UpToDate Single Sign-On

Customer Implementation Guide

November 2024

Wolters Kluwer

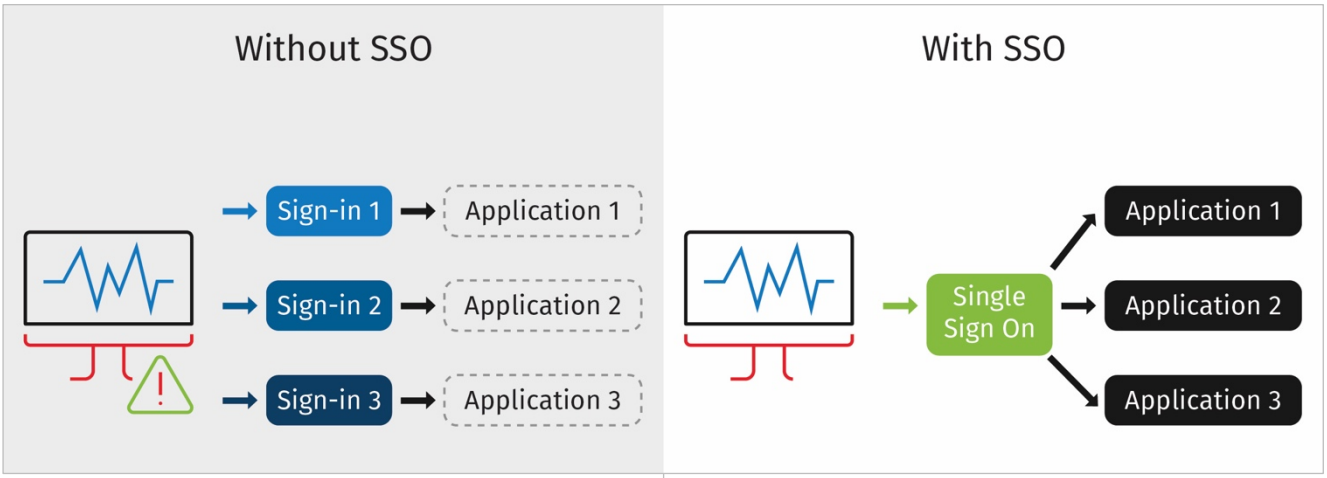
Content

1. Purpose of this Document

This document intends to help customers implement Single Sign-On (SSO) with UpToDate®. It covers the SSO capabilities offered with UpToDate and provides guidance to customers on how to implement SSO based on the SSO solutions or technologies they use.

2. About Single Sign-On

Single Sign-On (SSO) is an authentication mechanism that allows a user to **sign in with a single ID & password** to several, independent software systems.



2.1 How does SSO work?

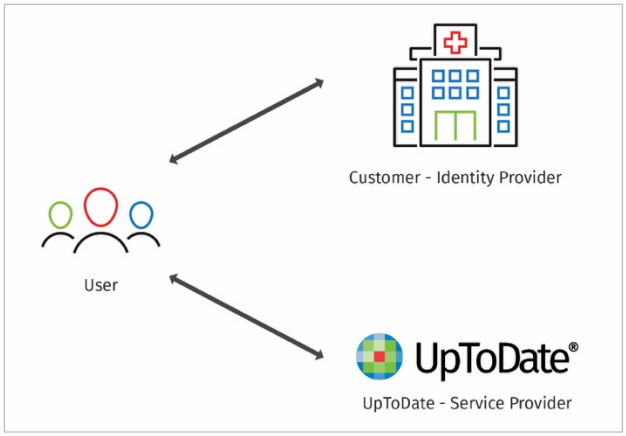
SSO is made possible by trust relationships between a user and their identity provider, and an application and the identity provider. The user trusts that their identity provider is secure and confidential. The application trusts that the identity provider will properly authorize users and properly represent their identity.

Service Provider – Delegates sign-ins to the identity provider and gives the user appropriate access to the requested resource.

Identity Provider – Performs authentication and passes the user's identity and authorization level to the service provider.

2.2 Definition of SSO relationships

The picture below outlines the relationships between UpToDate and the customer.



3. Benefits of SSO with UpToDate

Implementing Single Sign-On with UpToDate provides the following benefits to your clinicians.

SSO technology provides rapid scalability, simpler onboarding of new entities & clinicians and reduces password fatigue, while making it easier for your providers to access UpToDate clinical content.

