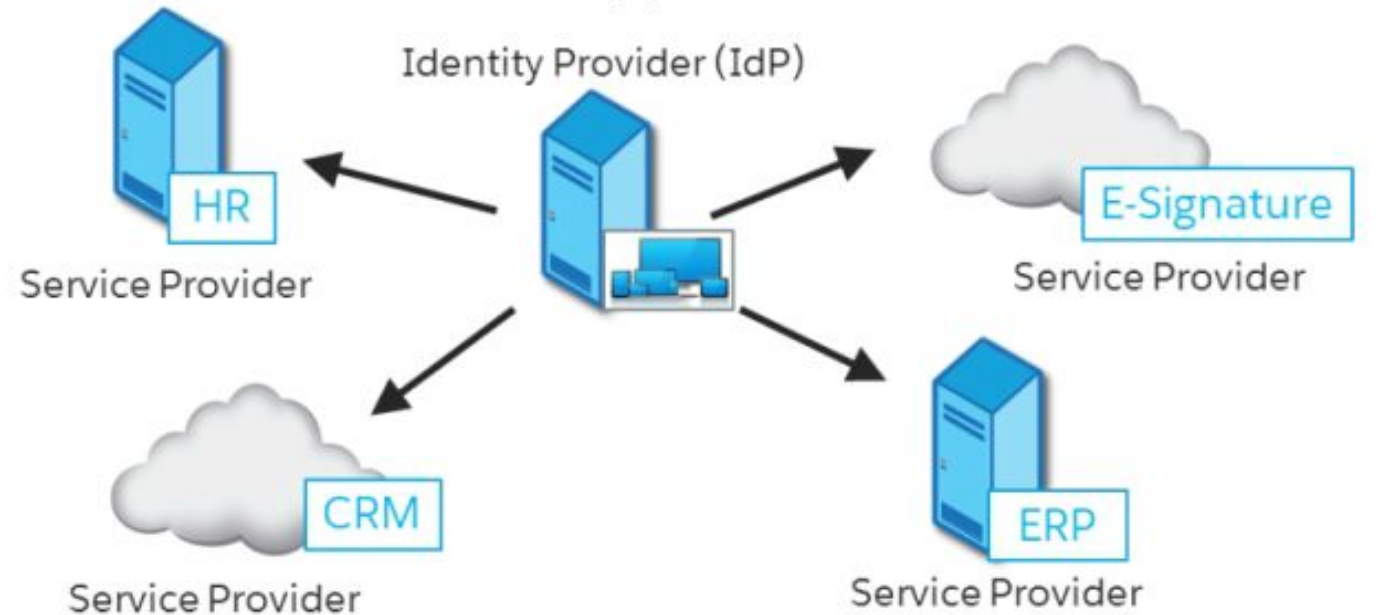
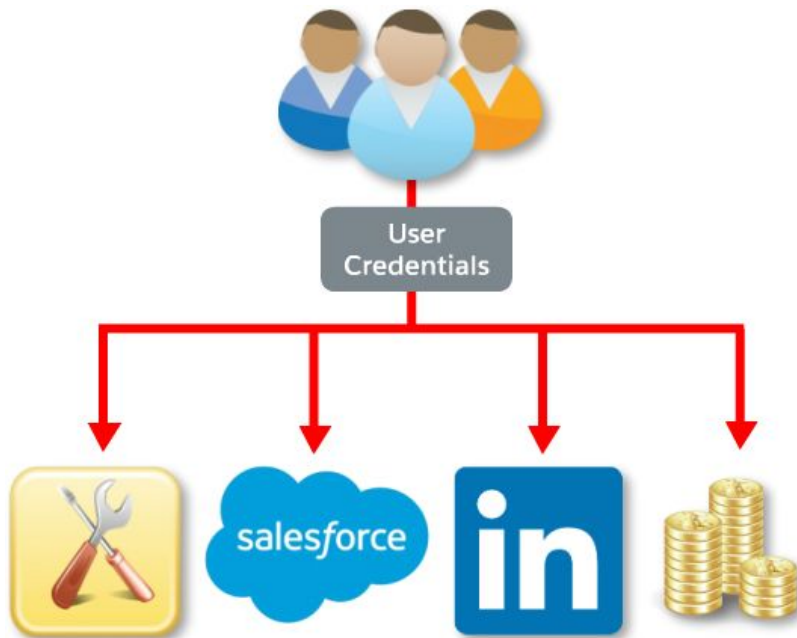
SSO & SAML



What is Single Sign-On (SSO)?



SSO is a process that allows network users to access all authorized networks without having to separately log in to each resource—one password fits all.



Salesforce Single Sign-On Architectures



Federated Authentication

- Uses SAML and industry standard protocols
- Is default form of single sign-on
- When enabled:
 - Salesforce does not validate user's password.
 - Platform receives an assertion in an HTTP POST

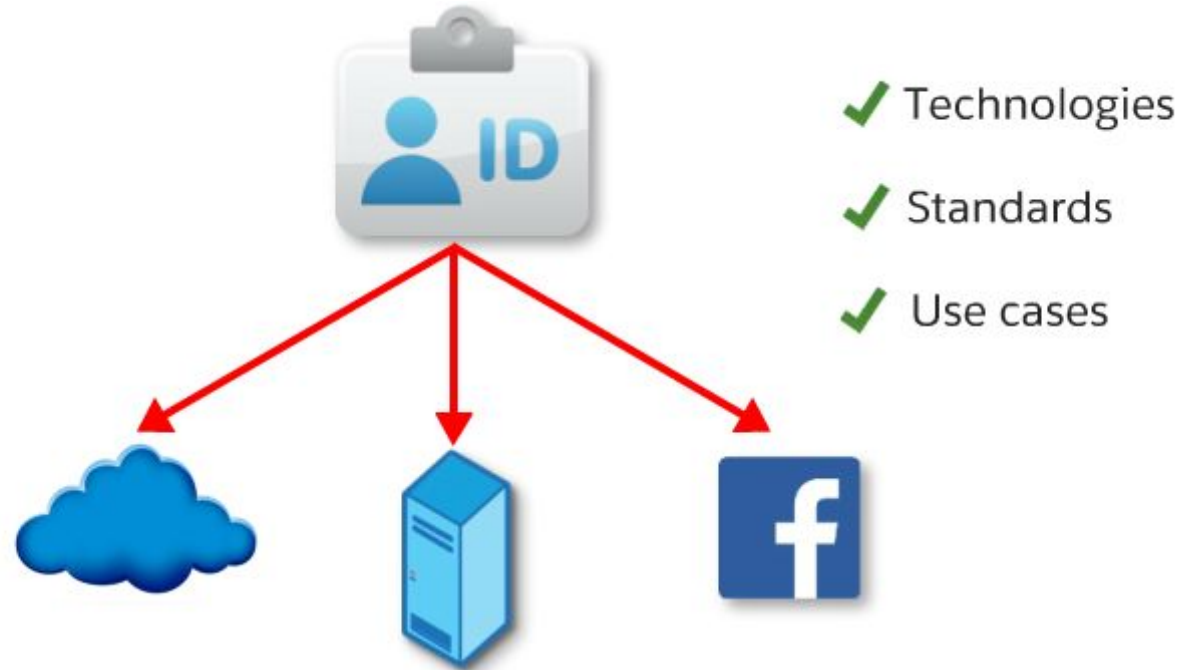
Delegated Authentication

- Is a Salesforce-specific technology
- When enabled:
 - Salesforce will make a Web service call to an external client to validate credentials.

- Send a request to Salesforce.com to enable delegated authentication.
- Many third-party tools on AppExchange can make the process of implementing single sign-on easier.



Federated Identity



Federated identity:

- Allows users of one domain to securely access data or systems of another domain seamlessly.
- Avoids redundant user administration.

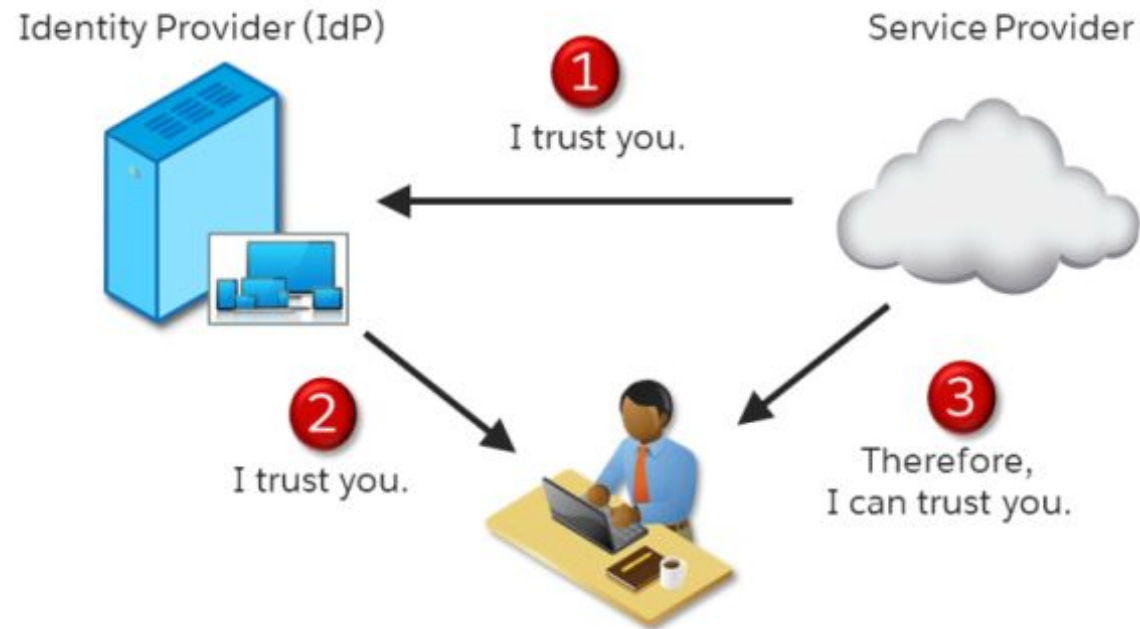


What is SAML?

