cisco Secure

SAML Basic

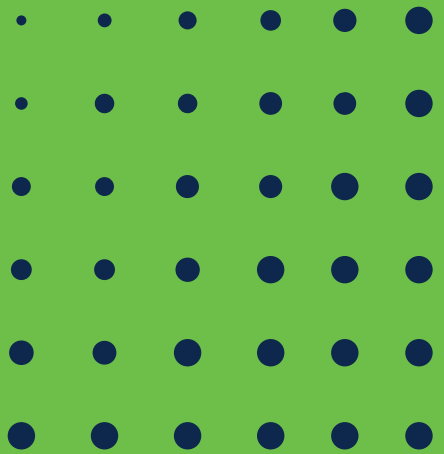
Duo も サポートする SSO / フェデレーション機能を理解する

シスコシステムズ合同会社
村上　英樹
2020年10月1日

Agenda

1. What is SAML?
2. SAMLアーキテクチャ
3. SAMLフェデレーション
4. Duo SAML連携
5. トラブルシューティングツール

What is SAML?



SAML が採用される要因

シングルサインオン

- ✓ 今までのSSOはブラウザのCookieに依存してユーザ認証状態情報を保持していたが、Cookieは別のドメインで利用することは出来ない
- ✓ SAMLはドメインに依存せず情報転送可能なため、ベンダーに依存しない環境を提供

フェデレーションID

- ✓ IDフェデレーションは、組織の境界を超えてユーザに関する情報を共有し、ユーザーを参照するための共通の共有名識別子を確立するための手段を提供
- ✓ 複数のサービスがID関連のデータ（パスワード、ID属性など）を個別に収集および維持する必要がないため、ID管理コストを削減

Webサービスおよびその他の業界標準

- ✓ SAMLでは、セキュリティアサーション形式を「ネイティブ」のSAMLベースプロトコルコンテキストの外部で使用できる
- ✓ SAMLアサーションの使用で得られる利点は、他のWS-Securityトークン形式で属性などの情報を簡単に交換できる標準ベースのアプローチを提供すること

OASIS SAML2.0 技術概要資料参照

SAML?!

SAML = Secure Assertion Markup Language

- SAML は、当事者間、特に ID プロバイダとサービスプロバイダ間で認証、属性および認可データを交換するためのオープンな標準
- SAML は、セキュリティ・アサーション（サービスプロバイダがアクセス制御の決定を行うために使用するステートメント）のための XMLベースの Markup Languageである。
- データの交換は、通常HTTP GETやPOSTを使い、ユーザのブラウザ経由で実施される。
- SAMLが利用される最も重要なユースケースは、ブラウザのシングルサインオン（SSO）