Improve your clinician's experience

- Reduce password fatigue
- Streamlined access to trusted content
- Eliminate reverification burden

Seamlessly integrate within your technology ecosystem

- Faster onboarding of new entities
- Provide easy and secure remote access

4. UpToDate SSO Access Points

UpToDate can provide access via SSO from the following access points. Depending on your product offering not all access points may be pertinent to your organization. We recommend that you use SSO across all access points so that your users have a consistent experience.

Web – desktop & mobile

Mobile app

Integration points in clinical workflows such as Electronic Health Records or software systems that your users would like to access UpToDate from.

5. Supported SSO Protocols and Solutions

5.1 SSO solution

UpToDate supports the following SSO solution providers:

- Microsoft Azure
- OpenAthens

5.2 SSO standard protocols

UpToDate supports the leading SSO open standard protocols:

- OpenID Connect
- SAML

5.3 Support for other SSO solutions

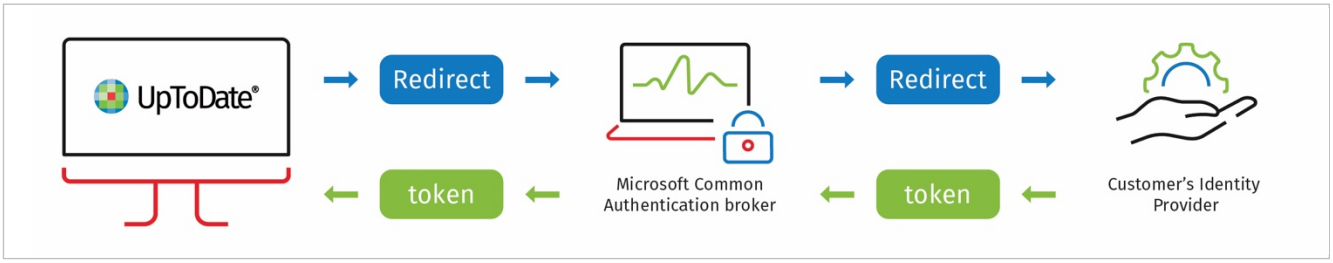
UpToDate can integrate with other SSO solutions via OpenID Connect or SAML. Examples include Okta, Amazon Cognito, and Google. Please reach out to the UpToDate Implementation Team if you have any questions or would like to discuss further.

6. Configuring SSO with UpToDate

This section covers the configuration details needed from the customer for different SSO solutions and protocols to implement SSO with UpToDate.

6.1 SSO using Microsoft Azure

- Customer's user directory is hosted or integrated with Microsoft Azure Active Directory
- Customer provides UpToDate with its "tenant id"
- UpToDate links customer account to tenant (issuer)
- Sign-in/Redirect URL is https://www.uptodate.com/login/customername.com or sign in through the Microsoft button on the UpToDate Sign-In page



6.2 SSO using OpenAthens

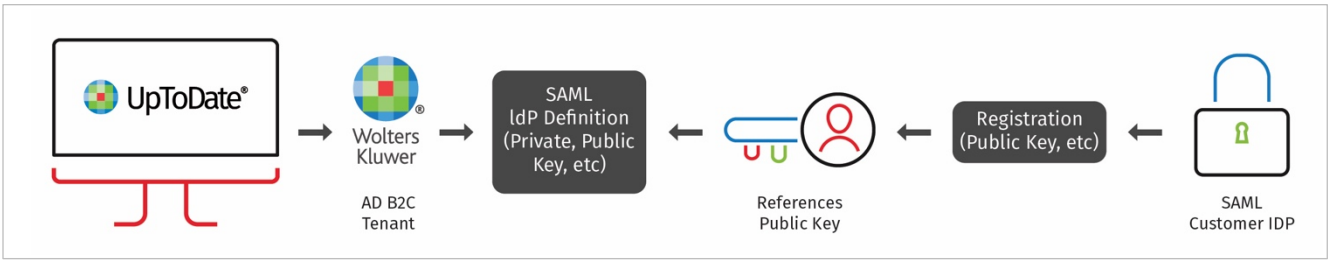
- Customer's user directory is federated by OpenAthens
- Customer provides UpToDate with its "org id"
- UpToDate links customer account to org id
- Sign in through the OpenAthens button on the UpToDate Sign-In page

6.3 SSO via OpenID Connect

- UpToDate provides Redirect URL to the customer
- Customer configures new client within their OIDC Identity Provider and provides UpToDate with:
  - Well-known configuration URL
  - Client ID
  - Client Secret
  - Scopes
- UpToDate configures new OIDC IdP integration
- UpToDate links customer account to new IdP
- Sign-in/Redirect URL is https://www.uptodate.com/login/customername.com