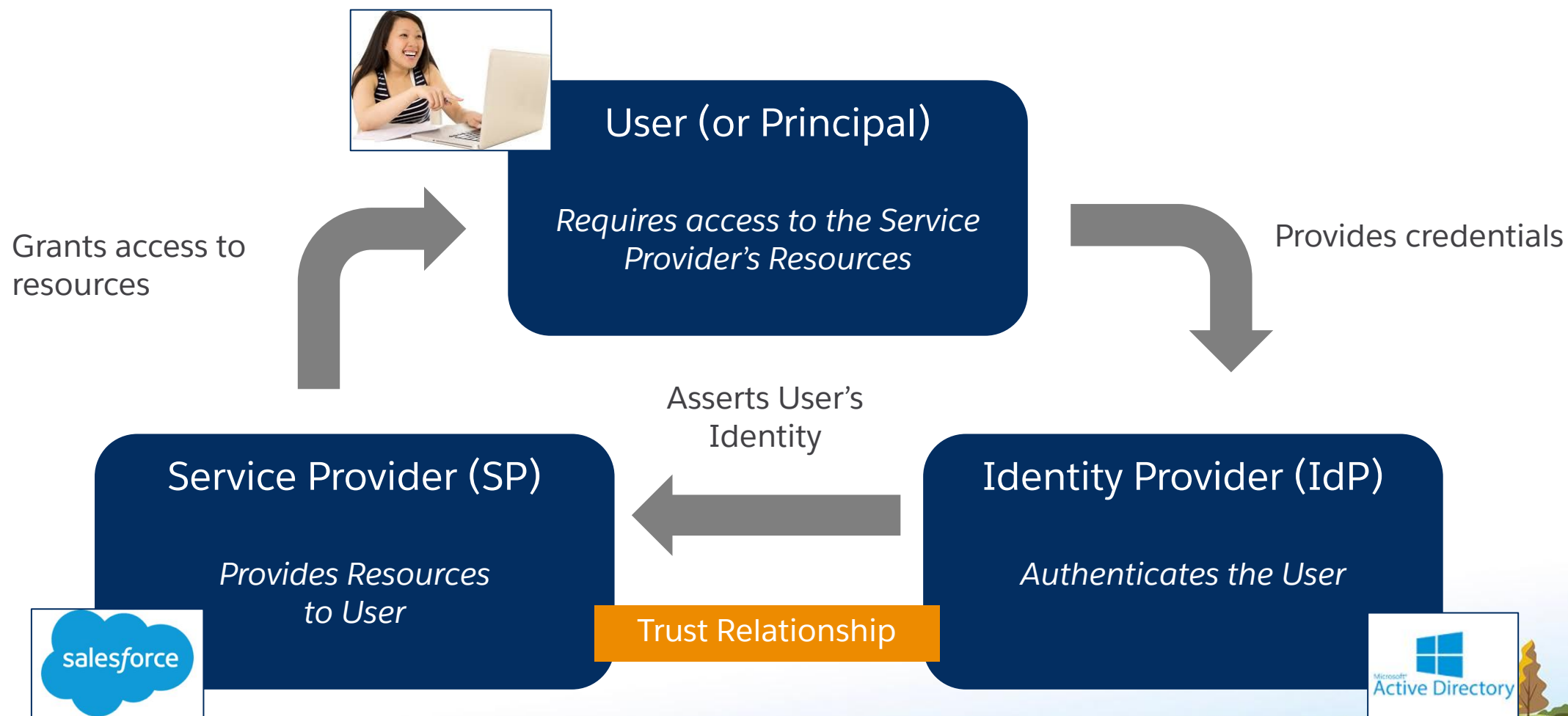


SAML is:

- An OASIS standard for single sign-on.
- Security Assertion Markup Language.
- XML-based.
- Designed to exchange authorization and authentication data.
- Trust-based.



SAML Components – The Three Parties



Trust Establishment



- Trust is established during SAML configuration.
- The IdP's public key certificate is stored on the service provider's system.
- The IdP includes its public key certificate with the service provider in its assertions.



- The service provider uses the certificate to validate that the digital signature originated from the IdP.
- No passwords are shared between the systems.



2 Types of SAML Flow



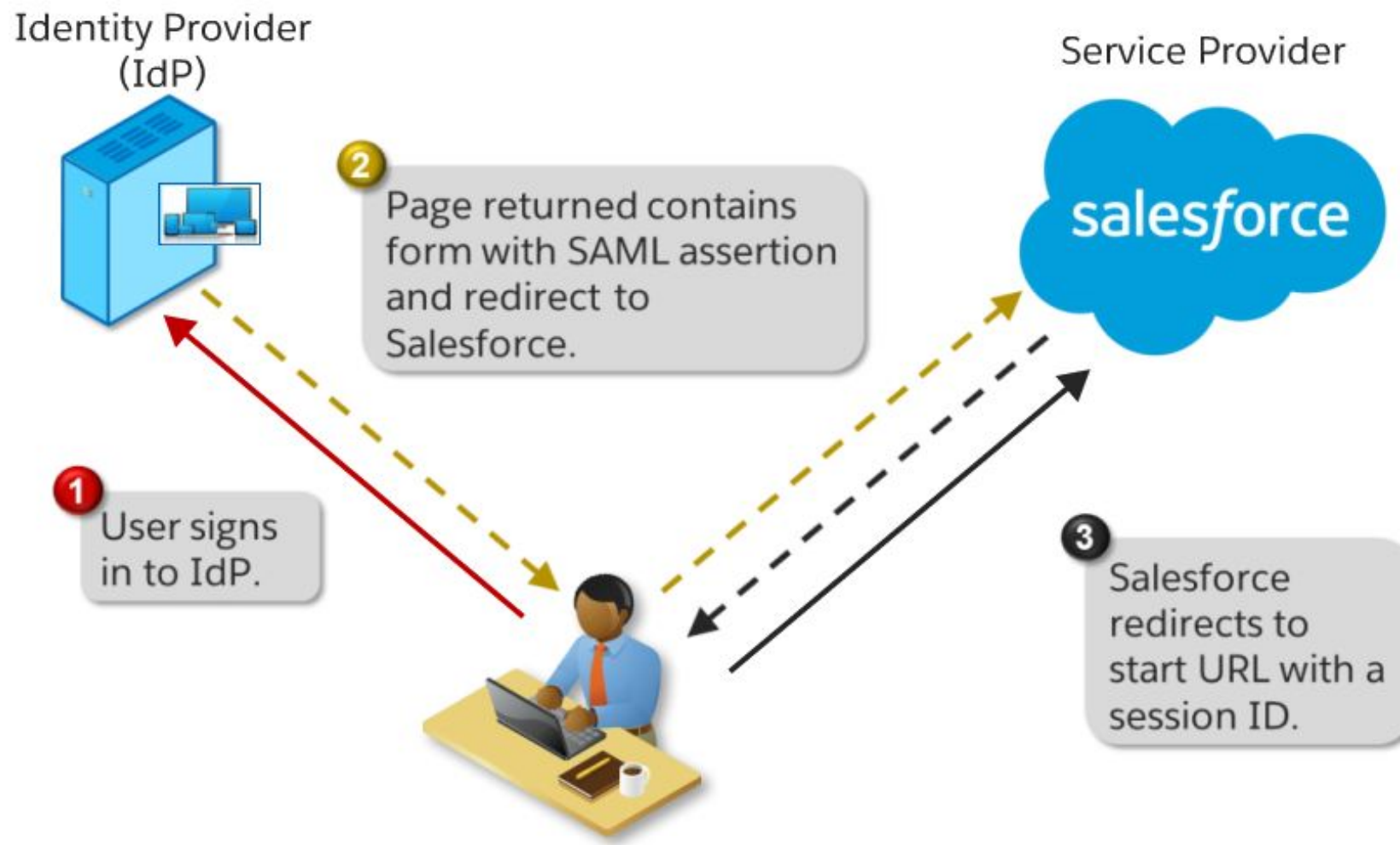
IdP sends an
unsolicited SAML
assertion to Salesforce



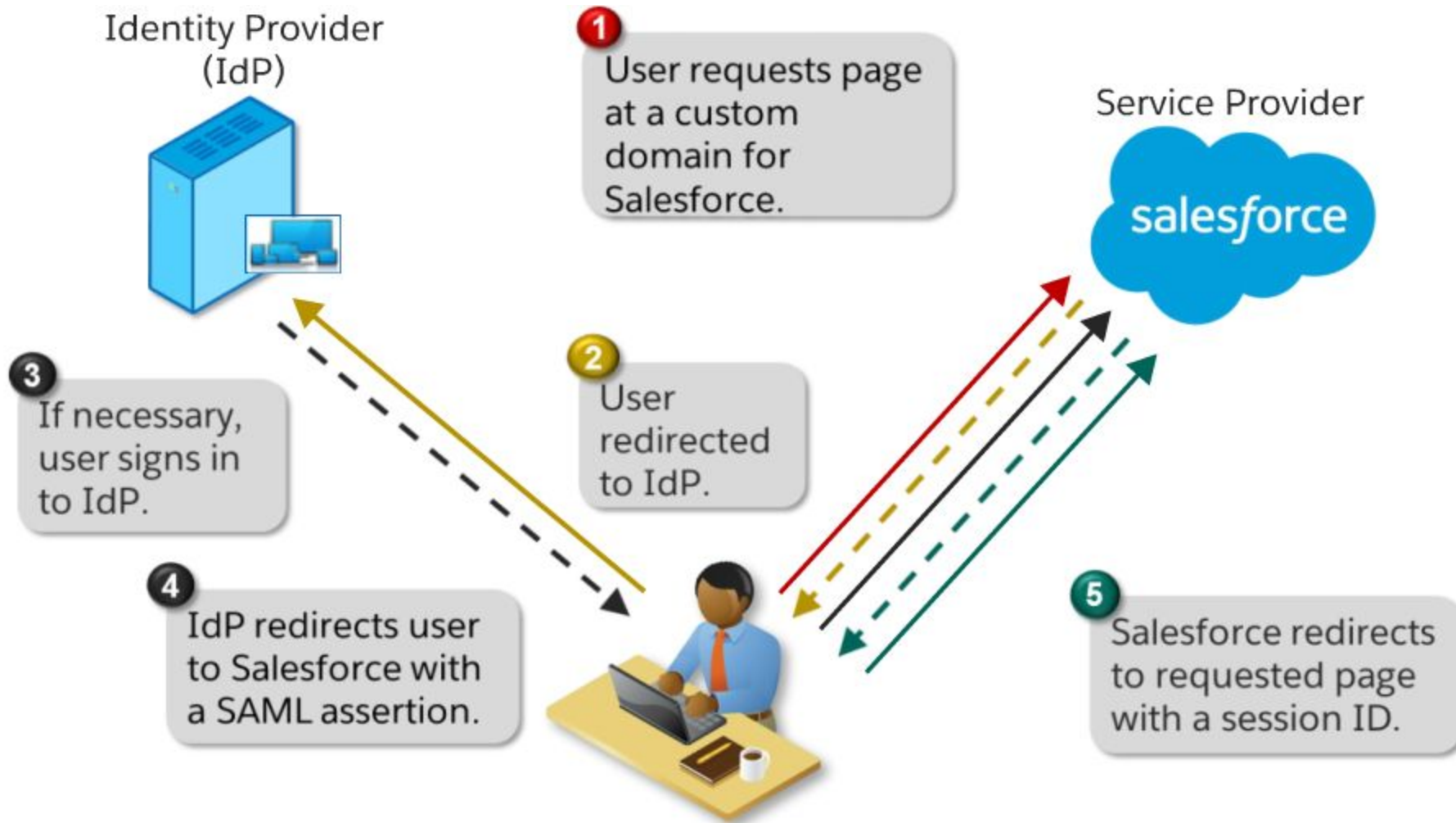
Starts with Salesforce, which
solicits a SAML assertion
from the IdP



IDP-Initiated SAML Flow



SP initiated SAML flow



How is SAML Secure?



SAML Security is based on the trust relationship between SP and IdP



IdP's Digital Certificate – uploaded to Salesforce



Assertion is signed with certificate – authenticates IdP and validates integrity of assertion



Use of HTTPS



Assertions can also be encrypted



Best Practice – SP Initiated Flow

Service provider initiated flow:

- Has the best user experience.
- Is required for using SSO with Salesforce mobile and desktop applications.
- Supports deep links.



Recommended Salesforce
best practice.

Customizing the Login Experience: My Domain



My Domain allows:

- Custom branding of URL.
- Redirection of users to an identity provider.
- Access to Salesforce through "deep links."

