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-rabbitt

Decoding SAML Runes

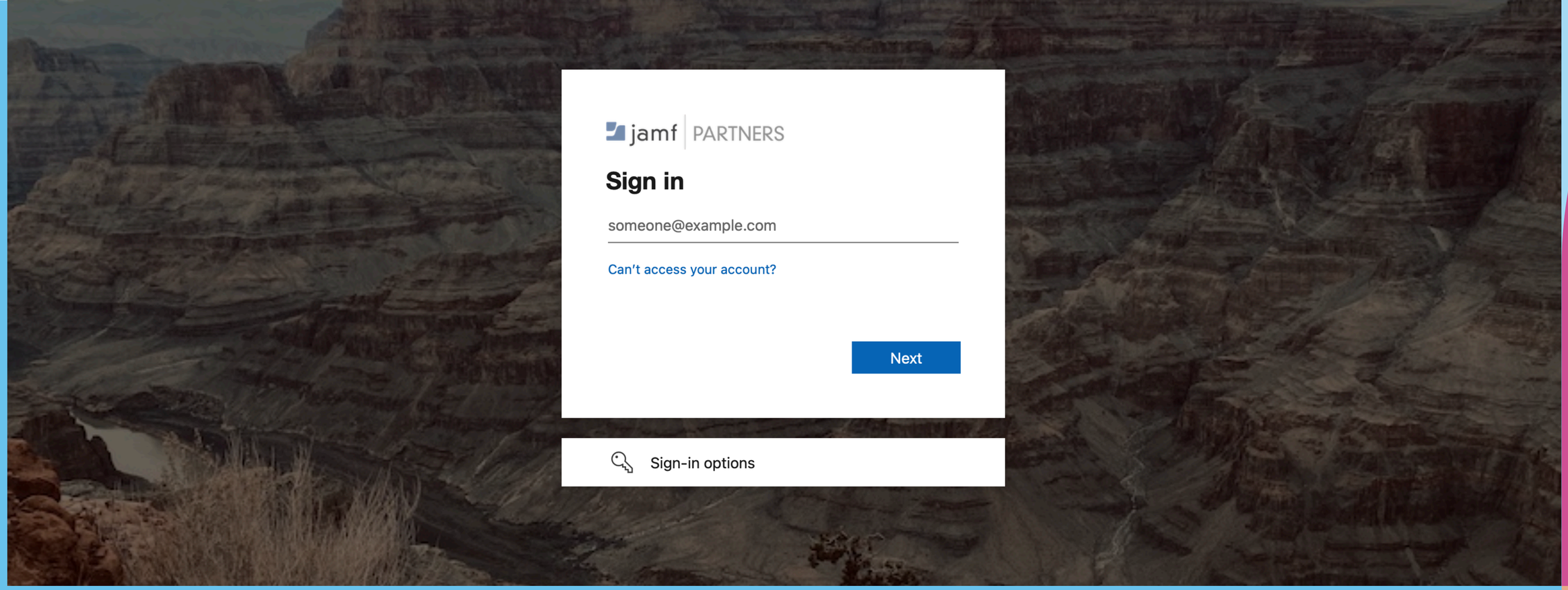
Anatomy of a SAML Token

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/rkSoLYAWrWE6jtb7QZIiEQvlA4RIBSdZ4aL6wTGqEAWFqAZRx/4H3vgmKMn2yEeSS+EUC7PRMG+ZQYQmblFwMbe7uFfZQHGu139VMlBeL9w5V333sIIeFdrHfMWR0Uw3MbFnX
</SignatureValue>
<KeyInfo>
<X509Data>
<X509Certificate>
MIIC8DCCAdigAwIBAgIQUeemG1XMFqdAuECB1P/Q7TANBgkqhkiG9w0BAQsFADA0MTIwMAYDVQQDEylNaWNyb3NvZnQgQXp1cmUgRmVkZXJhdGVkIFNTTyBDZXJ0aWZpY2F0ZTAeFw0yMDA1MDEyMDUyMzZaFw0yMzA1MDEyMDUyMzZaMDQxMjAwBgNVBAMTKU1pY3Jvc29
</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="ht
<KeyDescriptor use="signing">
<KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
<X509Data>
<X509Certificate>
MIIC8DCCAdigAwIBAgIQUeemG1XMFqdAuECB1P/Q7TANBgkqhkiG9w0BAQsFADA0MTIwMAYDVQQDEylNaWNyb3NvZnQgQXp1cmUgRmVkZXJhdGVkIFNTTyBDZXJ0aWZpY2F0ZTAeFw0yMDA1MDEyMDUyMzZaFw0yMzA1MDEyMDUyMzZaMDQxMjAwBgNVBAMTKU1pY3Jvc29
</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? ”

—

Anyone who has had to figure out acronyms ever

SAML:

Security

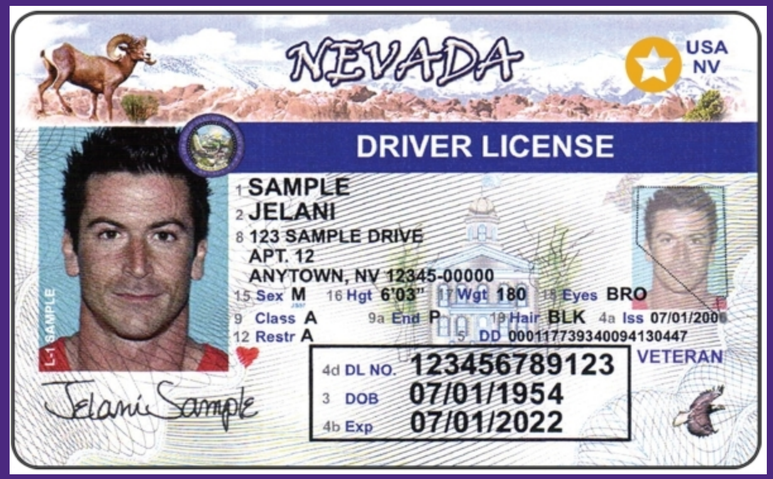
Assertion

Markup

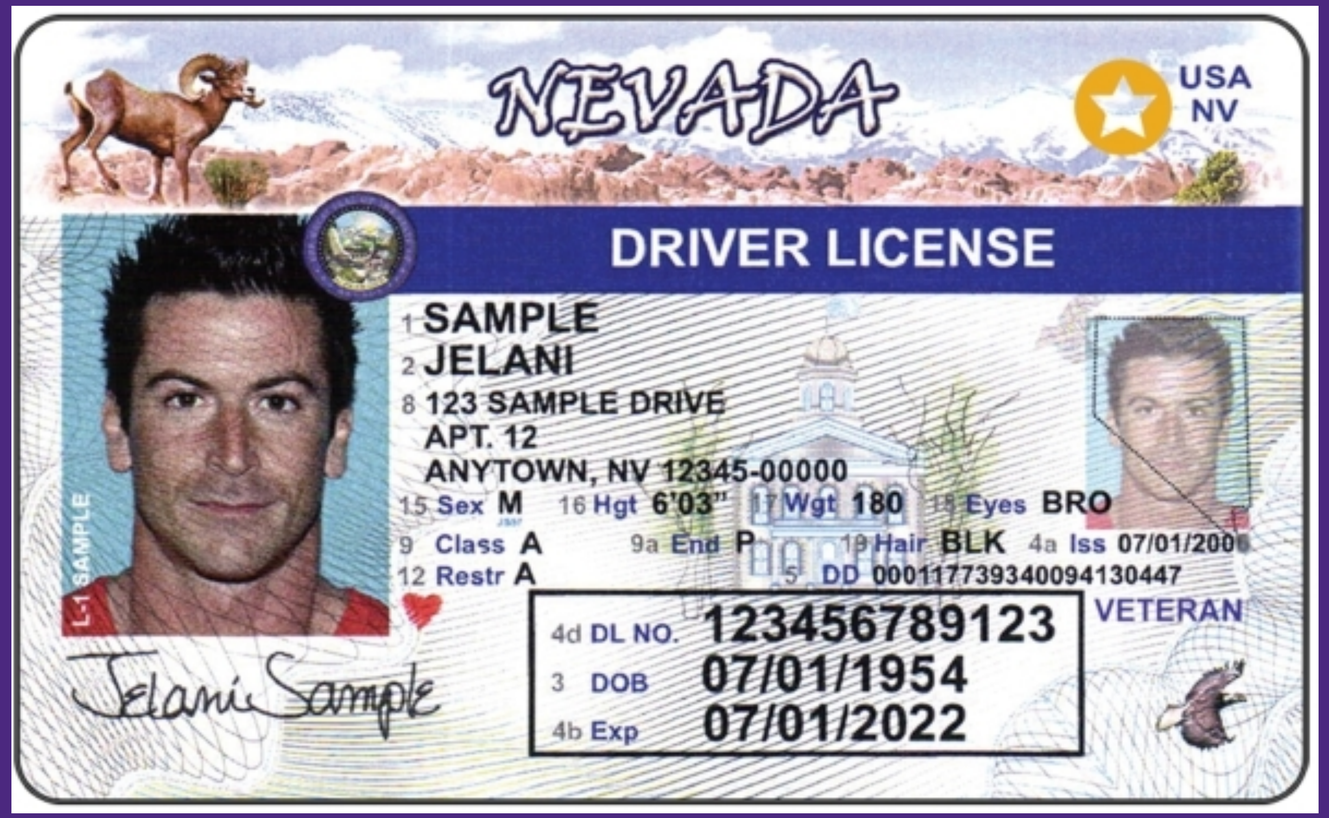
Language

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="id267106664555415408895437065"
                 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="#id267106664555415408895437065">
        <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>mW7oYyS9DYnWfzIODYlwvr5iIbQFoa2NDMjZN0FBVbw=</ds:DigestValue>
      </ds:Reference>
    </ds:SignedInfo>
```

