Enrollment Customizations and Jamf Connect with Azure

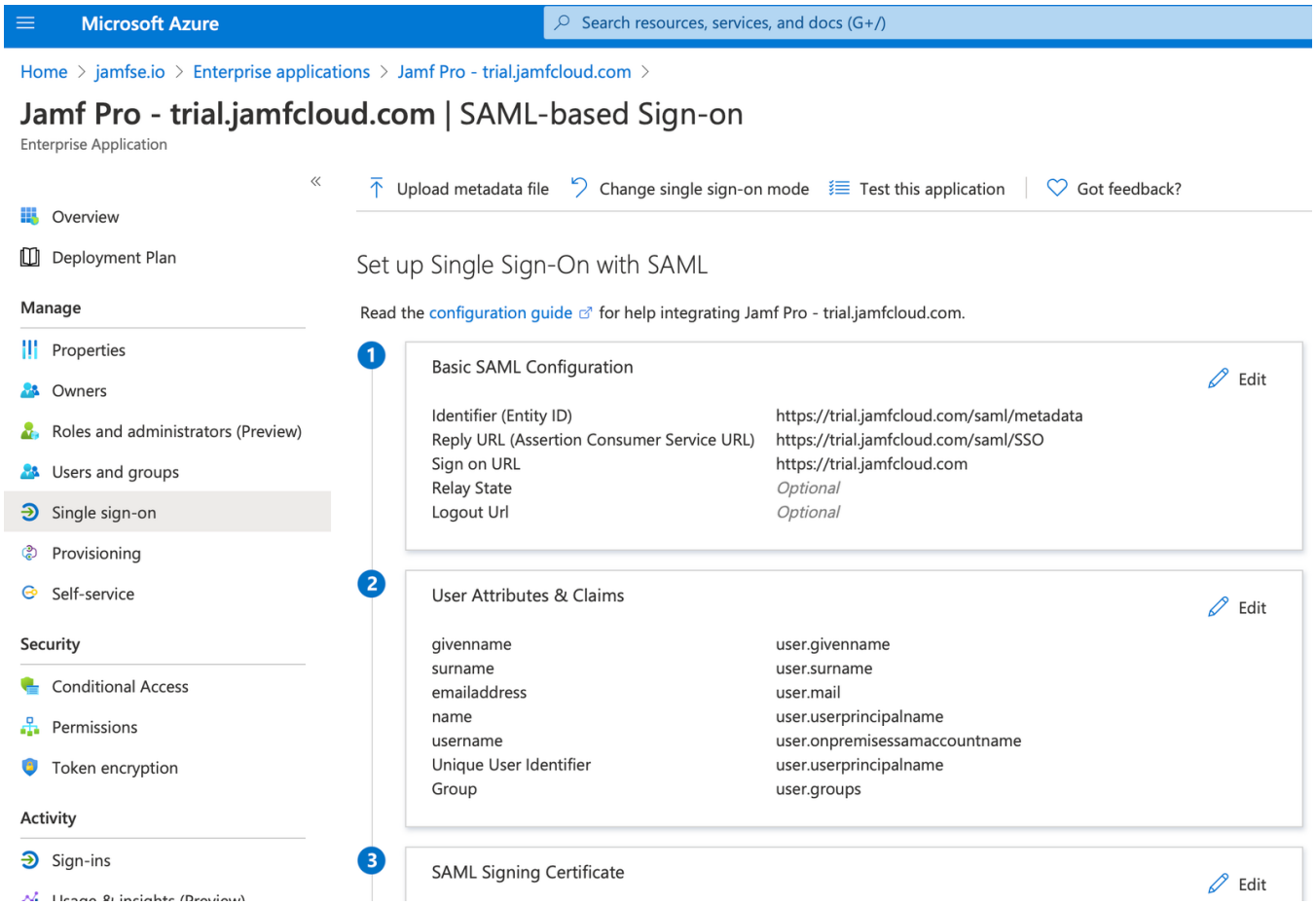
Overview: Jamf Pro can pass information obtained in the SAML token for single sign-in to Jamf Pro to automate creating a user with Jamf Connect. This requires modifying the Jamf Pro single sign-on SAML token to include the information needed for Connect.