`https://universalcontainers.my.salesforce.com/`

The protocol

The subdomain prefix

The domain

My Domain Considerations:

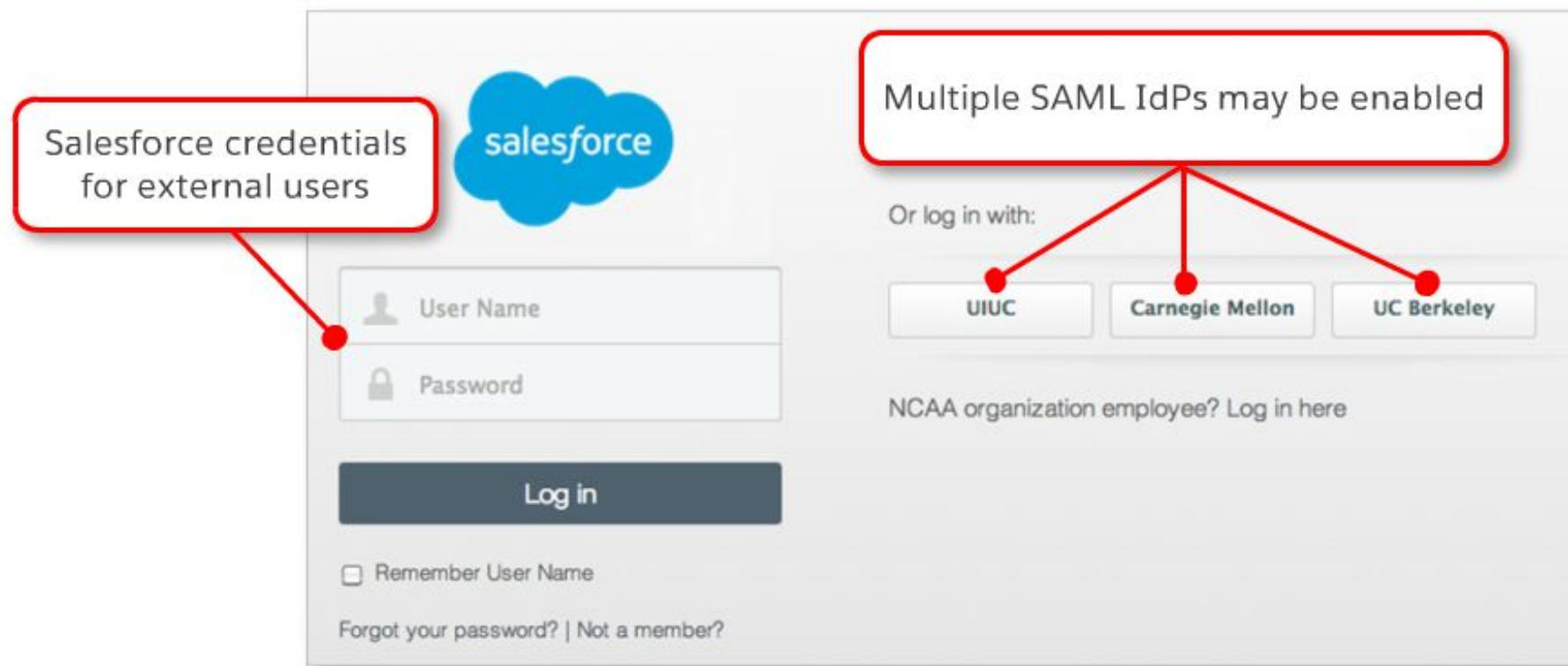
- My Domain deployment cannot be reversed.
- Each Salesforce org is only allowed one My Domain.
- Salesforce Communities have separate domains.



Advantages of Using My Domain with SAML



Enable multiple login options using My Domain with SAML for external users coming to Salesforce communities:

A screenshot of the Salesforce login page with several annotations. A red box on the left contains the text "Salesforce credentials for external users" with a red line pointing to the "User Name" and "Password" input fields. Another red box on the right contains the text "Multiple SAML IdPs may be enabled" with three red lines pointing to the "UIUC", "Carnegie Mellon", and "UC Berkeley" buttons. The login page itself features the Salesforce logo at the top left, followed by "User Name" and "Password" input fields, a "Log in" button, a "Remember User Name" checkbox, and links for "Forgot your password?" and "Not a member?". To the right of the login fields, there is a section titled "Or log in with:" followed by three buttons: "UIUC", "Carnegie Mellon", and "UC Berkeley". Below these buttons is a link that says "NCAA organization employee? Log in here".

Salesforce credentials for external users

Multiple SAML IdPs may be enabled

Or log in with:

UIUC Carnegie Mellon UC Berkeley

NCAA organization employee? Log in here

Log in

☐ Remember User Name

[Forgot your password?](#) | [Not a member?](#)

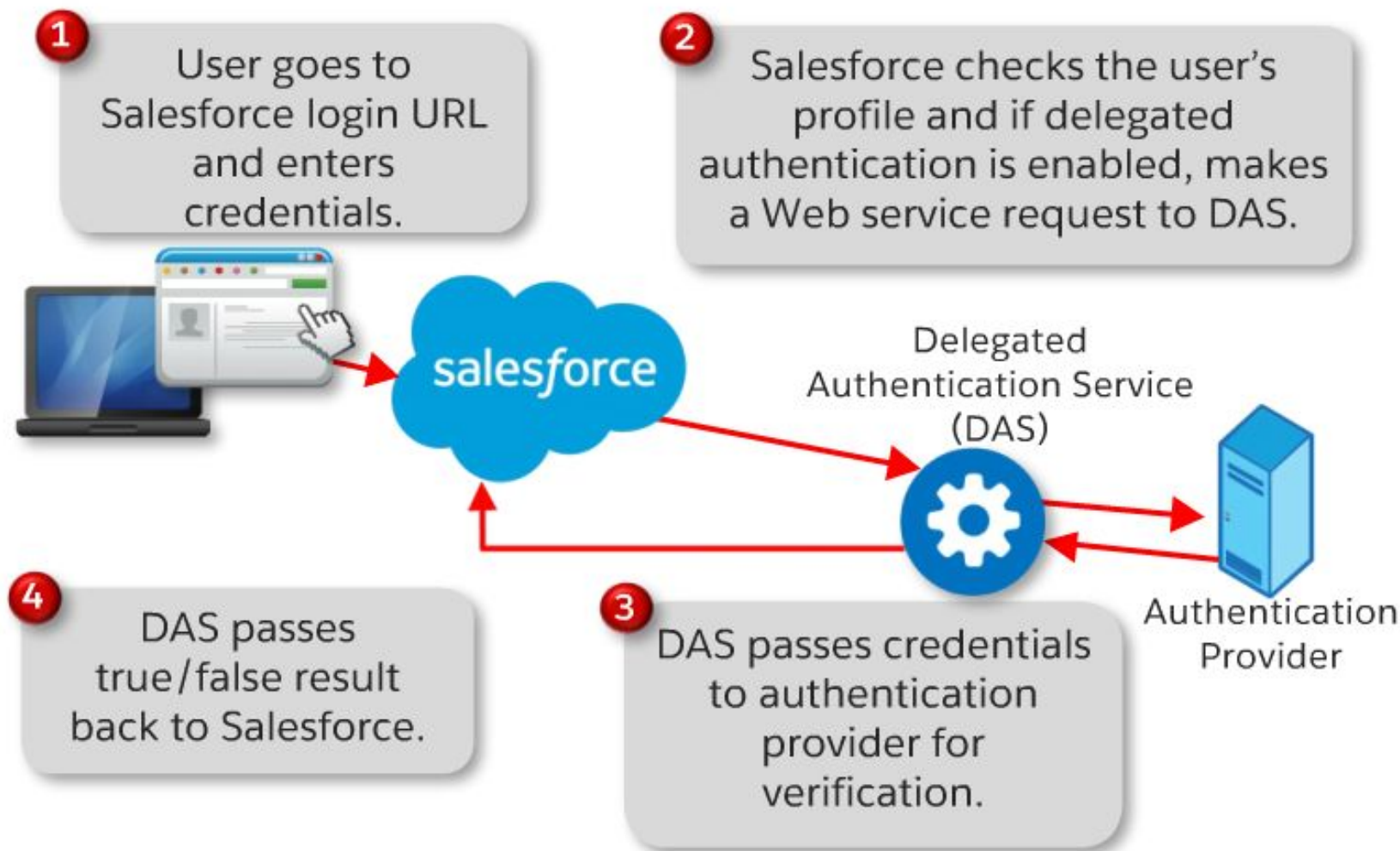
SAML with Multiple ORGs & Considerations



- Adding additional orgs to single sign-on with SAML is just configuration.
- Many possible topologies are available:
 - Single enterprise identity provider, multiple service provider orgs.
 - One org as identity provider, others as service provider.
- Delegated authentication is optional.
- Users may still log in through traditional methods.
- No proxy server required.



Delegated Authentication

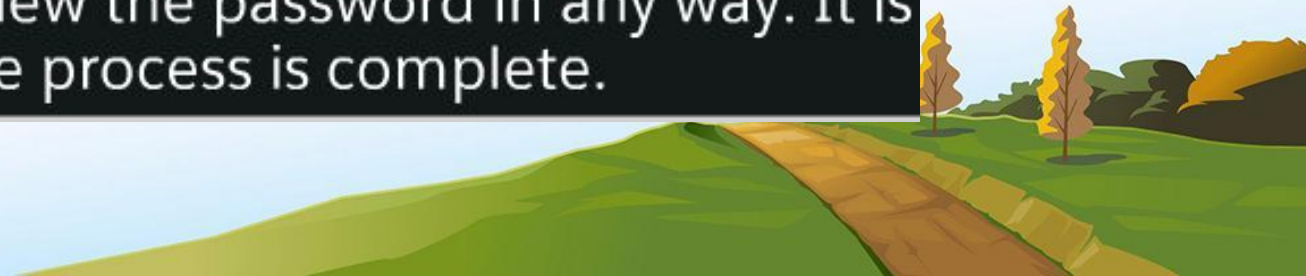


Delegated Authentication Considerations



- User credentials are encrypted and passed from Salesforce to DAS.
- Delegated authentication:
 - Activated at the profile level.
 - Requires a proxy server that Salesforce can access.
 - More cost for infrastructure and maintenance.
 - Requires a valid certificate if an SSL or HTTPS connection is used with the authentication service.

Salesforce doesn't store, log, or view the password in any way. It is disposed of immediately once the process is complete.



Salesforce As An Identity Provider

Identity Providers & Service Providers



- An **identity provider** is a trusted provider that lets you use single sign-on (SSO) to access other websites.
- A **service provider** is a website that hosts apps.
- You can enable Salesforce as an identity provider and define one or more service providers.
- Your users can then access other apps directly from Salesforce using SSO. SSO is a great help to your users—instead of having to remember many passwords, they only have to remember one.

USER PERMISSIONS NEEDED	
Define and modify identity providers and service providers:	Customize Application



Identity Providers & Service Providers (cont.)



