CONTENTS

LexisNexis®

Overview and Important Information

Welcome to Lexis+ South Africa

This document sets out how to access Lexis+ South Africa, using your network/active directory credentials.

What is SAML/SSO?

This method of access manages both session and user authentication. This service permits a user to use one set of network login credentials to access multiple applications. SAML is the implementation standard for Lexis+.

Users who previously accessed their subscriptions through IP-fixed/Self-Reg on the legacy platform will now use the new Lexis+ South Africa platform with their network credentials, eliminating the need to remember different passwords.

When can I access the SSO URL?

You will be informed by your organisation's administrator about the start date for accessing the SSO URL once implementation and testing are complete. Please refrain from attempting to access the platform before this date.

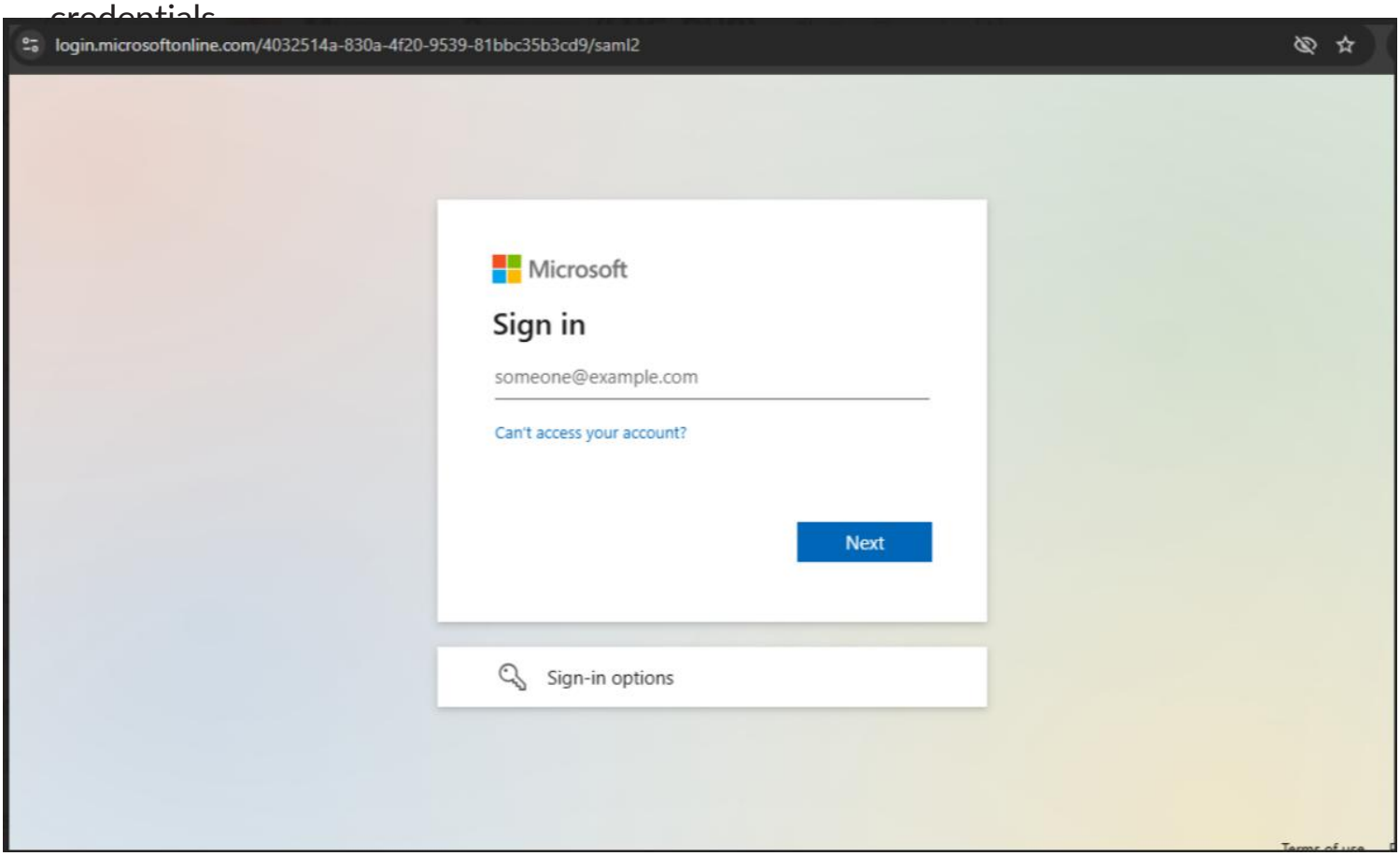
How to access Lexis+ SA via SSO/SAML

1. Your Administrator will communicate the go-live date to access the platform.

- On this date, go to the URL https://plus.lexis.com/za?federationidp=QZKR9574967

provided . This link is referred to as your South African SSO URL.