```
    <ds:SignatureValue>
hPxgWc3XHc/wlsAoRxQJnzQiu4zAMcEU5vx+ScvONL5EtQRUq6mHL8ymbDh7vOFHds7osZA8vd7Vx2Mp1T02iKn0DkGJxPrPwo0pbWZj8xNZIH1pe8oolcuY2wMYb7M6+qrKyeExe2iuHEowOIkXmKj64UkPLvHu40jw73VD1yrb3l1WPxxnBvsVaP9bgeefYH51/XyJj3NFwI4se93xLBB92z5W+69IRsowJ+jyPBa87rrHG5JW17cHxRT9Tm+WFtUCgGi0vs9qxHAgFD2235OddxdiHL471mjxN+FBjmAg46YfCbkhEwcLujV35piti8xOkqdohStcPL58ufqMBQ==
</ds:SignatureValue>
      <ds:KeyInfo>
        <ds:X509Data>
          <ds:X509Certificate>
MIIDnDCCAoSgAwIBAgIGAW3/TBAFMA0GCSqGSIb3DQEBCwUAMIGOMQswCQYDVQQGEwJVUzETMBEG A1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsGA1UECgwET2t0YTEU MBIGA1UECwwLU1NPUHJvdmlkZXIxDzANBgNVBAMMBmphbWZzZTEcMBoGCSqGSIb3DQEJARYNaW5m b0Bva3RhLmNvbTAeFw0xOTEwMjQxOTQyNTdaFw0yOTEwMjQxOTQzNTdaMIGOMQswCQYDVQQGEwJV
            UzETMBEGA1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsGA1UECgwE T2t0YTEUMBIGA1UECwwLU1NPUHJvdmlkZXIxDzANBgNVBAMMBmphbWZzZTEcMBoGCSqGSIb3DQEJ ARYNaW5mb0Bva3RhLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKPBBLTj9WZF gsq3GKug5gNcW5hOBzgggjpAEZQyoCGvRj9o5k00uzhIl4MKLNzwjk4OY9wW3gfBrzpHDU5UDnGh6
            KEaA4N1Esewvmlq PgDGDtqtTVow4sQBsV8avSpp/A72js/Dy/VTBoDg0RcyQ8InkYARqOwadieyR AtdOlKewTYfgxzbZpHUazJM2ZDvrbuVEfAnGxrBy7fdP4pBgIPfV6k2T74qroddlKJFjdmkLbjZ3 J5fvgcDU/L+bCiNY/Ov3oXAEqgNHJinj2YRSQziARLjFxFT4wdhOuiTKTjF036sODcnkqVmGJ5hl htKaI2uL/kMgYAF4kvzZxI4T9WsCAwEAATANBgkqhkiG9w0BAQsFAAOCAQEAEA2xUskDggft6unO
            yV7WwQCPA8Che8Yu7Dja6ycBMZbZfv5FHtjSZYUg9t/5Xg8JsSGLvNZArmC6sMgFmCU6k01/ibsv 0ya7pZZy2XWHUnRIM0mloSJ+8wB4Vk+wsuSVB16XYEntVqq3Rl541EsdysMPvXNAaVyDZR++q8rm xSSVkujssutPcavWhcRr8jylB/bERj1ex5E6v0mkwsiyeYiogUQnsnkJEiCgImjlQexVDplHqvTe B7RK4Lj3ukJGiVG3bdJXifJTHgl0HK5etj1S8Fo9mmJFxUnQ9CNZ0ryfrW47WNsNA2EDH4kINKp1
            boEcddqYrxxvydZ8euaxgw==

</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/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="#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>4VzkYuQ4mqVMo6lIbRl1Cz+lkL1xqTPB5LA7U4crTnI=</ds:DigestValue>
      </ds:Reference>
    </ds:SignedInfo>
```

```
      <ds:SignatureValue>
Anr3rTSCR32JO0+vPeAgGM405veOlCeDANby7bSLySOnmX+q82/GQy+/EIWAlGJIf1lxN+nW+7use1kW1j8tfESjPWqTSe8OcEoquRsqRCdVAZt5Q1FZ/BR8Jmi/2aebjP0PXYlV1My/FZYElUndUFPwtLX8Hm1KDwuC+Ww+SGRh3sopFMO78N2d/bpjY2CVOT0GFDc4X8outgqAfe8nKLQygK0GiDov0nq9dOiNgmJFOqaAy+Z5Tlqzi8rDxrTTEJfR/O4N6Y5yDJv+d1An5T/2MgsLYk2oye7H9FJGqV5cfE4B+ynW8cpTkOGgUQgy/X6ZJk4ycPIJZndnOThISQ==
</ds:SignatureValue>
      <ds:KeyInfo>
        <ds:X509Data>
          <ds:X509Certificate>
MIIDnDCCAoSgAwIBAgIGAW3/TBAFMA0GCSqGSIb3DQEBCwUAMIGOMQswCQYDVQQGEwJVUzETMBEG A1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsGA1UECgwET2t0YTEU MBIGA1UECwwLU1NPUHJvdmlkZXIxDzANBgNVBAMMBmphbWZzZTEcMBoGCSqGSIb3DQEJARYNaW5m b0Bva3RhLmNvbTAeFw0xOTEwMjQxOTQyNTdaFw0yOTEwMjQxOTQzNTdaMIGOMQswCQYDVQQGEwJV
            UzETMBEGA1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsGA1UECgwE T2t0YTEUMBIGA1UECwwLU1NPUHJvdmlkZXIxDzANBgNVBAMMBmphbWZzZTEcMBoGCSqGSIb3DQEJ ARYNaW5mb0Bva3RhLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKPBBLTj9WZF gsq3GKug5gNcW5hOBzgggjpAEZQyoCGvRj9o5k00uzhIl4MKLNzwjk4OY9wW3gfBrzpHDU5UDnGh6
            KEaA4N1Esewvmlq PgDGDtqtTVow4sQBsV8avSpp/A72js/Dy/VTBoDg0RcyQ8InkYARqOwadieyR AtdOlKewTYfgxzbZpHUazJM2ZDvrbuVEfAnGxrBy7fdP4pBgIPfV6k2T74qroddlKJFjdmkLbjZ3 J5fvgcDU/L+bCiNY/Ov3oXAEqgNHJinj2YRSQziARLjFxFT4wdhOuiTKTjF036sODcnkqVmGJ5hl htKaI2uL/kMgYAF4kvzZxI4T9WsCAwEAATANBgkqhkiG9w0BAQsFAAOCAQEAEA2xUskDggft6unO
            yV7WwQCPA8Che8Yu7Dja6ycBMZbZfv5FHtjSZYUg9t/5Xg8JsSGLvNZArmC6sMgFmCU6k01/ibsv 0ya7pZZy2XWHUnRIM0mloSJ+8wB4Vk+wsuSVB16XYEntVqq3Rl541EsdysMPvXNAaVyDZR++q8rm xSSVkujssutPcavWhcRr8jylB/bERj1ex5E6v0mkwsiyeYiogUQnsnkJEiCgImjlQexVDplHqvTe B7RK4Lj3ukJGiVG3bdJXifJTHgl0HK5etj1S8Fo9mmJFxUnQ9CNZ0ryfrW47WNsNA2EDH4kINKp1
            boEcddqYrxxvydZ8euaxgw==

</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.rabbitt@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

Note: To support uncommon IdP configurations, the GET binding (less secure than POST) can be used for SAML Single Logout.