- Enabling Salesforce as an identity provider requires a Salesforce certificate and key pair that's signed by an external certificate authority (CA-signed) or self-signed.
- If you haven't generated a Salesforce certificate and key pair, one is created for you when you enable Salesforce as an identity provider.
- Optionally, you can pick an existing generated certificate or create one yourself.
- Salesforce uses the SAML 2.0 standard for SSO and generates SAML assertions when configured as an identity provider.
- Before you can enable Salesforce as an identity provider, you must set up a subdomain with My Domain



Authenticate Apps With OAuth



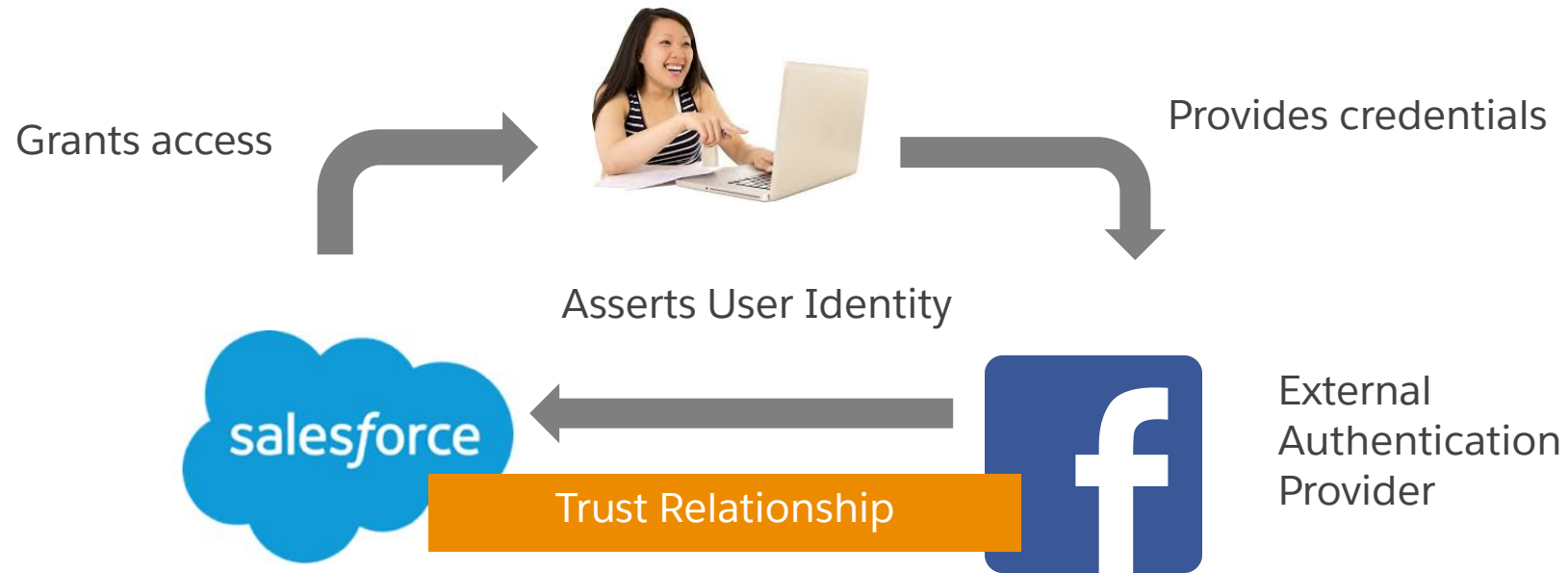
- When users request Salesforce data from within the external app (the consumer's page), Salesforce authenticates the user.
- The authentication flow consists of several steps, dictated by the OAuth standard and who is trying to access Salesforce

USER PERMISSIONS NEEDED	
To manage, create, edit, and delete OAuth apps:	Manage Connected Apps



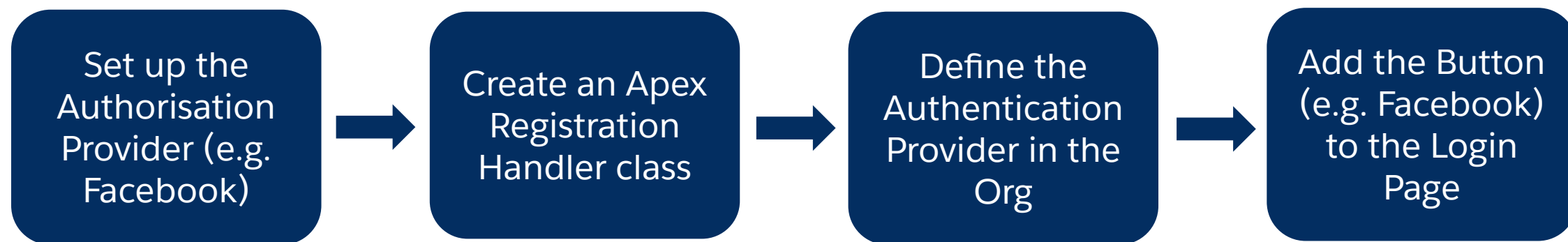
Authentication Providers

Authentication Providers Overview



An Apex registration handler class is required – to manage user provisioning

Setting Up an Authentication Provider



If the provider doesn't support OpenID Connect but does support OAuth, an Apex custom authenticator provider plug-in can be created



Authentication Providers



1. An authentication provider lets your users log in to your Salesforce org using their login credentials from an external service provider.
2. Salesforce provides authentication providers for apps that support the OpenID Connect protocol, such as Google, Facebook, Twitter, and LinkedIn.
3. For apps that don't support OpenID Connect, Salesforce provides an Apex `Auth.AuthProviderPluginClass` abstract class to create a custom authentication provider.

USER PERMISSIONS NEEDED	
To view the settings:	View Setup and Configuration
To edit the settings:	Customize Application AND Manage Auth. Providers

Configure Authentication Provider



Auth. Provider Edit Save Save & New Cancel

Provider Type	<input type="text" value="Salesforce"/>
Name	<input type="text"/>
URL Suffix	<input type="text"/>
Consumer Key	<input type="text"/> i
Consumer Secret	<input type="text"/> i
Authorize Endpoint URL	<input type="text" value="https://login.salesforce.com/services/oauth2/authorize"/> i
Token Endpoint URL	<input type="text" value="https://login.salesforce.com/services/oauth2/token"/> i
Default Scopes	<input type="text"/> i
Custom Error URL	<input type="text"/>
Custom Logout URL	<input type="text" value="https://www.salesforce.com"/> i
Registration Handler	<input type="text"/> i Automatically create a registration handler template
Execute Registration As	<input type="text"/> i
Portal	<input type="text" value="--None--"/>
Icon URL	<input type="text"/> Choose one of our sample icons

Save Save & New Cancel





Define Your Authentication Provider

Enable users to login to Salesforce organisation using external credentials

[Facebook](#)

[Google](#)

[LinkedIn](#)

[Microsoft Access Control Service](#)

[Salesforce](#)

[Twitter](#)

[Janrain](#)

[Amazon](#)

[Microsoft Azure AD](#)

In Addition :

[Any service provider who implements the OpenID Connect protocol](#)

[Any service provider who supports OAuth but not the OpenID Connect protocol](#)

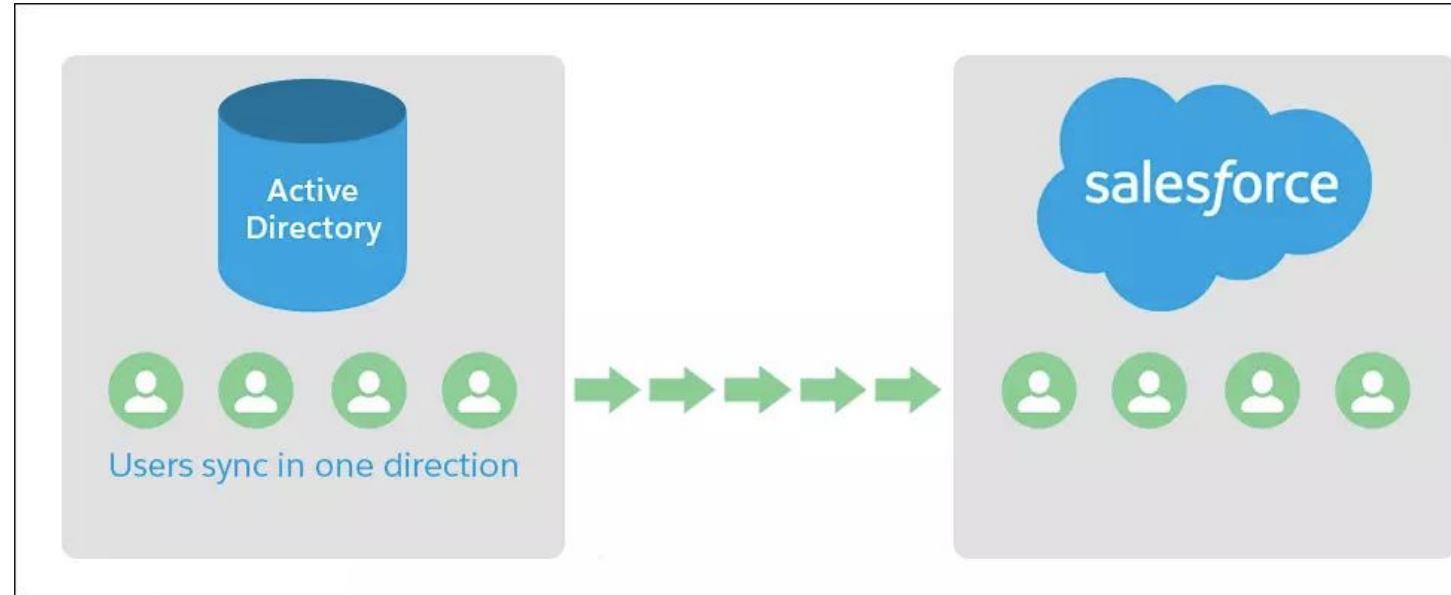


Salesforce Identity

Identity Connect



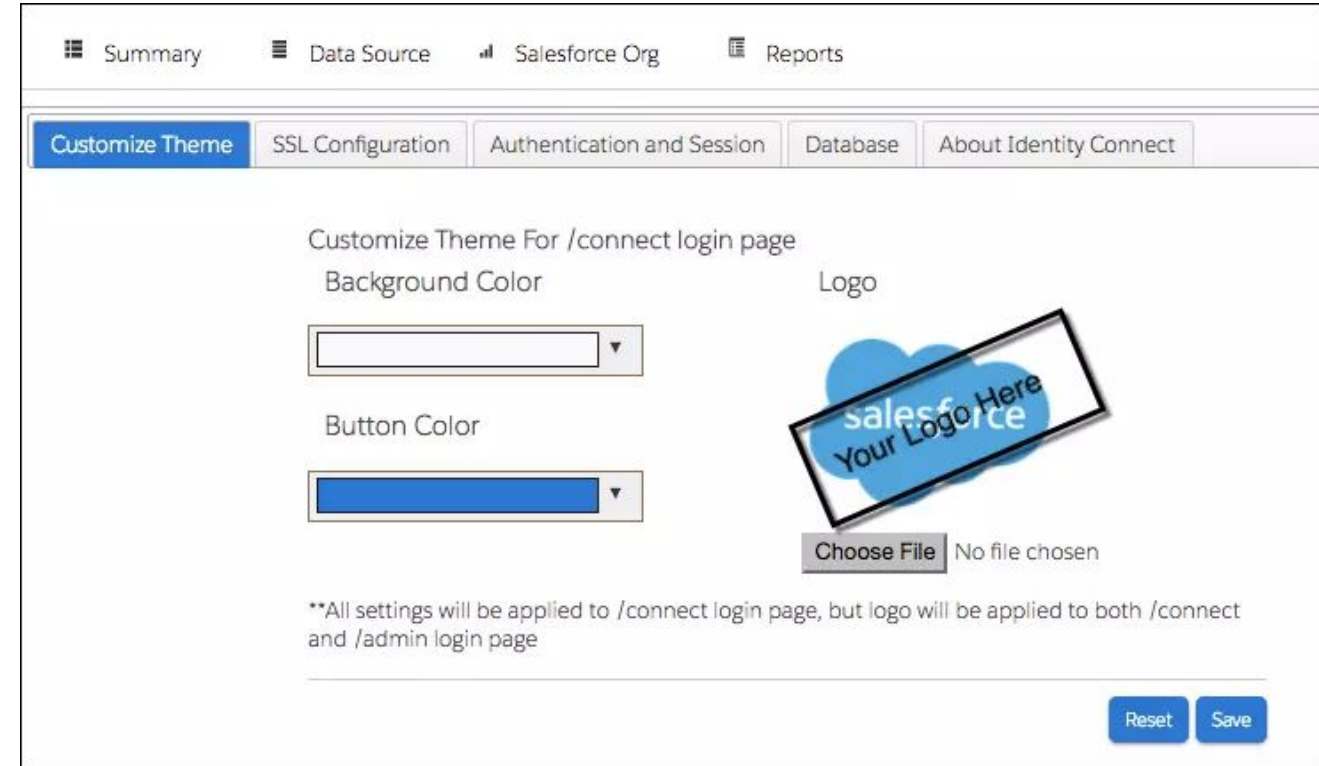
- Synchronise Salesforce with Active Directory
- Provision Users
- Single Sign-On
- Multiple Production Orgs
- Multiple Sandbox Orgs
- Can't manage mix of production with sandbox orgs
- Connects to Active Directory through LDAP or LDAPS & HTTPS



Identity Connect



- Add custom branding to login page
- Live updates catch
- Also enable scheduled updates in case in case Identity Connect or AD Server goes down to ensure nothing missed
- Scheduled should be daily or weekly as consumes more resources than live including REST API calls (org limits)
- Reconciliation Reporting available
- Use IC Login page with MyDomain
- Disable Salesforce passwords to force AD

A screenshot of the 'Customize Theme' configuration page in the Identity Connect interface. The page has a top navigation bar with 'Summary', 'Data Source', 'Salesforce Org', and 'Reports'. Below this is a sub-navigation bar with 'Customize Theme' (selected), 'SSL Configuration', 'Authentication and Session', 'Database', and 'About Identity Connect'. The main content area is titled 'Customize Theme For /connect login page'. It contains two color selection fields: 'Background Color' (a white box with a dropdown arrow) and 'Button Color' (a blue box with a dropdown arrow). To the right of these fields is a 'Logo' section showing a preview of a blue cloud logo with the text 'salesforce Here Your Logo'. Below the preview is a 'Choose File' button and the text 'No file chosen'. At the bottom of the page, there is a disclaimer: '**All settings will be applied to /connect login page, but logo will be applied to both /connect and /admin login page'. At the bottom right, there are 'Reset' and 'Save' buttons.