2. You will be presented with the screen below. Please insert your network credentials

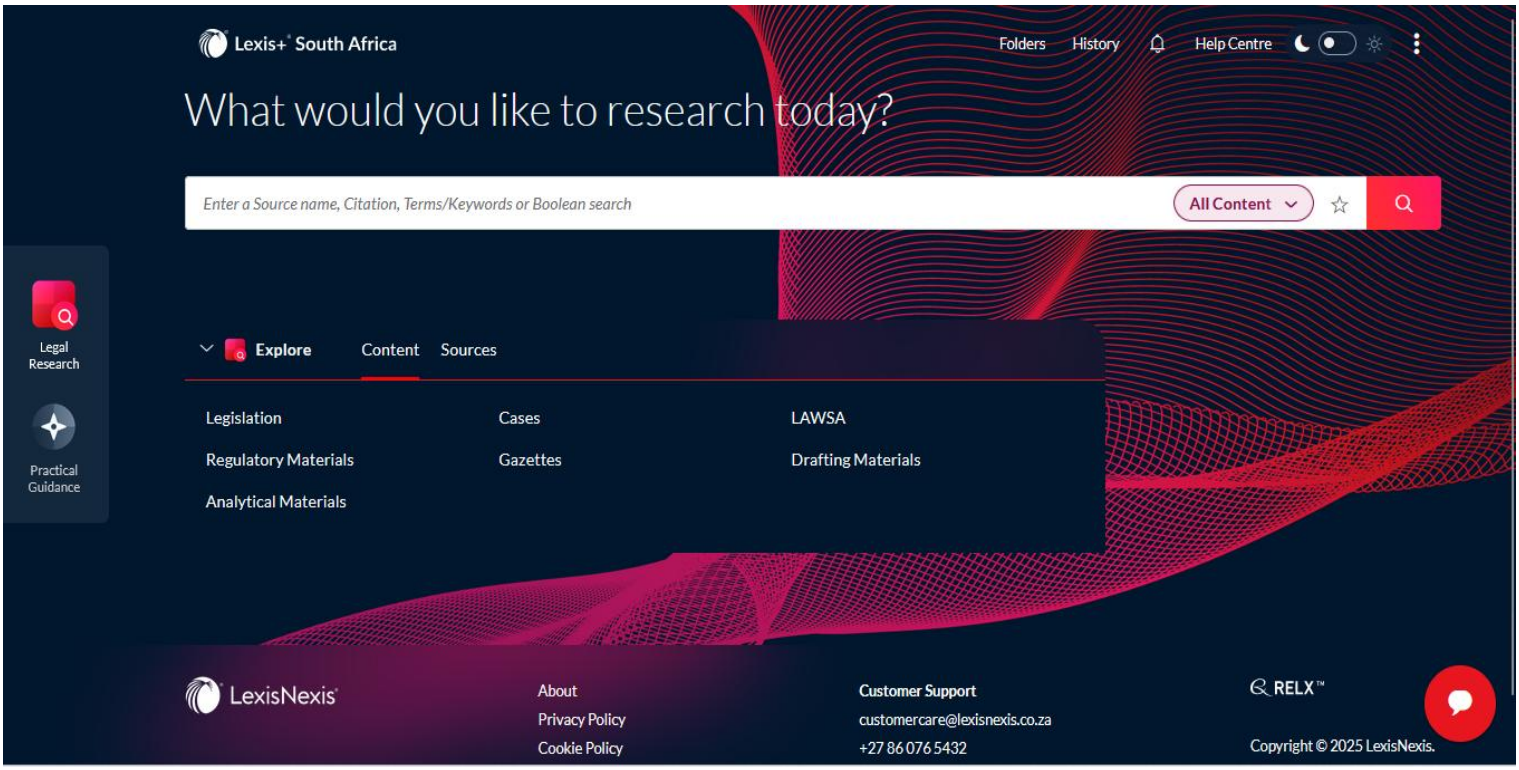


Note: Depending on your organisation's setup, you might need to use Multi-Factor Authentication (MFA). This means after your first attempt to log in using your credentials, the system will prompt you for a second verification factor. This could be like a PIN or one-time password (OTP) to be entered to verify your identity.

