Enrollment Customizations and Jamf Connect with Okta

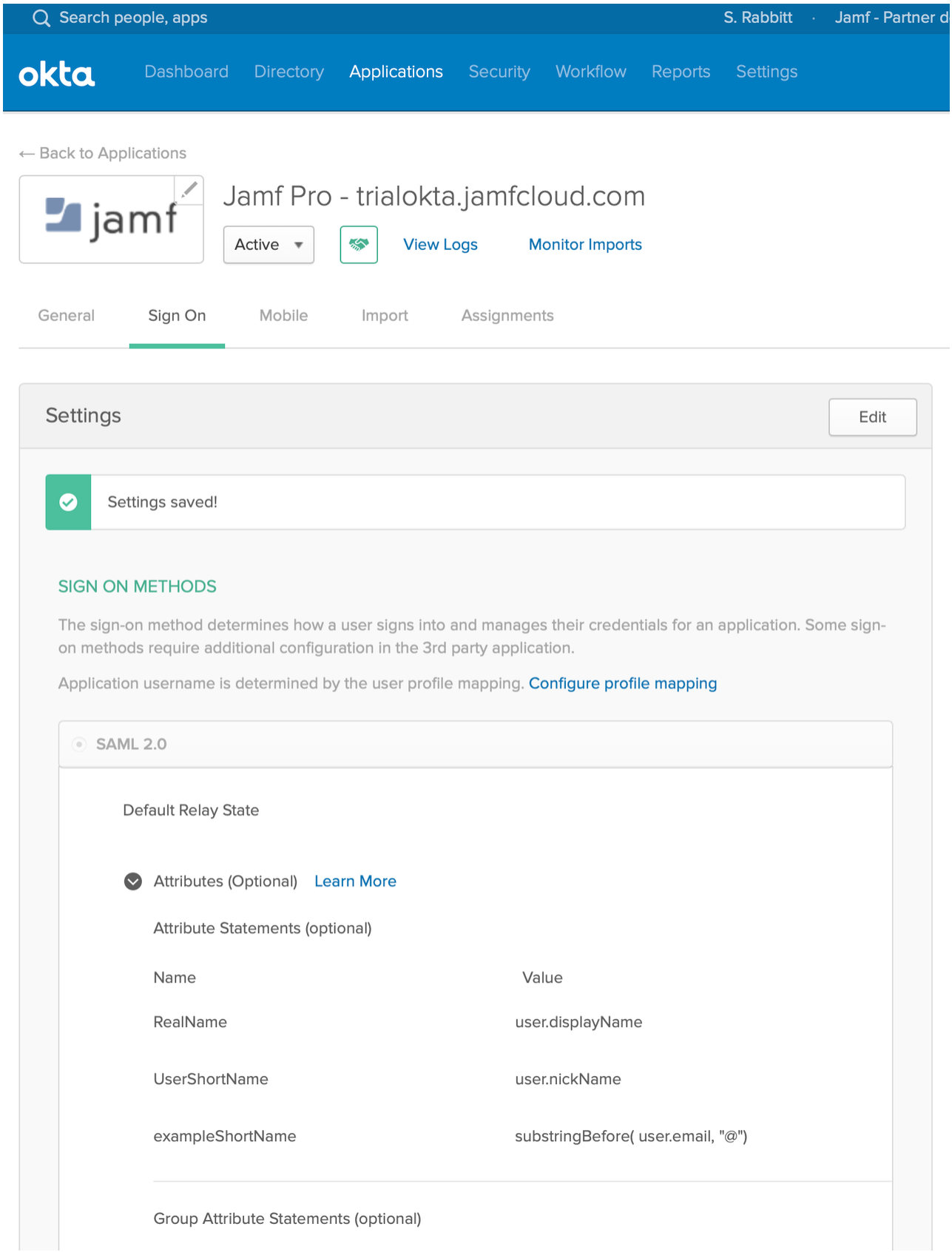
Overview: Jamf Pro can pass information obtained in the SAML token for single sign-in to Jamf Pro to automate creating a user with Jamf Connect. This requires modifying the Jamf Pro single sign-on SAML token to include the information needed for Connect.