Summary Data Source Salesforce Org Reports

Customize Theme SSL Configuration Authentication and Session Database About Identity Connect

Customize Theme For /connect login page

Background Color

Button Color

Logo

Choose File No file chosen

**All settings will be applied to /connect login page, but logo will be applied to both /connect and /admin login page

Reset Save

Identity Connect Licensing



- Identity Connect is an add-on license available for Salesforce users on most Salesforce products
 - Salesforce platform
 - Sales Cloud
 - Service Cloud
 - Analytics Cloud
 - Identity for Employees.

NOTE : There is no extra charge for installing on multiple servers (eg. Load balancing when a domain controller is being used) as licensing is per user and not per CPU (unlike competing products)



Identity Licensing



Identity Licensing and where they can be used

License Type

Description

Where can it be used ?

Identity

Grants users access to Salesforce Identity features. Salesforce Identity connects Salesforce users with external applications and services, while giving administrators control over authentication and authorization for these users.

For more information, see the [Salesforce Identity Implementation Guide](#).

Enterprise, Unlimited, Performance, and Developer Editions
Ten free Identity user licenses are included with each new Developer Edition organization.

External Identity

Provides Identity features for users outside of your organization's user base (such as non-employees). Store and manage these users, choose how they authenticate (username/password, or Single Sign-On social sign-on through Facebook, Google+, LinkedIn, and others), and allow self-registration.

Enterprise, Unlimited, Performance, and Developer Editions
Five free External Identity user licenses are included with each new Developer Edition organization.



Communities : Partner & Customers



- Enable self-registration to allow unlicensed guest users to join your community.
- When your users self-register, you can choose to save them as contacts under a business account or create a person account for each self-registering user.

USER PERMISSIONS NEEDED

To create, customize, or publish a community:

Create and Set Up Communities AND View Setup and Configuration



NOTE You can specify [dynamic branding](#) URLs when you customize the self-registration form. This way, you can control which registration form a user sees depending on who is accessing the community and from where.



User Provisioning

Provisioning External Community Users

Customers Or Partners

- Programmatic (SOAP/REST API)
- SAML JIT
- Social Sign On
- Identity Connect
- User Provisioning for Connected Apps
- Data Loader
- Bulk API



Programmatic Options SOAP / REST / BULK



- Individual record creation – REST & SOAP
 - Using the User Object – associate to a valid Contact & Account
 - Enable Partner User / Enable Customer User
 - `createPortalUser(user, accountId, password)`, `createPersonAccountPortalUser(user, ownerId, password)`
- Bulk API
 - `createPortalUser`
 - `createPersonAccountPortalUser`
 - 10,000 users owner limit



SAML Just-In-Time Provisioning



- Use a SAML assertion to create regular and portal users on the fly the first time they try to log in.
- This eliminates the need to create user accounts in advance
- Benefits
 - Reduced Administrative Costs – accounts created on-demand
 - Increased User Adoption – single password to remember
 - Increased Security – password policies, single use auth credentials, etc



Just-in-Time Provisioning for SAML



- With Just-in-Time provisioning, you can use a SAML assertion to create regular and portal users on the fly the first time they try to log in. This eliminates the need to create user accounts in advance.
- For example, if you recently added an employee to your organization, you don't need to manually create the user in Salesforce. When they log in with single sign-on, their account is automatically created for them, eliminating the time and effort with on-boarding the account.
- Just-in-Time provisioning works with your SAML identity provider to pass the correct user information to Salesforce in a SAML 2.0 assertion. You can both create and modify accounts this way.
- Because Just-in-Time provisioning uses SAML to communicate, your organization must have SAML-based single sign-on enabled.



Just-in-Time Provisioning



- Just-in-time (JIT) provisioning uses attributes in the SAML assertion to create and update user records in Salesforce.
- The SAML assertion must provide (at least):
 - Email
 - LastName
 - UserName
 - ProfileId - 15 character ID or profile name
- It can also include any other optional attributes, such as:
 - FirstName
 - Phone
 - Manager



Access Management Concepts

Login Hours



- You can restrict the hours during which users can log in and the range of IP addresses from which they can log in and access Salesforce.
- If IP address restrictions are defined for a user's profile and a login originates from an unknown IP address, Salesforce does not allow the login.
- These restrictions help protect your data from unauthorized access and phishing attacks.



IP Ranges / Org-Wide Trusted IP Ranges



- For all users, you can set a list of IP address ranges from which they can always log in without receiving a login challenge
- You can restrict all access to Salesforce to the IP addresses included in Login IP Ranges in users' profiles



Login Flows



- A login flow directs users through a login process before they access your Salesforce org or community.
- You can use a login flow to control the business processes that your users follow when they log in to Salesforce.
- After Salesforce authenticates a user, the login flow directs the user through a process, such as enforcing strong authentication or collecting user information.
- When users complete the login flow successfully, they are redirected to their Salesforce org or community.
- If unsuccessful, the flow can log out users immediately.



Two-Factor Authentication



- Two-factor authentication is the most effective way to protect your org's user accounts. Admins enable two-factor authentication through permissions or profile settings.
- Users register for two-factor authentication through their own personal settings, using secondary authenticators such as mobile authenticator apps or U2F security keys.



High Assurance Sessions



To secure different setup areas in your org, require a high-assurance level of security for sensitive operations, like accessing reports and managing IP addresses.

You can also block users from accessing these setup areas.

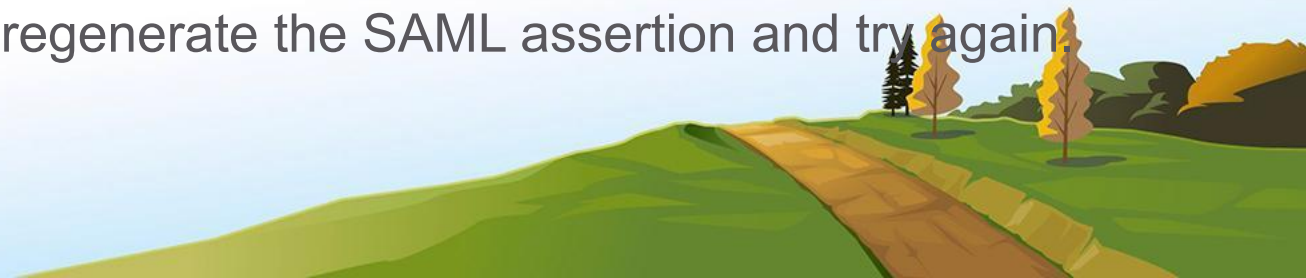
User Permissions Needed	
To modify session security settings:	Customize Application



Troubleshooting SAML



- In Salesforce, from Setup, enter Single Sign-On Settings in the Quick Find box, then select **Single Sign-On Settings**.
- Click **SAML Assertion Validator**. The SAML Validator shows the last recorded SAML login failure with some details as to why it failed.
- To test the SAML assertion from the Axiom app, copy the **Formatted SAML Response** from the Axiom app.
- In the Salesforce SAML Validator, paste the SAML assertion in the **SAML Response** box at the bottom of the page.
- Click **Validate**. The page displays some results to help you troubleshoot the assertion. For example, if the assertion was generated a while before it was used to log in, the timestamp expires and the login isn't valid. In that case, regenerate the SAML assertion and try again.



Connected Apps

Connected Apps



An application enabling an OAuth request to Salesforce must be registered as a **Connected App**.

- Provides a consumer secret key to be used by the external application.

Connected App framework provides:

- Security controls for who may access the applications.
- OAuth Scope controls.
- OAuth policies for system behavior when user reconnects.
- SAML service provider settings (optional).
- Mobile application policy settings to enable screen locking and PIN protection (optional).



Configure Connected App



To publish an app, you need to be using a Developer Edition organization with a namespace prefix chosen.

Basic Information

Connected App Name

API Name

Contact Email

Contact Phone

Logo Image URL

Icon URL

Info URL

Description

Upload logo image or Choose one of our sample logos

Choose one of our sample logos

Required Information

API (Enable OAuth Settings)

Enable OAuth Settings

Callback URL

Use digital signatures

Selected OAuth Scopes

Available OAuth Scopes

Access and manage your Chatter data (chatter_api)

Access and manage your data (api)

Access custom permissions (custom_permissions)

Access your basic information (id, profile, email, address, phone)

Allow access to your unique identifier (openid)

Full access (full)

Perform requests on your behalf at any time (refresh_token, offline_access)

Provide access to custom applications (visualforce)

Provide access to your data via the Web (web)

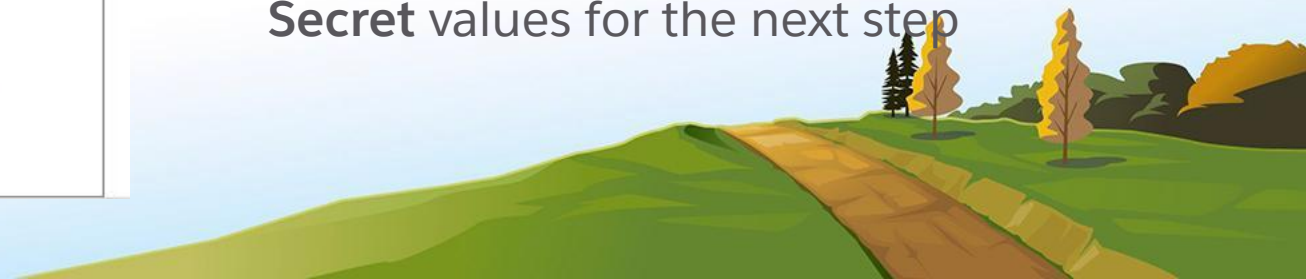
Add

Remove

Selected OAuth Scopes

--None--

- **Connected Name:** Choose your own, e.g. *AdvisoryOrg*
- **API Name:** Choose your own, e.g. *AdvisoryOrg*
- **Contact Email:** Any valid email
- **Callback URL:** Paste the value from the Authentication Provider in the previous step
- **Selected OAuth Scopes:** Select *Access and manage your data (api)* and *Perform requests on your behalf at any time (refresh_token, offline_access)*
- Copy the **Consumer Key** and **Consumer Secret** values for the next step