これが、SAML XML


```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" ID="_e3f70b93a3f7c7c109299982eecfdc4330268194f3" Version="2.0"
IssueInstant="2015-11-30T20:16:41Z" Destination="https://duosandbox.greenhouse.io/users/saml/consume" InResponseTo="_16c32050-79cd-0133-7e73-2e1fe3a32e97"><saml:Issuer>https://
samltoo.duo.local/dag/saml2/idp/metadata.php</saml:Issuer><ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <ds:SignedInfo><ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
    <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
  <ds:Reference URI="#_e3f70b93a3f7c7c109299982eecfdc4330268194f3"><ds:Transforms><ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/><ds:Transform
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/></ds:Transforms><ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/
><ds:DigestValue>wd3hD2xeJkOI7megKNyz4xy3EhQ=</ds:DigestValue></ds:Reference></ds:SignedInfo><ds:SignatureValue>h7PEy/
YLxnxFiuWlLlL5NFH90oXnN47WJ81smXeSRPp4MT23rqMbZnRV3eIRSLkHDwFDe6W75A1JQ9yuKldpx41YF4CgHDaCdkuI1gFYKx+9O2wJySMmO/+t5jTsmhbHU7wvxFLssv2UgK28U88JlWyNJpeTKbw0e+c82DrLxVM=</
ds:SignatureValue>
<ds:KeyInfo><ds:X509Data><ds:X509Certificate>MIICXDCCAcWgAwIBAgIBADANBgkqhkiG9w0BAQUFADBLMQswCQYDVQQGEwJVUzELMAkGA1UECAwCTUkxEjAQBgNVBAcMCUFubiBBcmJvcjEbMBkGA1UECgwSRHVvIFNlY3VyaXR
5LCBJbmMuMB4XDTE1MDUxMjEyNTM0OFoXDTI1MDUwOTEyNTM0OFowSzELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAk1JMRIwEAYDVQQHDAlBbm4gQXJib3IxGzAZBgNVBAoMEkR1byBTZWN1cml0eSwgSW5jLjCBnzANBgkqhkiG9w0BAQEFAAO
BjQAwgYkCgYEAu/TiSA7ojMVvFLlMr3O+iFYHTqdLcCoMlrya2+eCGeFx+HyIjK9kg76UY0q4A2CUFjKph2yI1BMXOC3LkVApdCR0pQWGvdVZaH6c6csVXGvVZg4uHk64ZbEa0IA2Nlf09G63RPIvpH58o
+LFHhvGePx7m7AiWq7jIPwqc3WQR0UCAwEAAaNQME4wHQYDVR0OBBYEFJLtPfP2eSwFvS3vfSFRHKSm155/MB8GA1UdIwQYMBaAFJLtPfP2eSwFvS3vfSFRHKSm155/
MAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQADgYEArsGvew4ozUWXPLcRebB4W+Cc9xQxAFn+2VnL8t1/basWfnye3ElaT//vVP+idU1ADhJ5drLeQYuumMVhwQfXZ3CcCvOdQyiG9y+RzgattNs8u/
5QZUf60F4i8Jtd07LvauaL0TiGv0Jho9tKXcRH6JJQm1K7hEjhWSzRfN3cps8=</ds:X509Certificate></ds:X509Data></ds:KeyInfo></ds:Signature><samlp:Status><samlp:StatusCode
Value="urn:oasis:names:tc:SAML:2.0:status:Success"/></samlp:Status><saml:Assertion xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xs="http://www.w3.org/2001/XMLSchema"
ID="_b5baf0c34a12a1a245f7a189aa1df54829012de630" Version="2.0" IssueInstant="2015-11-30T20:16:41Z"><saml:Issuer>https://samltoo.duo.local/dag/saml2/idp/metadata.php</
saml:Issuer><ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <ds:SignedInfo><ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
    <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
  <ds:Reference URI="#_b5baf0c34a12a1a245f7a189aa1df54829012de630"><ds:Transforms><ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/><ds:Transform
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/></ds:Transforms><ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/
><ds:DigestValue>fUs2LtuX6r0JTIztoCUsqAJzBbg=</ds:DigestValue></ds:Reference></ds:SignedInfo><ds:SignatureValue>EPcXsJMCulDTr3MpeMJWjXfkLX/SoC5fJDgmH4+3Em+vtmQLZIVXZqM/
xpycLyOY6kY0jqgwLibGlsTuIbMTvw5mkwBYgu+GsJQSRWknz2F0+cz+kXKOIipcWQYkOGnBlq7Ldjwu6IwDO9BgxwnAdWarI04eRt9/t2+qSHdbWtM=</ds:SignatureValue>
<ds:KeyInfo><ds:X509Data><ds:X509Certificate>MIICXDCCAcWgAwIBAgIBADANBgkqhkiG9w0BAQUFADBLMQswCQYDVQQGEwJVUzELMAkGA1UECAwCTUkxEjAQBgNVBAcMCUFubiBBcmJvcjEbMBkGA1UECgwSRHVvIFNlY3VyaXR
5LCBJbmMuMB4XDTE1MDUxMjEyNTM0OFoXDTI1MDUwOTEyNTM0OFowSzELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAk1JMRIwEAYDVQQHDAlBbm4gQXJib3IxGzAZBgNVBAoMEkR1byBTZWN1cml0eSwgSW5jLjCBnzANBgkqhkiG9w0BAQEFAAO
