

Decoding SAML Runes - How to set up SSO quickly in Jamf Pro



Sean Rabbitt

Jamf

Senior Consulting Engineer, Identity

Decoding SAML Runes

Anatomy of a SAML Token

Intercepting SAML Tokens

Modifying SAML Tokens

CMD-C CMD-V to Jamf Pro

Passing info to Jamf Connect

**Handouts for this Session will be
available at**

<https://github.com/sean-rabbit>

Decoding SAML Runes

Anatomy of a SAML Token

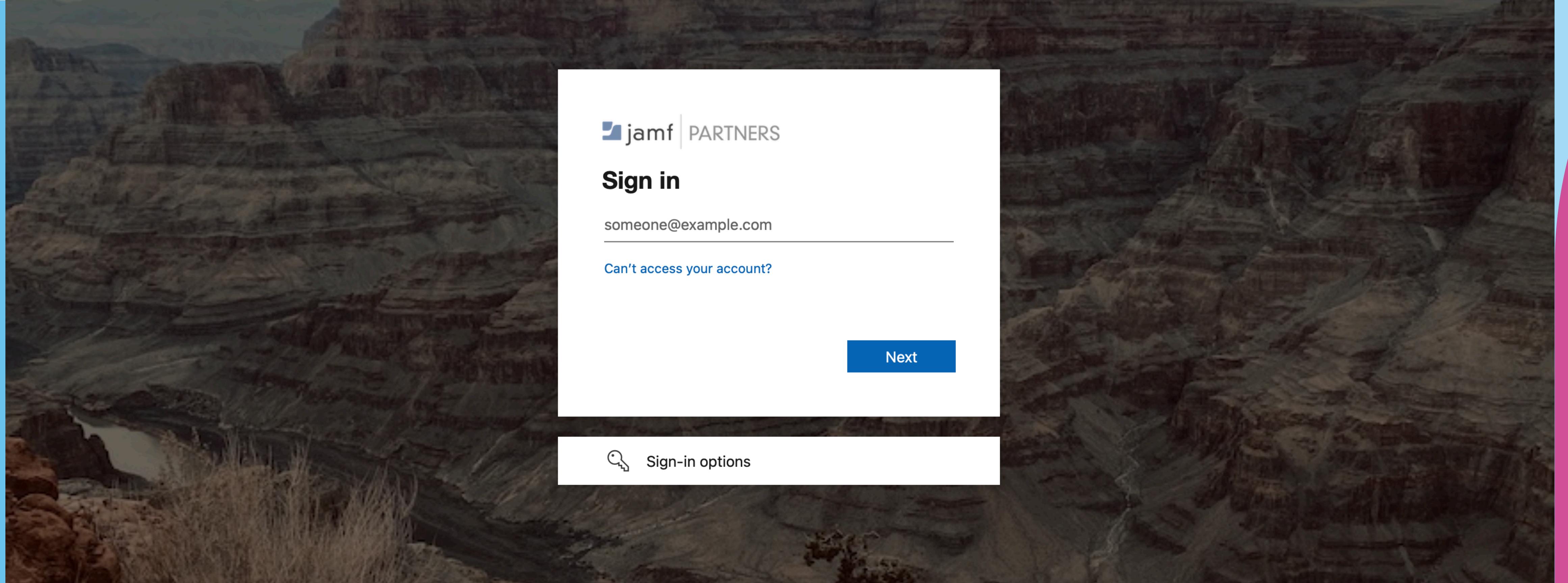
Intercepting SAML Tokens

Modifying SAML Tokens

CMD-C CMD-V to Jamf Pro

Passing info to Jamf Connect





Anatomy of a SAML token



This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" ID="_6ed97b27-9071-4e47-b85d-81155c25c89c" entityID="https://sts.windows.net/f83fb0da-8168-4bf9-aff2-3571c69c1000/">
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
<SignedInfo>
<CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
<SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
<Reference URI="#_6ed97b27-9071-4e47-b85d-81155c25c89c">
<Transforms>
<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
<Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
</Transforms>
<DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
<DigestValue>MuTvBzr/phB/XE/KBe68QGD9ajlogTxNuW/Q1IyXJyA=</DigestValue>
</Reference>
</SignedInfo>
<SignatureValue>
pN2j+zmcXanVNUtFLRDJpe+WSXmLOGdoLXu/1FGIIQzrSoxj8I7wYyZ/GAMTIl1Kkuubp/rkSoLYAWrWE6jt b7QZIiEQvlA4RIBSdZ4aL6wTGqEAWFqAZRx/4H3vgmKMn2yEeSS+EUC7PRMG+ZQYQmbLFwMbe7uFfZQHGu139VMlBeL9w5V333sIIeFdrHfMWR0Uw3MbFnX
</SignatureValue>
<KeyInfo>
<X509Data>
<X509Certificate>
MIIC8DCCAdigAwIBAgIQUuemG1XMFqdAuECB1P/Q7TANBgkqhkiG9w0BAQsFADA0MTIwMAYDVQQDEy1NaWNyb3NvZnQgQXp1cmUgRmVkJhdGVkIFNTTyBDZXJ0aWZpY2F0ZTAeFw0yMDA1MDEyMDUyMzZaFw0yMzA1MDEyMDUyMzJaMDQxMjAwBgNVBAMTKU1pY3Jvc29
</X509Certificate>
</X509Data>
</KeyInfo>
</Signature>
<RoleDescriptor xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:fed="http://docs.oasis-open.org/wsfed/federation/200706" xsi:type="fed:SecurityTokenServiceType" protocolSupportEnumeration="http://docs.oasis-open.org/wsfed/federation/200706#ProtocolSupportEnumeration">