Named Credentials

And Why Should I Care


- Introduced in Spring 15 Release
- Allows you to store an endpoint URL and its credentials (OAuth or Username/Password) and reuse in Apex code without writing any authentication code!
- Easier and more secure to use versus storing credentials in code or custom settings
 - No Remote Site settings required
 - Passwords, Access Tokens and Refresh Tokens are stored behind the scenes and not visible in the Salesforce UI
 - Can be secured via Profiles and Permission Sets




Configure Named Credential




Save Cancel

Label 

Name 


URL

▼ Authentication

Certificate 

Identity Type

Authentication Protocol

Authentication Provider 

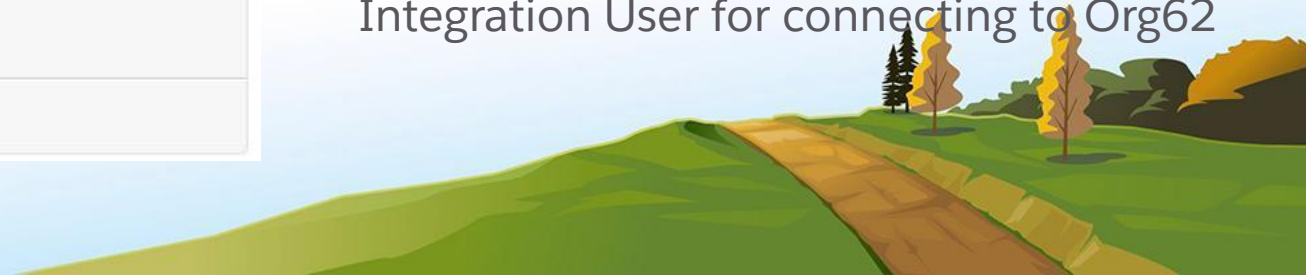
Scope

Authentication Status Pending

Start Authentication Flow on Save ☐

Save Cancel

- **Label/Name:** Enter an appropriate value, e.g. *Org62APIUser*
- **URL:** Enter the base endpoint URL, e.g. *https://org62.my.salesforce.com*
- Paste the values for **Consumer Key** and **Consumer Secret** from the previous step into the corresponding fields
- Enter *api refresh_token* into the **Default Scopes** field as shown to the left
- **Authentication Provider:** Select the one you created earlier
- Check **Start Authentication Flow on Save** box and when you save the record, it will start the OAuth flow to log you into your target org. In this case, we have an Integration User for connecting to Org62



OAuth

What is OAuth?



OAuth 2.0, provides authorization which:

- Allows an application to access Force.com resources on a user's behalf.
- Does not reveal a user's password or other credentials to those applications.
- Is an open protocol that allows a user to authorize one site to access another site on behalf of the user.
- Has two main roles:
 - Service provider: Salesforce
 - Service consumer: External applications
- Is often known as a valet key.
- Can be used with single sign-on.



OAuth Advantages



- Simple:
 - Protocol is HTTP based
 - Interfaces already exist
- Additionally:
 - Works great for mobile
 - Reduces the security and management issues with passwords



OAuth Overview and Terminology



Client

Application that requires access to resources on the Resource Server.

Client applications must be pre-registered by the authorisation server.

Authenticates and authorises access

grants



Access Token

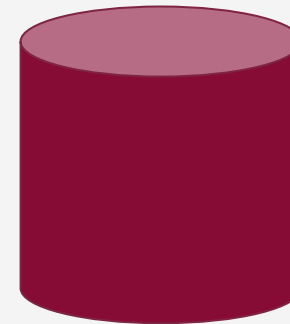
A token used to access protected resources

Used to access



Authorisation Server

A server which issues access tokens after successfully authenticating a client and resource owner, and authorizing the request



Resource Server

A server which sits in front of protected resources and provides an API that accepts and responds to protected resource requests using access tokens

OAuth Tokens



Access Token

Used to access protected resources.
Expire after session timeout.

Submitted with REST API requests in `access_token` value in the header.

Granted with OAuth authorisation flows.

Generally have a finite lifetime.



Refresh Token

Long lived token that is used to get a new access token, after the original one has expired.

Scopes (Connected App Config)

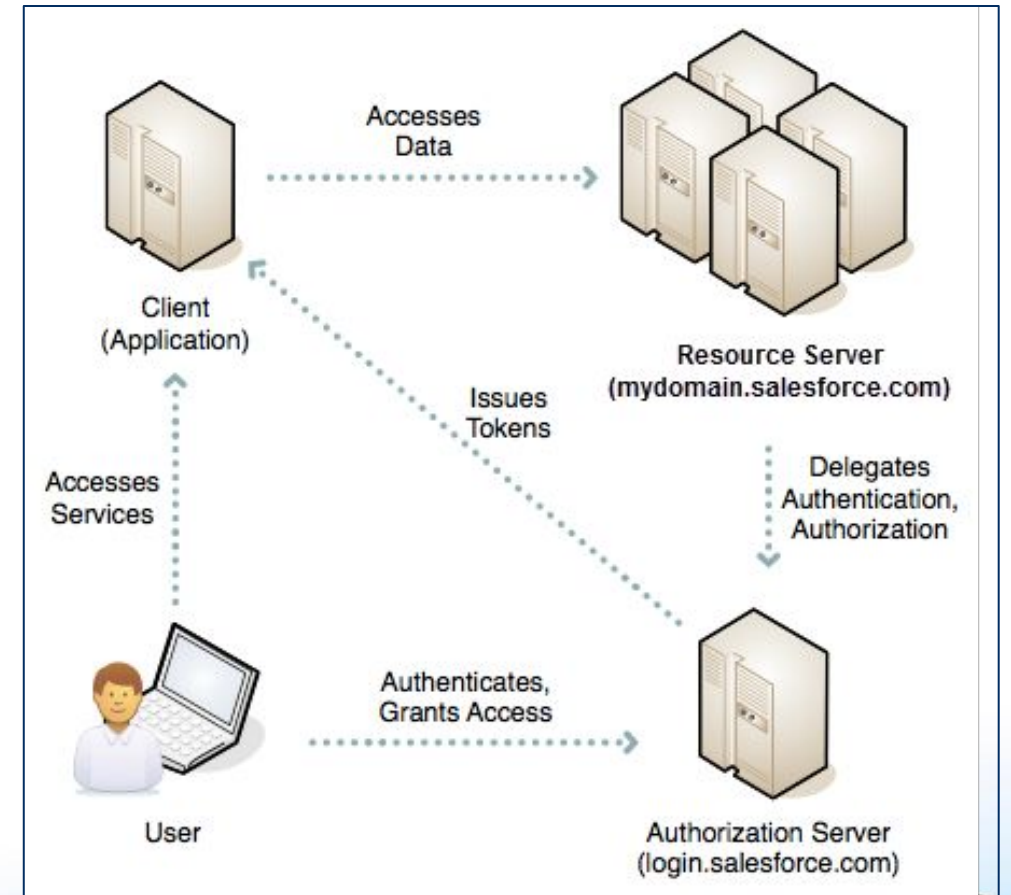
Available OAuth Scopes

- Access and manage your Chatter data (chatter_api)
- Access and manage your data (api)
- Access custom permissions (custom_permissions)
- Access your basic information (id, profile, email, address, phone)
- Allow access to your unique identifier (openid)
- Full access (full)
- Perform requests on your behalf at any time (refresh_token, offline_access)
- Provide access to custom applications (visualforce)
- Provide access to your data via the Web (web)

OAuth Basics



- OAuth is sometimes described as a valet key for the web.
- A valet key restricts access to a car. A person can drive it, but can't use the key to open the trunk or glove box.
- In the same way, OAuth gives a client application restricted access to your data on a resource server.
- To allow access, an authorization server grants tokens to the client app in response to an authorization.



OAuth Flows Overview

User Agent Flow

Mobile, Desktop and JavaScript applications

Web Server Flow

Apps hosted on secure web servers

SAML

Combines OAuth with SAML SSO

Refresh

Retrieve a new token after expiry

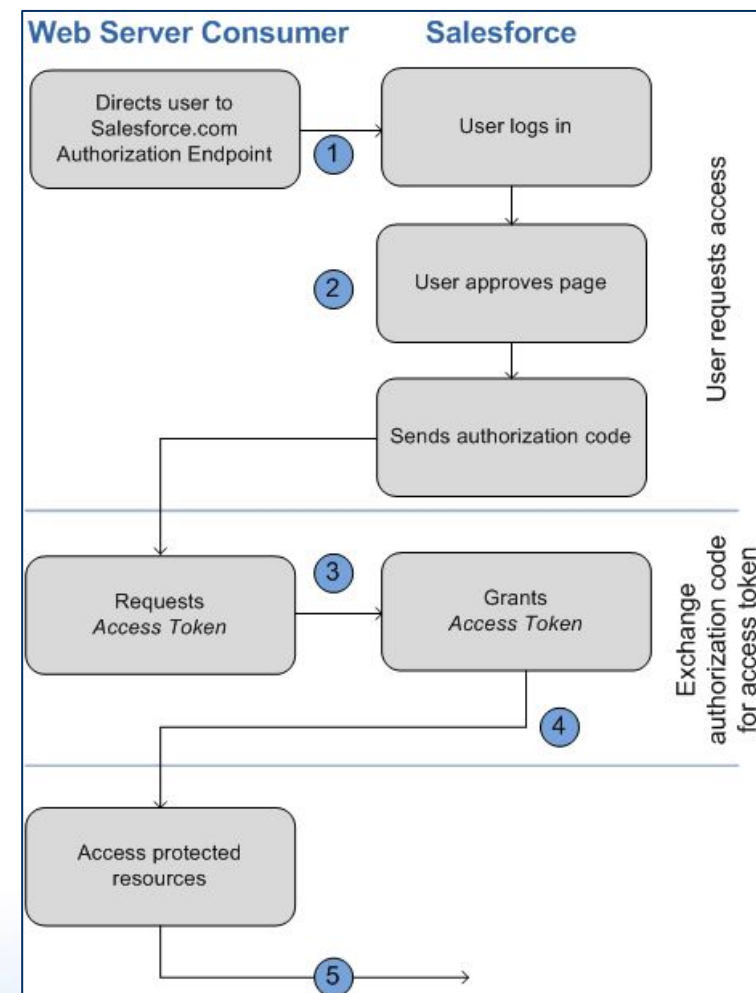
Username/Password Flow

Only where no other flow is possible

OAuth 2.0 Web Server Authentication Flow



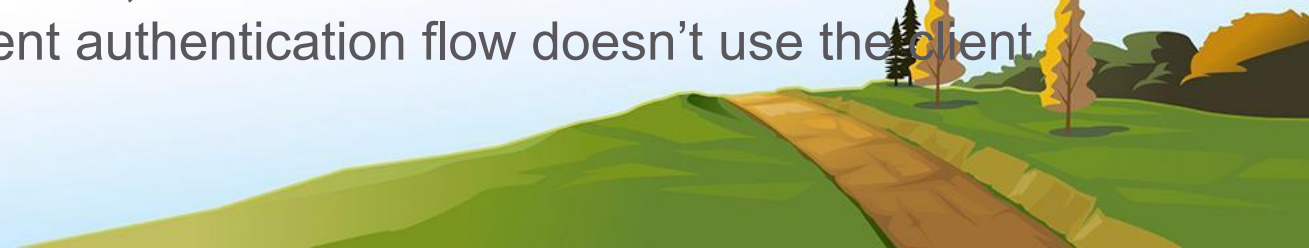
1. The web server redirects the user to Salesforce, which authenticates and authorizes the server to access the data on the user's behalf.
2. After the user approves access, the web server receives a callback with an authorization code.
3. The web server passes back the authorization code to get a token response.
4. After validating the authorization code, Salesforce passes back a token response. If there's no error, the token response includes an access code and additional information.
5. After the token is granted, the web server accesses the user's data.