Step One: Modifying the SAML app for Jamf Pro in Azure

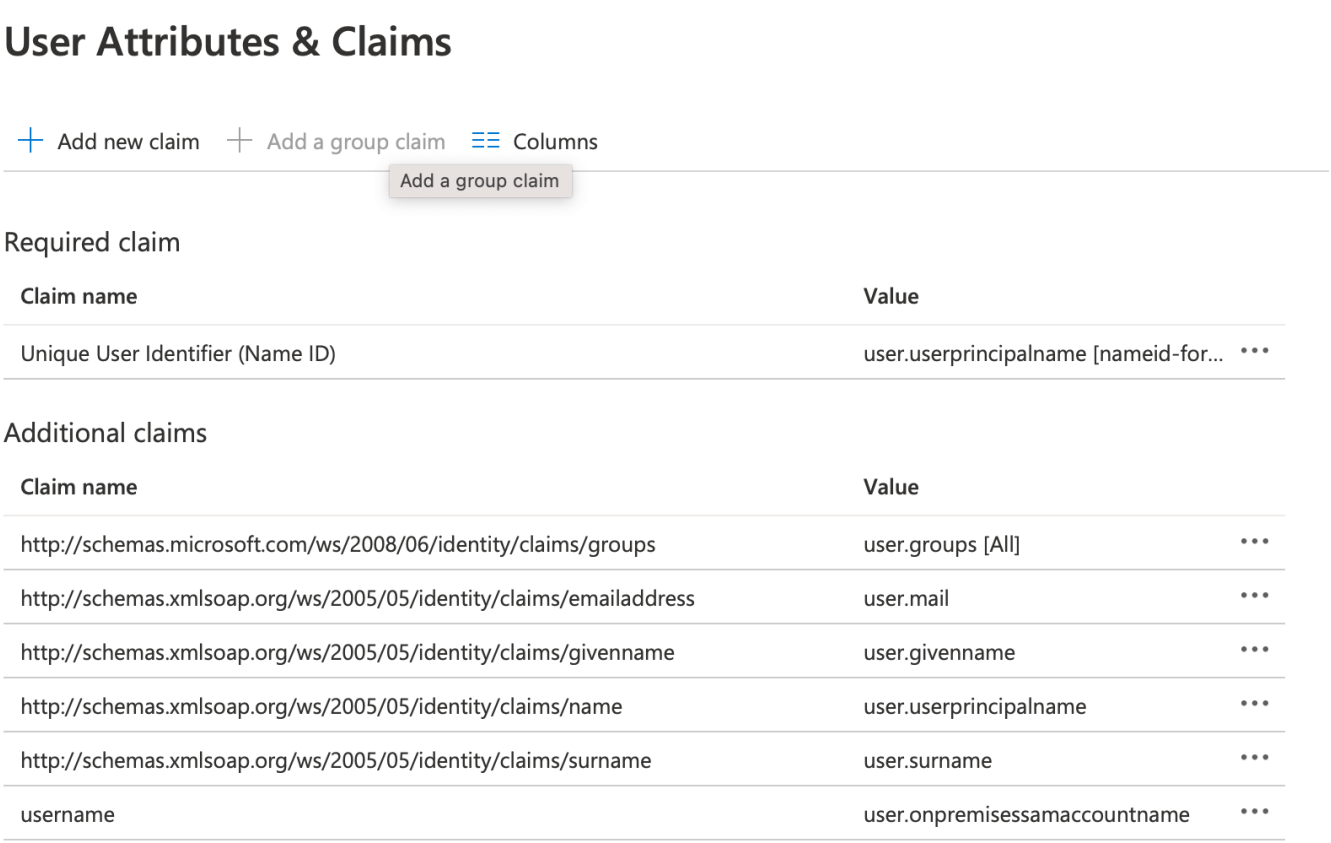
Jamf Connect needs two user attributes to create a new user:

