dreamforce 20 Years

GROUNDSWELL CLOUD SOLUTIONS
a GyanSys company

Named Credentials

Securing and Simplifying API Callouts

Pei Huang, CTO Salesforce Practice
pei@gscloudsolutions.com

Pei Huang

CTO, Salesforce Practice
Groundswell Cloud Solutions Inc
(a GyanSys Company)

Forward Looking Statements

This presentation contains forward-looking statements about, among other things, trend analyses and future events, future financial performance, anticipated growth, industry prospects, environmental, social and governance goals, and the anticipated benefits of acquired companies. 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, Salesforce's results could differ materially from the results expressed or implied by these forward-looking statements. The risks and uncertainties referred to above include those factors discussed in Salesforce's reports filed from time to time with the Securities and Exchange Commission, including, but not limited to: the impact of, and actions we may take in response to, the COVID-19 pandemic, related public health measures and resulting economic downturn and market volatility; our ability to maintain security levels and service performance meeting the expectations of our customers, and the resources and costs required to avoid unanticipated downtime and prevent, detect and remediate performance degradation and security breaches; the expenses associated with our data centers and third-party infrastructure providers; our ability to secure additional data center capacity; our reliance on third-party hardware, software and platform providers; 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; current and potential litigation involving us or our industry, including litigation involving acquired entities such as Tableau Software, Inc. and Slack Technologies, Inc., and the resolution or settlement thereof; regulatory developments and regulatory investigations involving us or affecting our industry; our ability to successfully introduce new services and product features, including any efforts to expand our services; the success of our strategy of acquiring or making investments in complementary businesses, joint ventures, services, technologies and intellectual property rights; our ability to complete, on a timely basis or at all, announced transactions; our ability to realize the benefits from acquisitions, strategic partnerships, joint ventures and investments, including our July 2021 acquisition of Slack Technologies, Inc., and successfully integrate acquired businesses and technologies; our ability to compete in the markets in which we participate; the success of our business strategy and our plan to build our business, including our strategy to be a leading provider of enterprise cloud computing applications and platforms; our ability to execute our business plans; our ability to continue to grow unearned revenue and remaining performance obligation; the pace of change and innovation in enterprise cloud computing services; the seasonal nature of our sales cycles; our ability to limit customer attrition and costs related to those efforts; the success of 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 ability to preserve our workplace culture, including as a result of our decisions regarding our current and future office environments or work-from-home policies; our dependency on the development and maintenance of the infrastructure of the Internet; our real estate and office facilities strategy and related costs and uncertainties; fluctuations in, and our ability to predict, our operating results and cash flows; the variability in our results arising from the accounting for term license revenue products; the performance and fair value of our investments in complementary businesses through our strategic investment portfolio; 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 our strategic investment portfolio; our ability to protect our intellectual property rights; our ability to develop our brands; the impact of foreign currency exchange rate and interest rate fluctuations on our results; 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; uncertainties regarding our tax obligations in connection with potential jurisdictional transfers of intellectual property, including the tax rate, the timing of the transfer and the value of such transferred intellectual property; uncertainties regarding the effect of general economic and market conditions; the impact of geopolitical events; uncertainties regarding the impact of expensing stock options and other equity awards; the sufficiency of our capital resources; our ability to comply with our debt covenants and lease obligations; and the impact of climate change, natural disasters and actual or threatened public health emergencies, including the ongoing COVID-19 pandemic.

Agenda

- Background
- Common Options for Credential Storage
- Why Named Credentials?
- Examples
- Advanced Use Cases
- What’s New in Named Credentials
- Recap and Resources

What are Callouts?

HTTP Callouts

Apex to integrate Salesforce with external systems via API

- Legacy or 3rd party back office applications - REST, SOAP APIs or even scraping web pages
- Online services such as Stripe.com for payment processing, Twilio.com for SMS/telephony, JIRA for Bug Tracking

```
HttpRequest req = new HttpRequest();
req.setEndpoint('https://example.com/path/to/my/fancy/api');
req.setMethod('GET');
Http h = new Http();
HttpResponse res = h.send(req);
```

Authenticating Callouts

Securing Your Integrations

Many APIs will require authentication

- Can’t let just anyone access the API (think: confidential data, sensitive commercial secrets)

Different credentials for different environments

- Production, test, dev … and others?

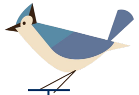
Different authentication mechanisms

- Password based
- JWT Tokens
- Secret keys
- OAuth 2.0
- AWS Signatures
- Custom Authentication Schemes

Named Principal or Per-User

- System/integration user, or different credentials per user

Hardcoding Credentials



"Why can't I just put usernames and passwords in my Apex code?"

Maintenance Nightmare™

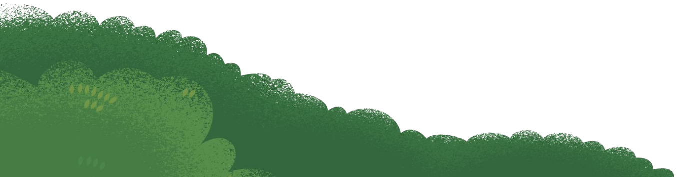
- What if the password has to be changed (e.g. password expires every 90 days)? Deploy code changes every time

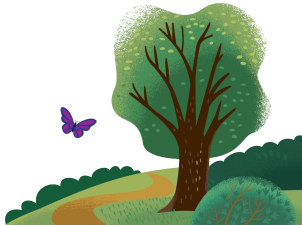
Difficult to maintain changes in different environments

- How do you maintain different credentials between Development, QA, Staging, and Production orgs?

Not very secure!

- Code committed to Git; credentials visible to everyone
- Sandbox refresh, important production credentials become visible in plaintext to developers and others

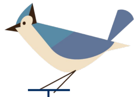




Custom Settings, Objects, or Labels

“But what if I put it in a protected custom setting to keep it safe?”

“But what if I use Custom Labels to store my credentials?”