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:

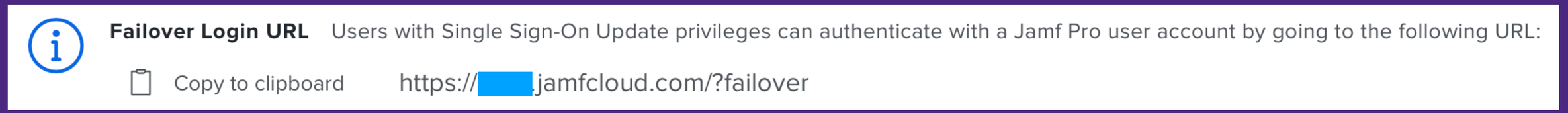
- Configuring Single Sign-On with Okta
- Configuring Single Sign-On with Active Directory Federation Services
- Configuring Single Sign-On with Shibboleth
- Configuring Single Sign-On with OneLogin
- Configuring Single Sign-On with Ping Identity
- Configuring Single Sign-On with G Suite (Google Apps)
- 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/jamfprosamlconnector-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/easysso

FAILOVER URL



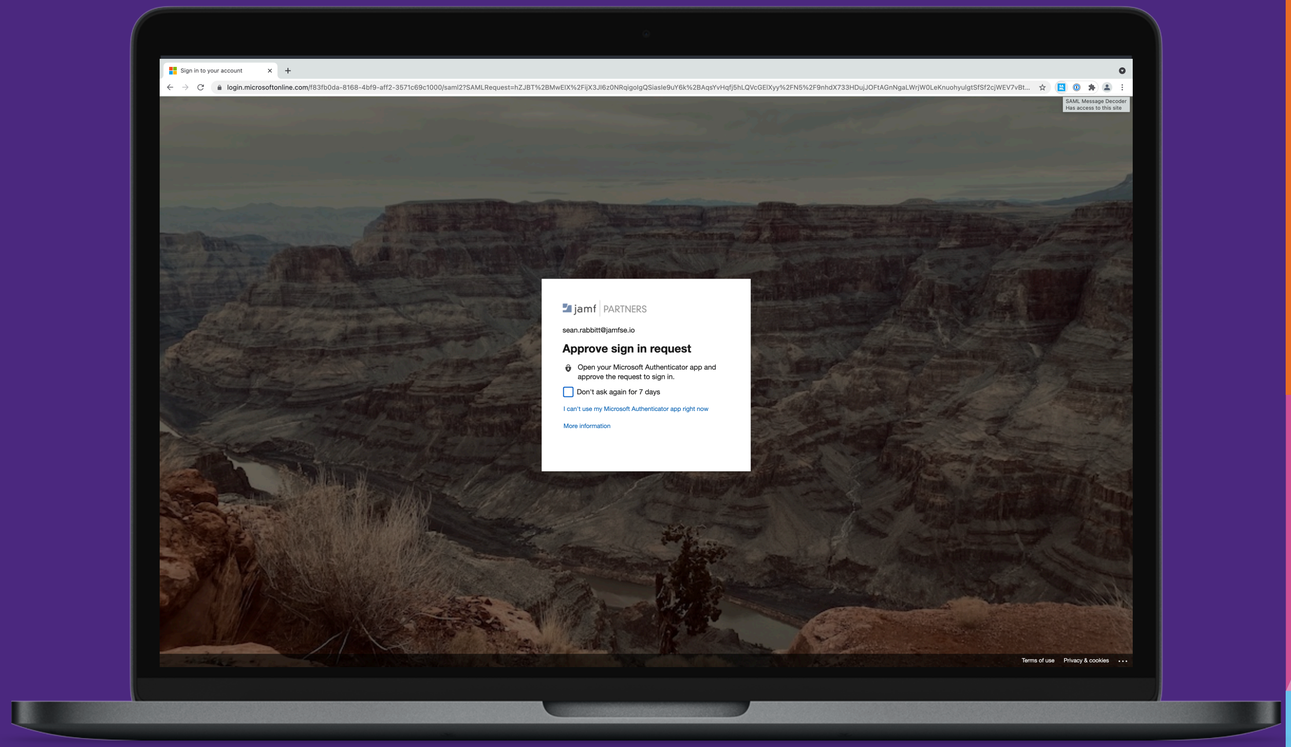
https://[your_server]/?failover

Intercepting SAML Requests

- GoogleChrome
- 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

jamf.com

English

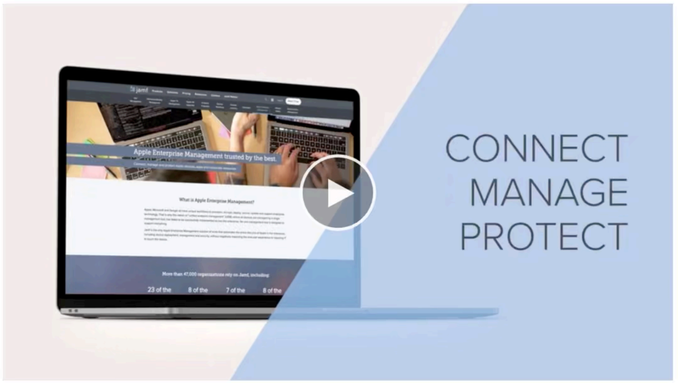
jamf Products Solutions Pricing Resources Contact Jamf Nation Log in Start Trial

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?



We help organizations succeed with Apple.

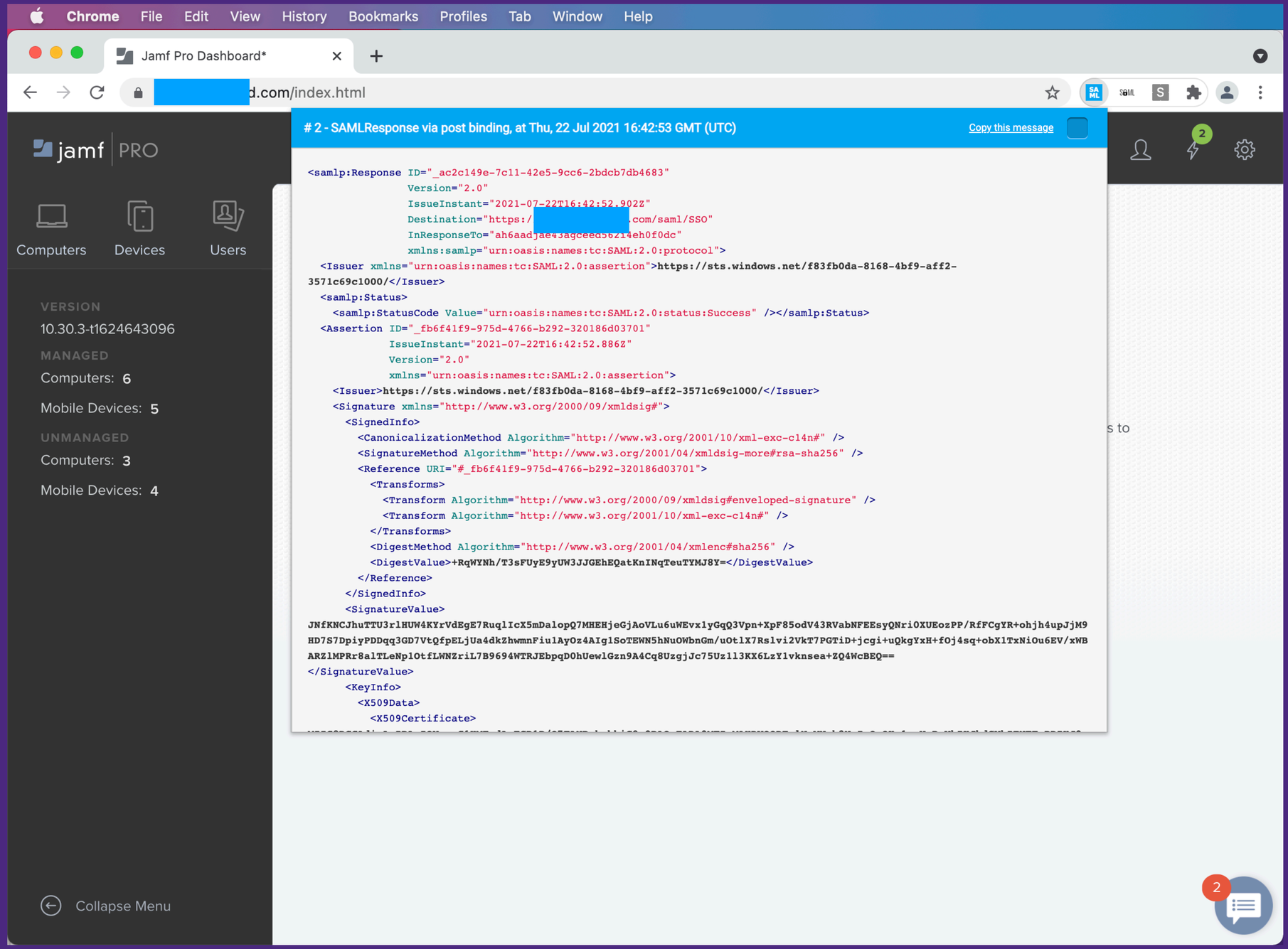
With sole focus on the Apple ecosystem, industry leaders across the globe choose Jamf to:

- 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



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

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 LDA

Settings : System Settings

← Jamf Pro User Accounts & Groups

+ New | Password Policy

USERNAME	FULL NAME	EMAIL	TYPE	ACCESS	SITE	PRIVILEGES
[redacted]			Standard User	Full Access		Administrator
[redacted]	DemoKitAPIUser		Standard User	Full Access		Custom
enroll			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		[redacted]	Standard User	Full Access		Administrator

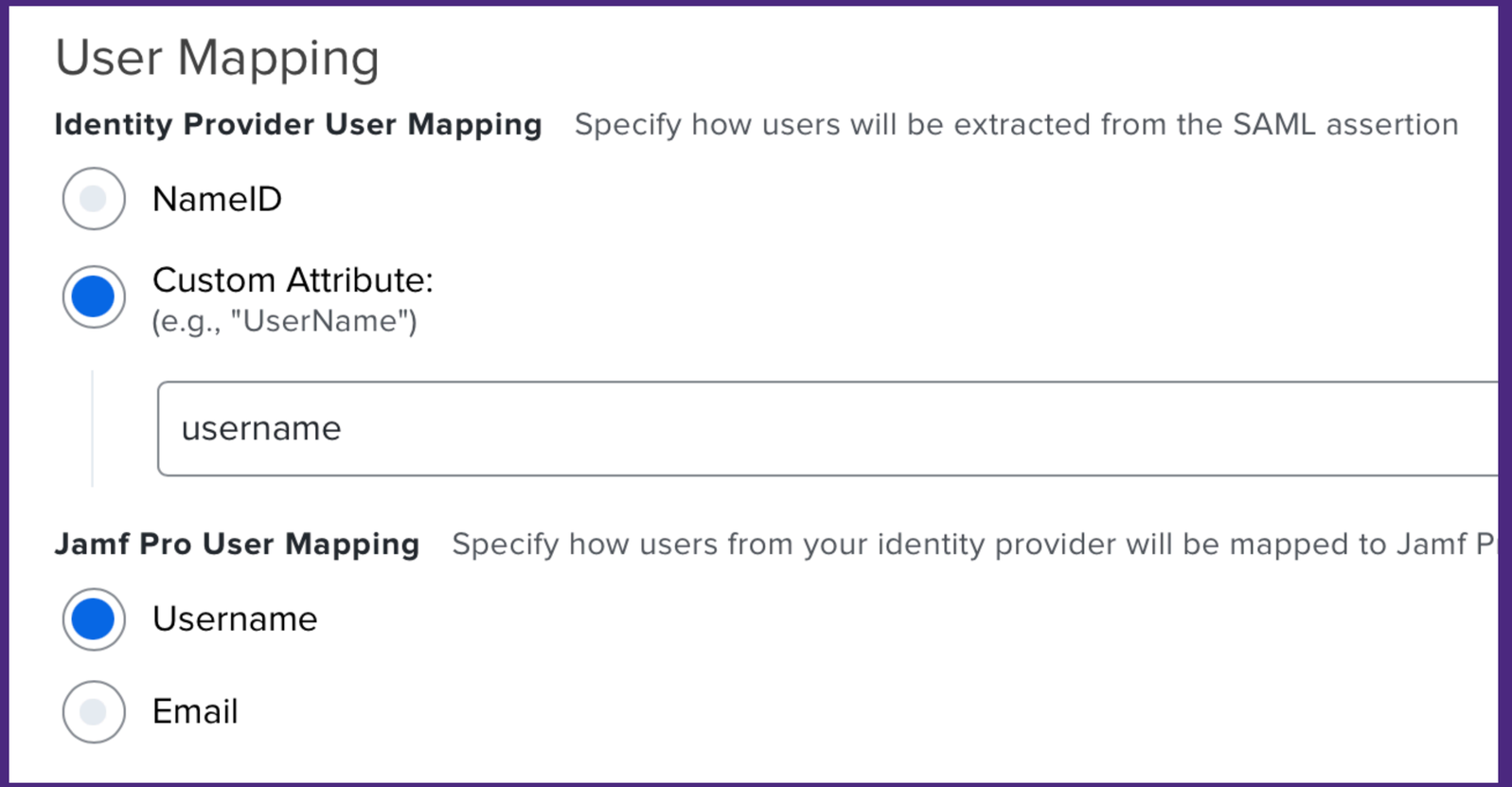
API Only Users

Enrollment User

User for initial JPS setup

Jamf Pro User Groups (1)

GROUP NAME	TYPE	MEMBERS	ACCESS	SITE	PRIVILEGES
System Engineers	Standard Group	0	Full Access		Administrator



User Mapping

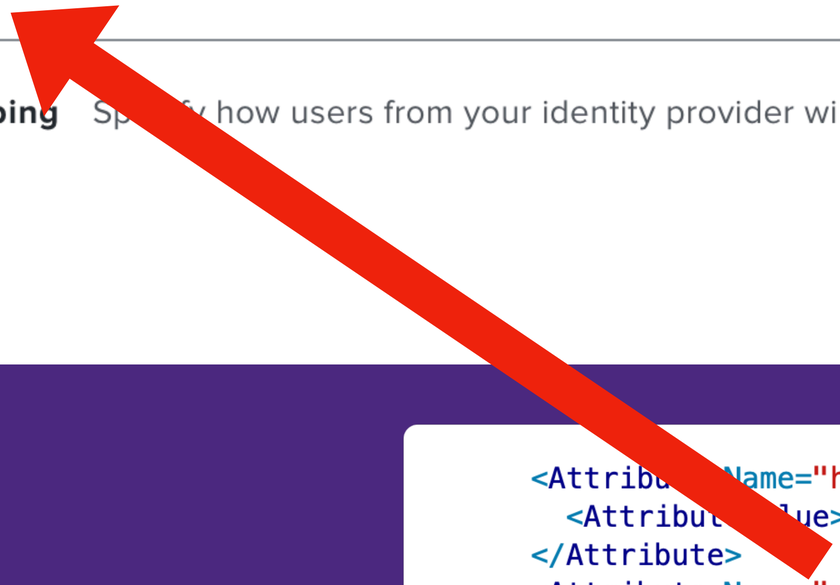
Identity Provider User Mapping Specify how users will be extracted from the SAML assertion

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

  username

Jamf Pro User Mapping Sp[illegible]y how users from your identity provider will be mapped to Jamf P[illegible]

- ◉ Username
- ○ Email

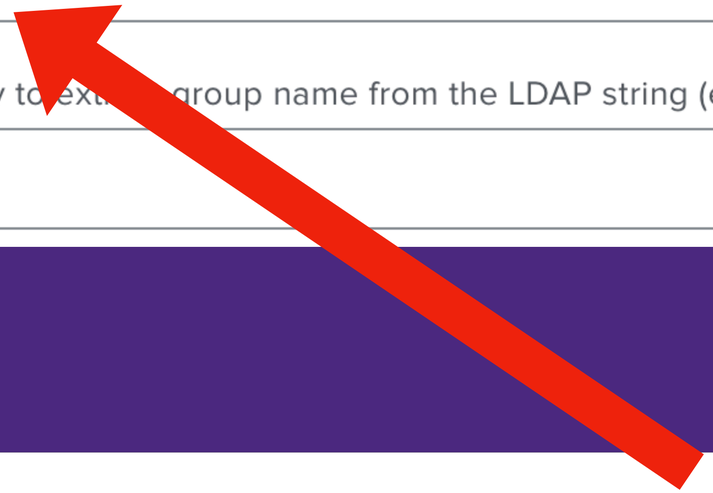


```
<Attribu  Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name">
  <Attribut  lue>sean.rabbitt@jamfse.io</AttributeValue>
</Attribute>
<Attribute Name="username">
  <AttributeValue>sean.rabbitt</AttributeValue>
</Attribute>
```