If you are saving the URL as a favourite, you would need to go into the favourite and edit the URL to be the actual SSO URL

How to register as a user: Verifying your account

1. Once you have entered your details and clicked “Save”, the Home Page will appear as shown below.



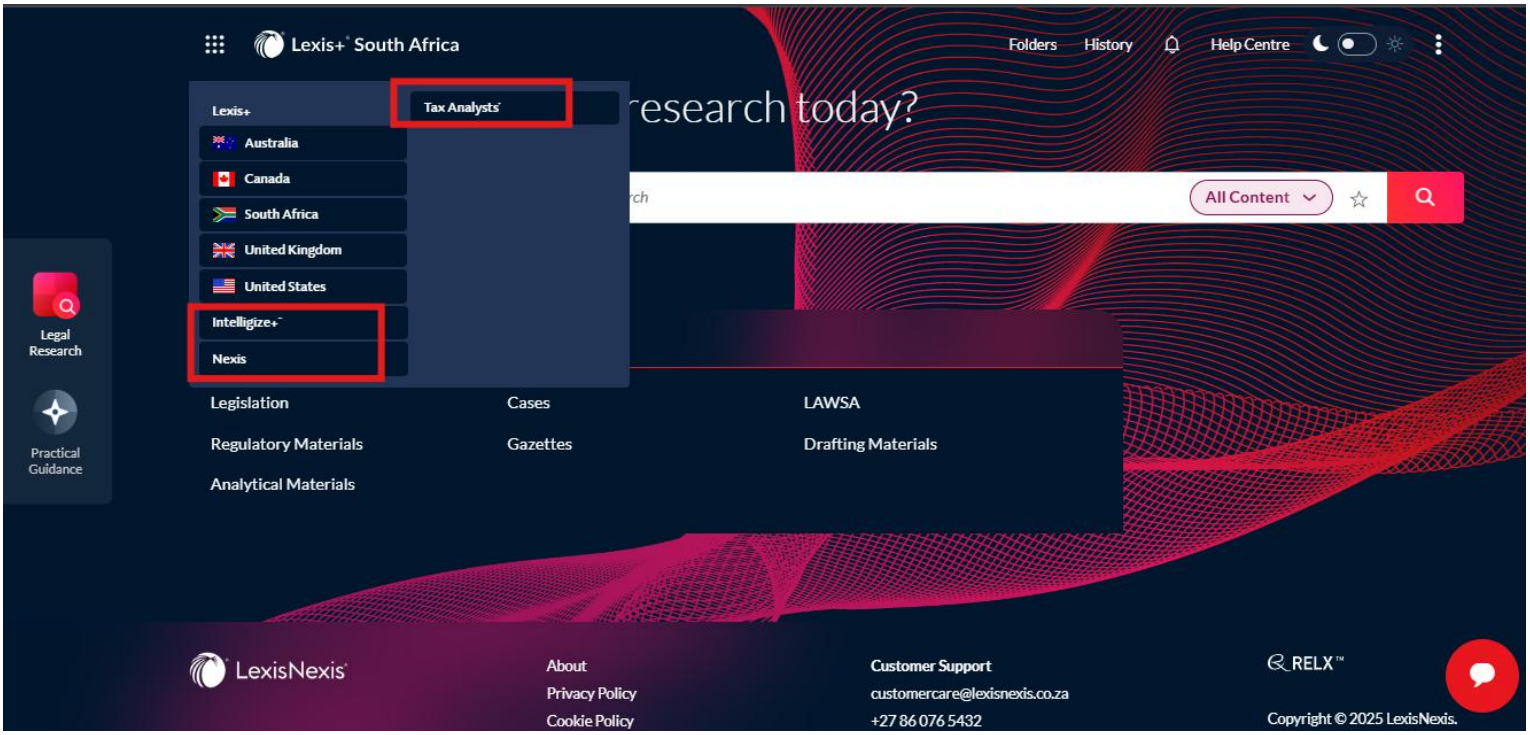
Tip: Remember to bookmark your SSO URL for easy access later on.

Accessing other products via Product Switcher

1. You will need to access your South African SSO URL.

2. Your log in ID will be the one being used for South Africa.

3. If you subscribe to other LexisNexis global products, you will be able to view and access these products using the product switcher.



Support and Administrator's Contact Details

LexisNexis Contact Details

Please contact your LexisNexis Support team to escalate queries:

- **Account Manager**: Keith Ndlovu

  Account Manager Email: keith.ndlovu@lexisnexis.co.za

- **Customer Care**:

  Email: customercare@lexisnexis.co.za

  Phone: +27 86 076 5432

- SAML Certificate update or configuration change requests email: SAML/SSO@lexisnexis.com

Annexure: Error Codes

Here is the complete list of all possible error codes that could be returned.