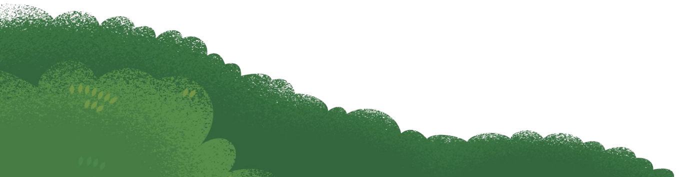


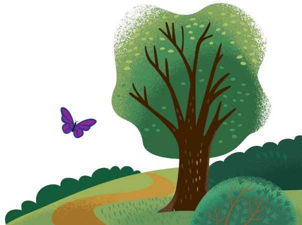
Store credentials inside a Custom Setting/Metadata Type/Object

- Can avoid hard-coding this way
- Have to implement your own utility classes

Not really intended to store secrets

- Custom Labels are intended for localization, not for credentials
- Some unexpected ways to get access to custom settings





“Named credentials … offloads the storage of credentials and authentication to a declaratively controlled process.”

Kevin Poorman
Salesforce MVP | @codefriar | codefriar.com

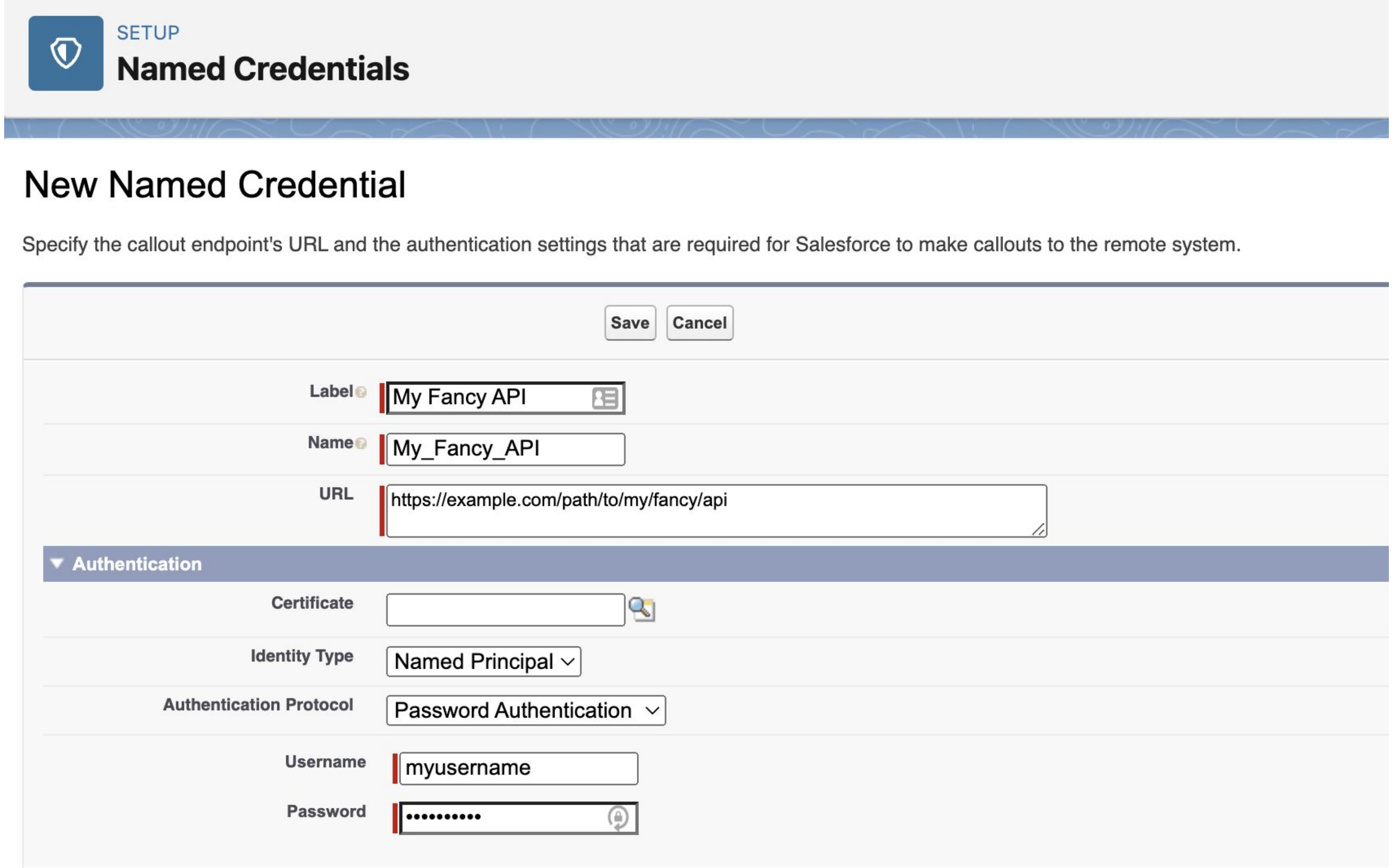
Basic Auth Example

The Traditional Way

```
HttpRequest req = new HttpRequest();
req.setEndpoint('https://example.com/path/to/my/fancy/api');
req.setMethod('GET');

String username = 'myusername';
String password = 'mypassword'; // Or retrieve from Custom Setting

Blob headerValue = Blob.valueOf(username + ':' + password);
String authorizationHeader = 'BASIC ' +
EncodingUtil.base64Encode(headerValue);

req.setHeader('Authorization', authorizationHeader);

Http h = new Http();
HttpResponse res = h.send(req);
```

Basic Auth Example

Create a Named Credential



New Named Credential

Specify the callout endpoint's URL and the authentication settings that are required for Salesforce to make callouts to the remote system.

Label: My Fancy API

Name: My_Fancy_API

URL: https://example.com/path/to/my/fancy/api

▼ Authentication

Certificate:

Identity Type: Named Principal

Authentication Protocol: Password Authentication

Username: myusername

Password: ••••••••••

Basic Auth Example

With Named Credentials

```
HttpRequest req = new HttpRequest();
req.setEndpoint('callout:My_Fancy_API/something');
req.setMethod('GET');
// No need to manually set any headers here. Salesforce will add this for us automatically
Http h = new Http();
HttpResponse res = h.send(req);
```

Complexity of OAuth 2.0

A Secure Industry Standard

Multiple steps with consumer keys/client IDs, client secrets, callbacks, scopes, access tokens, refresh tokens....

