Custom attribute map rules

Last Modified on 12/23/2024 1:17 pm EST

Sometimes, you can't directly map values in your SAML attribute map.

This most often occurs with:

- **Groups**, either because the IdP doesn't have groups, or the groups the IdP has aren't relevant to KnowledgeOwl.
- **Custom fields** that have a different value/meaning in your IdP and need to be "translated" to a different value in KnowledgeOwl.

In these situations, it can be useful to define a rule that will look at some attribute coming from the IdP and then update a KnowledgeOwl field based on that rule. We call these Custom attribute map rules.

There are two things to keep in mind when working with custom attribute map rules:

- **The SAML attribute map always overrides custom attribute mappings**.
  This means that you can't, for example, have a SAML attribute map entry for the Reader Groups field and also have a custom attribute map rule that sets the Reader Groups field. The SAML attribute mapping always overrides the custom mapping. If you're going to set a field using a custom attribute map rule, it's best to leave the SAML attribute map for that field blank.
- At this time, **only one rule can be applied to a specific reader/attribute combination**.
  If you have five rules for what happens with the groups field, only the first rule that is a match will be applied for a given reader, even if a reader technically matches all 5 rules. Generally, the oldest rule is the one which is applied first.

We offer three types of custom attribute map rules:

1. **Default**: The simplest of rules, the default rule will check to see if a specified IdP attribute is present at all and will set a reader field when it is. It does not care what the actual value of the IdP attribute is.

2. **Exact matches**: These will look for an exact match for an attribute value coming from the IdP and set a reader field only when it finds that exact match.

3. **Regex pattern**: The most flexible and complex rule. Define a regular expression (regex) pattern to match an IdP value and set a reader field accordingly. We use the PHP flavor of regex.

Default rules

Default rules are our simplest rule. The rule basically says: if an incoming IdP attribute has *any* value, set the selected KnowledgeOwl field for the reader.

It doesn't matter what the value of the attribute actually is.

You can only set one default rule per IdP attribute name (so, for example, you can't have two default rules that both checked the custom1 attribute coming from your IdP).

Default rules have a rule logic of **IS EQUAL TO * (anything)**.

Use case

Default rules are a fantastic choice if you want to assign all readers to one or more reader groups, or set one of the custom fields to be the same value for all SSO readers.

Setup

To create a default rule:

1. Go to **Security and access > Single sign-on**.
2. Open the **SAML attribute map** tab.
3. In the **Custom attribute map rules** section, select **+ Create New Rule**. The **Create Advanced SAML Map Rule** modal opens for you to define the rule:

4. Enter the **IdP attribute name** you'd like to base the rule on. This should be formatted exactly as it appears in the IdP.
    - If you're not sure of the attribute name, review your IdP settings or **Enable debug mode to troubleshoot issues** in the **SAML Settings** tab and try to login--debug mode shows the list of the attributes coming from the IdP.
    - For a default rule you'd like applied to all readers coming in through SSO, use any attribute that is always populated from your IdP. Email address, username or user ID, first name, or last name are often good candidates.
5. Select **Default** as the **IdP attribute value matching type**.
6. Use the **Reader attribute** dropdown to select the reader field you'd like to update based on this rule.
7. Add the **Reader attribute value** you'd like that reader attribute set to.
8. Select **Create Rule** to create and save the rule.

Once created, you can view, edit, and delete the rule in the **Custom attribute map rules** section.

Example

To set all of your incoming SSO readers to a single group, you can match against an IdP attribute which is always populated, such as the userID or email address.

In our SAML attribute map, we've mapped these fields:

- **SSO ID:** uid
- **Username / email:** email
- **First name:** firstName
- **Last name:** lastName

We set up our default **Custom attribute map rule** using these settings:

- **IdP attribute name:** uid
- **IdP attribute value matching type:** Default
- **Reader attribute:** Reader Groups
- **Assign to reader groups:** Production, Support

Once saved, this rule logic creates "**IF** uid **IS EQUAL TO** * (anything) **SET** Reader Groups **TO** Production, Support".

With this rule in place, every reader who logs in will be assigned to the Production and Support Reader Groups.

