DOTS
Technical Requirements

Davy Vande Cappelle
Last update: 2021-02-01

attentia

feeling good works great

Table of Contents

attentia

1. DOTS Essentials

DOTS Essentials is the universal access to the DOTS Platform. It provides access to the DOTS Solutions and allows you to manage users, security and privacy on your DOTS Platform.

We strive to make all web applications HTML5 compliant without the use of additional plug-ins. Some exceptions are described below.

1.1 DOTS on a desktop PC

1.1.1 Minimum client hardware requirements

Processor	Current dual-core processor
RAM	2 GB on top of the OS requirements
Hard drive	80 GB
Screen resolution	At least 1024x768; preferably higher
Network connection	At least 100 Mbps

1.1.2 Supported operating systems

Windows 32-bit	Windows 7 Windows 8 Windows 10
Windows 64-bit	Windows 7 64-bit Windows 8 64-bit Windows 10 64-bit
Apple OS X	Safari OS X

attentia

Browser support

Browsers	Support
IE11 Chrome	Full support, including testing of all features of the web platform during the product development phase
Firefox	Support including only happy flow testing of the web platform during product development
Edge	Happy flow testing in the UAT phase, during which we selectively solve issues (mainly blocking problems)
Safari OS X	Production issues solved reactively
IE10 or lower	No support

1.2 DOTS on a tablet

DOTS is only supported on tablets in landscape mode, and only if the landscape mode has a minimum resolution of 1000 pixels. At lower resolutions, or when using the tablet in portrait mode, DOTS will fall back to the DOTS Mobile version.

| Tablet browsers	Support
Safari iOS on iPad or iPad mini	Full support, including testing of all features of the web platform during the product development phase
Chrome on Android	Happy flow testing in the UAT phase, during which we selectively solve issues (mainly blocking problems)

1.3 DOTS Mobile

DOTS Mobile is a slimmed-down version of DOTS, only containing features that are relevant for smartphone use. DOTS will switch to DOTS Mobile whenever the screen resolution is lower than 1000 pixels.

Phone browsers	Support
Safari iOS on iPad / iPad mini	Full support, including testing of all features of the web platform during the product development phase
Chrome on Android 7 or higher	Happy flow testing in the UAT phase, during which we selectively solve issues (mainly blocking problems)

attentia

1.3.1 Known issues on Safari

A blank screen is shown after a successful login.

This is caused because Safari doesn't allow 3rd party cookies to be used inside a frame anymore. Unfortunately, the current ADAL library that is used to handle user authentication heavily relies on iFrames and cookies. The current workaround is to allow cookies by disabling the "Prevent Cross-Site Tracking" toggle as shown in the screenshot below.

attentia
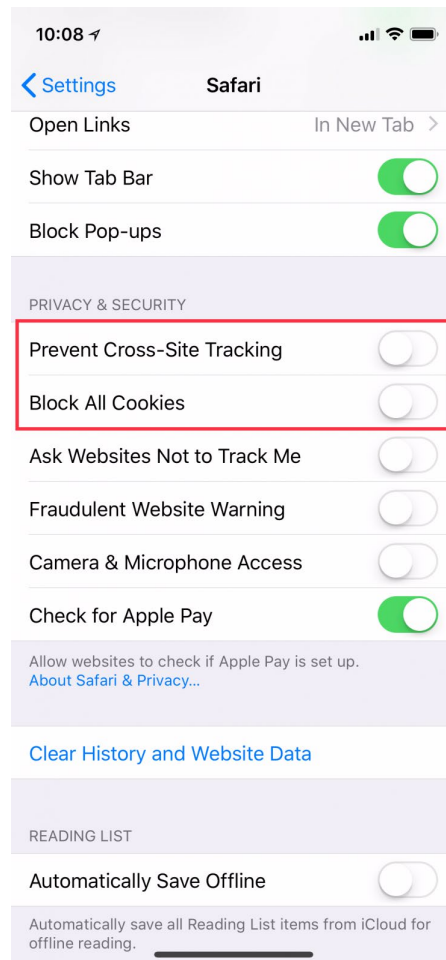
1.4 Security

1.4.1 What actions are needed to prevent DOTS e-mails from being regarded as spam?

Some customers' systems may consider large numbers of e-mails (e.g. activation e-mails) sent simultaneously to be spam. In such cases, it may be necessary to have the e-mail and IP addresses whitelisted. For DOTS, e-mails are sent from the following IP addresses:

- 85.118.209.75
- 85.118.209.76
- 85.118.209.77
- 85.118.209.81
- 85.118.211.49
- 85.118.211.50
- 85.118.211.51
- 85.118.211.52
- 167.89.54.158

The sender of these e-mails is always no_reply@attentia.be.

attentia

1.4.2 Is it possible to use a federation setup with an external identity provider?

Yes. DOTS uses Windows Server 2016 ADFS (Active Directory Federation Services) to authenticate users. ADFS can be set up in a federation with external identity providers (IdP) by means of WS-Federation or SAML2.

DOTS Federation metadata is exposed at https://auth.attentia.be/FederationMetadata/2007-06/FederationMetadata.xml

Prerequisites:
- The supported protocols are WS-Federation or SAML.
- All employees who need to be able to log in via SSO have an e-mail address with a suffix that is managed by the external Identity Provider (e.g. @attentia.be).
- The external Identity Provider can link this e-mail address back to us as a claim. This e-mail address must be the same as the username in DOTS.
- To enable the login_hint the e-mail address must be a valid upn.
- The external Identity Provider offers its metadata via URL to allow automatic refreshes of certificates.
- It is the responsibility of the external Identity Provider to check regularly whether there are any changes in the metadata of the DOTS Identity Provider. 20 days before the expiration of the DOTS Identity Provider certificates, new certificates will be made available in this metadata. 5 days later, the new certificates will be used.
- Due to technical limitations of our current setup the external IDP its non-interactive responses can't contain an x-frame-options header.