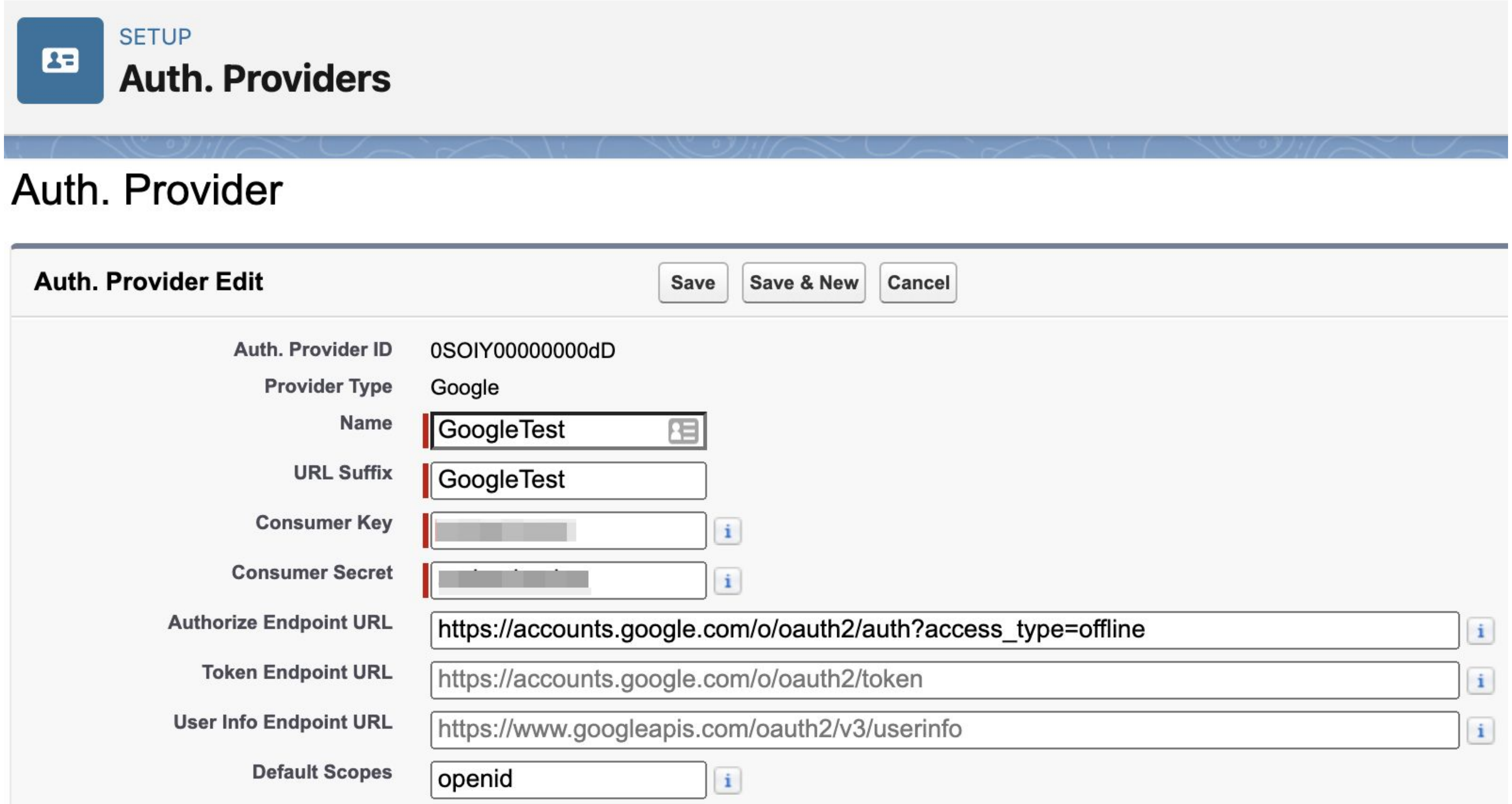
- Many moving parts

Token expiry and refresh

- Handing of refresh_token when sessions expire requires an extra step

OAuth Example

Create Auth. Provider

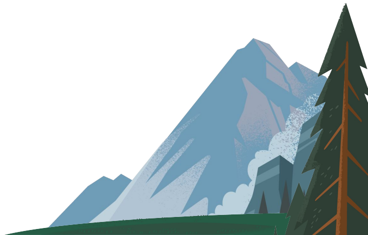


SETUP

Auth. Providers

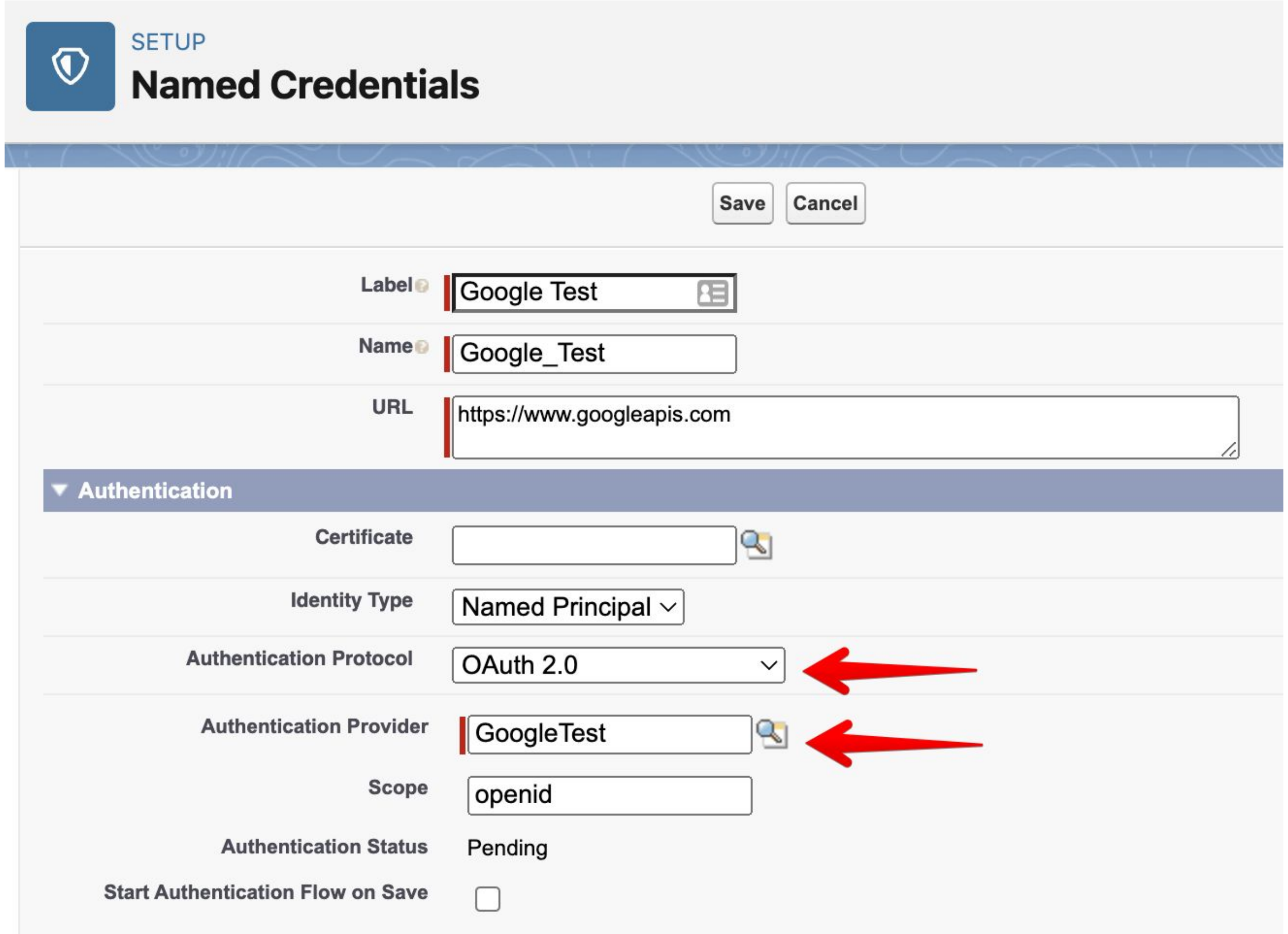
Auth. Provider

Auth. Provider ID	0SOIY00000000dD
Provider Type	Google
Name	GoogleTest
URL Suffix	GoogleTest
Consumer Key	[redacted]
Consumer Secret	[redacted]
Authorize Endpoint URL	https://accounts.google.com/o/oauth2/auth?access_type=offline