6.4 SSO via SAML

- UpToDate will provide our Metadata URL and Assertion attribute details.
- Customer provides UpToDate with:
  - Public x509 Certificate
  - SAML Metadata URL
- UpToDate configures customer set up and provides Application Callback (redirect) URL
- Customer configures SAML IdP to send Required Attributes to UpToDate
- UpToDate links customer account to new IdP
- Sign-in/Redirect URL is https://www.uptodate.com/login/customername.com

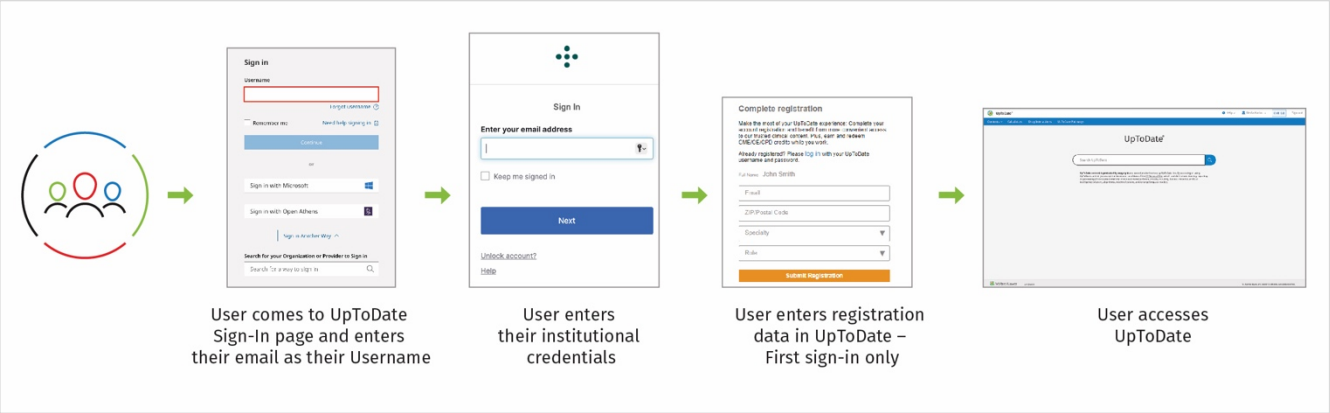


7. User Sign-In Experience

This section explains how SSO users would sign in to the UpToDate web or mobile app from the UpToDate Sign-In page.

7.1 Accessing via Email

If you assign emails with your registered domain to your users, they can simply enter their email.



User comes to UpToDate Sign-In page and enters their email as their Username

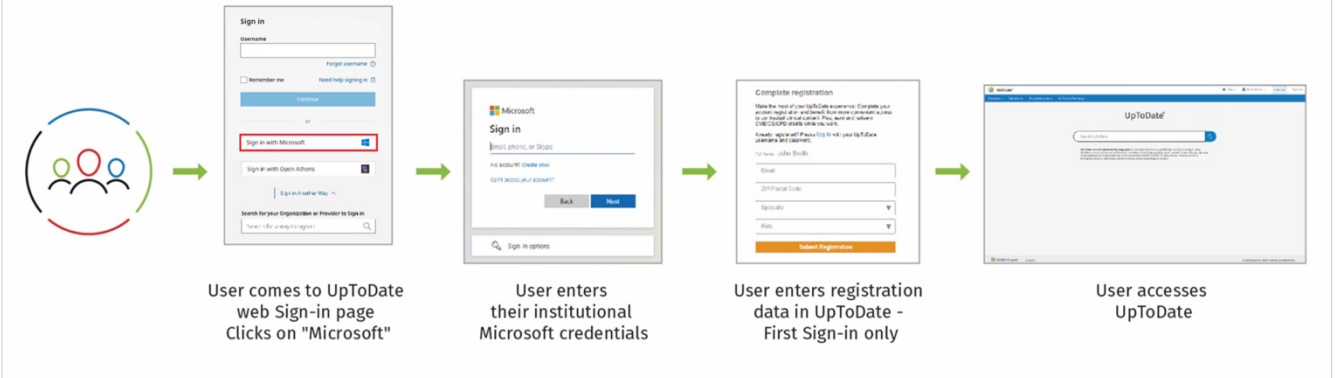
User enters their institutional credentials

User enters registration data in UpToDate – First sign-in only

User accesses UpToDate

7.2 Accessing via Microsoft Azure

If your organization uses Microsoft SSO, users can also use the Microsoft button.