<KeyDescriptor use="signing">
<KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
<X509Data>
<X509Certificate>
MIIC8DCCAdigAwIBAgIQUuemG1XMFqdAuECB1P/Q7TANBgkqhkiG9w0BAQsFADA0MTIwMAYDVQQDEy1NaWNyb3NvZnQgQXp1cmUgRmVkJhdGVkIFNTTyBDZXJ0aWZpY2F0ZTAeFw0yMDA1MDEyMDUyMzZaFw0yMzA1MDEyMDUyMzJaMDQxMjAwBgNVBAMTKU1pY3Jvc29
</X509Certificate>
</X509Data>
</KeyInfo>
</KeyDescriptor>
<fed:ClaimTypesOffered>
<auth:ClaimType xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706" Uri="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name">
<auth:DisplayName>Name</auth:DisplayName>
<auth:Description>The mutable display name of the user.</auth:Description>
</auth:ClaimType>
<auth:ClaimType xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706" Uri="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier">
<auth:DisplayName>Subject</auth:DisplayName>
<auth:Description>
An immutable, globally unique, non-reusable identifier of the user that is unique to the application for which a token is issued.
</auth:Description>
</auth:ClaimType>
<auth:ClaimType xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706" Uri="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname">
<auth:DisplayName>Given Name</auth:DisplayName>
<auth:Description>First name of the user.</auth:Description>
</auth:ClaimType>
<auth:ClaimType xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706" Uri="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname">

```

“ What the heck does SAML stand for anyway? ”

Anyone who has had to figure out acronyms ever

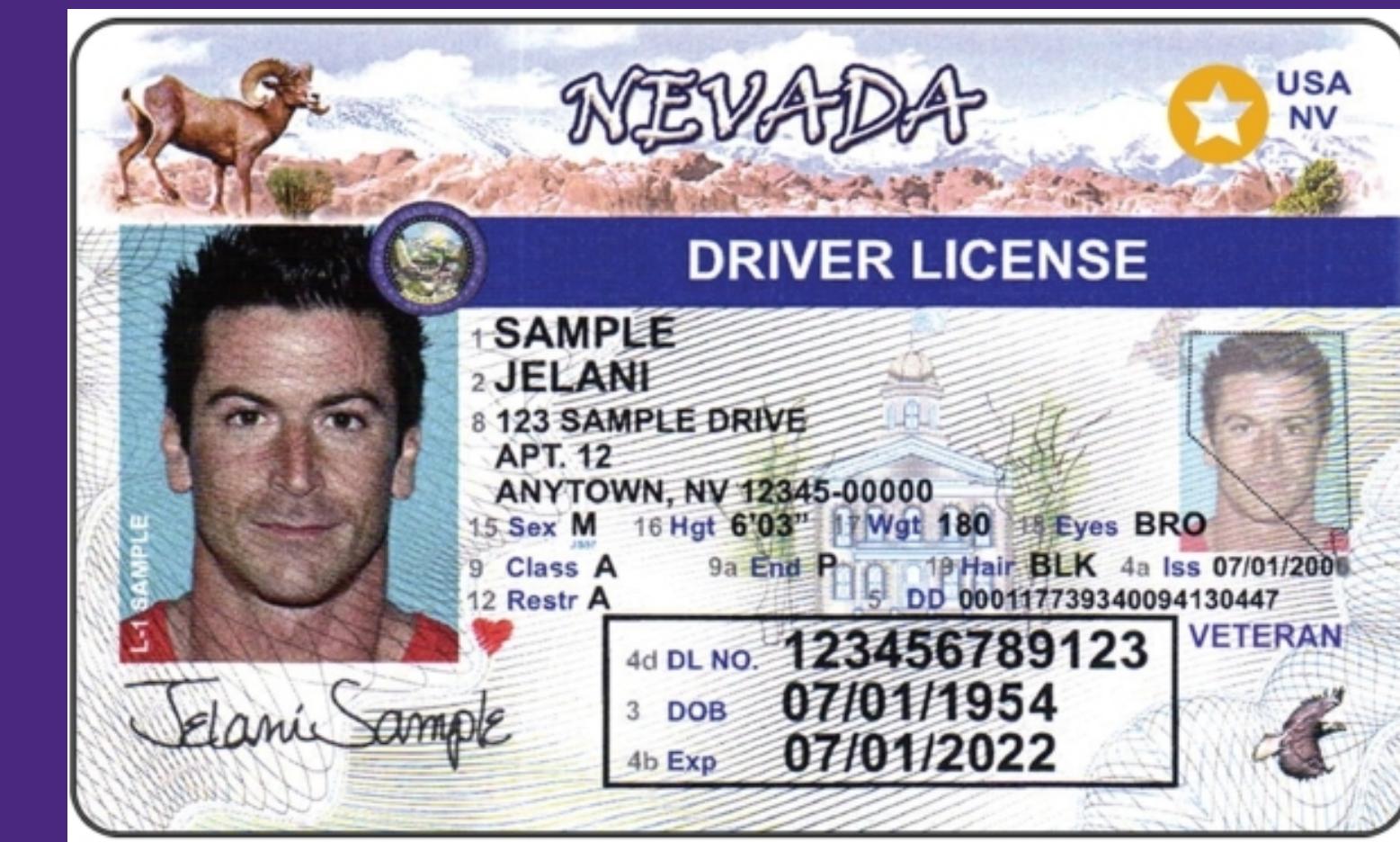
**“ What the heck
does SAML stand
for anyway? ”**

SAML:
Security
Assertion
Markup
Language

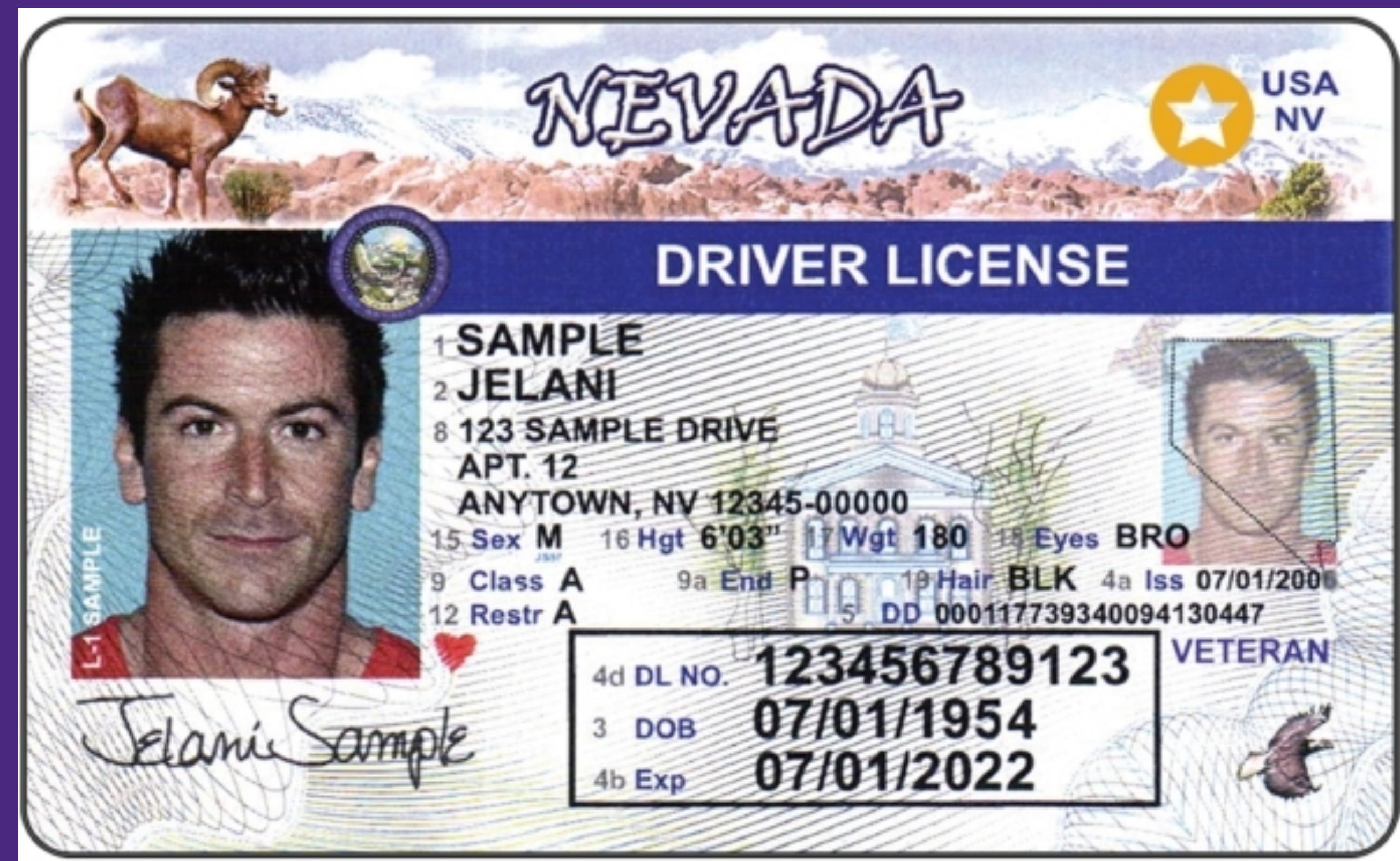
Anyone who has had to figure out acronyms ever

Anatomy of a SAML Token

- Application
- XML response
- Metadata
- Claims



Anatomy of a SAML Token