BjQAwgYkCgYEAu/TiSA7ojMVvFLlMr3O+iFYHTqdLcCoMlrya2+eCGeFx+HyIjK9kg76UY0q4A2CUFjKph2yI1BMXOC3LkVApdCR0pQWGvdVZaH6c6csVXGvVZg4uHk64ZbEa0IA2Nlf09G63RPIvpH58o
+LFHhvGePx7m7AiWq7jIPwqc3WQR0UCAwEAAaNQME4wHQYDVR0OBBYEFJLtPfP2eSwFvS3vfSFRHKSm155/MB8GA1UdIwQYMBaAFJLtPfP2eSwFvS3vfSFRHKSm155/
MAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQADgYEArsGvew4ozUWXPLcRebB4W+Cc9xQxAFn+2VnL8t1/basWfnye3ElaT//vVP+idU1ADhJ5drLeQYuumMVhwQfXZ3CcCvOdQyiG9y+RzgattNs8u/
5QZUf60F4i8Jtd07LvauaL0TiGv0Jho9tKXcRH6JJQm1K7hEjhWSzRfN3cps8=</ds:X509Certificate></ds:X509Data></ds:KeyInfo></ds:Signature><saml:Subject><saml:NameID
SPNameQualifier="duosandbox.greenhouse.io" Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress">jpringle@duosecurity.com</saml:NameID><saml:SubjectConfirmation
Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"><saml:SubjectConfirmationData NotOnOrAfter="2015-11-30T20:21:41Z" Recipient="https://duosandbox.greenhouse.io/users/saml/consume"
InResponseTo="_16c32050-79cd-0133-7e73-2e1fe3a32e97"/></saml:SubjectConfirmation></saml:Subject><saml:Conditions NotBefore="2015-11-30T20:16:11Z"
NotOnOrAfter="2015-11-30T20:21:41Z"><saml:AudienceRestriction><saml:Audience>duosandbox.greenhouse.io</saml:Audience></saml:AudienceRestriction></
saml:Conditions><saml:AuthnStatement AuthnInstant="2015-11-30T20:16:41Z" SessionNotOnOrAfter="2015-12-01T04:16:41Z"
SessionIndex="_7588e3a316c90526d718c56bd53b740f55ff59a739"><saml:AuthnContext><saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Password</
saml:AuthnContextClassRef></saml:AuthnContext></saml:AuthnStatement><saml:AttributeStatement><saml:Attribute Name="sn" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic"><saml:AttributeValue xsi:type="xs:string">Pringlez</saml:AttributeValue></saml:Attribute><saml:Attribute Name="givenName" NameFormat="urn:oasis:names:tc:SAML:
2.0:attrname-format:basic"><saml:AttributeValue xsi:type="xs:string">Jamie</saml:AttributeValue></saml:Attribute><saml:Attribute Name="distinguishedName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"><saml:AttributeValue xsi:type="xs:string">CN=jpringle,CN=Users,DC=duo,DC=local</saml:AttributeValue></
saml:Attribute><saml:Attribute Name="objectGUID" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"><saml:AttributeValue xsi:type="xs:string">rHG9cfdw8Uae8+5LAfxKeg==</
saml:AttributeValue></saml:Attribute><saml:Attribute Name="sAMAccountName" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"><saml:AttributeValue
xsi:type="xs:string">jpringle</saml:AttributeValue></saml:Attribute><saml:Attribute Name="userPrincipalName" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic"><saml:AttributeValue xsi:type="xs:string">jpringle@duo.local</saml:AttributeValue></saml:Attribute><saml:Attribute Name="mail" NameFormat="urn:oasis:names:tc:SAML:
2.0:attrname-format:basic"><saml:AttributeValue xsi:type="xs:string">jpringle@duosecurity.com</saml:AttributeValue></saml:Attribute><saml:Attribute Name="duo_username"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"><saml:AttributeValue xsi:type="xs:string">jpringle</saml:AttributeValue></saml:Attribute><saml:Attribute
Name="User.LastName" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"><saml:AttributeValue xsi:type="xs:string">Pringlez</saml:AttributeValue></
saml:Attribute><saml:Attribute Name="User.FirstName" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"><saml:AttributeValue xsi:type="xs:string">Jamie</
saml:AttributeValue></saml:Attribute></saml:AttributeStatement></saml:Assertion></samlp:Response>
```

