On this tab, you can adjust settings related to Claims-based authentication.

⚠ **Note**: You may need to set up SSL for your site to use certain identity providers.

General	
Enable WIF authentication	Enables claims-based authentication. Users need to log in through the identity provider specified by the settings below (for example Active Directory Federation Services). Disables the standard authentication mechanisms in Kentico.
Identity provider URL	Specify the URL of your identity provider's **WS-Federation passive endpoint**. You can find the value in the provider's configuration interface or WS-Federation metadata. Example: *https://adfs.net/adfs/ls*
Security realm	Enter a URI that identifies your website or application. You can use your website's **domain name** (and virtual directory if applicable) in most cases. The value must be exactly the same as in the **relying party** configuration of your identity provider, including letter case, any trailing slashes and the protocol (http or https).
Allowed audience URIs	URIs of allowed audience for the identity provider, separated by semicolons. The value must match the corresponding relying party settings of your identity provider, including letter case, any trailing slashes and the protocol (http or https). To allow the authentication for all restricted sections of your website and the Kentico administration interface, use the base domain name of the website.
Trusted certificate thumbprint	Enter the thumbprint of the certificate used to secure the communication between Kentico and the identity provider. You can typically find the certificate thumbprint in the provider's Key/Certificate configuration.
Certificate validator	Sets the validation mode used for the X.509 certificate specified in the **Trusted certificate thumbprint** setting. • **Chain trust** – accepts certificates whose chain of trust leads to a trusted certification authority. The certificate must be installed on the server hosting Kentico in the *Local Computer -> Trusted People* certificate store. • **Peer trust** – accepts self-issued certificates. The certificate must be installed on the server hosting Kentico in the *Local Computer -> Personal* certificate store. • **Peer or chain trust** – accepts self-issued certificates, or certificates with a chain that leads to a trusted certification authority. • **None** – no validation of the certificate is done and the system accepts any certificate with the given thumbprint. See Working with Certificates.