- User “real name” - an attribute that contains the user’s full name like “John Jacob Jingleheimer Schmidt”
- User “short name” - an attribute that contains what will become the local macOS user’s short user name like “john.schmidt”. For OIDC providers, Jamf Connect can also use an attribute like an email address formatted like “john.schmidt@domain.tld” and will strip the information before the “@” sign to create a short name.
    - Note: In most cases, Azure user names correspond to the organizational email address associated with a user. The NameID claim in a SAML identity token will correspond to the Azure user name. Jamf Pro will default to using NameID for Account Name unless otherwise mapped to another attribute.

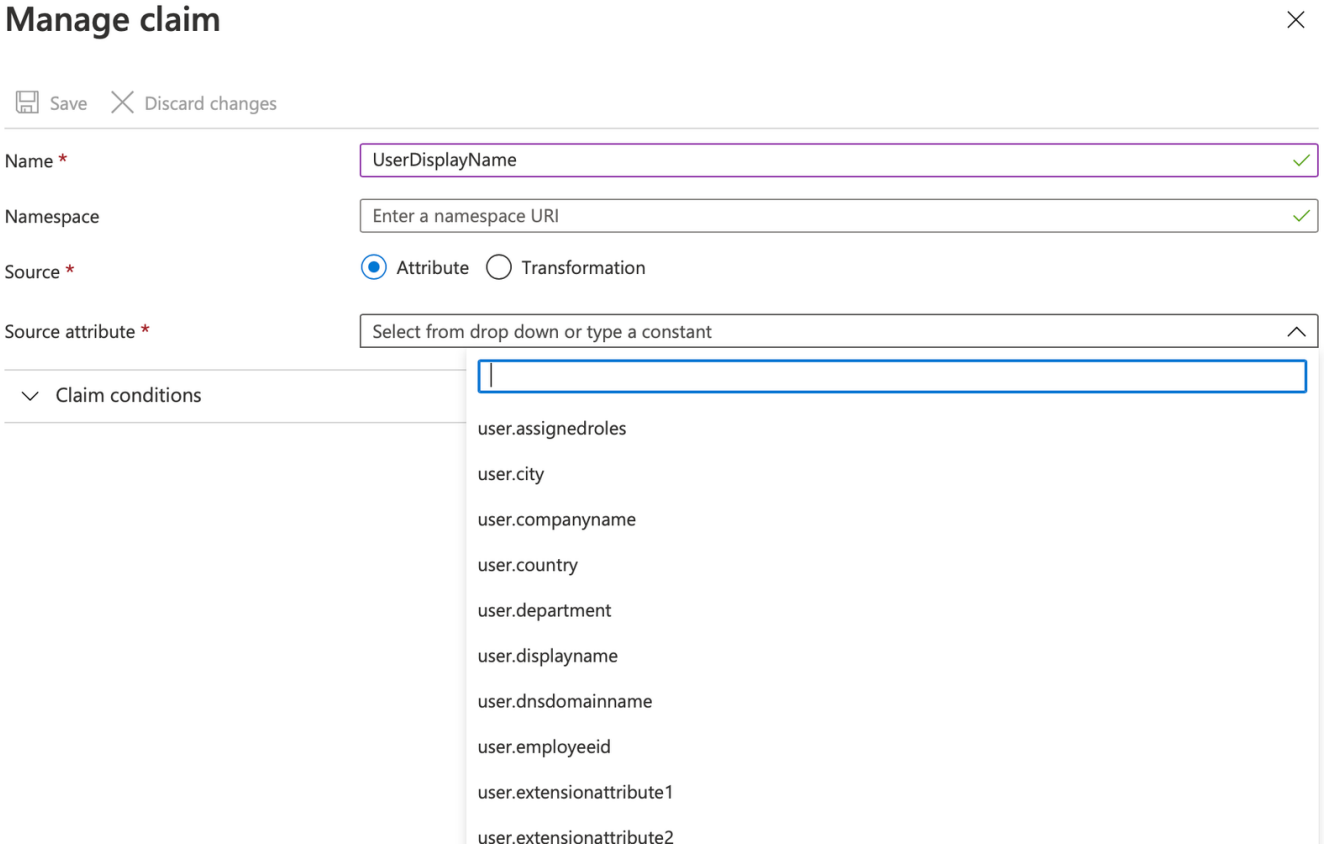
In the Azure administrator portal, navigate to Azure Active Directory → Enterprise Applications. Select the app you created for Jamf Pro single sign-on.