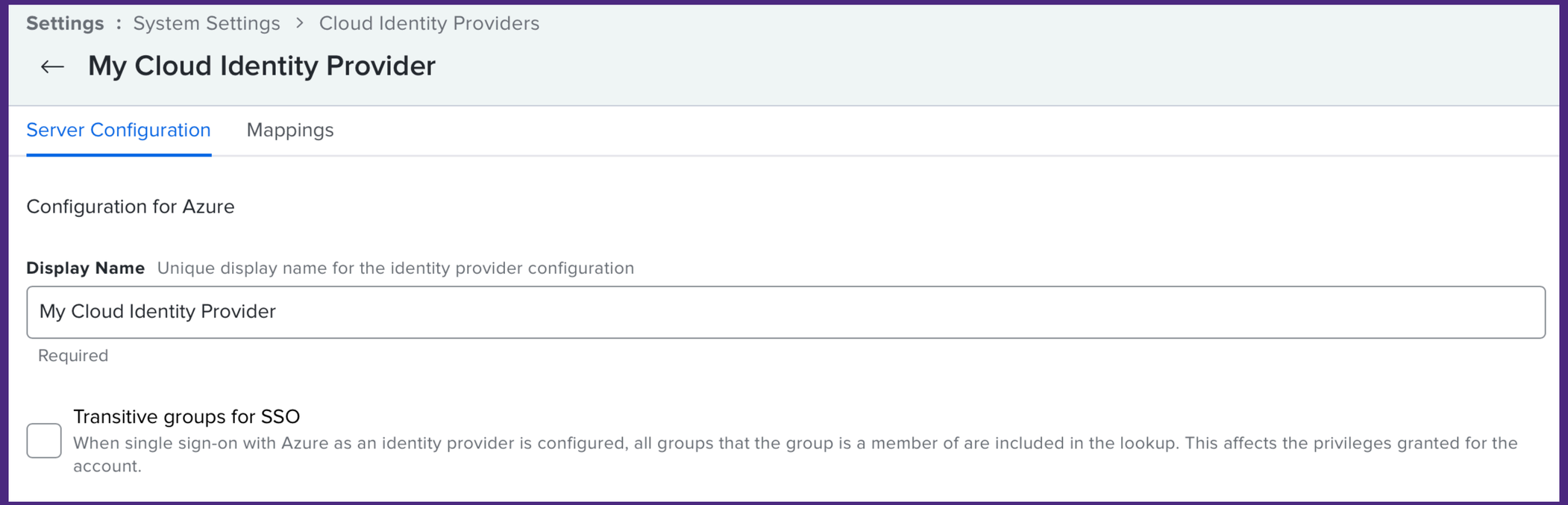
Identity Provider Group Attribute Name Name of the SAML assertion attribute containing your group (e.g., "GroupName")