```
<?xml version="1.0" encoding="UTF-8"?>
<saml2p:Response Destination="https://server.jamfcloud.com/saml/SSO"
    ID="id26710666455415408895437065"
    InResponseTo="a45a5j96bcg8db658de7h7i6474f7"
    IssueInstant="2021-04-28T19:55:07.331Z"
    Version="2.0"
    xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns:xs="http://www.w3.org/2001/XMLSchema">
    <saml2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity"
        xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">http://www.okta.com/exk1j9bj5yvWHTlCT0h8</saml2: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/2001/04/xmldsig-more#rsa-sha256" />
            <ds:Reference URI="#id26710666455415408895437065">
                <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#">
                        <ec:InclusiveNamespaces PrefixList="xs"
                            xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" />
                    </ds:Transform>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
                <ds:DigestValue>mW7oYyS9DYnWfzI0DYlwvr5iIbQFoa2NDMjZN0FBVbw=</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
    </ds:Signature>
```

```

<ds:SignatureValue>
hPxgWc3XHc/wlsaoRxJnZQiu4zAMcEU5vx+ScvONL5EtQRUq6mHL8ymbDh7v0Fhs7osZA8vd7Vx2Mp1T02iKn0DkGjxPrPwo0pbWzj8xNzIh1pe8o0lcuY2wMyb7M6+qrKyeExe2iuHeow0IkXmKj64UkPlvHu40jw73V01yrb3l1WPxxnBvsVaP9bgeefYH51/XyJj3NFwI4se93xLBB92z5W+69IRsowJ+jyPBa87rrHG5JW17chRT9Tm+WftUCgGi0vs9qxHAgFD22350ddxdxiHL471mjxN+FBjmAg46YfcBkhEwcLuJv35pit8x0kqdohStcPL58ufqMBQ==

</ds:SignatureValue>
</ds:X509Data>
</ds:KeyInfo>
</ds:Signature>
</ds:X509Certificate>
MIIDnDCCAOsgAwIBAgIGAW3/TBAfMA0GCSqGSIb3DQEBCwUAMIGOMQswCQYDVQQGEwJVUzETMBEG A1UECAwKQ2FsaWZvcn5pYTEWMBQGA1UEBwwNU2FuIEZyW5jaXnjbzENMASGA1UECgwET2t0YTEU MBIGA1UECwLU1NPUHJvdmlkZXIxDzANBgNVBAMMBmphbWzzZTEcMBoGCSqGSIb3DQEJARYNaW5m b0Bva3RhLmNvbTAefw0x0TEwMjQx0TQyNTdaFw0y0TEwMjQx0TQzNTdaMIGOMQswCQYDVQQGEwJV
UzETMBEGAIUECAwKQ2FsaWZvcn5pYTEWMBQGA1UEBwwNU2FuIEZyW5jaXnjbzENMASGA1UECgwE T2t0YTEUMBIGA1UECwLU1NPUHJvdmlkZXIxDzANBgNVBAMMBmphbWzzZTEcMBoGCSqGSIb3DQEJ ARYNaW5mb0Bva3RhLmNvbTCASiW0QYJKoZIhvNAQEBBQADggEPADCCAQcCggEBAKPBLTj9WF gsq3GKug5gNcW5h0BzggjpaEZQyoCgVRj9o5k00uzhI4MKLNzwjk40Y9w3gfrzPHDUSUDnGh6
KEa4N1Esewm1qpgDgtqtTVow4sQBsV8avSpp/A72js/Dy/VTBoDg0RcyQ8InkYARq0wadieyR Atd0lKewTYfgxbzPbHuazJM2ZDvrbuVEfAnGxrBy7fdP4pBgiPfV6k2T74qroddlKJFjdmkLbjZ3 J5fvgcDU/L+bCiNY/Ov3oXAeqgNHJinj2YRSQziARLjfxFT4wdh0uiTKTjF036s0DcnkqVmGJ5h htKaI2uL/kMgYAF4kvzXzI4T9WsCaWEATANBgkqhkiG9w0BAqsFAAACQEAEA2xUskDgfft6un0
y7Ww0CPA8Che8Yu7Dja6ycBMzbZfv5FhtjSYUg9t/5Xg8JsSGLvnZArC6sMgFmCU6k01/ibsv 0ya7pZzy2XWHUnRIM0mloSJ+8wB4Vk+wsuSVB16XYEntVqq3Rl541EsdsMPvXNaAyDZR++q8rm xSSVkujsutPcavWhcRr8jyl/bERj1ex5E6v0mkws1yeYiogUQnsnkJEicgImjlQexVdpLhqvTe B7RK4Lj3ukJGivG3bdJXifJThg10HK5etj1s8Fo9mmJfxUnQ9CNZ0ryfrW47WNsNA2EDH4kINKp1
boEcddqYrxxydZ8euaxgw==

</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</ds:Signature>

```

```

<saml2p>Status xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol">
<saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" /></saml2p>Status>
<saml2:Assertion ID="id267106664554917852115280765" IssueInstant="2021-04-28T19:55:07.331Z" Version="2.0" xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:xs="http://www.w3.org/2001/XMLSchema">
<saml2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity" xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">http://www.okta.com/exk1j9bj5yyWHTlCT0h8</saml2:Issuer>
<saml2: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/2001/04/xmldsig-more#rsa-sha256" />
<ds:Reference URI="#id267106664554917852115280765">
<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#" />
<ec:InclusiveNamespaces PrefixList="xs" xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" />
</ds:Transform>
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
<ds:DigestValue>4Vzkyu04mqVMo6l1bRl1cz+lKL1xqTPB5LA7U4crTni=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>

```

```

<ds:SignatureValue>
Anr3tTSR3J00+v0lCeDANby7bSLyS0nmX+q82/GQy+/EIWA1GJIf1lxN+nW+7use1kW1j8tfESjPWqTSe80cEoquRsqRCdVAZt5Q1FZ/BR8Jmi/2aebjP0PXylV1My/FZYElUndUFpwtLX8Hm1KDwuC+WW+SGRh3sopFM078N2d/bpjY2CV0T0GFdc4X8outgqAfe8nKL0ygK0GiDov0nq9d0iNgmJF0qaAy+Z5Tlqzi8rDxrTTEJfR/04N6Y5yDJv+d1An5T/2MgsLYk2oye7H9FJGqV5cfE4B+ynW8cpTk0GgUqy/X6ZJk4ycPIJZndn0ThISQ==