SAML 用語

- **Security Assertion Markup Language (SAML)** : XMLベースの標準で、認証のためのアイデンティティをフェデレートするために使用される
- **Service Provider (SP)** : SAMLに対応したクラウドアプリケーション (Google, Salesforce, Box, Slackなど)
- **Identity Provider (IdP)** : ユーザの認証、ユーザのアイデンティティに関する情報を提供（一般的な IdP には、Azure AD, AD FSなど）
- **アサーション** : 1 つ以上のステートメントを提供する情報のパッケージ（ステートメントには、認証、属性、認可の 3 種類）
- **信頼関係** : SP と IdP の間で確立されたアイデンティティフェデレーションとシングルサインオン（SSO）を機能させる

SAML SPとIdP間の信頼を確立

- メッセージはユーザーのブラウザを経由して交換
- IdPは、キーペアを生成する
- 管理者は、IdP の証明書（公開鍵を含む）とその他の情報を SP に提供し、IdP を信頼するように指示する – *フェデレーション*
- IdP は、秘密鍵を使用して SAML レスポンスまたは SAML アサーションのいずれかまたは両方に署名する
- SPは、SAML レスポンスまたは SAML アサーションの署名を、IdPで生成された公開鍵で検証する

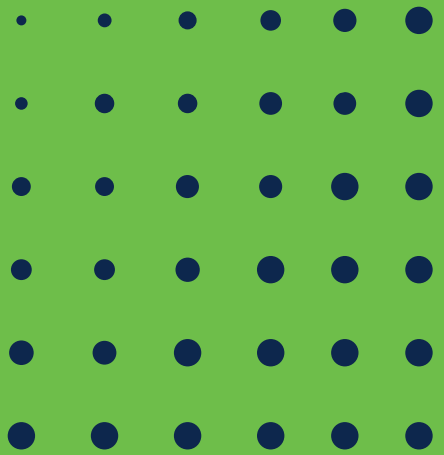
シングルサインオン（SSO）

実装方式（現状、SAMLがメイン）

- SAML Identity Provider (IdP)
- OpenID Identity Provider (IdP)
- ケルベロス認証
- リバースプロキシ型
- エージェント型

source: wikipedia

SAMLアーキテクチャ



SAML URL

- Single Sign-On (SSO) URL :
  - ✓ SAML認証リクエストを受信、処理を行う SAML IdP エンドポイント
- Assertion Consumer Service (ACS) URL :
  - ✓ Identity Provider (IdP) による SAMLレスポンスメッセージを受信する SAML SPエンドポイント
  - ✓ Assertionは、レスポンスに含まれる