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

RDN Key For LDAP Group Relative Distinguished Name key to ext... 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>
```



Decoding SAML Runes

~~Anatomy of a SAML Token~~

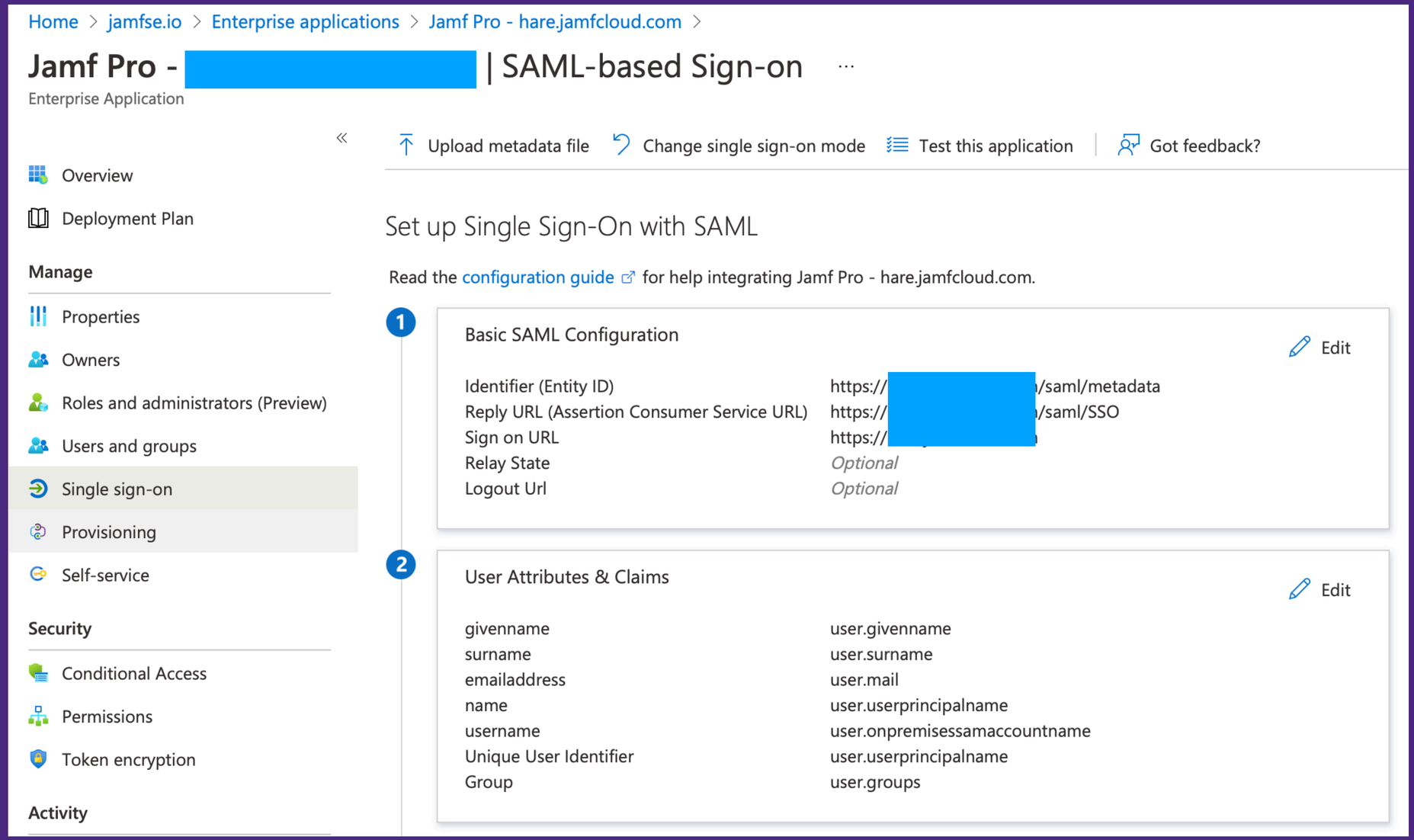
~~Intercepting SAML Tokens~~

Modifying SAML Tokens

CMD-C CMD-V to Jamf Pro

Passing info to Jamf Connect

Microsoft Azure



Microsoft Azure

User Attributes & Claims ...

+ Add new claim | + Add a group claim | Columns

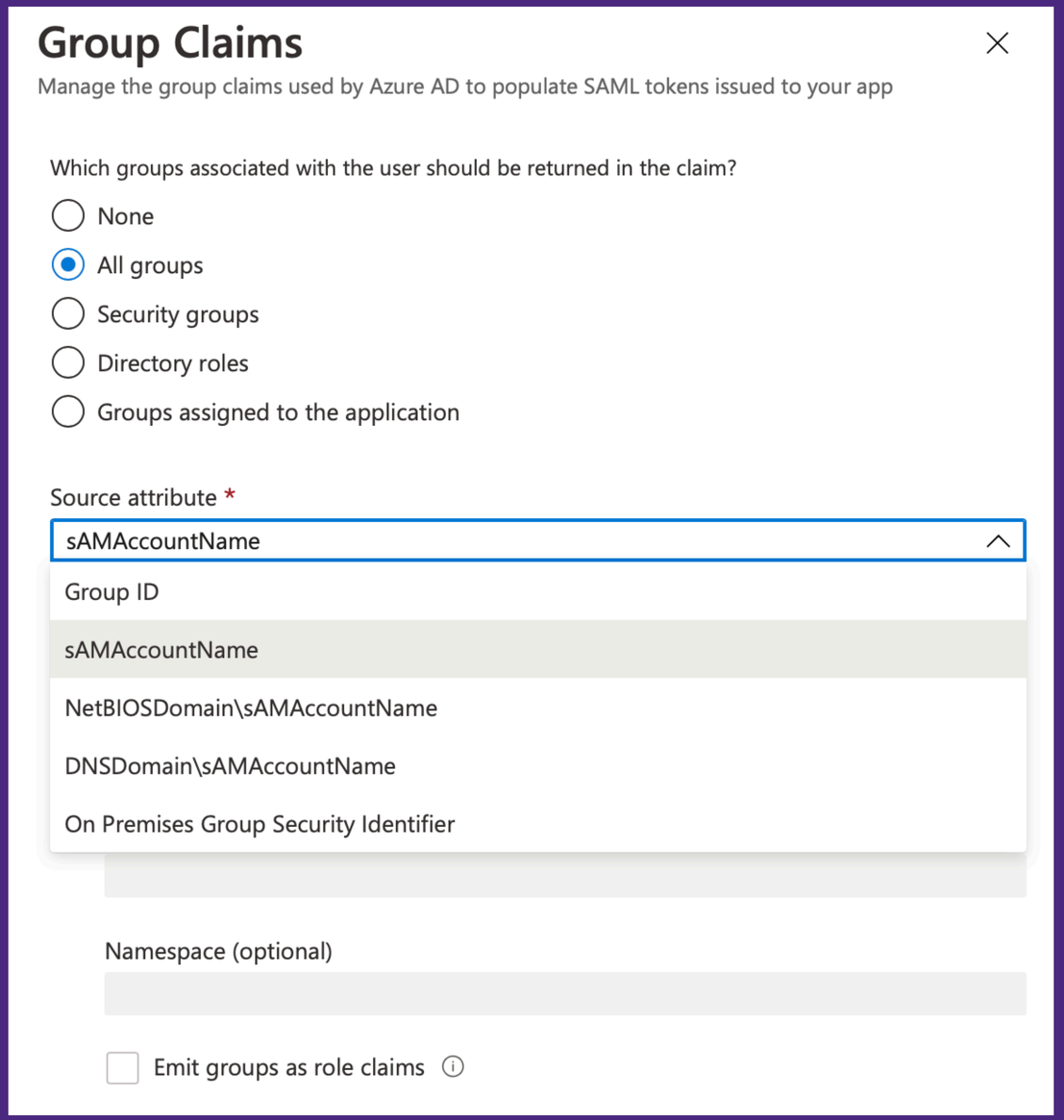
Required claim

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

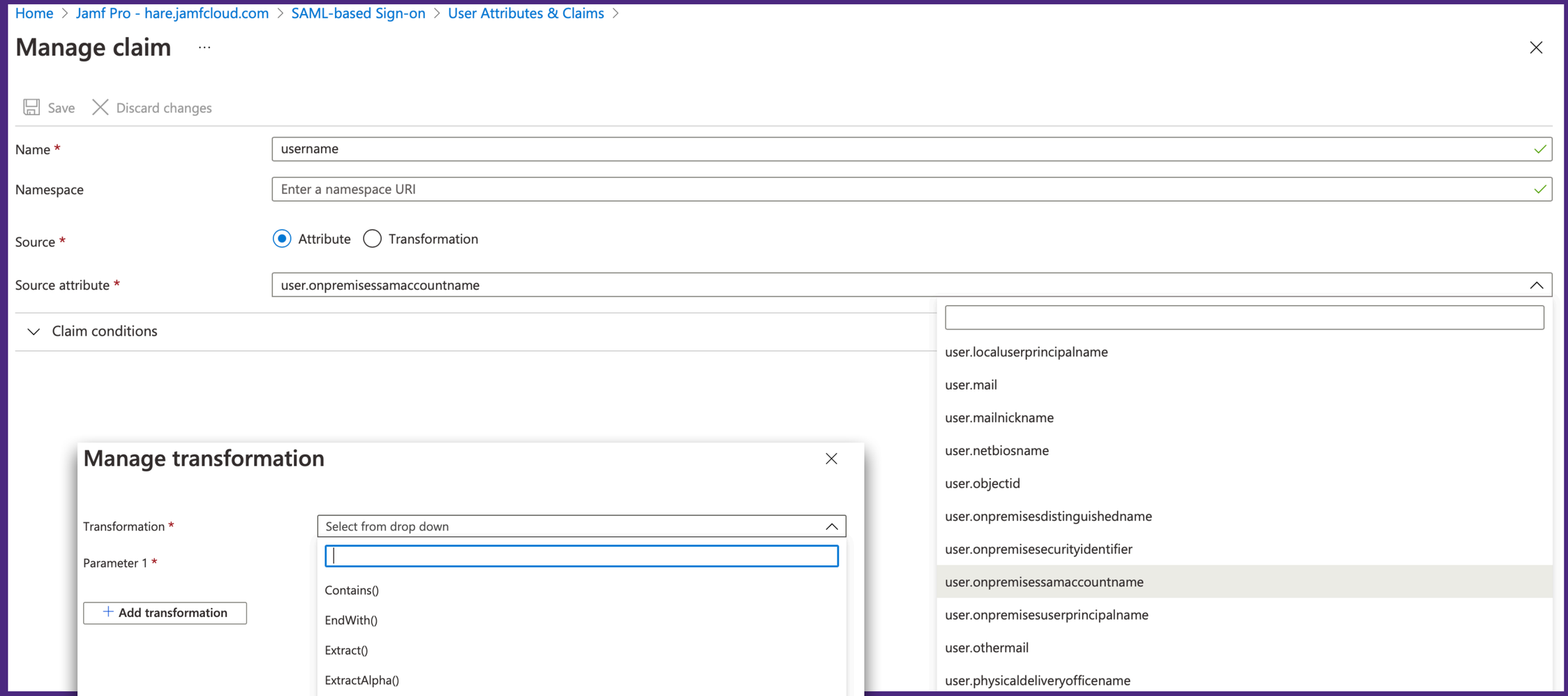
Additional claims

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.onpremisessamaccountname •••