</ds:SignatureValue>
<ds:KeyInfo>
<ds:X509Data>
<ds:X509Certificate>
MIIDnDCCAOsgAwIBAgIGAW3/TBAfMA0GCSqGSIb3DQEBCwUAMIGOMQswCQYDVQQGEwJVUzETMBEG A1UECAwKQ2FsaWZvcn5pYTEWMBQGA1UEBwwNU2FuIEZyW5jaXnjbzENMASGA1UECgwET2t0YTEU MBIGA1UECwLU1NPUHJvdmlkZXIxDzANBgNVBAMMBmphbWzzZTEcMBoGCSqGSIb3DQEJARYNaW5m b0Bva3RhLmNvbTAefw0x0TEwMjQx0TQyNTdaFw0y0TEwMjQx0TQzNTdaMIGOMQswCQYDVQQGEwJV
UzETMBEGAIUECAwKQ2FsaWZvcn5pYTEWMBQGA1UEBwwNU2FuIEZyW5jaXnjbzENMASGA1UECgwE T2t0YTEUMBIGA1UECwLU1NPUHJvdmlkZXIxDzANBgNVBAMMBmphbWzzZTEcMBoGCSqGSIb3DQEJ ARYNaW5mb0Bva3RhLmNvbTCASiW0QYJKoZIhvNAQEBBQADggEPADCCAQcCggEBAKPBLTj9WF gsq3GKug5gNcW5h0BzggjpaEZQyoCgVRj9o5k00uzhI4MKLNzwjk40Y9w3gfrzPHDUSUDnGh6
KEa4N1Esewm1qpgDgtqtTVow4sQBsV8avSpp/A72js/Dy/VTBoDg0RcyQ8InkYARq0wadieyR Atd0lKewTYfgxbzPbHuazJM2ZDvrbuVEfAnGxrBy7fdP4pBgiPfV6k2T74qroddlKJFjdmkLbjZ3 J5fvgcDU/L+bCiNY/Ov3oXAeqgNHJinj2YRSQziARLjfxFT4wdh0uiTKTjF036s0DcnkqVmGJ5h htKaI2uL/kMgYAF4kvzXzI4T9WsCaWEATANBgkqhkiG9w0BAqsFAAACQEAEA2xUskDgfft6un0
y7Ww0CPA8Che8Yu7Dja6ycBMzbZfv5FhtjSYUg9t/5Xg8JsSGLvnZArC6sMgFmCU6k01/ibsv 0ya7pZzy2XWHUnRIM0mloSJ+8wB4Vk+wsuSVB16XYEntVqq3Rl541EsdsMPvXNaAyDZR++q8rm xSSVkujsutPcavWhcRr8jyl/bERj1ex5E6v0mkws1yeYiogUQnsnkJEicgImjlQexVdpLhqvTe B7RK4Lj3ukJGivG3bdJXifJThg10HK5etj1s8Fo9mmJfxUnQ9CNZ0ryfrW47WNsNA2EDH4kINKp1
boEcddqYrxxydZ8euaxgw==

</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</ds:Signature>
<saml2:Subject xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
<saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">sean.rabbit@jamfse.io</saml2:NameID>
<saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
<saml2:SubjectConfirmationData InResponseTo="a45a5j96bcg8db658de7h7i6474f7" NotOnOrAfter="2021-04-28T20:00:07.331Z" Recipient="https://server.jamfcloud.com/saml/SSO" /></saml2:SubjectConfirmation>
</saml2:Subject>
<saml2:Conditions NotBefore="2021-04-28T19:50:07.331Z" NotOnOrAfter="2021-04-28T20:00:07.331Z" xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
<saml2:AudienceRestriction>
<saml2:Audience>https://server.jamfcloud.com/saml/metadata</saml2:Audience>
</saml2:AudienceRestriction>
</saml2:Conditions>
<saml2:AuthnStatement AuthnInstant="2021-04-28T19:54:27.999Z" SessionIndex="a45a5j96bcg8db658de7h7i6474f7" xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
<saml2:AuthnContext>
<saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</saml2:AuthnContextClassRef>
</saml2:AuthnContext>
</saml2:AuthnStatement>

```

```
<saml2:AttributeStatement xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
  <saml2:Attribute Name="http://schemas.xmlsoap.org/claims/Group"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
    <saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:type="xs:string">macadmin</saml2:AttributeValue>
    <saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:type="xs:string">System Engineers</saml2:AttributeValue>
  </saml2:Attribute>
  <saml2:Attribute Name="RealName"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
    <saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:type="xs:string">Sean Rabbitt</saml2:AttributeValue>
  </saml2:Attribute>
  <saml2:Attribute Name="UserName"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
    <saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:type="xs:string">sean.rabbitt</saml2:AttributeValue>
  </saml2:Attribute>
  <saml2:Attribute Name="ShoeSize"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
    <saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:type="xs:string">10.5 Wide</saml2:AttributeValue>
  </saml2:Attribute>
</saml2:AttributeStatement>
```

The name of the attribute/claim/assertion

The value inside of the attribute/claim/assertion

```
<saml2:Attribute Name="RealName"  
                  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">  
    <saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"  
                          xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  
                          xsi:type="xs:string">Sean Rabbitt</saml2:AttributeValue>  
</saml2:Attribute>  
<saml2:Attribute Name="UserName"  
                  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">  
    <saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"  
                          xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  
                          xsi:type="xs:string">sean.rabbitt</saml2:AttributeValue>  
</saml2:Attribute>
```

The name of the attribute/claim/assertion

