Single Sign-on Using SAML Overview

Security Assertion Markup Language (SAML) is an industry standard which allows two or more systems to share a common source of credentials. The credential source is known as an **"Identity Provider"** and is a secure source of personal information. An Identity Provider controls access to a user account via a strong password and login process. In Visual Antidote's implementation of SAML this Identity Provider is **iMIS**.

Other participating websites or applications are known as **"Service Providers"**. A Service Provider is another website or application which has been provided a link to the iMIS Identity Provider. Visual Antidote is now offering an improved Single Sign-on package for our iMIS / Kentico clients that leverages iMIS as the Identity Provider and Kentico as a Service Provider.

Setting up SAML

Setting up SAML integration is easy. Here are the steps:

- A new Identity Provider iPart is installed on iMIS along with a shared encryption key. This iPart works with the native Login applicable to your iMIS version.
- Kentico is updated to use an iMIS URL as its login page instead of using the native login process. The shared encryption key is also installed on Kentico.
- IQAs are used to define the information that will be sent from iMIS to Kentico. Visual Antidote provides standard IQAs as part of the installation which are adjusted as needed.

How it Works

When someone tries to access secure resources on a Service Provider (Kentico) website it sends a request to the iMIS Identity Provider instead of asking the user to login. The iMIS Identity Provider handles the login (either asking the user to login or, if they are already logged in, confirming their status) and authenticates the user. Once the user is authenticated, then an encrypted message is flowed back to the Service Provider in XML format. This message contains information about the user (ID, name, email, personal details) and their roles (customer, administrator, member, etc.).

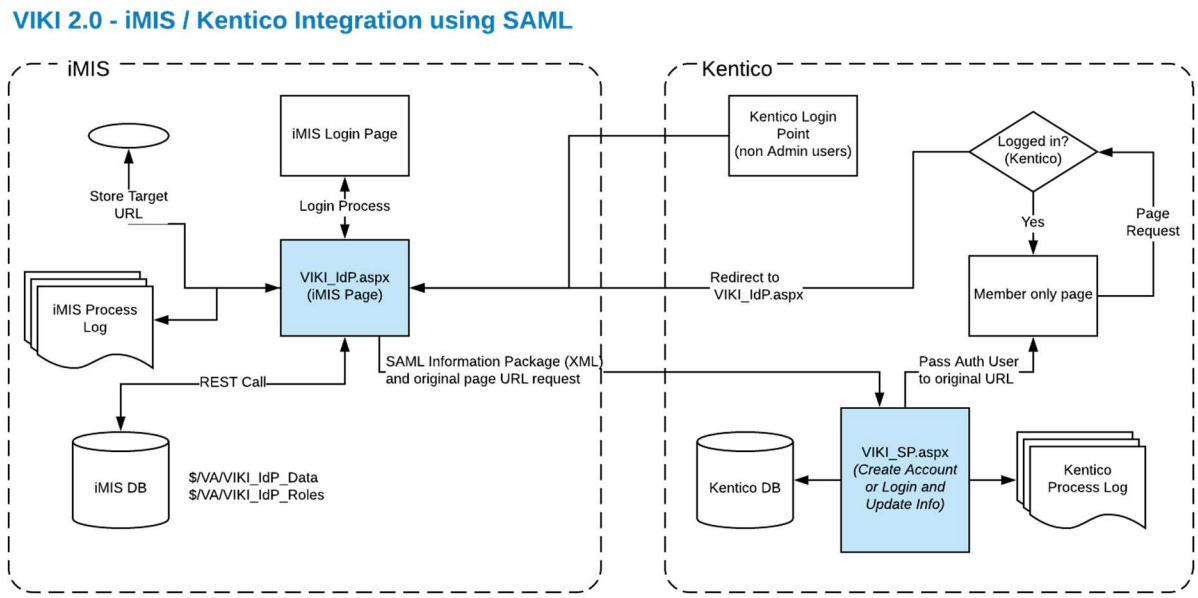
The Service Provider uses the shared encryption key to decrypt messages from the Identity Provider. If the message decrypts properly, then the Service Provider logs the user in without further interaction being required and refreshes the user's information in Kentico.

SAML uses **assertions** to enable an Identity Provider to securely communicate attributes and privileges of a user to a Service Provider. Assertions carry detailed information about the user, including: what application rights they have, if they are allowed to access multiple applications, how long they may access the application and much more.

Visual Antidote's SAML implementation uses IQAs to define the assertions provided by the iMIS Identity Provider. This means that each client can easily tailor their SAML configuration to provide exactly what data is required by the receiving system(s). For example, if someone has a member type of "Life" and status of "Gold" then a badge could be displayed on the Service Provider site since this information can be passed forward from iMIS to Kentico.

Benefits

- SAML is an **industry standard** approach to Single Sign-on and is supported by multiple applications and services. Because it is platform independent, clients can expand their supported systems and services easily by using SAML integration. For example, an association partnering with a regional affiliate can allow their members to access the affiliate website without having to share any data or logins directly.
- SAML is **highly secure**. By using a shared encryption key between systems clients can have a high degree of confidence that user data is fully protected while in transit.
- SAML offers an excellent **user experience**. SAML provides the ability for users to securely access multiple applications with a single set of credentials entered **once**. Visual Antidote's implementation between Kentico and iMIS also allows our clients to ensure that a user is logged into all related web properties in a single step and similarly ensures that a logout event is processed on all websites. Using SAML, users can seamlessly access multiple applications, allowing them to conduct business faster and more efficiently.



Find out more

Visual Antidote's SAML integration is available as a specific implementation package and is tailored to the specific versions of iMIS and Kentico used by your organization. For more information, please contact Visual Antidote.