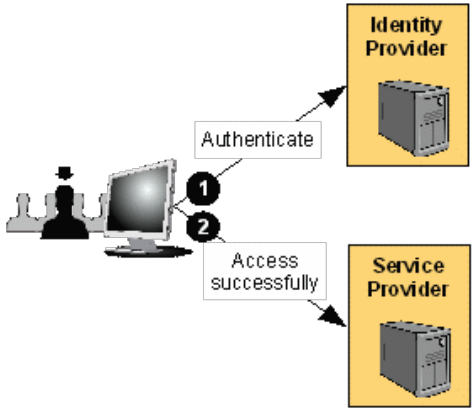
SAML メッセージ

- Entity ID <Issuer>： SAML当事者のユニークなID、メッセージのIssuer
- <NameID>：認証されたユーザーを識別するための必須のレスポンス要素
  - ✓ 共通 NameID フォーマット
    - urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
    - urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
    - urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
    - urn:oasis:names:tc:SAML:2.0:nameid-format:transient
- <Attribute>：IdP から送信されるアサーションには、1つあるいは複数の属性が含まれ、SPによってアクセス制御などで利用される
- <Authentication Context>：IdPによって認証されたことを示す

SAMLフェデレーション

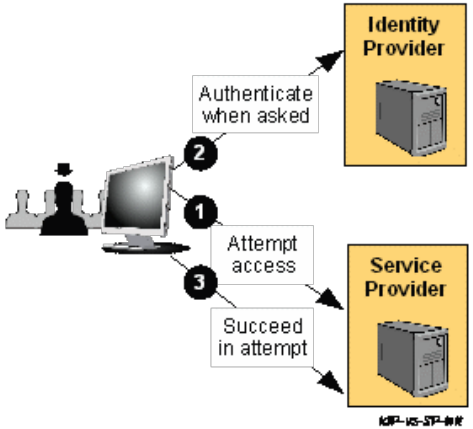
IdP-initiated と SP-initiated