```
<saml2:AttributeStatement xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
  <saml2:Attribute Name="http://schemas.xmlsoap.org/claims/Group"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
    <saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:type="xs:string">macadmin</saml2:AttributeValue>
    <saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:type="xs:string">System Engineers</saml2:AttributeValue>
  </saml2:Attribute>
```

The value(s) inside of the attribute/claim/assertion

Decoding SAML Runes

Anatomy of a SAML Token

Intercepting SAML Tokens

Modifying SAML Tokens

CMD-C CMD-V to Jamf Pro

Passing info to Jamf Connect

**“ But Sean, you said this was
the easy mode to setting up
Jamf Pro? ”**

Everyone watching this webinar now

Read The Fantastic Manual



jamf PRO

Jamf Pro Administrator's Guide

Version 10.30.0 | [Other Versions](#)

- › Preface
- › Overview of Technologies
- › Before You Begin
- › Jamf Pro System Settings
 - Jamf Pro User Accounts and Groups
 - Integrating with LDAP Directory Services
- › Cloud Identity Providers
- Single Sign-On**
 - Integrating with an SMTP Server
 - Email Notifications
 - Activation Code

Identity Provider Configuration Settings

To implement single sign-on (SSO) with Jamf Pro, you must configure settings in your identity provider's console, portal, or a similar tool. Configuring settings in an IdP usually must be completed before you enable SSO in Jamf Pro, and some commonly used IdPs have pre-configured SSO settings specific to Jamf Pro.

Important: Depending on your IdP, setting up SSO may require simultaneous configuration between your IdP and Jamf Pro to ensure some settings are mapped correctly. Additional settings or steps may also be required.

For IdP-specific instructions for configuring SSO, see the following articles:

- [Configuring Single Sign-On with Okta](#)
- [Configuring Single Sign-On with Active Directory Federation Services](#)
- [Configuring Single Sign-On with Shibboleth](#)
- [Configuring Single Sign-On with OneLogin](#)
- [Configuring Single Sign-On with Ping Identity](#)
- [Configuring Single Sign-On with G Suite \(Google Apps\)](#)
- [Configuring Single Sign-On with Centrify](#)

: For information on configuring SSO with Azure AD, see the following documentation from Microsoft: <https://docs.microsoft.com/azure/active-directory/saas-apps/jamfprosamiconnector-tutorial>.

For information on configuring SSO with Entrust Identity as a Service, see the following documentation from Entrust:
https://entrust.us.trustedauth.com/documentation/help/admin/Integrate_Jamf_Pro.htm.

<https://jamf.it/easyssso>

FAILOVER URL



Failover Login URL Users with Single Sign-On Update privileges can authenticate with a Jamf Pro user account by going to the following URL:



Copy to clipboard

[https://\[your_server\]/?failover](https://[your_server]/?failover)

[https://\[your_server\]/?failover](https://[your_server]/?failover)

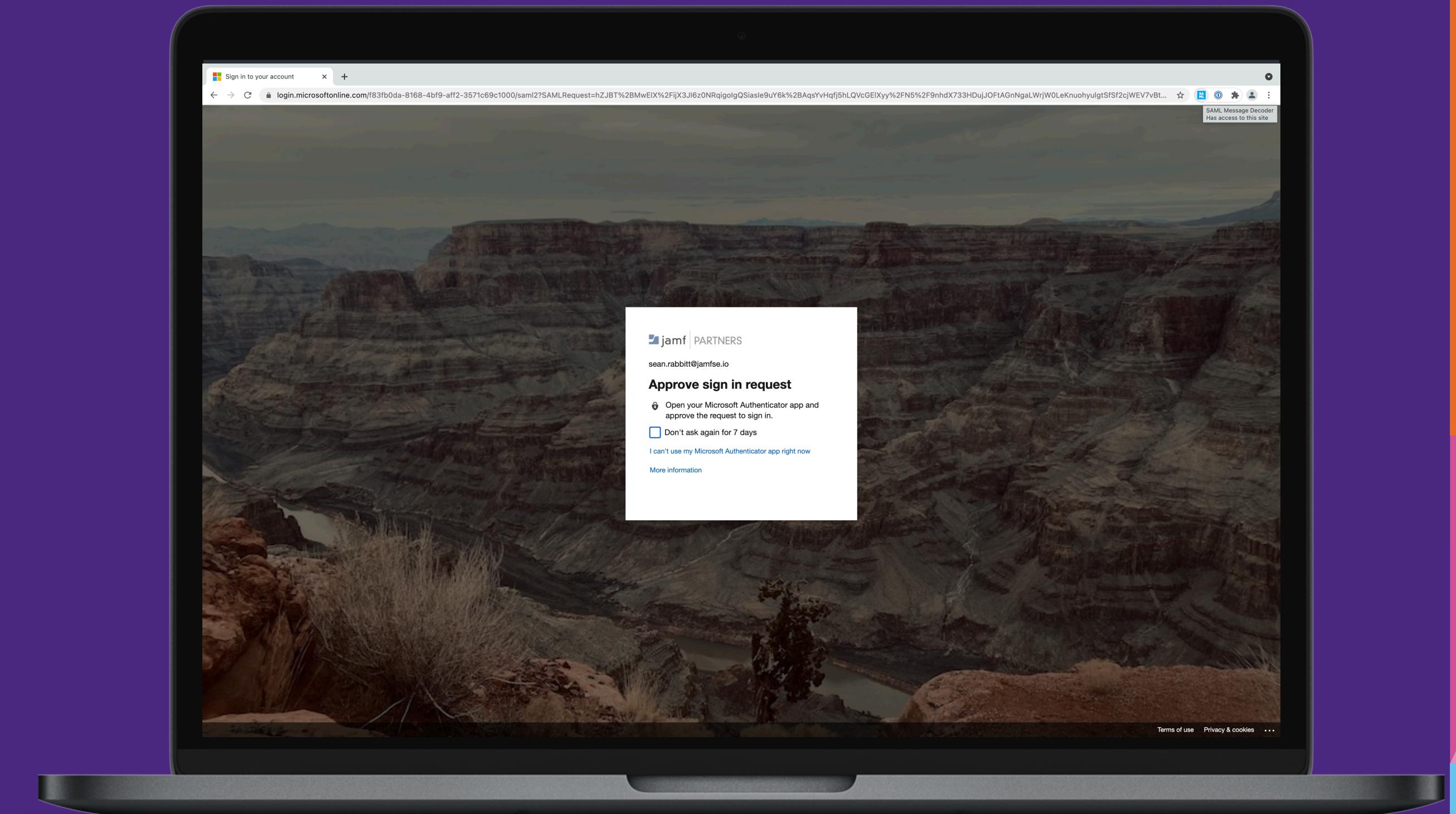
Intercepting SAML Requests

- Google Chrome
- SAML plugin

OR

- A proxy application
- SAML Decoder

like <https://www.samltool.com>



SAML Decoder Plugins

- SAML Message Decoder - <https://bit.ly/3hMROkM>
<https://github.com/magnussuther/saml-message-decoder-extension>
- SAML Chrome Panel - <https://bit.ly/2UCI2JK>
- SAML Webtools Extension - <https://bit.ly/36p1We8>

Mac, iPad, iPhone, and Apple T X +

jamf.com

English ▾

jamf Products Solutions Pricing Resources Contact Jamf Nation Log in Start Trial

The Standard in Apple Enterprise Management

Jamf is trusted by 50,000+ businesses, schools and hospitals to maximize their Apple initiatives.

Try Jamf for Free

Why choose Jamf?



CONNECT
MANAGE
PROTECT

We help organizations succeed with Apple.

With sole focus on the Apple ecosystem, industry leaders across the globe choose Jamf to:

- Automate the entire lifecycle of Apple management
- Personalize Apple devices to a specific user's needs
- Preserve the Apple device experience users demand
- Access the largest Apple IT community on the planet