Error Number	Description	Resolution
1	Generic Federation error – an unknown error occurred in the LexisNexis® Authentication system while attempting to establish the federation.	Contact your LexisNexis® representative to begin an investigation into the root cause.
100	The Subject Confirmation received from the Identity Provider was not valid. The subjectConfirmation attribute associates an Assertion to a Service Provider and a timeframe. Example: <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"> <saml:SubjectConfirmationData InResponseTo="id-35nXLhFIPCUPjQcZAD9F" NotOnOrAfter="2013-06-27T15:48:08Z" Recipient="http://SP_SSO_URL"/> </saml:SubjectConfirmation>	Check that the Service Provider URL matches the actual Service Provider in the Assertion. Also check that the Time restriction would have been valid when the Service Provider received the Assertion. If these conditions are acceptable, then contact a LexisNexis® representative to investigate the issue.
101	The Conditions attribute in the Assertion received from the Identity Provider was not valid. This attribute defines the limited time frame in which the Assertion is valid. Example: <saml:Conditions NotBefore="2013-06-27T15:33:08Z" NotOnOrAfter="2013-06-27T15:38:08Z"> <saml:AudienceRestriction> <saml:Audience> http://dvc7730.lexis-nexis.com:26486/oam/fed </saml:Audience> </saml:AudienceRestriction> </saml:Conditions> It is also possible that the Audience Restriction does not match the Entity ID of the Service Provider to whom the Assertion was sent.	Validate that the time frame is accurate and would have been acceptable when the Service Provider received the request. This error typically occurs if there is a difference in the system times between the Identity Provider and Service Provider servers. It will likely be necessary to work with a LexisNexis® representative to validate that the system times are close enough, or the Identity Provider may need to expand the time frame that the Assertion is valid to account for the difference. If the error persists, ensure that the Identity Provider's Audience Restriction and the Service Provider's Entity ID match.
102	The Signature in the Assertion received from the Identity Provider was not valid. The Identity Provider includes a digital signature in the Metadata XML during configuration in the Service Provider's system. That signature is used to validate the signature provided with the Assertion to make sure the Assertion can be trusted.	Validate that the signature was not changed, and that the certificate is not expired.
103	More than one user in the LexisNexis® Authentication system matched the Assertion Identity.	Use LexisNexis® Admin Tool to find users with the same assertion values. Change one so that both are unique. If you are unable to determine the conflicting users, contact your LexisNexis® representative to investigate the issue.

104	No users in the LexisNexis® Authentication system matched the Assertion Identity.	Use the LexisNexis® Admin Tool to configure the appropriate user. Ensure that the user has an assertion value for the Identity Provider that matches a user in the LexisNexis® Authentication system.
105	The Assertion was not valid XML or did not conform to the Schema for the Assertion XML. For more information, see http://docs.oasis-open.org/security/saml/v2.0/saml-schema-assertion-2.0.xsd.	Check the Assertion XML that was sent to the Service Provider and validate it against the Schema to determine the root cause of the error.
106	No SAMLRESPONSE parameter was included in the POST body. The SAMPLRESPONSE parameter is a Base64-encoded version of the SAML Assertion. It must be included as a parameter in the POST request to the Delete URL. This error occurs when it is not.	Check the Identity Provider system to verify that the parameter is being included correctly in the Request Body. If you believe it is, please contact a LexisNexis® representative referencing the error code and Identity Provider Federation ID so an internal investigation into the error can be initiated.
111	The LexisNexis system was unable to complete the request for an internal error with its SSO system.	Contact your LexisNexis® representative to begin an investigation into the root cause. This error generally indicates a failure within the LexisNexis® Authentication system. Please provide the Identity Provider and Assertion value that was used in the attempted assertion.
112	The user that was found matching the identity in the assertion was in SUSPENDED status in the Lexis Advance system.	Contact your LexisNexis representative if you believe the user should not be suspended.
113	This error occurs when a user assertion is attempting just in time provisioning because no users were mapped, but a user with the same first name, last name, and email address already exists in the system for the given customer account.	A user administrator needs to use MyLexis to associate the existing user to the assertion ID provided in the assertion. If this does not resolve the error, please contact your LexisNexis® representative to begin an investigation into the root cause.
114	A Profile ID was not supplied or able to be identified from the configuration for an assertion that required Just In Time ID Provisioning.	Contact your LexisNexis® representative to begin an investigation into the root cause. This error generally indicates an improper or outdated configuration for the identity provider in the LexisNexis® Authentication system.
115	The assertion was missing.	Attributes associated with the attribute to profile ID mapping configuration were not present in the assertion. The Identity Provider administrator and your Lexis Nexis® representative need to verify the assertion and configurations are correct. Please provide the Identity Provider ID, Assertion value, and timestamp of the request that was are associated to the attempted federation.