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

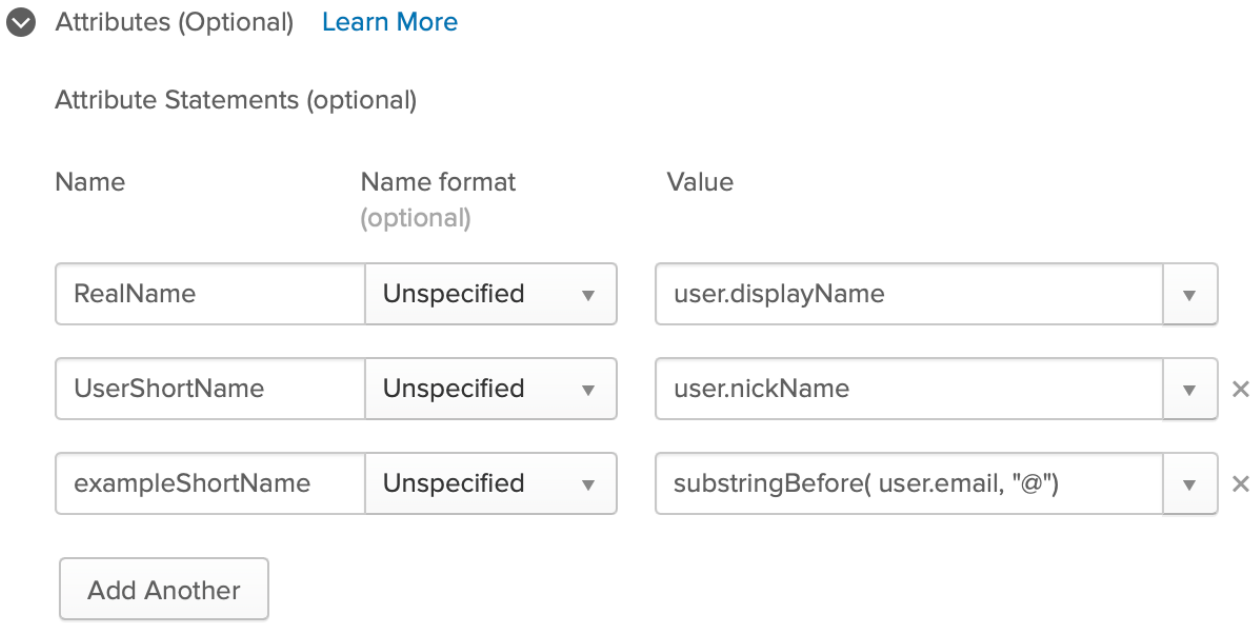
Jamf Connect needs two user attributes to create a new user:

- 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”

Navigate to your Okta tenant and select Admin. Navigate to Applications → Applications. Select your Jamf Pro Single Sign-On application. In the tab marked Sign On, select the Edit button


Search people, apps
S. Rabbitt · Jamf - Partner d
okta
Dashboard
Directory
Applications
Security
Workflow
Reports
Settings
← Back to Applications
jamf
Jamf Pro - trialokta.jamfcloud.com
Active
View Logs
Monitor Imports
General
Sign On
Mobile
Import
Assignments
Settings
Edit
Settings saved!
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
RealName
user.displayName
UserShortName
user.nickName
exampleShortName
substringBefore(user.email, "@")
Group Attribute Statements (optional)

In the section for SAML 2.0, use the “Add Another” to add an additional attribute. Map the attribute to information in your Okta user directory to add the values needed by Jamf Connect



In this example, we are adding an attribute called “RealName” which will appear in the SAML token and contain the user’s given name and family name. We are adding an attribute called “UserShortName” which will contain a field from Okta’s user directory mapped from a federated Active Directory which contains a “nickname” or “firstname.lastname” for user name. Lastly as an example, we are adding an attribute called “exampleShortName” which uses the Okta Expression Language (https://developer.okta.com/docs/reference/okta-expression-language/) to strip the user name from the email address stored in Okta’s user directory. In this example, if a user’s email address was “tyler.durden@soap.co”, the result would be “tyler.durden”.