OAuth 2.0 User-Agent Flow

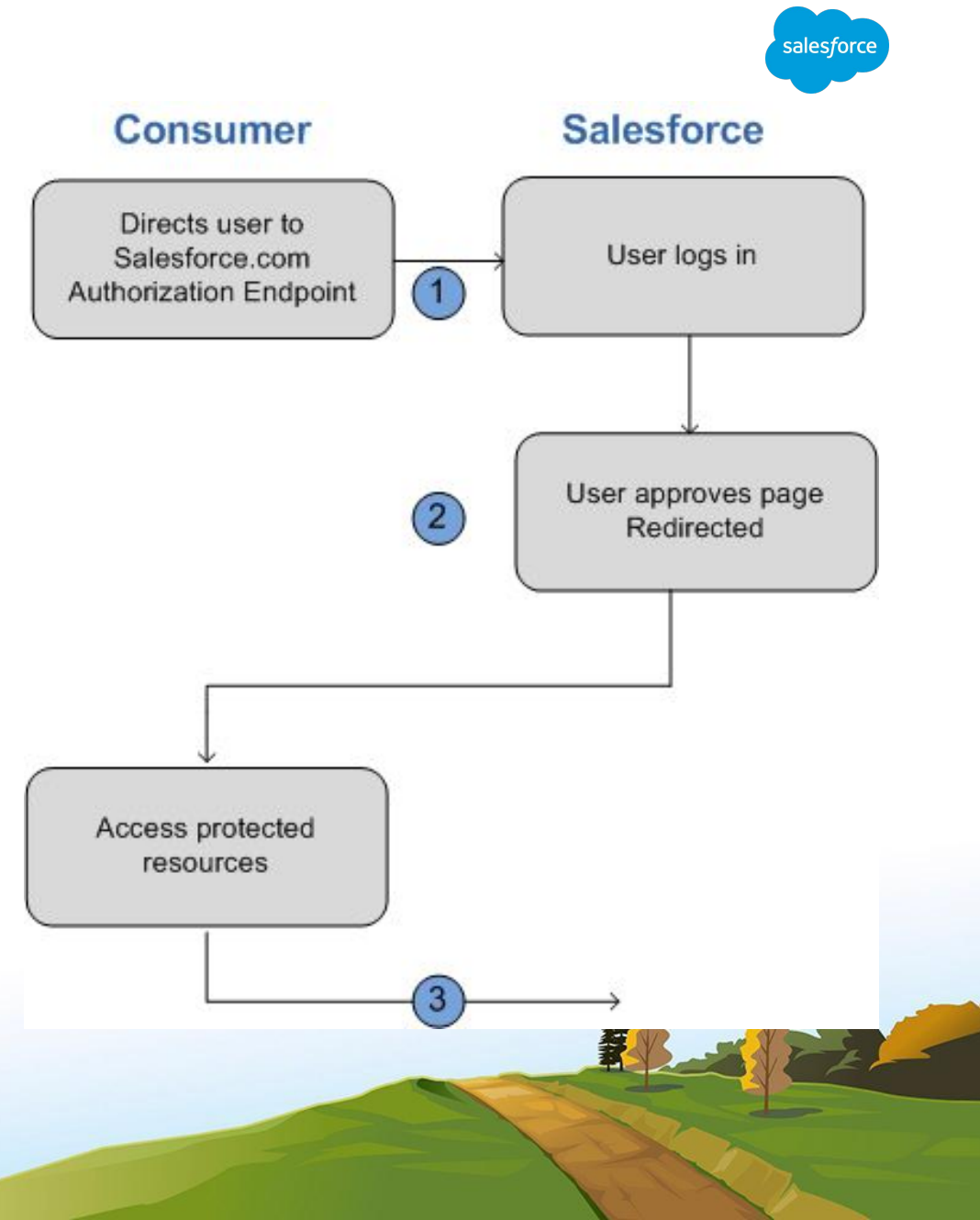


- The user-agent authentication flow is used by client apps (consumers) that reside on the user's device or computer.
- It's also used by client apps running in a browser using a scripting language such as JavaScript.
- These apps can protect per-user secrets however because the apps are widely distributed, the client secret can't be confidential.
- Authentication is based on the user-agent's same-origin policy.
- With the user-agent authentication flow, the client app receives the access token as an HTTP redirection.
- The client executables reside on the user's device, which makes the client secret accessible and exploitable. For this reason, the user-agent authentication flow doesn't use the client secret.



OAuth 2.0 User-Agent Flow

1. The client app directs the user to Salesforce to authenticate and authorize the app.
2. The user approves access for this authentication flow.
3. The app receives the callback from Salesforce.



SAML Assertion Flow



The OAuth 2.0 JWT asset token flow involves these general steps

- The SAML assertion flow is an alternative for orgs that are currently using SAML to access Salesforce and want to access the web services API the same way.
- You can use the SAML assertion flow only inside a single org. You don't have to create a connected app to use this assertion flow.
- Clients can use this assertion flow to federate with the API using a SAML assertion, the same way they federate with Salesforce for web single sign-on.
- SAML Assertion Flow is NOT supported by Communities
- A refresh_token is never issued in this flow



OAuth 2.0 JWT Bearer Token Flow



- A JSON Web Token (JWT) enables identity and security information to be shared across security domains.
- When a client wants to use previous authorization, the client posts an access token request that includes a JWT to Salesforce's OAuth token endpoint.
- Salesforce authenticates the authorized app through a digital signature that is applied to the JWT. Use the OAuth 2.0 JWT bearer token flow to define the authentication process.
- The OAuth 2.0 JWT bearer token flow is similar to a refresh token flow within OAuth.
- The JWT is posted to the OAuth token endpoint, which in turn processes the JWT and issues an access token based on prior approval of the app. Prior approval happens in one of these ways.



OAuth 2.0 JWT Bearer Token Flow



Steps required

1. The developer creates a connected app or uses an existing one, and registers an X509 Certificate for the app. The certificate corresponds to the private key of the app. When the connected app is saved, the consumer key (OAuth client_id) and consumer secret are generated and assigned to the app.
2. The developer writes an app that generates a JWT. The JWT is signed with the X509 Certificate's private key, and the connected app uses the certificate to verify the signature.
3. The JWT is posted to the token endpoint, <https://login.salesforce.com/services/oauth2/token>, or if implementing for a community, <https://community.force.com/customers/services/oauth2/token>.
4. The token endpoint validates the signature using the certificate registered by the developer.
5. The token endpoint validates the JWT's audience (aud), issuer (iss), validity (exp), and subject (sub).
6. Assuming that the JWT is valid and that the user or admin authorized the app previously, Salesforce issues an access token.



OAuth 2.0 SAML Bearer Assertion Flow

SAML assertion used to request an OAuth access token using a previous authorization

- The OAuth 2.0 SAML bearer assertion flow defines how a SAML assertion is used to request an OAuth access token **when a client wants to use a previous authorization**.
- Authentication of the authorized app is **provided by the digital signature** applied to the SAML assertion.
- A SAML assertion is an XML security token issued by an identity provider and consumed by a service provider.
- The service provider relies on its content to identify the assertion's subject for security-related purposes.

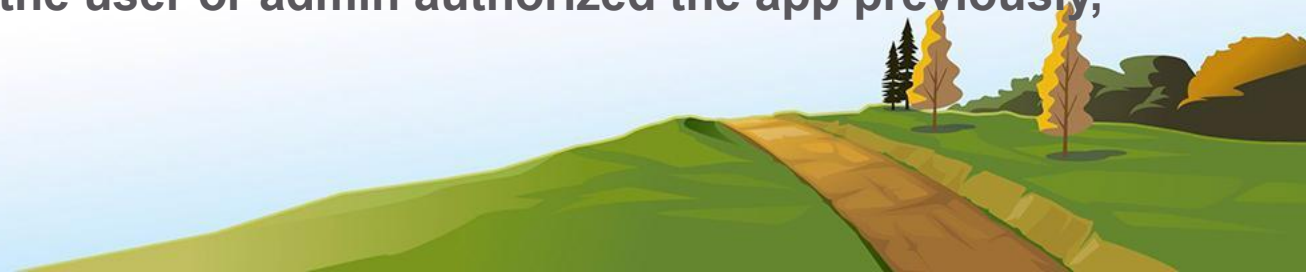


OAuth 2.0 SAML Bearer Assertion Flow (cont.)



Steps required

1. The developer creates a connected app and registers an X509 Certificate. This certificate corresponds to the private key of the app. When the connected app is saved, a consumer key (OAuth client_id) is generated and assigned to the app.
2. The developer writes an app that generates a SAML assertion and signs it with the private key.
3. The SAML Bearer assertion is posted to the token endpoint
<https://login.salesforce.com/services/oauth2/token>,
<https://test.salesforce.com/services/oauth2/token>, or
https://your_community_URL/services/oauth2/token (if implementing for a community).
4. The token endpoint validates the signature using the certificate registered by the developer.
5. The token endpoint validates the audience, issuer, subject, and validity of the assertion.
6. **Assuming that the assertion is valid and that the user or admin authorized the app previously, Salesforce issues an access token.**



OAuth 2.0 Device Authentication Flow



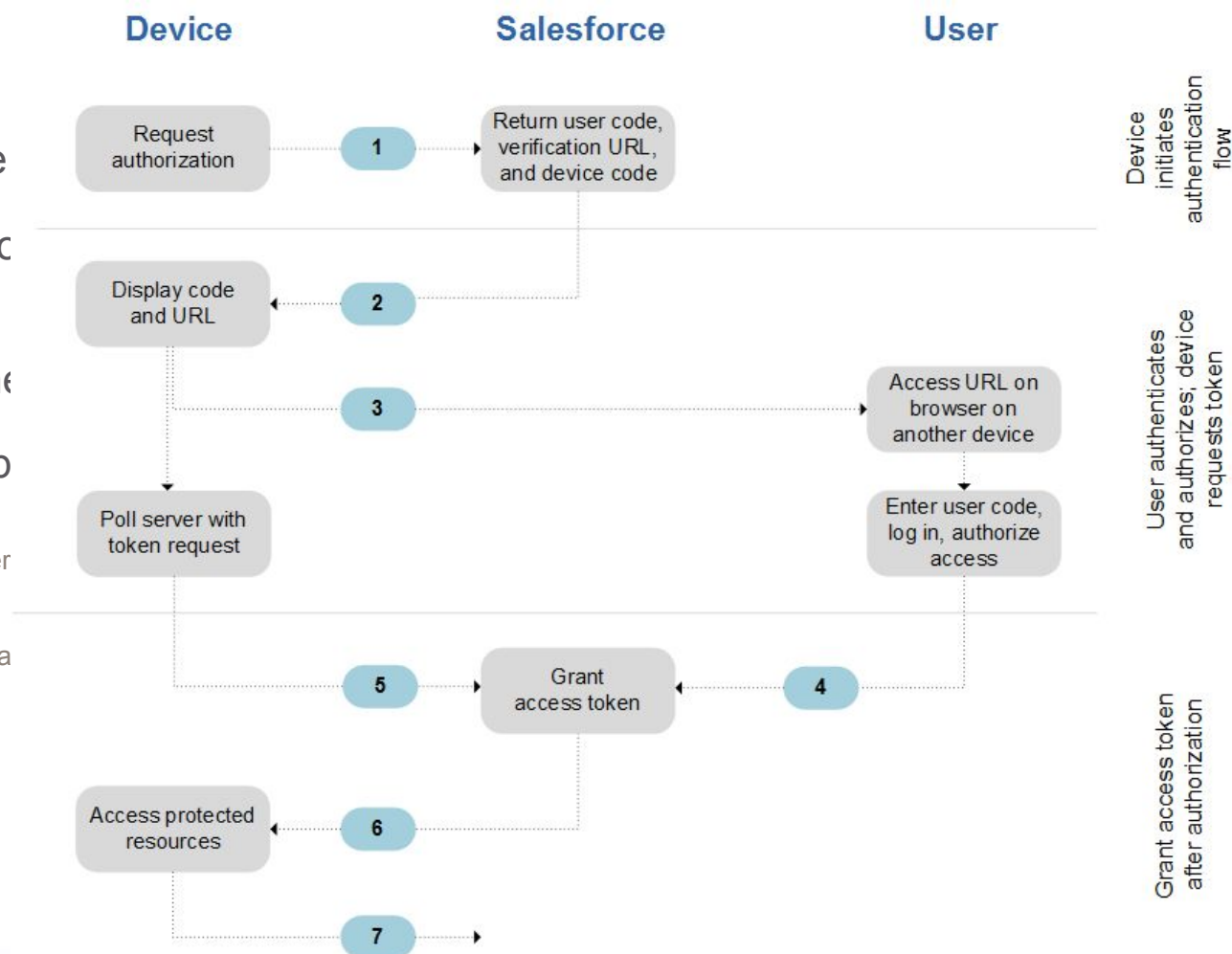
- The OAuth 2.0 device authentication flow is typically used by applications on devices with limited input or display capabilities, such as TVs, appliances, or command-line applications.
- Users can connect these client applications to Salesforce by accessing a browser on a separate device that has more developed input capabilities, such as a desktop computer or smartphone.