Token Endpoint URL	https://accounts.google.com/o/oauth2/token
User Info Endpoint URL	https://www.googleapis.com/oauth2/v3/userinfo
Default Scopes	openid



OAuth Example

Create Named Credential



SETUP

Named Credentials

Save Cancel

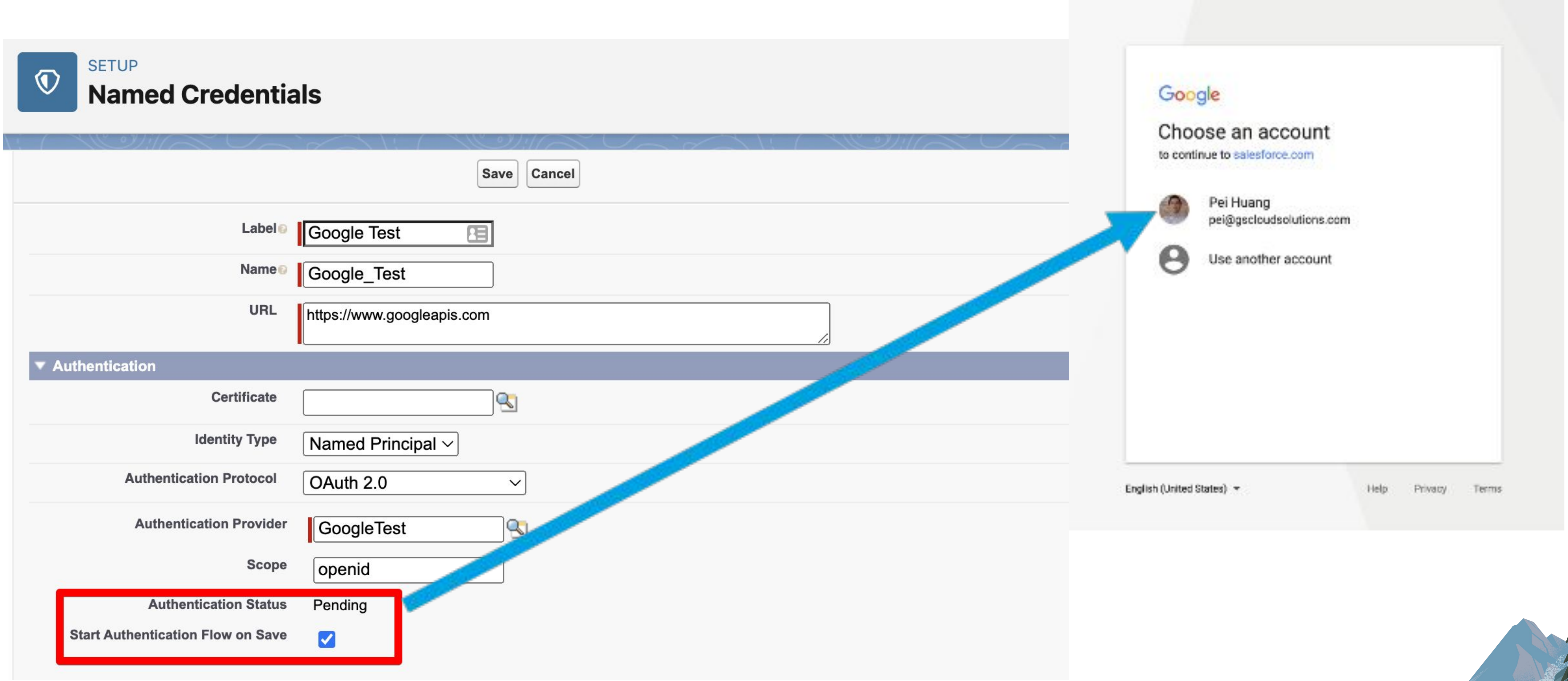
Label	Google Test
Name	Google_Test
URL	https://www.googleapis.com

▼ Authentication

Certificate	
Identity Type	Named Principal
Authentication Protocol	OAuth 2.0
Authentication Provider	GoogleTest
Scope	openid
Authentication Status	Pending
Start Authentication Flow on Save	□