Exact matches rules

With exact match rules, you define the incoming IdP attribute the rule should examine as well as a specific value it should match. If the exact value is matched when a reader authenticates, it will set a reader field based on the rule.

Don't use with arrays
You should not use exact match rules when an incoming attribute is an array (like a list of groups). We collapse array attributes into a single field. For attributes containing arrays, use a regex rule to match within the array.

Default rules will show a rule logic of **IS EQUAL TO** *value* in the display; if you add multiple exact matches, the IS EQUAL TO will show the exact matches as an OR list in square brackets for example: "**IF** country **IS EQUAL TO** [US **OR** USA **OR** United States of America]".

Use case

The exact match rule is useful when you have a specific attribute value in your IdP that you'd like to transform into a different value in KnowledgeOwl.

For example, maybe your company operates in five offices in three countries and your IdP captures an office attribute for each employee.

But in your knowledge base, you don't care about offices. You have a reader group for each country only.

You can set up an exact match rule for the offices of each country to map your readers to those groups:

- office attributes: Colorado or New York = US employees reader group
- office attributes: London or Manchester = UK employees reader group
- office attribute: Melbourne = Australia employees reader group

Must match exactly
Exact matches are true exact matches; if you need to do a fuzzier or more flexible match, use a regex rule.

Setup

To create an exact match rule:

1. Go to **Security and access > Single sign-on**.
2. Open the **SAML attribute map** tab.
3. In the **Custom attribute map rules** section, select **+ Create New Rule**. The **Create Advanced SAML Map Rule** modal opens for you to define the rule:

---

4. Enter the **IdP attribute name** you'd like to base the rule on. This should be formatted exactly as it appears in the IdP.
    - If you're not sure of the attribute name, review your IdP settings or **Enable debug mode to troubleshoot issues** in the **SAML Settings** tab and try to login--debug mode shows the list of the attributes coming from the IdP.
5. Select **Exact matches** as the **IdP attribute value matching type** (this is usually selected by default).
6. Enter the exact value of the incoming attribute you'd like to match against as the **IdP exact match value**.
7. If you'd like to look for multiple values to match against, select **+ Add value** to add additional values for this rule.
    - Multiple values will be treated as OR values--the exact match will match for the first value OR the second value OR the third value, etc.
8. Use the **Reader attribute** dropdown to select the reader field you'd like to update based on this rule.
9. Enter the **Reader attribute value** you'd like that reader attribute set to.
10. Select **Create Rule**.

Once created, you can view, edit, and delete the rule in the **Custom attribute map rules** section.

Example

Let's say our company operates in five offices:

- Denver, Colorado
- New York, New York
- London, England

- Manchester, England
- Melbourne, Australia

We've set up reader groups in our knowledge base for each country:

- US employees
- UK employees
- AUS employees

An employee can only belong to one office, and our IdP tracks this information for each employee in an "office" field.

We want to set up a rule that will check that office field and then assign readers to the appropriate country employee group.

In our SAML attribute map, we've mapped these fields:

- **SSO ID:** uid
- **Username / email:** email
- **First name:** firstName
- **Last name:** lastName

We set up our first default **Custom attribute map rule** using these settings:

- **IdP attribute name:** office
- **IdP attribute value matching type:** Exact matches
- **IdP exact match value:** Denver
- **IdP exact match value:** New York
- **Reader attribute:** Reader Groups
- **Assign to reader groups:** US employees

And created second and third rules for our UK employees and AUS employees.

Once saved, the rule logic creates:

- "**IF** office **IS EQUAL TO** [Denver **OR** New York] **SET** Reader Groups **TO** US employees".
- "**IF** office **IS EQUAL TO** [London **OR** Manchester] **SET** Reader Groups **TO** UK employees".
- "**IF** office **IS EQUAL TO** Melbourne **SET** Reader Groups **TO** AUS employees".

With these rules in place, every reader who logs in with an office in Melbourne will be assigned to the AUS employees reader group; every reader who logs in with an office of either London or Manchester will be assigned to the UK employees reader group, and every reader who signs in with an office of either Denver or New York will be assigned to the US employees reader group.

Regex pattern rules

Regex rules are the most complicated but also the most flexible. Regex is a common abbreviation of 'regular expressions'. Regular expressions are "a sequence of characters that specifies a *search pattern*. Usually such patterns are used by string-searching algorithms for "find" or "find and replace" operations on strings, or for input validation." (from Wikipedia - Regular expression).