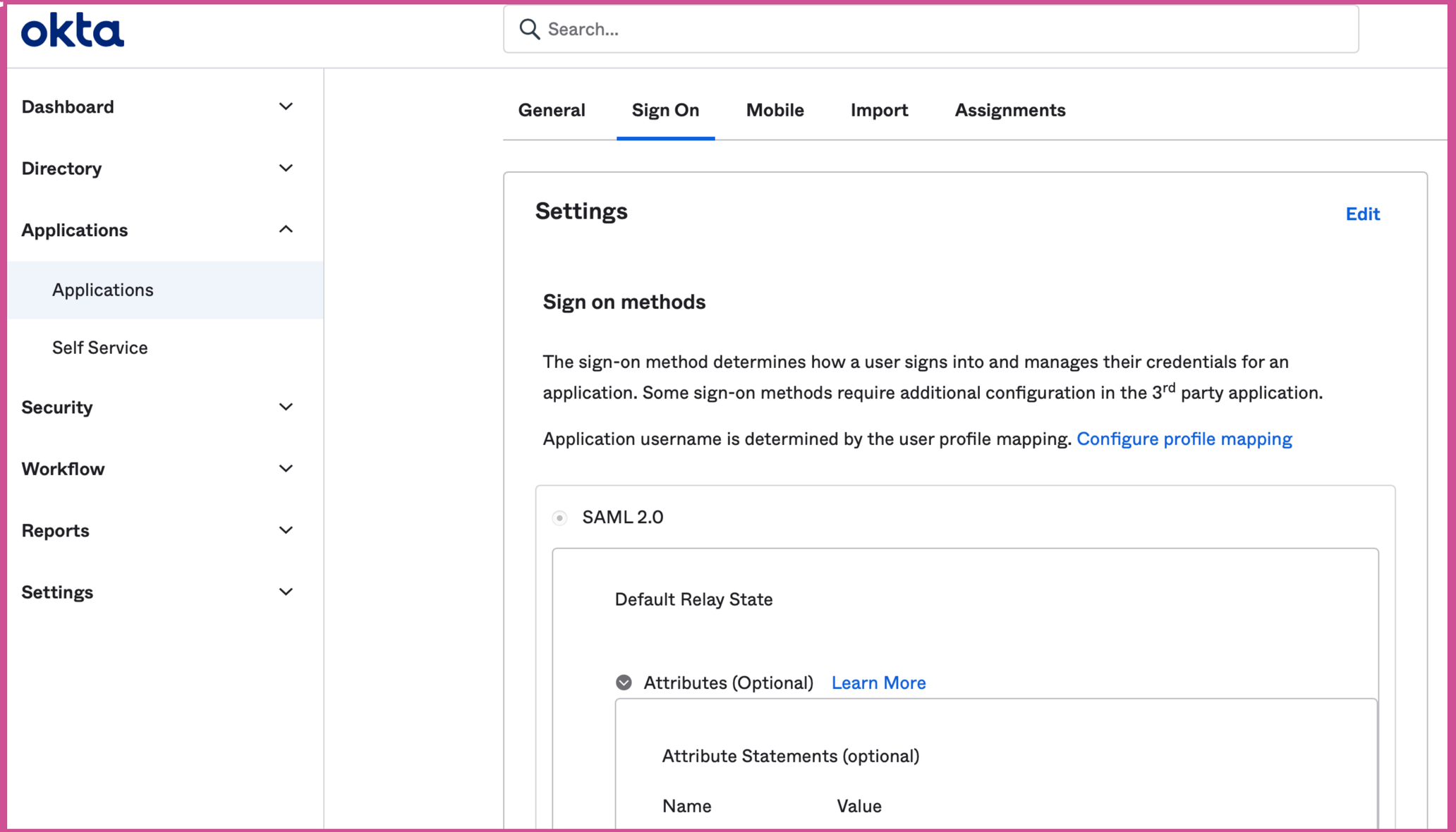
Microsoft Azure



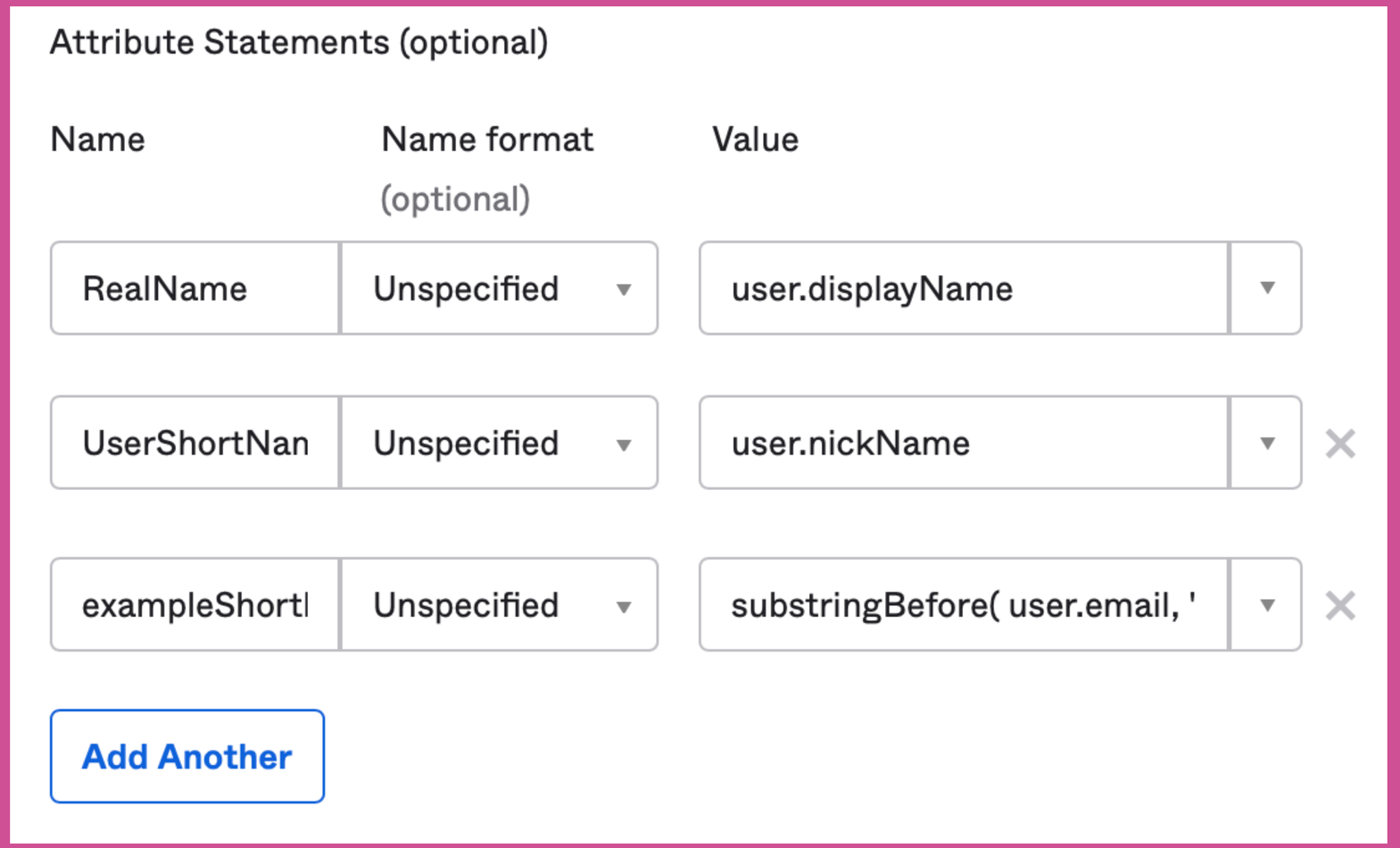
Microsoft Azure



Okta



Okta



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

Okta

substringBefore(user.email, "@")

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

Decoding SAML Runes

~~Anatomy of a SAML Token~~

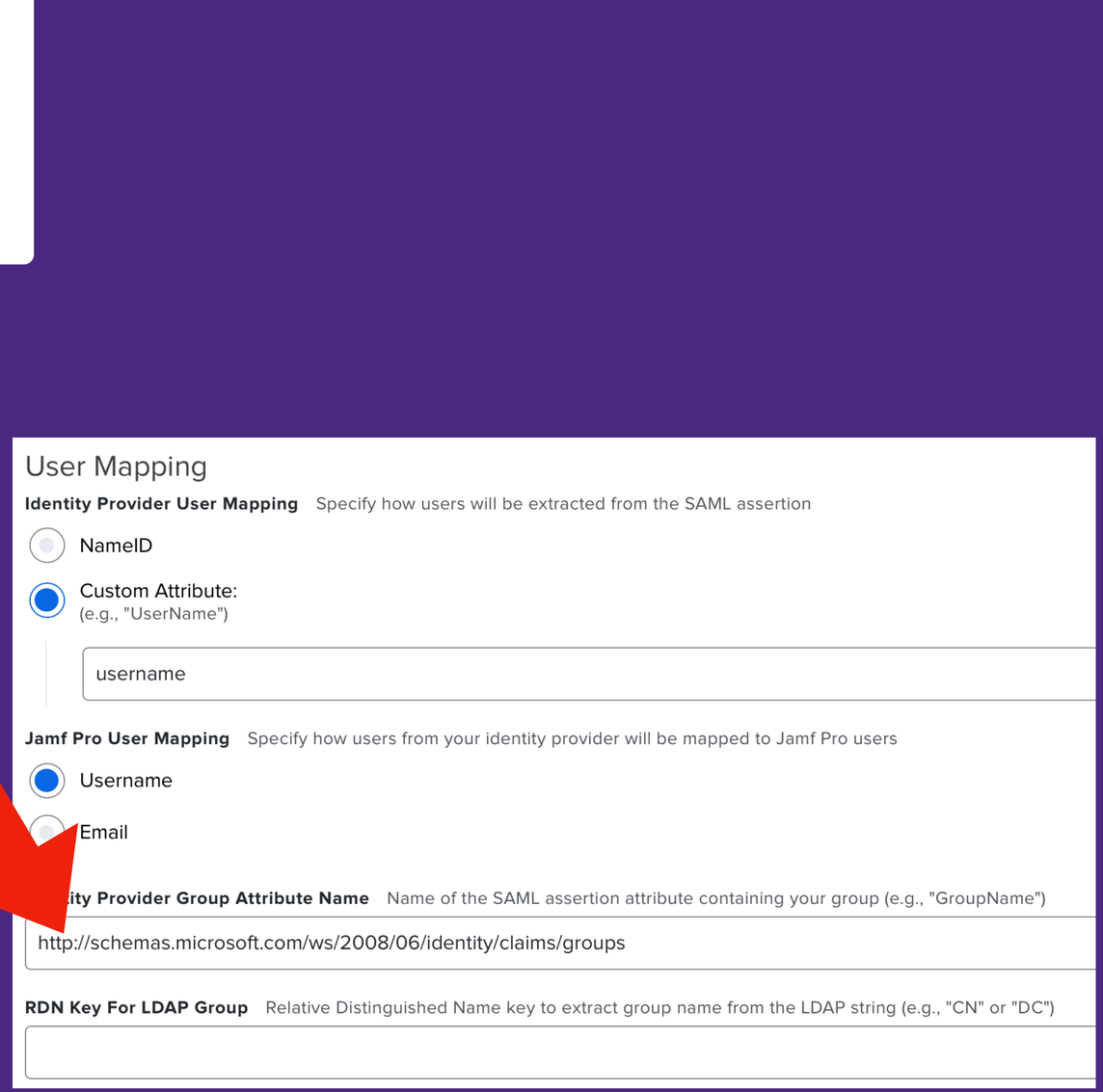
~~Intercepting SAML Tokens~~

~~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</AttributeVa
  <AttributeValue>Okta Admins</AttributeVal
  <AttributeValue>Jamf Protect Limited Acces ttributeValue>
  <AttributeValue>System Engineers</Attribute e>
  <AttributeValue>macadmin</AttributeValue>
  <AttributeValue>TrialServerAdmin</AttributeVal
  <AttributeValue>All Jamfs</AttributeValue>
</Attribute>
```