OAuth Example

Authenticate Named Credential



SETUP

Named Credentials

Label	Google Test
Name	Google_Test
URL	https://www.googleapis.com

Authentication

Certificate	
Identity Type	Named Principal
Authentication Protocol	OAuth 2.0
Authentication Provider	GoogleTest
Scope	openid
Authentication Status	Pending
Start Authentication Flow on Save	☑

Google

Choose an account

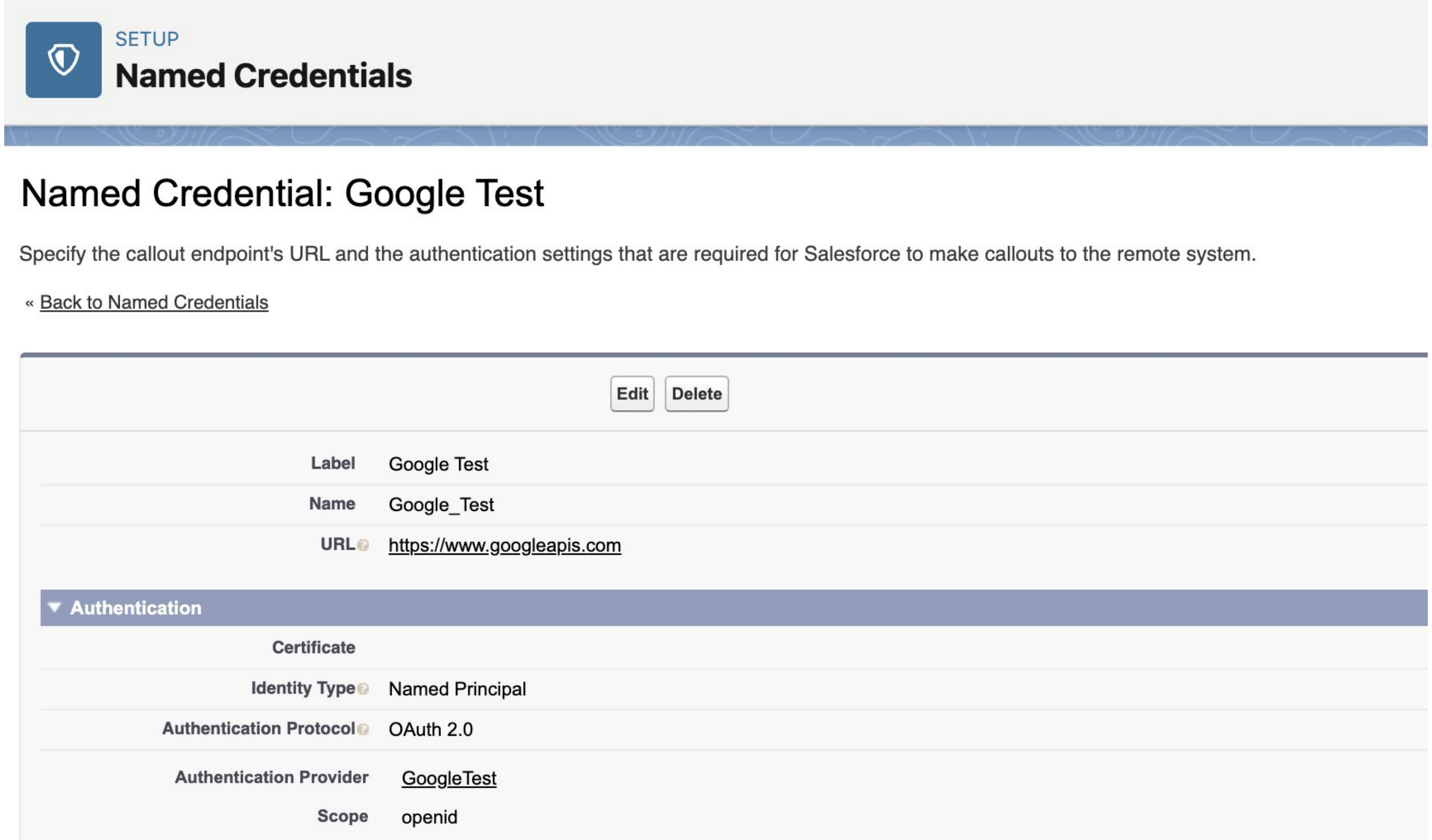
to continue to salesforce.com

Pei Huang
pei@gscloudsolutions.com

Use another account

OAuth Example

Named Credential Is Ready To Go!



SETUP

Named Credentials

Named Credential: Google Test

Specify the callout endpoint's URL and the authentication settings that are required for Salesforce to make callouts to the remote system.

« Back to Named Credentials

Label	Google Test
Name	Google_Test
URL	https://www.googleapis.com

▼ Authentication

Certificate	
Identity Type	Named Principal
Authentication Protocol	OAuth 2.0
Authentication Provider	GoogleTest
Scope	openid

OAuth Example – With Named Credentials

Simple Code

```
HttpRequest req = new HttpRequest();

req.setEndpoint('callout:Google_Test/oauth2/v3/userinfo');

req.setMethod('GET');

// No need to manually set any headers here.
// Notice how similar this code looks to the Username/Password Example?

Http h = new Http();
HttpResponse res = h.send(req);
```

OAuth 2.0 with Named Credentials

What Salesforce Does for You

Handles Web-Server Flow Via Declarative Setup Screens

- 100% declarative setup process.- no code required

Generates and Appends the Authorization Header

- Authorization Bearer header is automatically added to your HTTP request

Refresh OAuth Access Token

- Salesforce will handle the refresh flow for you

Merge Fields

What About APIs That Don’t Use The Authorization Header?