Why pair Jamf with Apple?

Jamf is the only Apple Enterprise Management solution of scale that remotely connects, manages and protects Apple users, devices and services.

Chat with Jamf Sales

Chrome File Edit View History Bookmarks Profiles Tab Window Help

Jamf Pro Dashboard*

d.com/index.html

2 - SAMLResponse via post binding, at Thu, 22 Jul 2021 16:42:53 GMT (UTC)

[Copy this message](#)

jamf PRO

Computers Devices Users

VERSION
10.30.3-t1624643096

MANAGED
Computers: 6
Mobile Devices: 5

UNMANAGED
Computers: 3
Mobile Devices: 4

<samlp:Response ID="_ac2c149e-7c11-42e5-9cc6-2bdcb7db4683"
Version="2.0"
IssueInstant="2021-07-22T16:42:52.902Z"
Destination="https://[REDACTED].com/saml/SSO"
InResponseTo="ah6aadjae43agceeed56z14eh0f0dc"
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
 <Issuer xmlns="urn:oasis:names:tc:SAML:2.0:assertion">https://sts.windows.net/f83fb0da-8168-4bf9-aff2-
3571c69c1000/</Issuer>
 <samlp:Status>
 <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" /></samlp:Status>
 <Assertion ID="_fb6f41f9-975d-4766-b292-320186d03701"
 IssueInstant="2021-07-22T16:42:52.886Z"
 Version="2.0"
 xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
 <Issuer>https://sts.windows.net/f83fb0da-8168-4bf9-aff2-3571c69c1000/</Issuer>
 <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
 <SignedInfo>
 <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
 <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
 <Reference URI="#_fb6f41f9-975d-4766-b292-320186d03701">
 <Transforms>
 <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
 <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
 </Transforms>
 <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
 <DigestValue>+RqWYNh/T3sFUyE9yUW3JJGEhEQatKnINqTeuTYMj8Y=</DigestValue>
 </Reference>
 </SignedInfo>
 <SignatureValue>
JNfKNCJhuTTU3rlHUW4KYrVdEgE7RuqlIcX5mDalopQ7MHEHjeGjAoVLu6uWEvxlyGqQ3Vpn+XpF85odV43RVabNFEEsyQNriOXUEozPP/RfFCgyR+ohjh4upJjM9
HD7S7DpiyPDDqq3GD7VtQfpELjUa4dkZhwmnFiulAyOz4AIg1SoTEWN5hNuOWbnGm/uOtIX7Rs1vi2Vkt7PGTiD+jcgi+uQkgYxH+fOj4sq+obX1TxNiOu6EV/xWB
ARZlMPRR8alTLeNp10tfLWNZriL7B9694WTRJEBpqD0hUewlGzn9A4Cq8UzgjJc75Uz113KK6LzY1vnsea+ZQ4WcBEQ==
 </SignatureValue>
 <KeyInfo>
 <X509Data>
 <X509Certificate>

Collapse Menu

virtual JNUK 2021

User Mapping

Identity Provider User Mapping Specify how users will be extracted from the SAML assertion



NameID



Custom Attribute:
(e.g., "UserName")

username

Jamf Pro User Mapping Specify how users from your identity provider will be mapped to Jamf P



Username



Email

Identity Provider Group Attribute Name Name of the SAML assertion attribute containing your group information

http://schemas.microsoft.com/ws/2008/06/identity/claims/groups

RDN Key For LDAP Group Relative Distinguished Name key to extract group name from the LDAP assertion

[+ New](#) [Password Policy](#)

USERNAME	FULL NAME	EMAIL	TYPE	ACCESS	SITE	PRIVILEGES
			Standard User	Full Access		Administrator
DemoKitAPIUser	API Only Users		Standard User	Full Access		Custom
enroll	Enrollment User		Standard User	Full Access		Enrollment
jamfSetup	API Service Account created on Fri May 8 09:22:02 EDT 2020 by superadmin		Standard User	Full Access		Custom
superadmin	User for initial JPS setup		Standard User	Full Access		Administrator
Jamf Pro User Groups (1)						
GROUP NAME	TYPE	MEMBERS	ACCESS	SITE	PRIVILEGES	
System Engineers	Standard Group	0	Full Access		Administrator	

User Mapping

Identity Provider User Mapping Specify how users will be extracted from the SAML assertion



NameID



Custom Attribute:
(e.g., "UserName")

username

Jamf Pro User Mapping Specify how users from your identity provider will be mapped to Jamf P



Username



Email

User Mapping

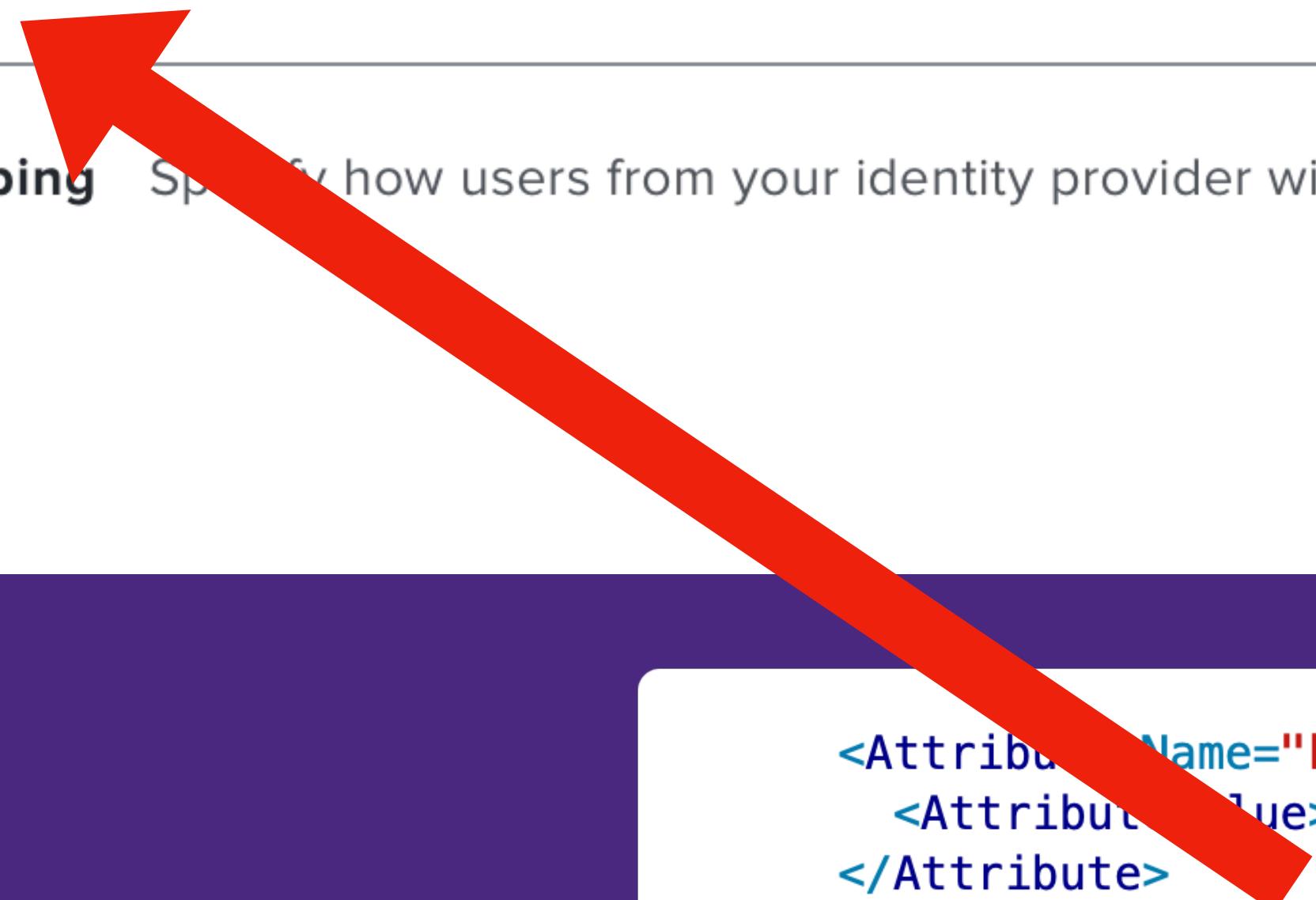
Identity Provider User Mapping Specify how users will be extracted from the SAML assertion

- NameID
- Custom Attribute:
(e.g., "UserName")

username

Jamf Pro User Mapping Specify how users from your identity provider will be mapped to Jamf Pro

- Username
- Email

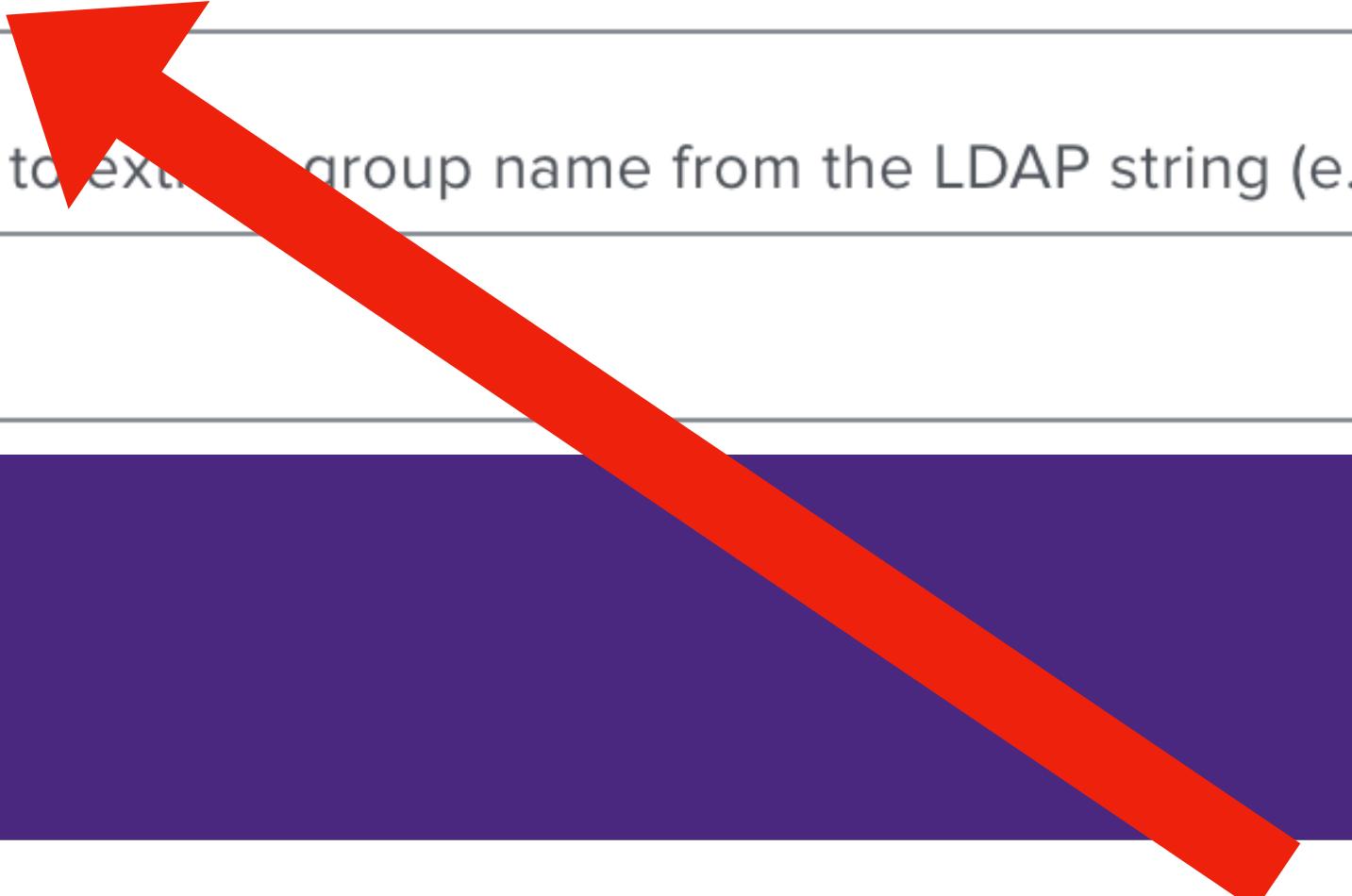