IdP-initiatedは、IdPを起点として認証を開始



IdP-initiated

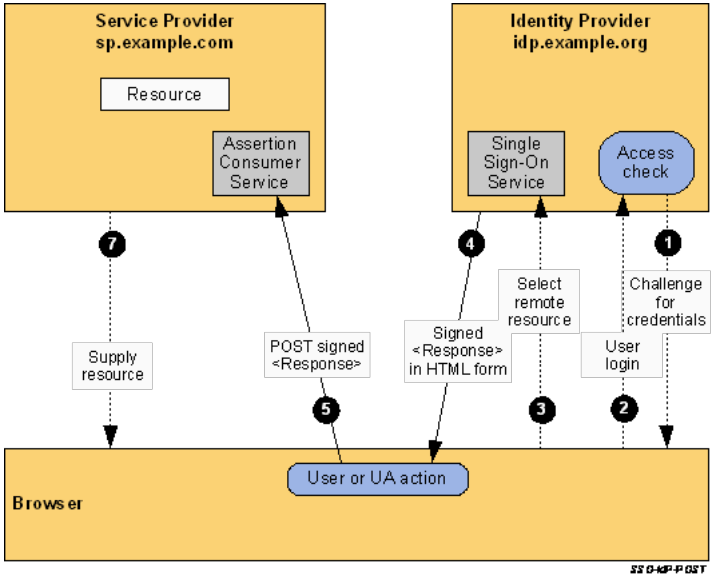
SP-initiatedは、SPを起点として認証を開始



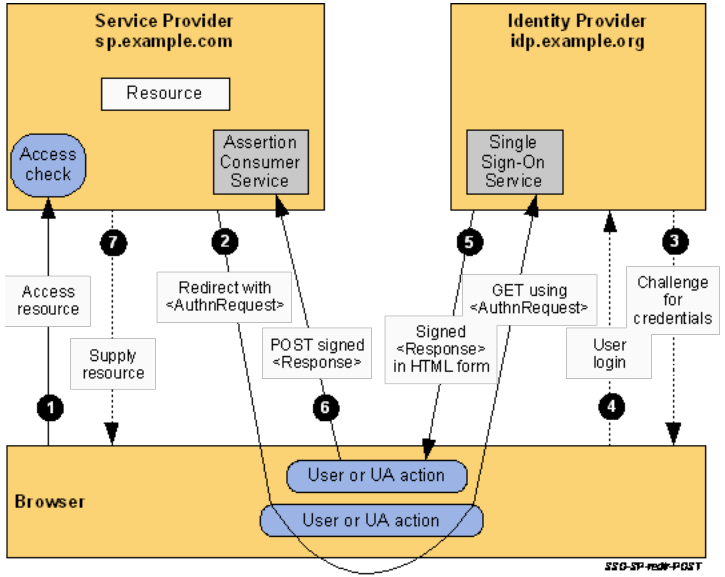
SP-initiated

SSO：バインディング（メッセージ交換方法の定義）

IdP-initiated：POSTバインディング

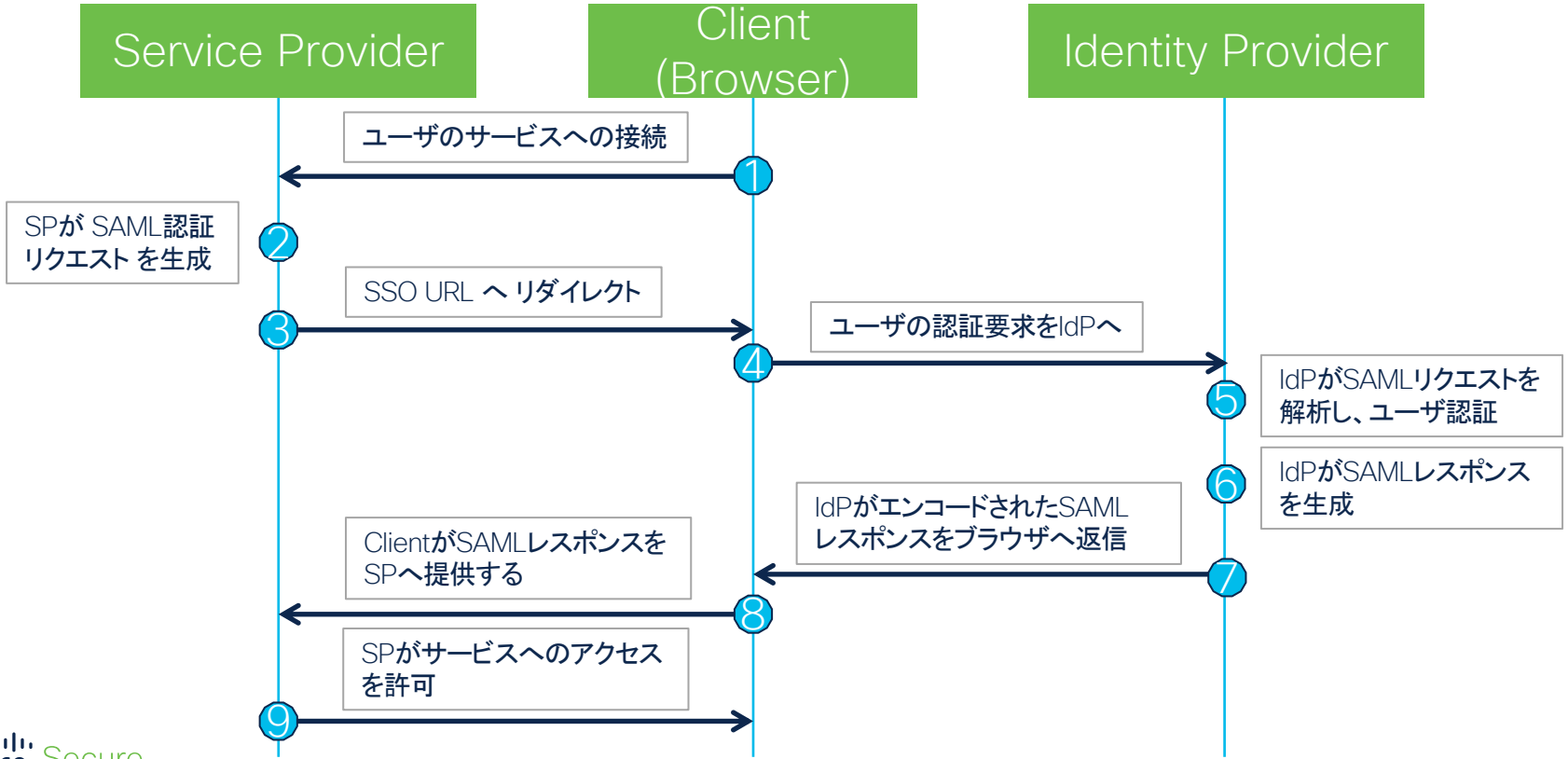


SP-initiated：リダイレクト/POSTバインディング

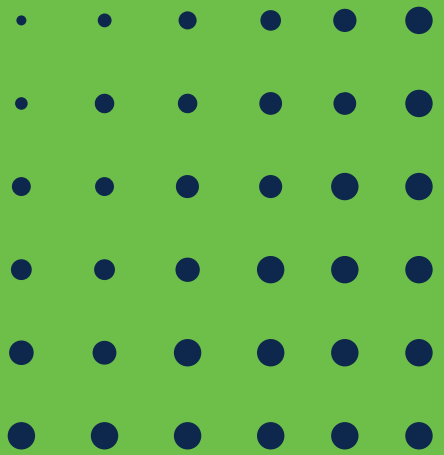


アーティファクトバインディングは省略

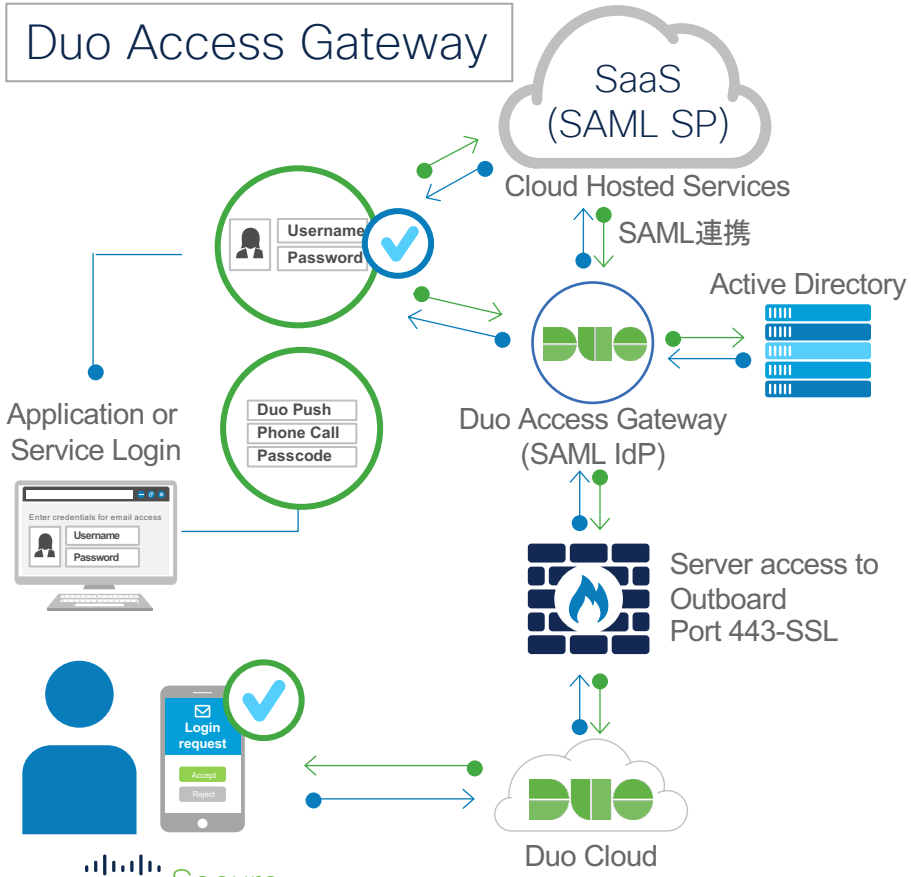
SAML Flow

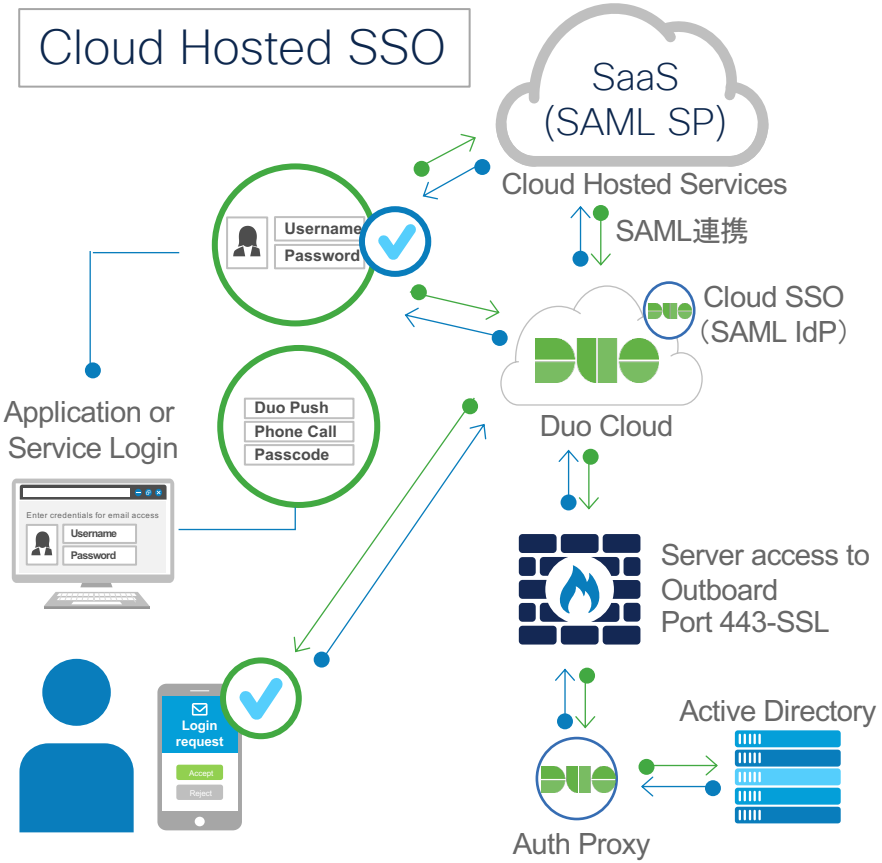


Duo SAML連携



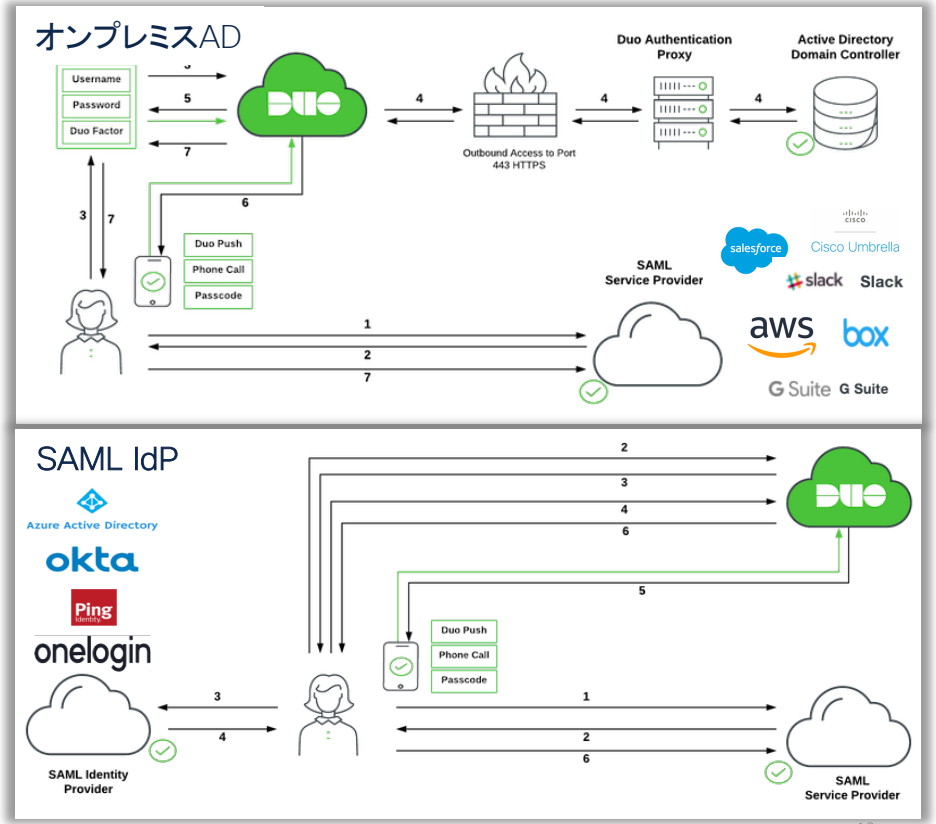
Duo SAML IdP





Duo Cloud SSO サポート

- SSO機能提供の拡張
  (オンプレIdP: Duo Access Gateway)
- すぐに、SSOを利用できる
- プライマリ認証のためのオンプレミスADとクラウドベースのSAML IDPの両方をサポート
- 全てのSAML対応アプリに SSO を提供



シンプルなセキュアSSO

ユーザとデバイスの信頼による Duoのシングルサインオン

- 1つのダッシュボードから全ての アプリケーションへ簡単にアクセス
- クラウドアプリケーションを通して 一貫したセキュリティ制御
- 全てのクラウドアプリケーションが セキュアに

連携するアプリケーション（一部）

Microsoft	VPNs	Cloud Apps	On-Premises	SSO	Custom
Office 365	cisco	salesforce	Epic	Microsoft Azure	REST APIS
Outlook	f5	Google Apps	ORACLE PEOPLESOFT	Active Directory Federation Services	WEB SDK
Remote Desktop Services	CITRIX	amazon web services	vmware Horizon View	okta	RADIUS
Windows Server	paloalto NETWORKS	box	>_SSH unix	PingIdentity	SAML
RRAS	Pulse Secure	slack	Shibboleth	onelogin	OIDC