Decoding SAML Runes

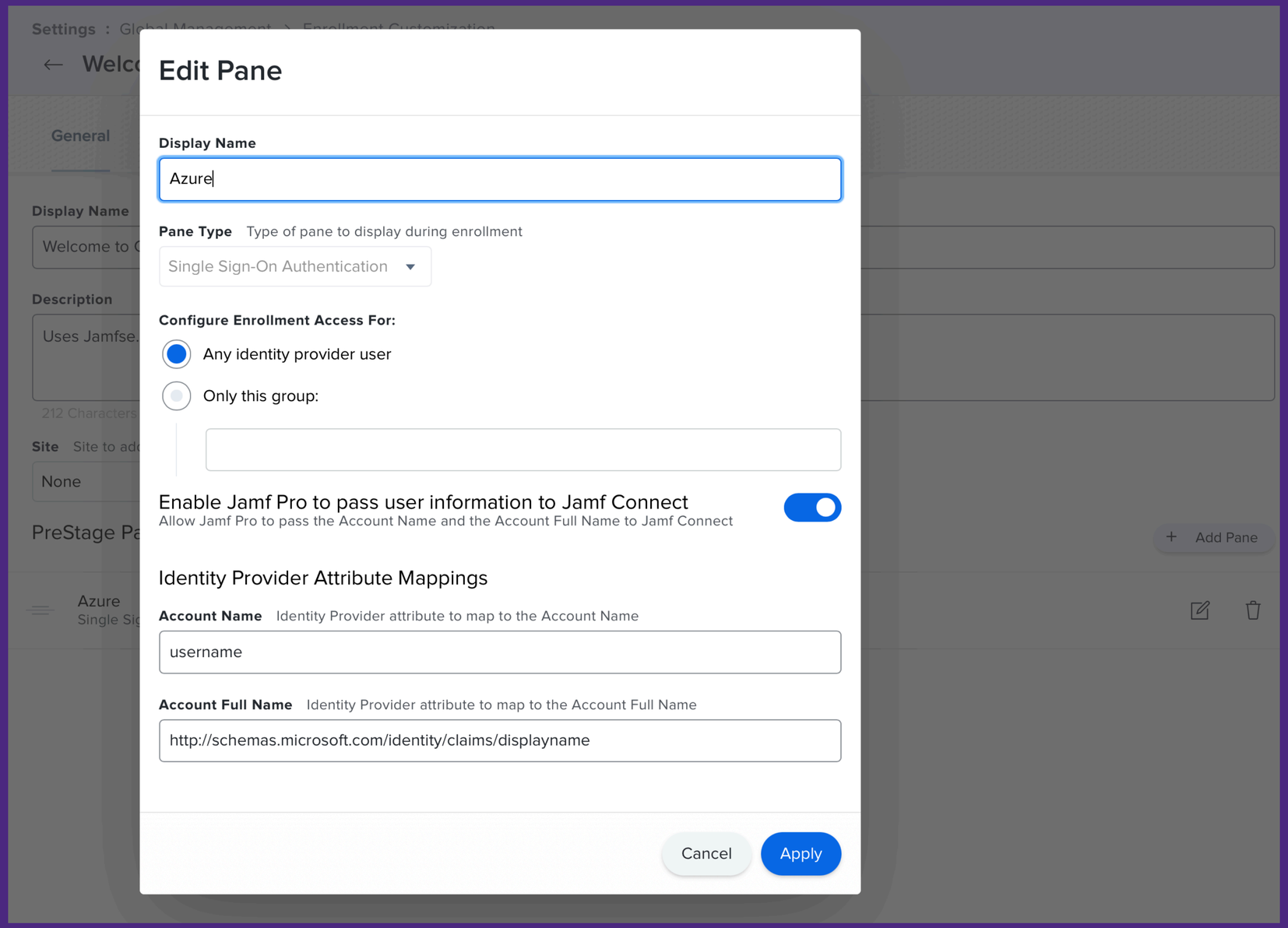
~~Anatomy of a SAML Token~~

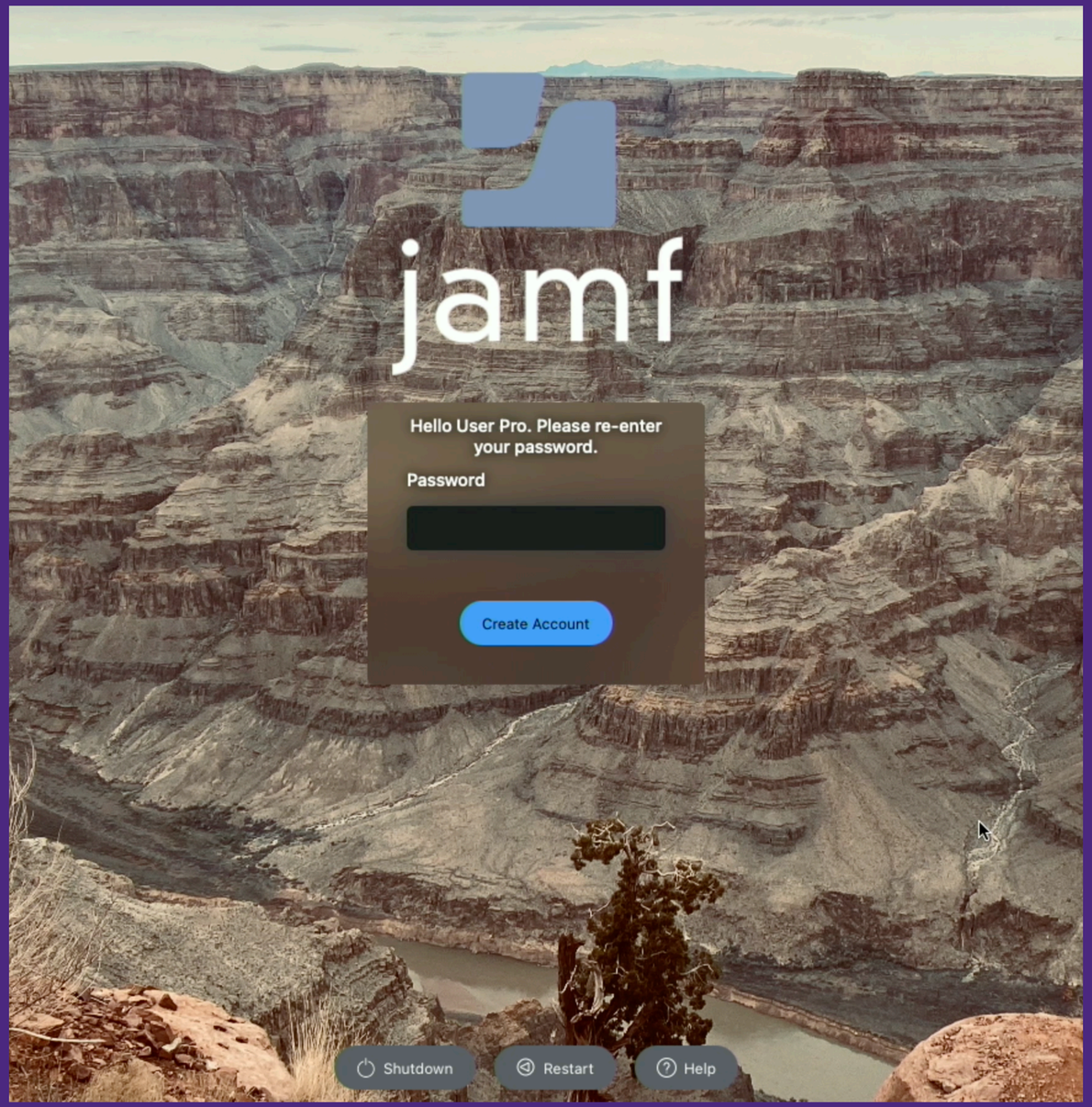
~~Intercepting SAML Tokens~~

~~Modifying SAML Tokens~~

~~CMD-C CMD-V to Jamf Pro~~

Passing info to Jamf Connect





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!