Generate Authorization Header

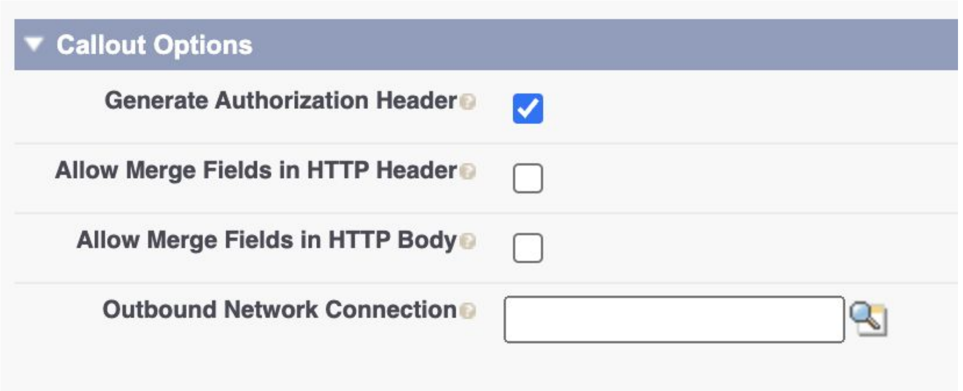
- Default – generates the Authorization header added to the HTTP request for you

Allow Merge Fields in HTTP Header

- Set your own custom header using values from the Named Credential – e.g. custom X-Auth headers or similar

Allow Merge Fields in HTTP Body

- Set your own custom values in an HTTP body – e.g. SOAP API with Salesforce’s Metadata API



▼ Callout Options

Generate Authorization Header ☑

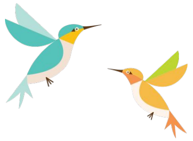
Allow Merge Fields in HTTP Header □

Allow Merge Fields in HTTP Body □

Outbound Network Connection

Merge Fields

Most Useful Merge Fields



Merge Fields	Description	Example

{!$Credential.Username}
{!$Credential.Password}
	Username and password of the running user. Available only if the named credential uses password authentication.	`// non-standard authentication`
		`req.setHeader('X-Username', '{!$Credential.UserName}');`
		`req.setHeader('X-Password', '{!$Credential.Password}');`

{!$Credential.OAuthToken}	OAuth token of the running user. Available only if the named credential uses OAuth authentication.	

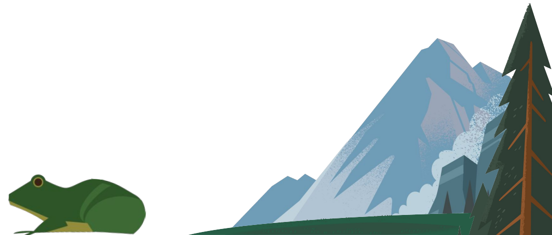
For full list, refer to
https://developer.salesforce.com/docs/atlas.en-us.apexcode.meta/apexcode/apex_callouts_named_credentials_merge_fields.htm

SOAP Example

Using Apex Wrapper for Metadata API

```
MetadataService.MetadataPort service = new
                  MetadataService.MetadataPort();

service.SessionHeader = new MetadataService.SessionHeader_element();
service.endpoint_x = 'callout:ApexMDAPI/services/Soap/m/41.0';
service.SessionHeader.sessionId = '{!$Credential.OAuthToken}';

// By using Named Credentials, we can now call Salesforce SOAP APIs
from batch classes and other contexts easily where a first-class
session ID is not readily available
```

Ref: My blog post at
https://gscloudsolutions.com/tips-tricks/using-named-credentials-with-the-apex-wrapper-salesforce-metadata-api/



Other Benefits

Why you should always use Named Credentials

No need to add Remote Site Settings

- Skip Remote Site Settings if you are using Named Credentials

Can reference the same Named Credential name in code across environments

- No need to change anything in your code when moving between environments – simply update the Named Credential in Setup

