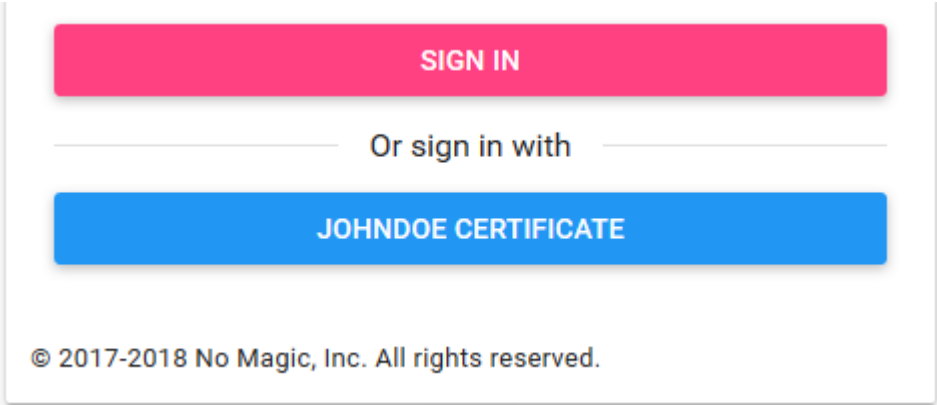


Authentication by certificate

The following parameters are utilized to authenticate the user by using certificates, e.g., certificates from CAC cards.

Parameter	Required	Description	Default value
server.ssl.client-auth	no	A flag indicating if a client certificate is needed or wanted. This flag is required if certificate authentication is enabled. The available value is want .	want
server.ssl.trust-store	no	The path to a truststore file in the file system. It can be relative to the Authentication Server directory or absolute. The path is required if certificate authentication is enabled. All certificates added into the <code>/config/truststore</code> directory will be imported into the truststore file.	config/truststore.jks
server.ssl.trust-store-type	no	A Truststore type, required if certificate authentication is enabled. The available type is JKS .	JKS
server.ssl.trust-store-password	no	A Truststore password, required if certificate authentication is enabled and the truststore is password-protected.	secret
authentication.certificate.enabled	no	An option that enables or disables certificate authentication. Available values are true and false .	false
authentication.certificate.headers.enabled	no	An option that enables or disables certificate authentication when authentication server is under proxy. Available values are true and false . This option by default is hidden and should be used only if authentication server is not accessible without a proxy.	false
authentication.certificate.username.source	no	Source of the username. Available values: dn (if username is constructed from the Subject Distinguished Name) or san (if username is constructed from the Subject Alternative Name).	dn
authentication.certificate.username.san.type	no	If <code>authentication.certificate.username.source</code> value is san , this parameter specifies the type of SAN to use. Available values: 0 - other name, 1 - RFC 822 name, 2 - DNS name, 4 - directory name (in case of this type parameter <code>authentication.certificate.username.template</code> is required).	4
authentication.certificate.username.template	no	Template that is used to create username from the subject DN (Distinguished Name) or SAN (Subject Alternative Name) of type 4 stored on the certificate. Required if certificate authentication is enabled. The template can contain ASCII characters as well as placeholders in round brackets that are replaced with relative distinguished name (RDN) values from the DN. For example, when subject DN or SAN of type 4 on the certificate is <code>CN=JohnDoe,O=MyCompany,C=GB</code> : • Template: <code>(CN)</code>, username: <code>JohnDoe</code> • Template: <code>(O)-(CN)</code>, username: <code>MyCompany-JohnDoe</code> • Template: <code>CERT_(CN)</code>, username: <code>CERT_JohnDoe</code>	(CN)
authentication.certificate.displayname.source	no	Source of the display name on login page. Available values: dn (if username is constructed from the Subject Distinguished Name) or san (if username is constructed from the Subject Alternative Name).	dn
authentication.certificate.displayname.san.type	no	If <code>authentication.certificate.displayname.source</code> value is san , this parameter specifies the type of SAN to use. Available values: 0 - other name, 1 - RFC 822 name, 2 - DNS name, 4 - directory name (in case of this type parameter <code>authentication.certificate.displayname.template</code> is required).	4

authentication.certificate.displayname.template	no	Template that is used to create a display of the subject DN (Distinguished Name) or SAN (Subject Alternative Name) of type 4 stored on the certificate. Required if certificate authentication is enabled. The template specified the same way as username template, except that display name is used for display purposes only. Display name is shown on authentication button that enables the user to authenticate with selected certificate. For example, when subject DN or SAN of type 4 on the certificate is <i>CN=JohnDoe,O=MyCompany,C=GB</i>, and the display template is <i>(CN) CERTIFICATE</i>, following authentication button will be displayed: 	(CN)
authentication.certificate.revocation.list.file	no	The absolute path to the certificate revocation list (CRL) file, if it is stored on the filesystem. Multiple files are available if there are several certificate revocation lists. If there are multiple files, separate each file by a comma (for example, <Path and file name 1>,<Path and file name 2>,<Path and file name 3>).	-
authentication.certificate.revocation.list.url	no	The URL of the certificate revocation list (CRL) file, if it is available on the web. Multiple URLs are available if there are several certificate revocation lists. If there are multiple URLs, separate each URL by a comma (for example, <URL1>,<URL2>,<URL3>).	-

A configuration example

```
server.ssl.trust-store=config/truststore.jks
server.ssl.trust-store-password=YOUR_TRUSTSTORE_PASSWORD
server.ssl.trust-store-type=JKS
server.ssl.client-auth=want
authentication.certificate.enabled=true
authentication.certificate.username.source=san
authentication.certificate.username.san.type=4
authentication.certificate.username.template=(0)-(CN)
authentication.certificate.displayname.source=dn
authentication.certificate.displayname.template=(CN)'s Smart Card
```