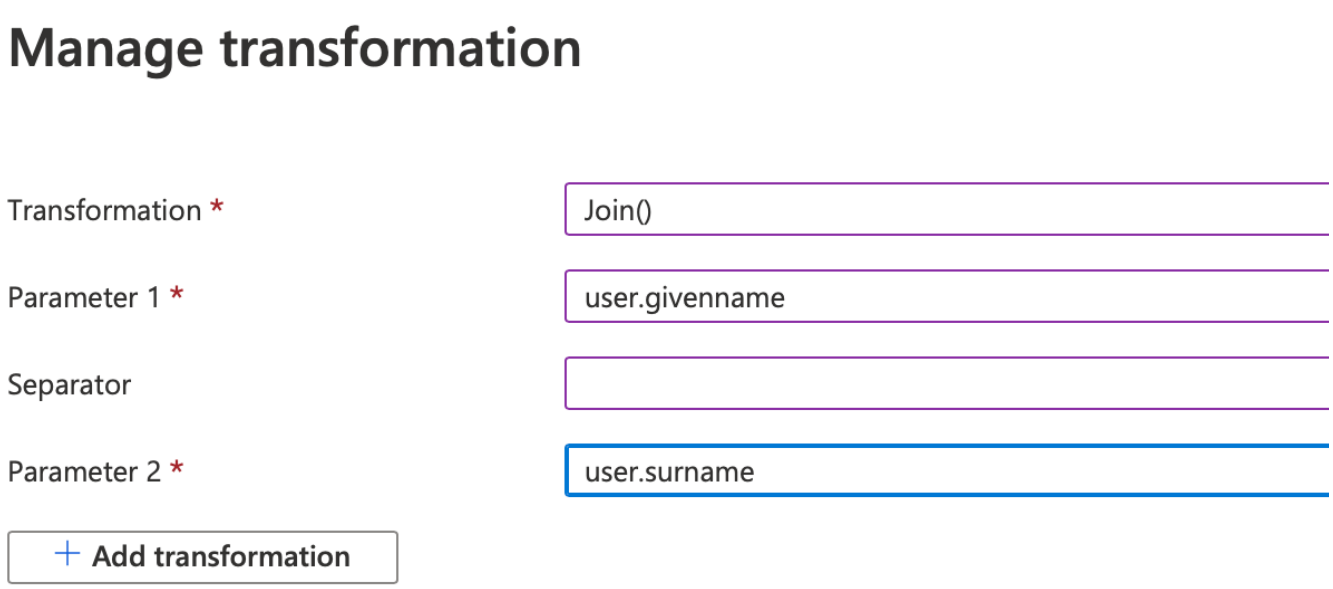
Navigate to Single sign-on and select the Edit button in section 2 named “User Attributes & Claims”.



