

# NativeSPNotify

The `<Notify>` element represents a resource inside an application protected by Shibboleth that is created to process "application notifications" of significant lifecycle events for a user session that the SP is processing.

Currently there are three "events" that cause notifications:

- logout/end of a session
- a change to a user's SAML `<NameID>` value sent from an IdP
- the termination of a user's SAML `<NameID>` value (a deprovisioning event)

There are also two kinds of notifications, "front-channel" and "back-channel", but only logout events support front-channel notifications in the current implementation.

## Attributes

- `Channel` ("front" or "back")
  - Required attribute to identify the method of notification.
- `Location` (absolute URL)
  - The URL to send the notification message to.

## Front-Channel Notifications

Front-channel notifications take place through the user's browser using redirection. The advantage is that you get real-time control over the UI as well as access to the active session (if you protect the endpoint itself). The downside is that the application has to ensure that it provides a response and properly forwards the browser to the "next" location in the notification chain.

The front-channel "protocol" is a redirection to the endpoint with a query string containing the following parameters:

- `action`
  - Currently only the value "logout" is possible.
- `return`
  - The URL to redirect the browser to when finished processing the event. The application **MUST** send the browser here to prevent problems during single logout.

## Back-Channel Notifications

Back-channel notifications are done behind the scenes using SOAP messages sent by the SP to the notification endpoint. The advantage is speed and invisibility to the user. The downside is that only limited information is made available to the application, and usually the application will require changes in how it maintains its own state to take advantage of the feature.

The back-channel protocol is a SOAP message using a custom schema supplied with the SP. A description follows. The XML namespace is `urn:mace:shibboleth:2.0:sp:notify`

Notification endpoints should respond to the event with a response containing an empty element named `<notify:OK>` or a SOAP fault.

## Logout Events

Logout event notification uses the `<notify:LogoutNotification>` element.

### Attributes

- `type` ("local" or "global")
  - Indicates the type of logout event. Local logout is confined to the SP, while global logout involves the IdP as well.

### Child Elements

- `<SessionID>` (one or more)
  - The ID of a session being logged out. The application is responsible for connecting the SP's session ID to its own state.

## NameID Management Events

NameID management event notification uses the `<notify:NameIDNotification>` element.

### Child Elements

- `<saml:NameID>` (required)
  - The original identifier associated with the user.
- `<samlp:NewID>` or `<samlp:Terminate>` (one or the other)
  - The new identifier to associate with the user, or the termination notice. These elements come directly from the SAML protocol schema and are simply copied from the actual protocol message.

---

For guidelines how to adapt a web application in order to support Single Log Out (SLO), please have a look at [SLOWebappAdaptation](#)