For regex custom attribute map rules, you define a regex pattern you'd like to search for and then define the KnowledgeOwl field and value you'd like to set when that pattern is found.

We recommend only using these rules when neither of the other custom rule types will meet your needs, as they are a bit harder to write and more intimidating if you're not familiar with regex. If an attribute you'd like to use is an array containing a list of values, you must use regex to properly search and match within that list.

regex101 is a handy site that allows you to try out regex rules against example words and phrases. When testing regex for use in KnowledgeOwl, select **PCRE2 (PHP >= 7.3)** under **FLAVOR**.

Regex pattern rules will show a rule logic of **MATCHES** [pattern] in the display, for example: "**IF** custom1 **MATCHES** /Brie/i **SET** Custom Field 2 **TO** Cheese lover".

Use case

Regex pattern rules are useful when there are patterns within one of your IdP attributes that doing exact matches for might be tedious. For example, if all our internal IdP groups are prefixed with KO_ and all of our contractor or customer IdP groups are prefixed with EXT_, and we really only care about this KO/not-KO distinction, a regex rule makes more sense than generating very large exact match rule lists.

Refer to Auto-Assign Groups By Email Rules (SSO Edition) for a walkthrough on how to set up a rule to auto-assign everyone at a given email domain to one or more reader groups.

Setup

To create an exact match rule:

1. Go to **Security and access > Single sign-on**.
2. Open the **SAML attribute map** tab.
3. In the **Custom attribute map rules** section, select **+ Create New Rule**. The **Create Advanced SAML Map Rule** modal opens for you to define the rule:

---

4. Wnrwethe **IdP attribute name** you'd like to base the rule on. This should be formatted exactly as it appears in the IdP.
    - If you're not sure of the attribute name, review your IdP settings or **Enable debug mode to troubleshoot issues** in the **SAML Settings** tab and try to login--debug mode shows the list of the attributes coming from the IdP.
5. Select **Regex pattern** as the **IdP attribute value matching type**.
6. Add the regex pattern you'd like to match that attribute value against as the **IdP value regex pattern**.
7. Use the **Reader attribute** dropdown to select the reader field you'd like to update based on this rule.

8. Add the **Reader attribute value** you'd like that reader attribute set to.

9. Select **Create Rule**.

Once created, you can view, edit, and delete the rule in the **Custom attribute map rules** section.

Example

Let's say the KnowledgeOwl IdP is used for authenticating KnowledgeOwl employees as well as KnowledgeOwl customers. Our employees might be segmented into different groups, like:

- KO_Support
- KO_Security
- KO_Development

Whereas our customers might be segmented into groups based on subscription extras:

- EXT_Base
- EXT_Base_plus_business
- EXT_Base_plus_enterprise

Within our knowledge base, we only segment content by two reader groups:

- Internal users (KO employees)
- External users (Customers)

No account belongs to both KO_ groups and EXT_ groups.

Since the two never overlap, we could create two regex pattern rules to look for these prefixes and assign our users to the appropriate reader group in our knowledge base.

In our SAML attribute map, we've mapped these fields:

- **SSO ID:** uid
- **Username / email:** email
- **First name:** firstName
- **Last name:** lastName

We set up our first default **Custom attribute map rule** using these settings:

- **IdP attribute name:** groups
- **IdP attribute value matching type:** Regex pattern
- **IdP regex pattern:** EXT_

Regex formatting note
KnowledgeOwl automatically includes the regex opening `/` and closing `/i`, so you don't need to include them in your **IdP value regex pattern**.

- **Reader attribute:** Reader Groups
- **Assign to reader groups:** External users

And created a second rule for our Internal users against the KO_ prefix

Once saved, the rule logic creates:

- **"IF groups MATCHES /EXT_/i SET Reader Groups TO External users".**
- **"IF groups MATCHES /KO_/i SET Reader Groups TO Internal users".**

With these rules in place:

- **Anyone with any IdP KO_ group would be assigned to the Internal users reader group.**
- **Anyone with any IdP EXT_ group would be assigned to the External users reader group.**