Select the option for “+ Add new claim”



Name will correspond to the AttributeName sent in the SAML token. Source attribute can map a value in the user's Active Directory information to the name attribute value. Alternatively, the source can be set to "Transformation" and the returned value can be the result of a macro to modify another value in the user's Active Directory information. For example, the returned value could concatenate the user's given name and family name into one "FirstName LastName" value:



To test your SAML tokens are sending the right information in the identity, use a tool like SAML Message Decoder (https://chrome.google.com/webstore/detail/saml-message-decoder/mpabchoaimgbdbbjjieoaeiibojelbhm) to sign in to the Jamf Pro administrator page with single sign-on. Examine the token for AttributeName fields which contain the user information like the following:

```
<Subject>
  <NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress">sherlock.holmes@jamfse.io</NameID>
  <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
    <SubjectConfirmationData InResponseTo="ac3669a99a4djj832f59919a9gcifi"
                             NotOnOrAfter="2020-12-23T18:06:08.719Z"
                             Recipient="https://trial.jamfcloud.com/saml/SSO" />
  </SubjectConfirmation>
</Subject>
<AttributeStatement>
  <Attribute Name="http://schemas.microsoft.com/identity/claims/
```

```
displayname">
    <AttributeValue>Sherlock Holmes</AttributeValue>
  </Attribute>
  <Attribute Name="username">
    <AttributeValue>sherlock.holmes</AttributeValue>
  </Attribute>
</AttributeStatement>
```

In this example, we see three attributes which can be used by Jamf Connect to create the user account:

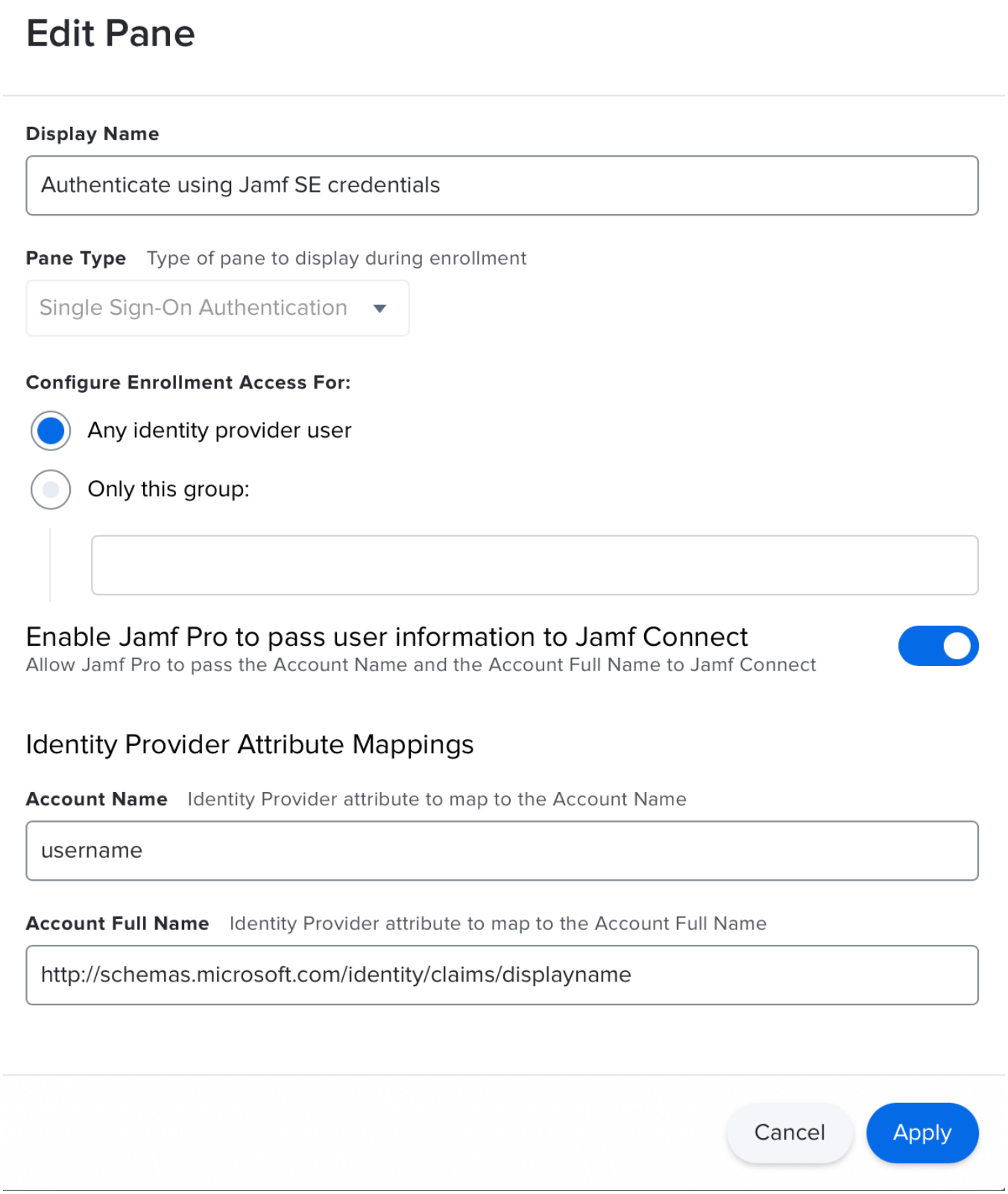
- NameID: The NameID format is an email address, therefore Jamf Connect will use the characters preceding the `@` sign as the short name.
- An attribute named `username`: The value is formatted in a method desired by the administrators for all macOS short names, in this example, `firstname.lastname`
- An attribute named `http://schemas.microsoft.com/identity/claims/displayname`: One of the default attributes sent in a Microsoft Azure SAML identity token which contains the user's given name and family name in one value.