User comes to UpToDate web Sign-in page Clicks on "Microsoft"

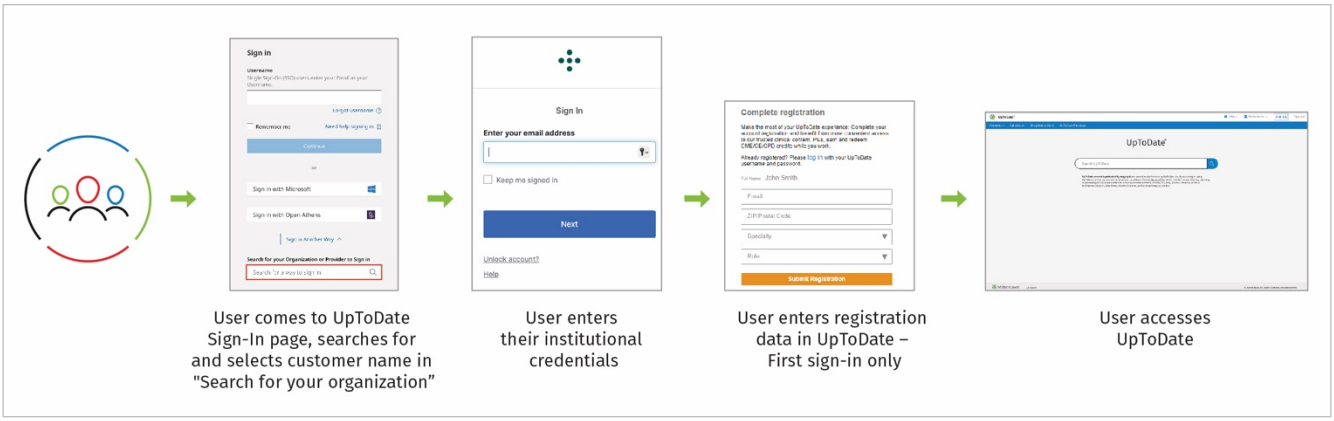
User enters their institutional Microsoft credentials

User enters registration data in UpToDate - First Sign-in only

User accesses UpToDate

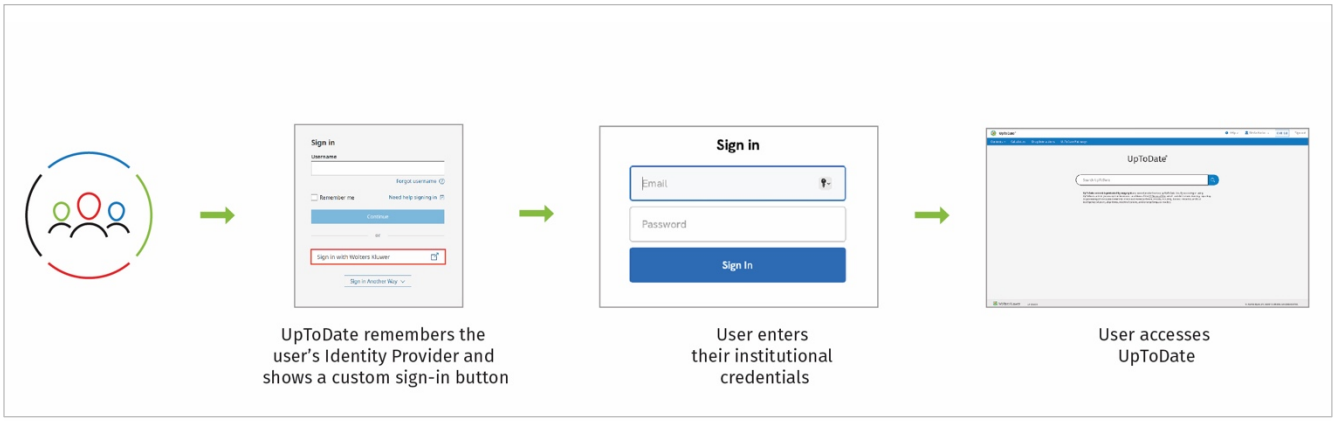
7.3 Accessing via Search

If you do not assign an enterprise email to all UpToDate users and you use an SSO solution other than Microsoft Azure or Open Athens, users will be able to search for your institution name.



7.4 Returning SSO Users

When a user signs in with SSO, the UpToDate Sign-In page notes the institution the user signed in with to tailor the page with an institution-specific button. On future visits, users can use this button for UpToDate access with a single click.