116	There are no Profiles matched in the attribute to profile ID configuration, and a default Profile ID was not configured.	User attributes provided in the assertion did not match any of the groupings defined for the identity provider to determine the correct profileID. Either new profile ID group needs to be added/a default to be configured. The Identity Provider administrator and your Lexis Nexis® representative need to verify the assertion and configurations are correct.
117	There are no Profiles matched in the attribute to profile ID configuration, and a default Profile ID was not configured.	User attributes provided in the assertion did not match any of the groupings defined for the identity provider to determine the correct profileID. Either new profile ID group needs to be added/a default to be configured. The Identity Provider administrator and your Lexis Nexis® representative need to verify the assertion and configurations are correct. Please provide the Identity Provider ID, Assertion value, and timestamp of the request that was are associated to the attempted federation.
118	There are more than one matching profileID for the attributes provided in the assertion.	This is a configuration issue with the SAML attribute to profile ID mapping associated to Just in Time Provisioning. The Identity Provider administrator and your Lexis Nexis® representative need to verify the assertion and configurations are correct. Please provide the Identity Provider ID, Assertion value, and timestamp of the request that was are associated to the attempted federation.
119	The Identity Provider is not mapped to the customer account that the Profile ID is associated to.	Either the customer account needs configured to accept the Identity Provider requesting Just in Time Provisioning for the given Profile ID, or the Identity Provider is using an invalid profileID in their configuration. The Identity Provider administrator and your Lexis Nexis® representative need to verify the assertion and configurations are correct. Please provide the Identity Provider ID, Assertion value, and timestamp of the request that was are associated to the attempted federation.
120	Multiple customers mapped error when retrieving a profile ID for Just in Time Provisioning	Contact a LexisNexis® representative, referencing the error code and Identity Provider Federation ID so an internal investigation into the error can be initiated.
10001	A General Federation error occurred.	Contact a LexisNexis® representative, referencing the error code and Identity Provider Federation ID so an internal investigation into the error can be initiated.
10002	Invalid Metadata was configured for the Identity Provider in the LexisNexis® system.	This error is generally encountered during initial setup, and not after the Identity Provider is integrated with the system. It identifies an issue with the XML provided during the Metadata Exchange.

10003	A Database Error occurred in the Lexis Advance® SSO Service.	Contact a LexisNexis® representative referencing the error code and Identity Provider Federation ID so an internal investigation into the error can be initiated.
10004	An Initialization error occurred in the Lexis Advance® SSO service	Contact a LexisNexis® representative referencing the error code and Identity Provider Federation ID so an internal investigation into the error can be initiated.
10005	A Configuration error was encountered in the Lexis Advance® SSO service.	Contact a LexisNexis® representative referencing the error code and Identity Provider Federation ID so an internal investigation into the error can be initiated.
10006	SAML Response Error	The Assertion Posted to the SSO URL (https://sign-in.lexisnexis.com/lnaccess/fed/sso) did not contain a SAMLRESPONSE parameter in the POST request. The SAMLRESPONSE parameter should contain the Base64-encoded SAML Assertion.
10007	General Assertion Error	An unknown error occurred in the system related to attempting to create the federation. Contact a LexisNexis® representative referencing the error code and Identity Provider Federation ID so that an internal investigation can be initiated.
10008	Parser Error	Contact a LexisNexis® representative referencing the error code so an internal investigation into the error can be initiated.
10009	Metadata Error	Contact a LexisNexis® representative referencing the error code and Identity Provider Federation ID.
10010	Signature Error	The signature in the SAML Assertion does not match the signature information stored for the IDP in the metadata. Contact a LexisNexis® representative referencing the error code and Identity Provider Federation ID.
10011	The Federation is configured in the system, but is marked as inactive.	The Identity Provider is marked as inactive in the LexisNexis® system. This may be due to various reasons. Most commonly, an identity provider will be marked inactive while being configured and having user assertions configured prior to going live. If this is not the case, please contact LexisNexis referring to the Federation ID provided to you when the Identity Provider was configured.