Step Two: Modify the Enrollment Customization in Jamf Pro

Reference: https://docs.jamf.com/jamf-pro/administrator-guide/Enrollment_Customization_Settings.html

Login as an administrator in your Jamf Pro server. Navigate to Settings → Global Management → Enrollment Customization. Create a new Enrollment Customization or edit an existing one.

Create or select an enrollment customization pane that contains the Single Sign-On payload:



In the section called “Identity Provider Attribute Mappings” under “Account Name” type the name of the attribute you created in Azure which will contain the user macOS short name. Using the examples from step one, we named this field

"username". **Note:** if left blank, Jamf Pro will use the NameID field for Account Name.

Under the section "Account Full Name" enter the name of the attribute you created in Azure which contains the user's full given and family name. Using the examples from step one, we can use the standard `http://schemas.microsoft.com/identity/claims/displayname` claim sent in the SAML identity token

Token names are case sensitive and must match precisely to the information in the token.

Step Three: Testing deployment with Jamf Connect

Reference: +Zero Touch Deployment with Jamf Pro and Jamf Connect

When a macOS device is enrolled in a prestage enrollment with the Enrollment Customization passing credentials to Jamf Connect, the Jamf Connect account creation page will only show one option for a user:


jamf
Hello User Pro, please enter your password.
Password
Create Account
Shutdown
Restart
Help

The user's real name (in this example above, "User Pro") will be prompted to enter their Okta password one more time to create a user account.

Jamf Pro is pushing a configuration profile scoped to the domain com.jamf.connect.login to the target computer similar to the following information:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
        <key>EnrollmentRealName</key>
        <string>Sherri Bobbins</string>
        <key>EnrollmentUserName</key>
        <string>sherri.bobbins@jamfse.io</string>
</dict>
</plist>

```

The string for `EnrollmentRealName` comes from the mapped "Account Full Name" attribute. The string for `EnrollmentUserName` comes from the mapped "Account Name" attribute. After a set period of time, the profile will be unscoped from the target computer. Administrators can confirm the presence of this profile by opening System Preferences → Profiles and looking for a profile named like `JamfConnect`.