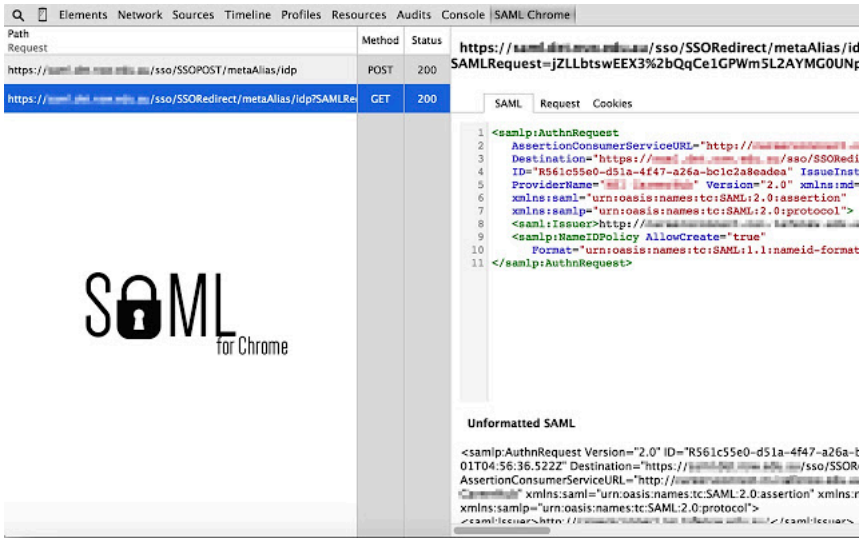
詳細情報: https://duo.com/docs

トラブルシューティング ツール

SAML Tools

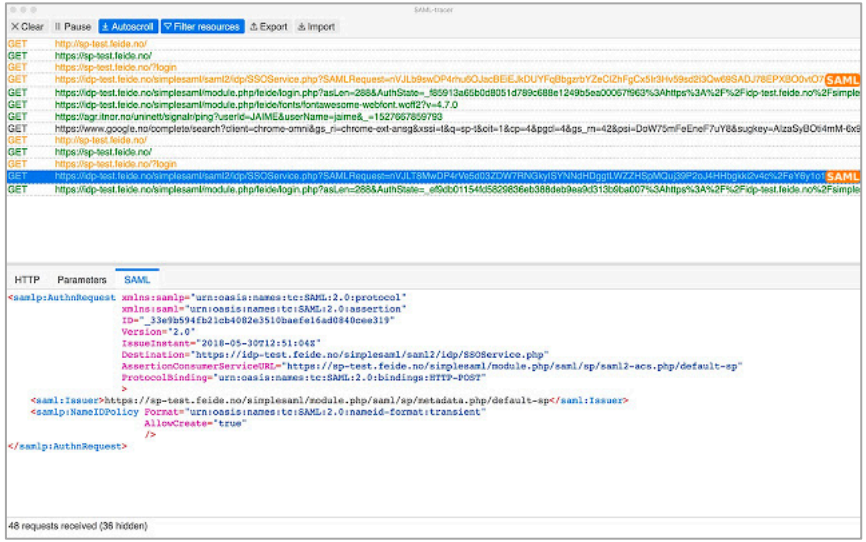
Chrome SAML Panel

- SAMLメッセージを可視化するデバッグツール
- Chrome のアドオン(拡張機能) としてインストール

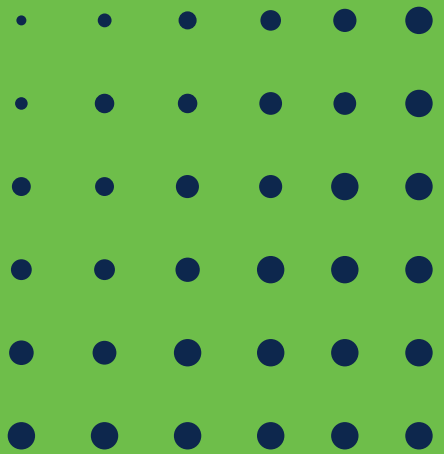


SAML-tracer

- SAMLメッセージを可視化するデバッグツール
- ブラウザ (Chrome, Firefox) のアドオンとしてインストール



Appendix



無償でDuoをご利用いただけます！

注）Duo Beyond機能をご利用の場合、ライセンスのアップグレードが必要となりますので、担当営業までご連絡ください。

■30日間フリートライアル申し込みサイト

https://www.cisco.com/c/m/ja_jp/duo/trial.html


cisco
Secure