Note that for Internet Explorer, if the external identity provider is located in the "Local Intranet Zone" or "Trusted Sites" zone, the following DOTS URLs must also be added to the "Trusted Sites" URLs:

- https://dots.attentia.be
- https://api-dots.attentia.be
- https://auth.attentia.be
- https://services.e-contract.be
- https://idp.iamfas.belgium.be (Optionally for authentication through itsme or eID)
- https://merchant.itsme.be (Optionally for authentication through itsme)
- https://discovery-dots.attentia.be (Optionally for Discovery)
- https://api-discovery-dots.attentia.be (Optionally for Discovery)
- https://uat-dots.attentia.be (Optionally for UAT)
- https://api-uat-dots.attentia.be (Optionally for UAT)

attentia

Remark
When a non chromium version of Edge starting from v40 or higher is used in combination with federation, the IDP has to be in the trusted sites as well.
Eg https://login.microsoftonline.com for federations with Azure AD.

This is a setting that can be pushed to the employees' computers via group policies.

1.4.3 Does the solution support two- or multi-factor authentication?

For the moment, Attentia deliberately does not support two- or multi-factor authentication in its own identity provider solution (ADFS). Two- or multi-factor authentication is often specific to the business context in which logins occur, so it is usually more efficient to have these types of logins occur within the confines of the organisation. In this case, we link our own identity provider to that of the organisation, thereby making two- or multi-factor authentication possible. See *"Is it possible to use a federation setup with an external identity provider?"*.

2. DOTS Document Management

2.1 DOTS Essentials

DOTS Essentials is required in order to get started with DOTS Document Management.
See DOTS Essentials for the technical requirements.

2.2 Digital signatures with eID & Itsme

In order to digitally sign documents with eID (within the Document Management solution), the employees need an eID reader and the following software:

2.2.1 Digital signatures with E-contract

E-Contract only supports eID

Internet Explorer	eID Web Browser Middleware + eID IE Extension
Chrome	eID Web Browser Middleware + eID Chrome Extension
Firefox	eID Web Browser Middleware + eID Chrome Extension

The latest version of the software can be found under https://www.e-contract.be/eid-chrome/releases/. More information can be found at http://e-contract.be/support.

attentia

Middleware installation

The eID Web Browser Middleware can be installed from central management for all browsers.

Extension installation

For Internet Explorer, the eID IE Extension can also be installed from central management. Once the extension is installed, it still needs to be activated. This can also be done from central management.

For Chrome and Firefox, users must install the required extension themselves.

When a user tries to sign a document without the necessary middleware and/or extension having been installed, the following screen is shown with download links to the middleware and extension for the user's browser:

Digital Signature Service

Document tekenen   *attentia*

eID Installatie

Alvorens je de eID-kaart binnen de webbrowser kan gebruiken, dien je 2 componenten te installeren.

1. eID Web Browser Middleware (v1.1.9)

Eerst dien je de eID Web Browser Middleware te installeren.

| Installeer de eID Web Browser Middleware voor Windows |

2. eID Extension

Installeer vervolgens de eID Extension. Belangrijk is om eerst de eID Web Browser Middleware te installeren.

- Installeer de eID Extension

attentia

2.2.2 Digital Signatures with Connective

Connective supports both eID and Itsme.

The Connective plugin is required to be able to sign documents using connective. Depending on the browser, a specific signing extension might be required. The detailed installation steps for Windows, Mac and organization wide or local installation can be found in Section 6 of the connective native documentation.

Important note: digital signing is only supported in the desktop version of DOTS. The tablet and mobile versions of DOTS do not support this feature.

3. DOTS Flexible Reward

3.1 DOTS Essentials

DOTS Essentials is required in order to get started with DOTS Flexible Reward.
See DOTS Essentials for the technical requirements.

There are no further specific technical requirements for DOTS Flexible Reward.

However, digitally signing addendums is done through DOTS Document Management, which does have certain technical requirements. See DOTS Document Management.

4. DOTS Payroll Essentials

4.1 DOTS Essentials

DOTS Essentials is required in order to get started with DOTS Payroll Essentials.
See DOTS Essentials for the technical requirements.

attentia

4.2 Citrix Receiver

For Payroll Essentials customers, all desktop applications are streamed via Citrix to the end user's desktop PC. This requires the installation of Citrix Receiver version 4.5 or higher. Support and information regarding Citrix Receiver available at https://www.citrix.nl/go/receiver.html.

In order to allow initialisation of Citrix sessions from DOTS, the following range of IP-addresses needs to be whitelisted:
- Ip range: 85.118.208.0/21
- Port: 443 / 22
- Protocol: https / ICA over SSL / sftp

5. DOTS Collaborative HR

5.1 DOTS Essentials

DOTS Essentials is required in order to get started with DOTS Collaborative HR.
See DOTS Essentials for the technical requirements.

There are no further specific technical requirements for DOTS Collaborative HR.

6. DOTS Connected Time

6.1 DOTS Essentials

DOTS Essentials is required in order to get started with DOTS Connected Time.
See DOTS Essentials for the technical requirements.

There are no further specific technical requirements for DOTS Connected Time.

7. DOTS Health & Safety

7.1 DOTS Essentials

DOTS Essentials is required in order to get started with DOTS Health & Safety.
See DOTS Essentials for the technical requirements.

There are no further specific technical requirements for DOTS Health & Safety.

attentia

8. DOTS Self Assessment

You can get started with DOTS Self Assessment right away, without DOTS Essentials.

There are no specific technical requirements for DOTS Self Assessment.

attentia