OAuth 2.0 Device Authentication Flow



1. The device requests authorization from Salesforce
2. Salesforce verifies the request and returns the follo and minimum polling interval (in seconds).
3. The device displays the user code and instructs the
4. On a separate device that has more developed inp opens a browser.
 1. The user navigates to the verification URL and is prompted to enter the user
 2. If the code is valid, the user is prompted to log in if not already logged in.
 3. After successful login, the user is prompted to allow the device to access Sa



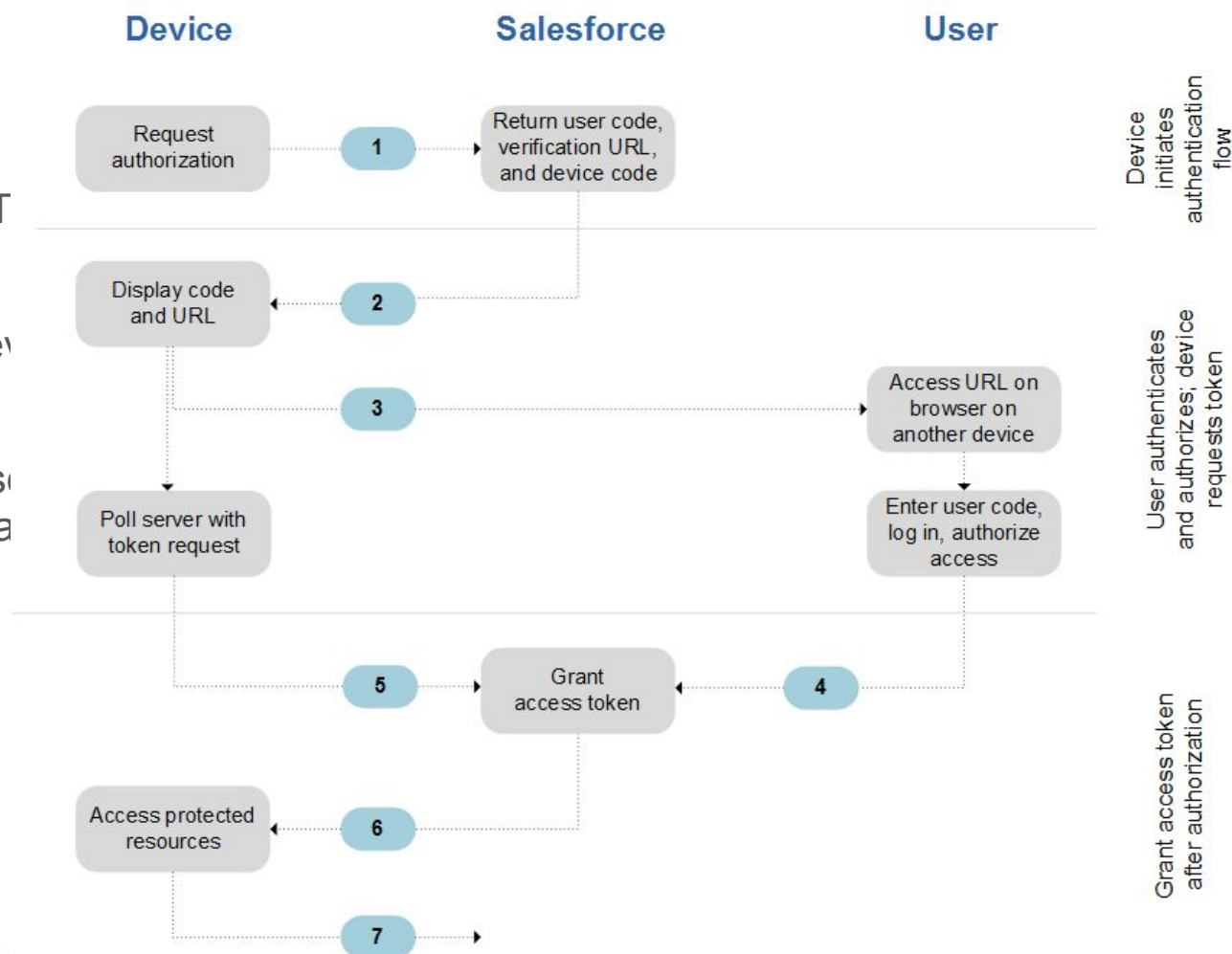
OAuth 2.0 Device Authentication Flow (cont.)



5. After displaying the user code and verification URL, frequency can't exceed the minimum polling interval. (To denied) access, or until the user code has expired.

6. If allowed, the authorization server returns to the device information.

7. After the access token is granted, the device can use a refresh token to get a new access token if the a



OAuth 2.0 Asset Token Flow



- Client applications use the OAuth 2.0 asset token flow to request an asset token from Salesforce for connected devices.
- In this flow, an OAuth access token and an actor token are exchanged for an asset token.
- This flow combines asset token issuance and asset registration for efficient token exchange and automatic linking of devices to Service Cloud Asset data.



OAuth 2.0 Asset Token Flow

The OAuth 2.0 JWT asset token flow involves these general steps

1. Create a new connected app or use an existing one that has asset tokens enabled and required settings configured.
2. [Get an access token](#) so that you can request an asset token.
3. [Create your asset token request](#).
 1. [Create your actor token payload JWT](#).
 2. Understand how [Salesforce attempts to register a new or existing Asset](#) using information from the actor token.
2. [Create your actor token JWT](#).
4. [Post your asset token request](#) to the token endpoint.
5. If the asset token JWT is valid, [Salesforce issues your asset token](#) in an access token response and publishes an asset token event.



OAuth 2.0 Refresh Token Flow

Renews tokens issued by the web server or user-agent flows

1. The consumer uses the existing refresh token to request a new access token.
2. After the request is verified, Salesforce sends a response to the client.



OAuth 2.0 Username-Password Flow



1. The consumer uses the user's username and password to request an access token (session ID.)
2. After the request is verified, Salesforce sends a response to the client.

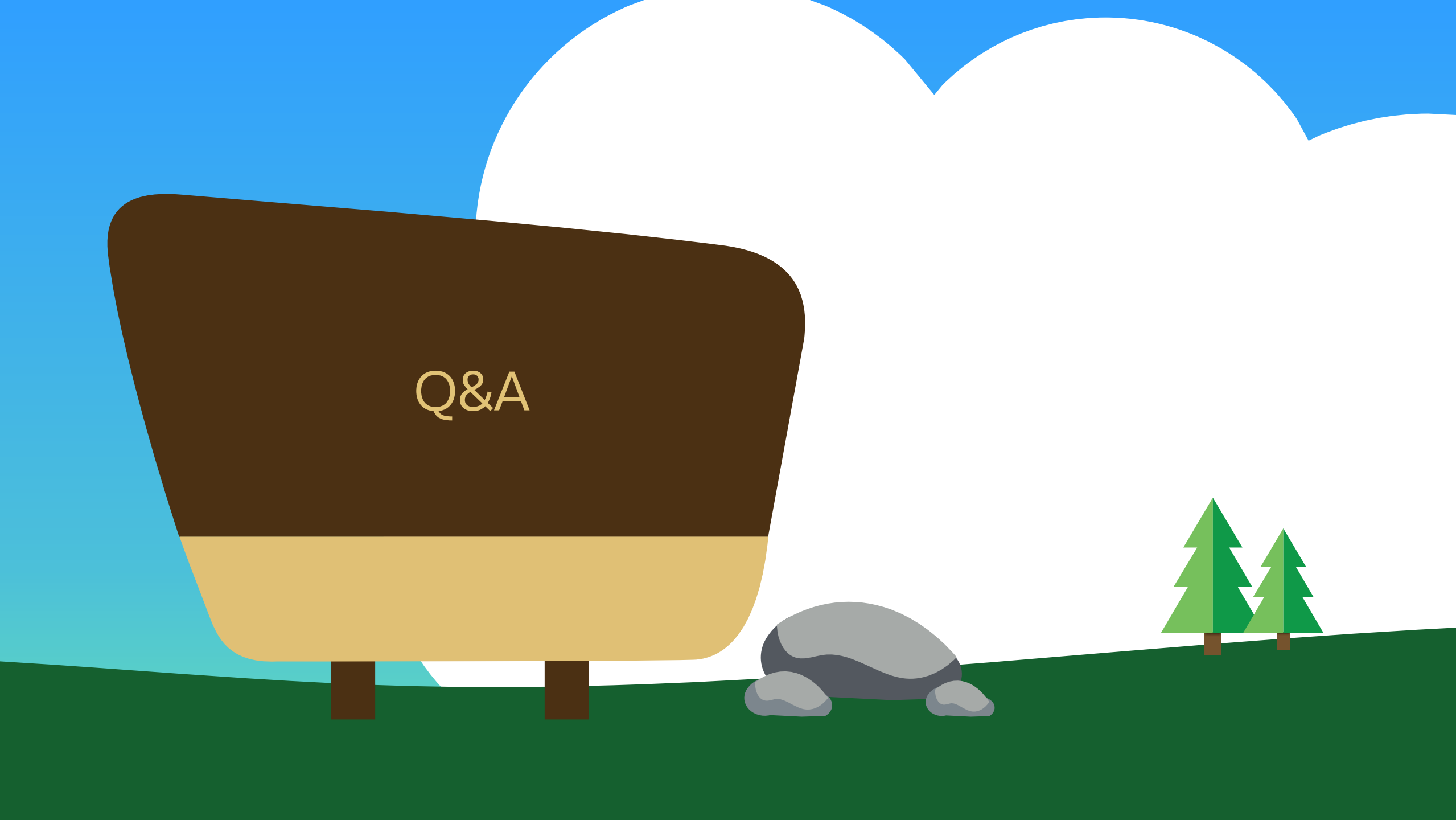


WARNING This OAuth authentication flow passes the user's credentials back and forth. Use this authentication flow only when necessary. No refresh token is issued.



IMPORTANT Salesforce communities don't support the OAuth 2.0 username-password authentication flow.





Q&A

thank
you

BLAZE
YOUR
TRAIL

salesforce