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:

```
<saml2:Attribute Name="RealName"
```

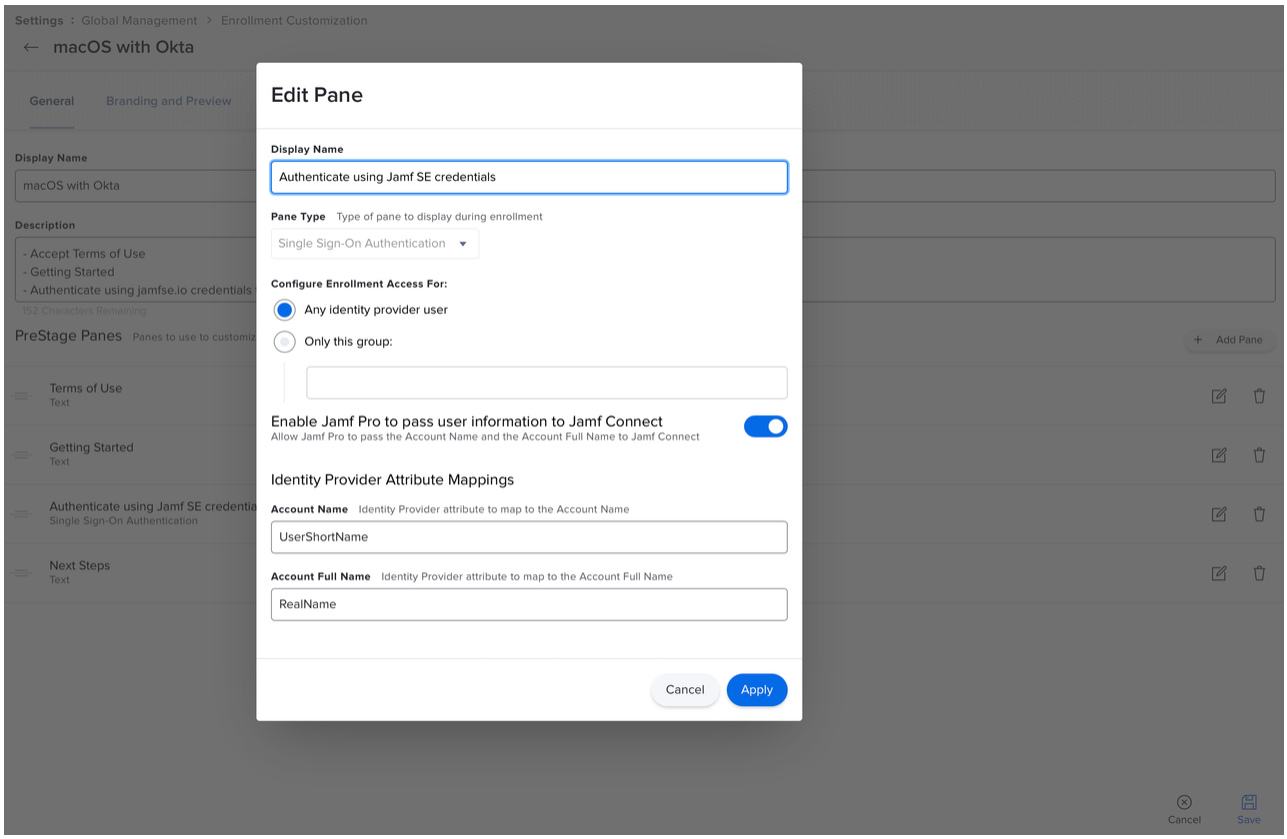
```
                        NameFormat="urn:oasis:names:tc:SAML:2.
0:attrname-format:unspecified">
        <saml2:AttributeValue xmlns:xs="http://www.w3.org/200
1/XMLSchema"
                              xmlns:xsi="http://www.w3.org/200
1/XMLSchema-instance"
                              xsi:type="xs:string">Robert Paul
son</saml2:AttributeValue>
      </saml2:Attribute>
      <saml2:Attribute Name="UserShortName"
                        NameFormat="urn:oasis:names:tc:SAML:2.
0:attrname-format:unspecified">
        <saml2:AttributeValue xmlns:xs="http://www.w3.org/200
1/XMLSchema"
                              xmlns:xsi="http://www.w3.org/200
1/XMLSchema-instance"
                              xsi:type="xs:string">robert.paul
son</saml2:AttributeValue>
      </saml2:Attribute>
```

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 Okta which will contain the user macOS short name. Using the examples from step one, we named this field “UserShortName”.

Under the section “Account Full Name” enter the name of the attribute you created in Okta which contains the user’s full given and family name. Using the examples from step one, we named this field “RealName”.

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 containing 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</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`.