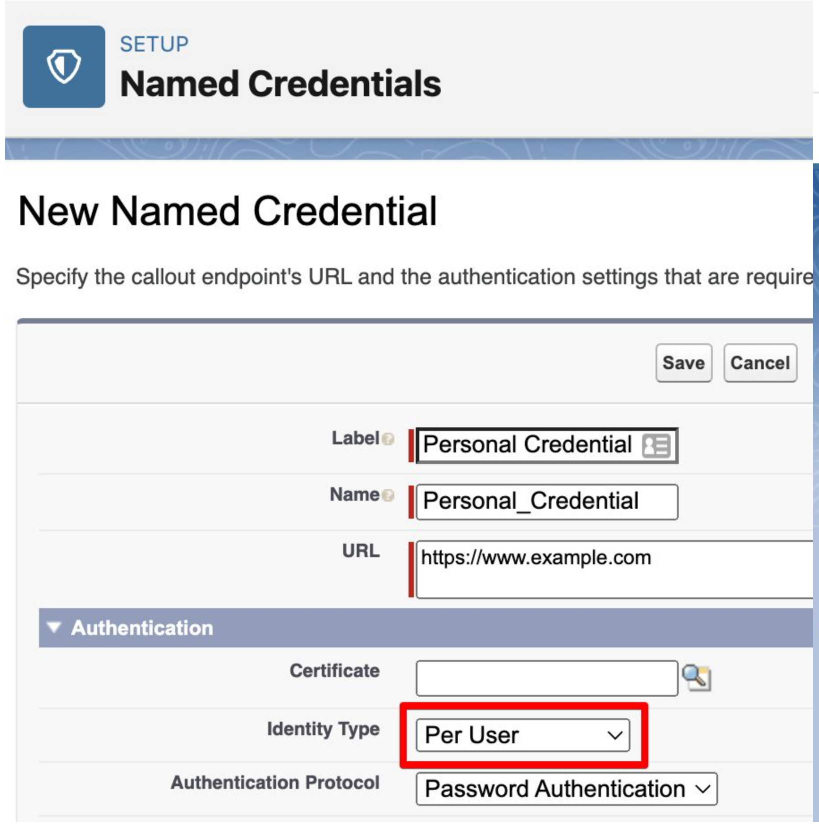
Easy for admins to maintain

- Developers can remain at arms-length of production credentials at all time

Secure storage of credentials in Salesforce

- Secrets are stored securely by Salesforce – no need to reinvent the wheel

Per User Credentials


SETUP

Named Credentials

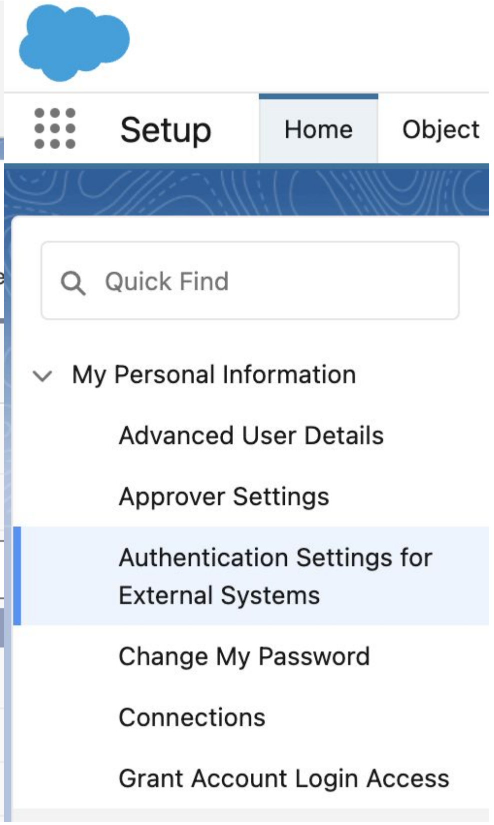
New Named Credential

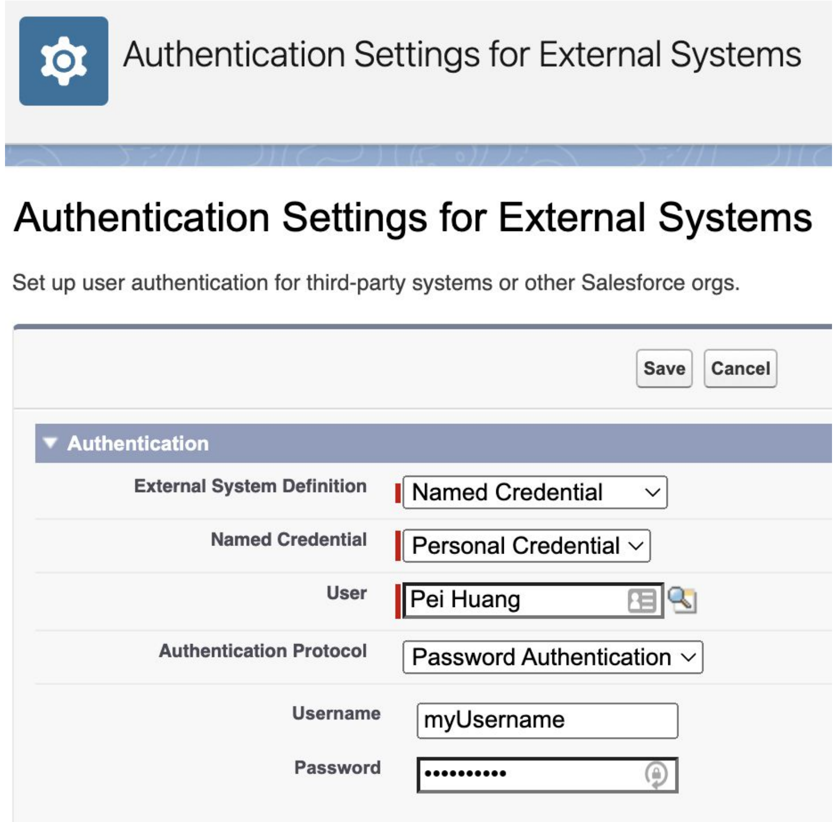
Specify the callout endpoint's URL and the authentication settings that are require

Label	Personal Credential
Name	Personal_Credential
URL	https://www.example.com

Authentication

Certificate	
Identity Type	Per User
Authentication Protocol	Password Authentication




Authentication Settings for External Systems

Authentication Settings for External Systems

Set up user authentication for third-party systems or other Salesforce orgs.

Authentication

External System Definition	Named Credential
Named Credential	Personal Credential
User	Pei Huang
Authentication Protocol	Password Authentication
Username	myUsername
Password	••••••••••

Recap

Named Credentials Are Awesome!

Named Credentials solve the common problem of storing and maintaining credentials used for API integrations in Salesforce

- Simplifies and streamlines your code

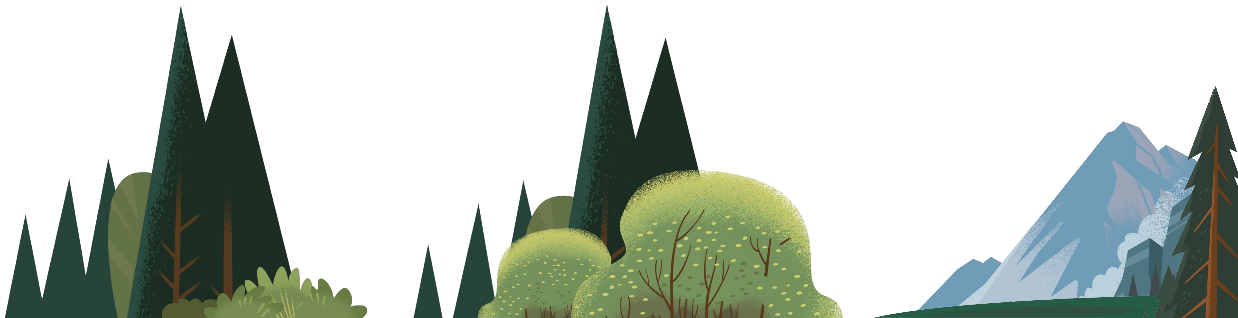
Don’t hard code your credentials in Apex!

- Maintenance, maintenance, maintenance

Empower admins to maintain and manage credentials

Secure storage of credentials in Salesforce

- Basic
- OAuth 2.0
- Custom schemes via merge fields



Did You Know?