```
<Attribute Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name">
  <AttributeValue>sean.rabbitt@jamfse.io</AttributeValue>
</Attribute>
<Attribute Name="username">
  <AttributeValue>sean.rabbitt</AttributeValue>
</Attribute>
```

Identity Provider Group Attribute Name Name of the SAML assertion attribute containing your group (e.g., "GroupName")

http://schemas.microsoft.com/ws/2008/06/identity/claims/groups

RDN Key For LDAP Group Relative Distinguished Name key to extract group name from the LDAP string (e.g., "CN" or "DC")



```
<Attribute Name="http://schemas.microsoft.com/ws/2008/06/identity/claims/groups">
  <AttributeValue>sudo</AttributeValue>
  <AttributeValue>AWS Admins</AttributeValue>
  <AttributeValue>Okta Admins</AttributeValue>
  <AttributeValue>Jamf Protect Limited Access</AttributeValue>
  <AttributeValue>System Engineers</AttributeValue>
  <AttributeValue>macadmin</AttributeValue>
  <AttributeValue>TrialServerAdmin</AttributeValue>
  <AttributeValue>All Jamfs</AttributeValue>
</Attribute>
```

Settings : System Settings > Cloud Identity Providers

← My Cloud Identity Provider

[Server Configuration](#) [Mappings](#)

Configuration for Azure

Display Name Unique display name for the identity provider configuration

My Cloud Identity Provider

Required

Transitive groups for SSO

When single sign-on with Azure as an identity provider is configured, all groups that the group is a member of are included in the lookup. This affects the privileges granted for the account.

Decoding SAML Runes

Anatomy of a SAML Token

Intercepting SAML Tokens

Modifying SAML Tokens

CMD-C CMD-V to Jamf Pro

Passing info to Jamf Connect

Microsoft Azure

Home > jamfse.io > Enterprise applications > Jamf Pro - hare.jamfcloud.com >

Jamf Pro - | SAML-based Sign-on

Enterprise Application

Overview Deployment Plan

Manage

- Properties
- Owners
- Roles and administrators (Preview)
- Users and groups
- Single sign-on**
- Provisioning
- Self-service

Security

- Conditional Access
- Permissions
- Token encryption

Activity

Set up Single Sign-On with SAML

Read the [configuration guide](#) for help integrating Jamf Pro - hare.jamfcloud.com.

1 Basic SAML Configuration

Identifier (Entity ID)	https://[REDACTED]/saml/metadata
Reply URL (Assertion Consumer Service URL)	https://[REDACTED]/saml/SSO
Sign on URL	https://[REDACTED]
Relay State	<i>Optional</i>
Logout Url	<i>Optional</i>

2 User Attributes & Claims

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
username	user.onpremisesaccountname
Unique User Identifier	user.userprincipalname
Group	user.groups

Microsoft Azure

User Attributes & Claims

...

+ Add new claim

+ Add a group claim

Columns

Required claim

Claim name	Value
Unique User Identifier (Name ID)	user.userprincipalname [nameid-for...]

Additional claims

Claim name	Value
http://schemas.microsoft.com/ws/2008/06/identity/claims/groups	user.groups [All]
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname
username	user.onpremisesaccountname

Microsoft Azure

Group Claims

Manage the group claims used by Azure AD to populate SAML tokens issued to your app

Which groups associated with the user should be returned in the claim?

None

All groups

Security groups

Directory roles

Groups assigned to the application

Source attribute *

sAMAccountName

Group ID

sAMAccountName

NetBIOSDomain\sAMAccountName

DNSDomain\sAMAccountName

On Premises Group Security Identifier

Namespace (optional)

Emit groups as role claims ⓘ

Microsoft Azure

Home > Jamf Pro - hare.jamfcloud.com > SAML-based Sign-on > User Attributes & Claims >

Manage claim

X

 Save  Discard changes

Name *

username



Namespace

Enter a namespace URI



Source *

Attribute Transformation

Source attribute *

user.onpremisesaccountname



Claim conditions

user.localuserprincipalname

user.mail

user.mailnickname

user.netbiosname

user.objectid

user.onpremisesdistinguishedname

user.onpremisessecurityidentifier

user.onpremisesaccountname

user.onpremisesuserprincipalname

user.othermail

user.physicaldeliveryofficename

Manage transformation

X

Transformation *

Select from drop down



Parameter 1 *

|

Contains()

EndWith()

Extract()

ExtractAlpha()

ExtractMailPrefix()

ExtractNumeric()

IfEmpty()

[Dashboard](#)[Directory](#)[Applications](#)[Applications](#)[Self Service](#)[Security](#)[Workflow](#)[Reports](#)[Settings](#)[General](#)[Sign On](#)[Mobile](#)[Import](#)[Assignments](#)

Settings

[Edit](#)

Sign on methods

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

Application username is determined by the user profile mapping. [Configure profile mapping](#)

 SAML 2.0

Default Relay State

Attributes (Optional) [Learn More](#)

Attribute Statements (optional)

Name	Value
------	-------

© copyright 2002-2021 Jamf

Okta

Attribute Statements (optional)

Name	Name format (optional)	Value
RealName	Unspecified ▾	user.displayName ▾
UserShortName	Unspecified ▾	user.nickName ▾ X
exampleShort	Unspecified ▾	substringBefore(user.email, ' ▾ X
Add Another		

<https://developer.okta.com/docs/reference/okta-expression-language/>

substringBefore(user.email, "@")

<https://developer.okta.com/docs/reference/okta-expression-language/>

Decoding SAML Runes

Anatomy of a SAML Token

Intercepting SAML Tokens

Modifying SAML Tokens

CMD-C CMD-V to Jamf Pro

Passing info to Jamf Connect