8. Custom URL

UpToDate provides a custom URL, with the exception of OpenAthens, by which users can be directed to their institution's sign-in. You can share this URL with your users.
Example: https://www.uptodate.com/login/customername.com

9. SSO Integration URL

To integrate UpToDate in a clinical workflow product such as an Electronic Health Record (EHR) system or internal portal, you can integrate the following URL with an UpToDate search box or link https://www.uptodate.com/login/customername.com?source=<Argument value>

The UpToDate implementation team will provide your unique “source” parameter. This provides the ability to collect analytics specific to each integration point. When accessing UpToDate through the SSO integration URL, you might have to sign in with SSO. This is to provide appropriate security, especially on computers that many people use.

9.1 Multiple integrations

If your institution has multiple integration points, then the UpToDate implementation team will provide the “source” parameter unique to each integration point.

9.2 Existing integration

If your institution has an existing UpToDate integration, we request that the current integration URL is replaced with the SSO URL explained here. This helps your users have the same identity from integrated access points as others.

10. UpToDate SSO & Search API

With the addition of SSO as an access method for UpToDate customers, we’ve also expanded the capabilities of our Search API to support direct links to UpToDate content and other features using SSO. Users who are not yet signed in to your institution’s identity provider will be prompted to sign in to the system before being directed to the UpToDate content specified in the link.

Users who are already authenticated will be brought to the content directly after a brief, automatic exchange of information between your institution’s system and UpToDate – no data input by the user needed.

UpToDate supports 2 formats for direct linking via SSO.

10.1 SSO Format One – Path-based

Many URL's can be SSO-enabled with a change to the path that includes your registered domain, for example, “wolterskluwer.com”.

The **search** parameter links to a specific topic by search term:
https://www.uptodate.com/login/customername.com?search=elbow

The **topicId** parameter links to a specific topic by topic ID (located at the bottom of a topic):
https://www.uptodate.com/login/customername.com?topicId=247

The **imageKey** parameter links to a particular image:
https://www.uptodate.com/login/customername.com?imageKey=LABI%2F115476

10.2 SSO Format Two – URL Parameter-based

Any URL can be SSO-enabled by simply adding the **domain_hint** URL parameter, for example, "domain_hint=wolterskluwer.com".

The following parameter-based URLs are completely equivalent to the 3 path-based URLs above (to link by search term, topic ID, and image).
https://www.uptodate.com/contents/search?search=elbow&domain_hint=customername.com

https://www.uptodate.com/contents/247?domain_hint=customername.com

https://www.uptodate.com/contents/image?imageKey=LABI%2F115476&domain_hint=customername.com

These are additional example of SSO-enabled URLs using the domain_hint path parameter:
To access the Table of Contents:
https://www.uptodate.com/contents/table-of-contents?domain_hint=customername.com

To access Calculators:
https://www.uptodate.com/contents/table-of-contents/calculators?domain_hint=customername.com

To access MyAccount (for users who have already registered):
https://www.uptodate.com/contents/search?myUpToDate=true&domain_hint=customername.com

10.3 Using the source URL Parameter

Some customer institutions provide their users with a variety of access points for UpToDate, from EHR systems to custom portals, intranet sites, and the like. We are often asked to help institutions better understand the different points of access their users are choosing when they consult UpToDate.

To that end, we've added an optional **source** identifier parameter that customers can put in their links to UpToDate. By doing so, usage report data created for the customer can be broken down by access point, if that's valuable to them.

For example, let's assume Customer A has an intranet portal page where they'd like to place a link to UpToDate, and they'd like to be able to tell whether their users are accessing UpToDate from there as opposed to navigating to the main UpToDate sign-in page directly from a browser.

In this case, the main URL that Customer A provides to its users would be:
https://www.uptodate.com/login/CustomerA

After requesting a source value from UpToDate, the link they publish on their portal would be:
https://www.uptodate.com/login/CustomerA?source=CustA-EMR123

Usage data could then be differentiated between sessions initiated from the main sign-in URL versus sessions initiated from their internal portal.

This attribute can be used in conjunction with the earlier example links (in both formats) as well. For example, if Customer A wants to put a link to the Table of Contents on their portal page, they could create the following link:
https://www.uptodate.com/contents/table-of-contents?domain_hint=customername.com&source=CustA-EMR123

10.4 SSO Integrations and iframes

When your institution initially integrated UpToDate into your EHR, portals, etc., the choice may have been made to embed UpToDate in an HTML iframe. This was permissible when using non-SSO access methods.

However, for security reasons, SSO authentication is not supported within iframes. This standard has been adopted by the industry and is not specific to UpToDate. Prior to converting existing URLs to their SSO versions as described above, the UpToDate integration must be implemented outside of an iframe.

11. Technical References

OpenID Connect
https://openid.net/connect/

SAML
https://wiki.oasis-open.org/security/FrontPage