A lot has changed in Named Credentials in last couple of years

New Authentication Protocols (Summer ‘19):

- AWS Signature V4
- JWT
- JWT Token Exchange

Outbound Connections via Private Connect (Summer ‘20)

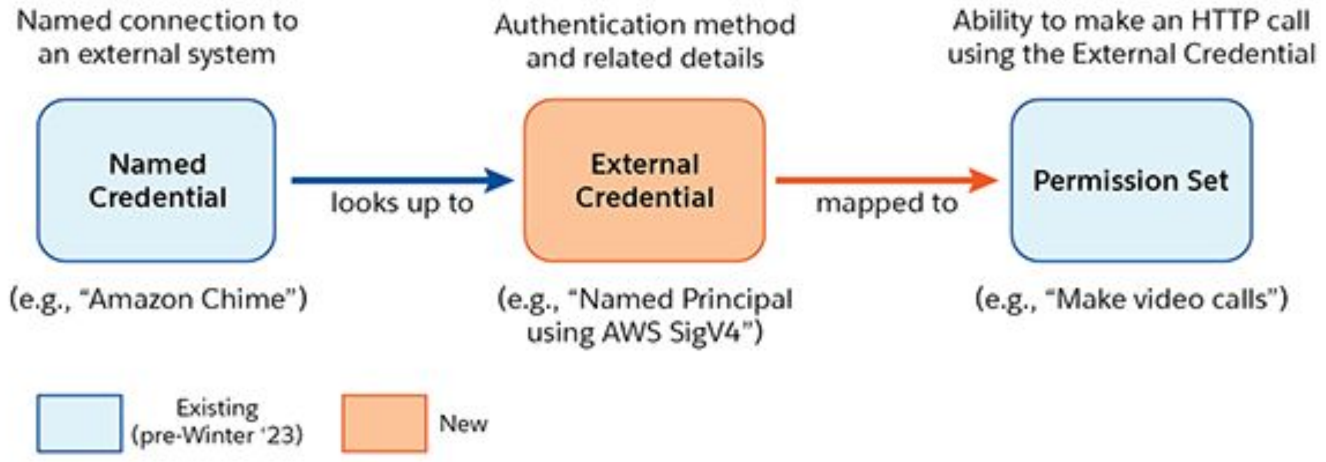
- Secure private access to your AWS environments

AWS PrivateLink

Coming in Winter ‘23 (SAFE HARBOR)

New architecture that supports:

- Custom name/value pairs for auth headers
- Per Permission Set assigned Credentials
- A new Lightning-native Setup UI



Named connection to an external system

Named Credential

(e.g., “Amazon Chime”)

looks up to

Authentication method and related details

External Credential

(e.g., “Named Principal using AWS SigV4”)

mapped to

Ability to make an HTTP call using the External Credential

Permission Set

(e.g., “Make video calls”)

Existing (pre-Winter ‘23)

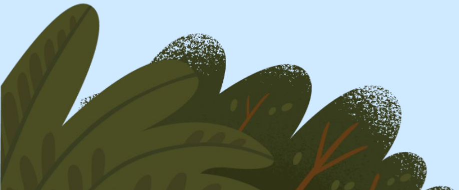
New

https://help.salesforce.com/s/articleView?id=release-notes.rn_security_other_custom_named_credentials.htm&type=5&release=240

Resources

Check Out Trailhead To Learn More!

- **Secure Secret Storage:**
  https://trailhead.salesforce.com/content/learn/modules/secure-secrets-storage
- **Apex REST Callouts:**
  https://trailhead.salesforce.com/modules/apex_integration_services/units/apex_integration_rest_callouts
- **APEX SOAP Callouts:**
  https://trailhead.salesforce.com/modules/apex_integration_services/units/apex_integration_soap_callouts
- **Data Integration Superbadge:**
  https://trailhead.salesforce.com/en/super_badges/superbadge_integration
- **Develop Secure Web Apps:**
  https://trailhead.salesforce.com/trails/security_developer



Groundswellers at Dreamforce

We’re all wearing “**G**” pins so come say hello!

Savio Jose

Product Practice Manager

Presented: [Best Practices for Data Security in Experience Cloud]()

Cameron Reid

Emerging Technologies Lead

Presented: [Diagramming for the Admin]()

Leonardo Berardino

Principal Developer

Presented: [Open-Source Mocking Framework Based on Apex Stub API]()

Gerauld Rivera

Marketing Cloud Product Lead

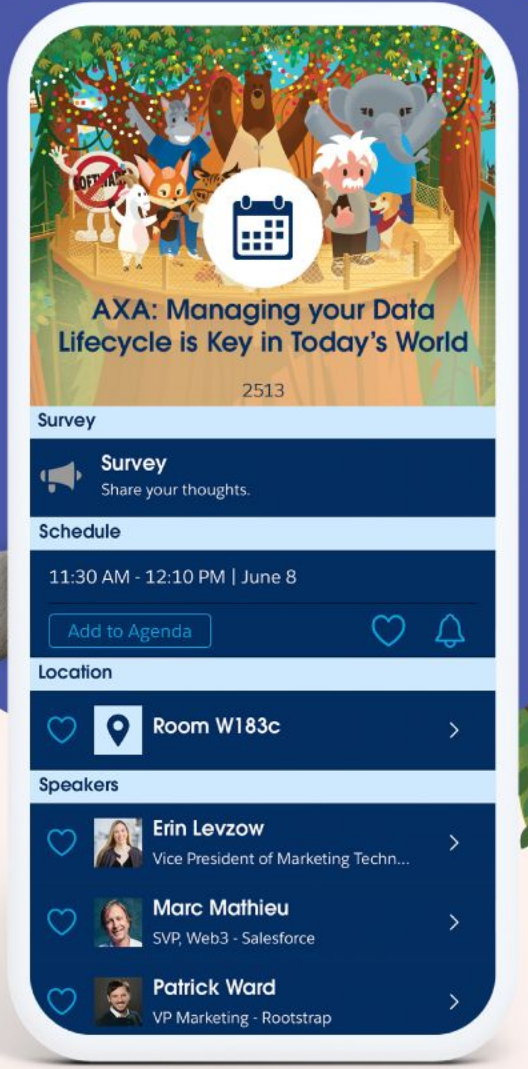
Colin Hamilton

Field Service Product Lead

dreamforce 20 Years

Share your feedback.

Provide your feedback on this session in the Salesforce Events mobile app and help make our content even better.



AXA: Managing your Data Lifecycle is Key in Today's World

2513

Survey

Survey
Share your thoughts.

Schedule

11:30 AM - 12:10 PM | June 8

Add to Agenda

Location

Room W183c

Speakers

Erin Levzow
Vice President of Marketing Techn...

Marc Mathieu
SVP, Web3 - Salesforce

Patrick Ward
VP Marketing - Rootstrap

#DF22

Q&A

dreamforce®
20 Years

Thank you