```
<Attribute Name="http://schemas.microsoft.com/ws/2008/06/identity/claims/groups">
  <AttributeValue>sudo</AttributeValue>
  <AttributeValue>AWS Admins</AttributeValue>
  <AttributeValue>Okta Admins</AttributeValue>
  <AttributeValue>Jamf Protect Limited Access</AttributeValue>
  <AttributeValue>System Engineers</AttributeValue>
  <AttributeValue>macadmin</AttributeValue>
  <AttributeValue>TrialServerAdmin</AttributeValue>
  <AttributeValue>All Jamfs</AttributeValue>
</Attribute>
```

User Mapping

Identity Provider User Mapping Specify how users will be extracted from the SAML assertion

- NameID
 Custom Attribute:
(e.g., "UserName")

username

Jamf Pro User Mapping Specify how users from your identity provider will be mapped to Jamf Pro users

- Username
 Email

Identity Provider Group Attribute Name Name of the SAML assertion attribute containing your group (e.g., "GroupName")

http://schemas.microsoft.com/ws/2008/06/identity/claims/groups

RDN Key For LDAP Group Relative Distinguished Name key to extract group name from the LDAP string (e.g., "CN" or "DC")

Decoding SAML Runes

Anatomy of a SAML Token

Intercepting SAML Tokens

Modifying SAML Tokens

CMD-C CMD-V to Jamf Pro

Passing info to Jamf Connect

Settings : Global Management > Enrollment Customization

← Welcome

Edit Pane

Display Name

Azure

Pane Type Type of pane to display during enrollment

Single Sign-On Authentication ▾

Configure Enrollment Access For:

Any identity provider user

Only this group:

Enable Jamf Pro to pass user information to Jamf Connect
Allow Jamf Pro to pass the Account Name and the Account Full Name to Jamf Connect

+ Add Pane

Identity Provider Attribute Mappings

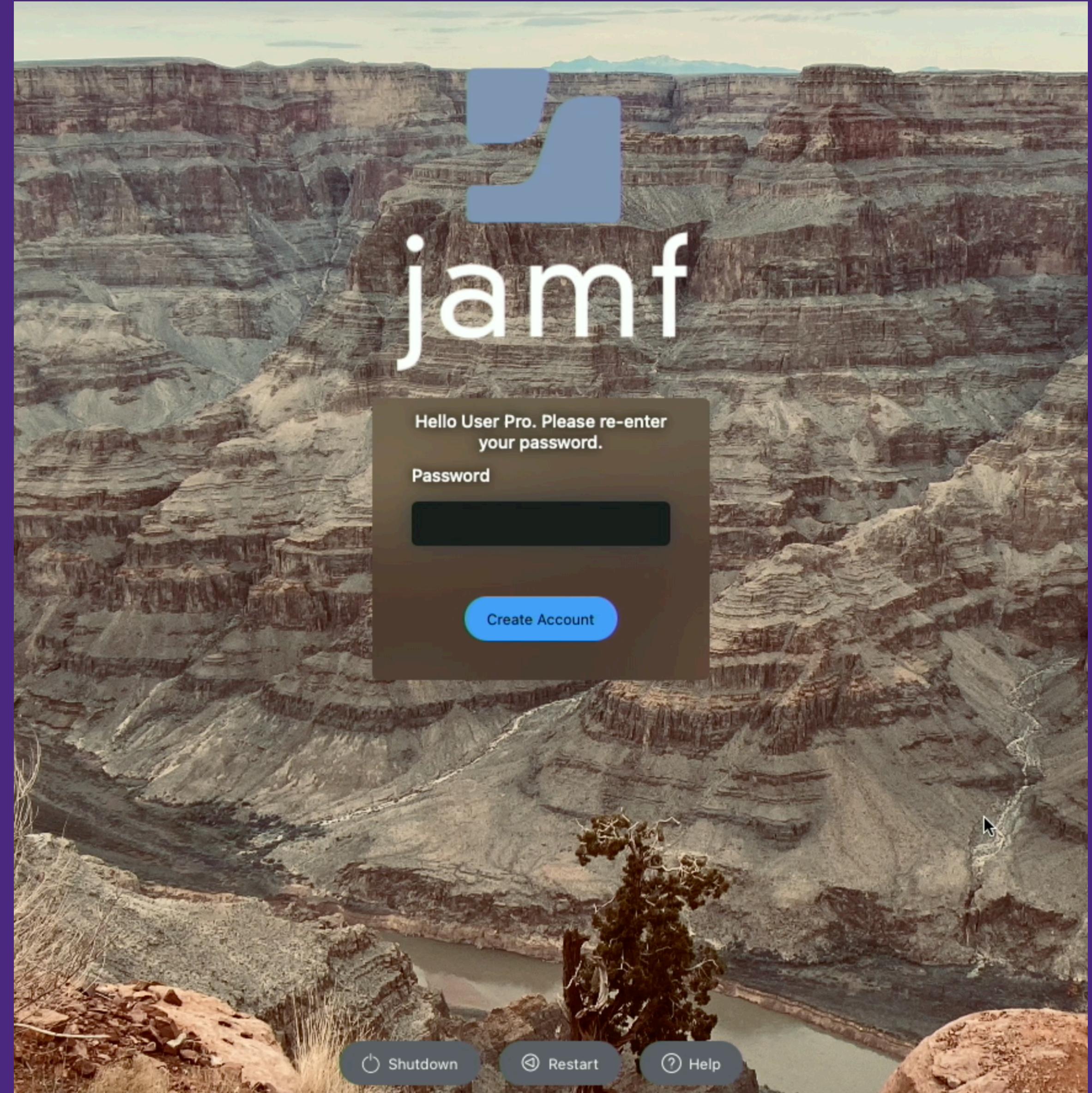
Account Name Identity Provider attribute to map to the Account Name

username

Account Full Name Identity Provider attribute to map to the Account Full Name

http://schemas.microsoft.com/identity/claims/displayname

Cancel Apply



© copyright 2002-2021 Jamf

<https://www.jamf.com/blog/zero-touch-deployment-with-jamf-pro-and-jamf-connect/>

Decoding SAML Runes

Anatomy of a SAML Token

Intercepting SAML Tokens

Modifying SAML Tokens

CMD-C CMD-V to Jamf Pro

Passing info to Jamf Connect

Thank you for listening!