

Annotations Security within viewone & viewone pro

Security, confidentiality and compliance continue to be key areas for all our customers. Our extensive Annotations Security capabilities within the Annotations Module for ViewONE and ViewONE Pro offer highly configurable mark-up security.

There are four options for applying security to your annotations data. The Annotations Module for ViewONE and ViewONE Pro offers a parameter (annotationSecurityModel) providing two methods for administrators to easily apply security controls for viewing, editing, printing and hyperlinking of annotations at a user group, individual user, document and even individual annotation level. The flexibility and openness of the Annotations data file (the '.ant' file) offers two further methods of security control through deeper integration into your existing server-side security models.

USING THE 'ANNOTATIONSECURITYMODEL' PARAMETER

Using the existing parameter, there are two defined security methods - Simple Annotations Security and Extended Annotations Security. Administrators are free to choose whichever method is best suited to their security requirements. To apply the methods, simply insert the HTML parameter 'annotationSecurityModel' within your ViewONE or ViewONE Pro implementation code: *Sample HTML* - `<param name="annotationSecurityModel" value="*">` where '*' is replaced by '1' for Simple Annotations Security and '2' for Extended Annotations Security.

1. SIMPLE ANNOTATIONS SECURITY

Our first annotations security option allows administrators to determine whether or not users can edit, view or print an individual annotation.

Whenever a user applies an annotation onto a document and clicks the 'save' button on the annotation toolbar, an 'annotations definition file' is created which includes all information about the annotation. This definition file is saved to your specified location on your server. At this point, all users who subsequently retrieve the document are able to view and edit the annotation.

By programmatically inserting the 'Edit' annotation property into the definition file, it is possible to control whether or not users can edit the annotation contents. Likewise, inserting the 'View' annotation property into the definition file allows administrators to control whether users can view the annotation.

To programmatically apply the 'Edit' and 'View' annotations properties, a server object is required (exe, asp, jsp etc) to allow you to control the content of the annotation file, either when it is first saved or when it is served out to the users.

The 'Edit' property has two settings: allow edits ('1') and disallow edits ('0'). The default setting when the 'Edit' property is used is '1' or allow edits. The 'View' property has four options: allow viewing and printing ('3'), allow printing but not viewing ('2'), allow viewing but not printing ('1') and disallow viewing and printing ('0'). The default setting for the 'View' property is '3' or allow viewing and printing. In both the 'Edit' and 'View' properties, these settings can be programmatically applied selectively for each annotation.

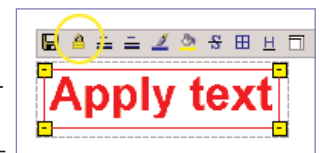
[There is also an HTML parameter 'annotateEdit', which can be used to disable the edit option for all annotations ('<param name="annotateEdit" value="false">') see the annotations manual, page 22 (visit <http://www.daeja.com/manuals/default.asp>) This is a global setting and will disable editing for all annotations.]

2. EXTENDED ANNOTATIONS SECURITY

To allow users to have control over the privileges that are assigned to the annotations they create, and to allow individual controls for modification, deletion and reading privileges, the extended Annotation Security system needs to be implemented.

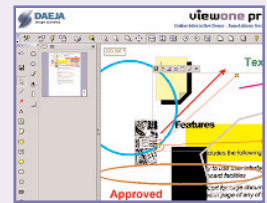
The extended Annotations Security system requires the use of the 'userId' HTML parameter see annotations manual, page 33 (visit <http://www.daeja.com/manuals/default.asp>) alongside the 'annotationSecurityModel' parameter (see overleaf). The 'userId' parameter identifies the user to the system and allows security settings to be applied for each new annotation created by that user.

Selecting option 2 within the 'annotationSecurityModel' parameter (and thereby choosing to use the extended Annotations Security system), adds the following additional properties into the annotations definition file: SECURITYMODEL; READ; MODIFY; EXECUTE; PRINT; DELETE; PASSWORDMODIFY; PASSWORDSECURITY; OWNER and MODIFYSECURITY.



Annotations context toolbar padlock

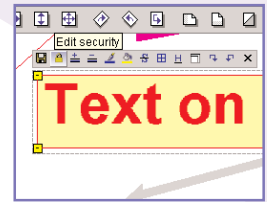
Within the new definitions properties are individual entries for read, modify, execute, print, delete and modify security, which allows each to be controlled independently by the user or server object (when the file is served back to the user). By default each property is set to a value of '1', or enabled. The 'MODIFYSECURITY' property indicates whether the user has the ability to edit all these properties within ViewONE or ViewONE Pro. When this property is enabled, an additional 'padlock' icon appears on the context toolbar for each annotation. If the user clicks this button they will see a dialog allowing them to change the other properties listed above.



Amending Definition Object Privileges

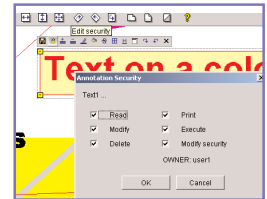
The 'owner' of the annotation is the user who created the annotation. If the owner matches the 'userId' parameter, then that user always has access to the security dialog.

If a user creates an annotation, then opens the security dialog and unticks the 'modify' option for that annotation, no other user (except system registered administrators) will be able to select, move or modify that annotation in any way. If the 'delete' option was unticked this would allow other users to modify the annotation but not delete it. If the 'read' option was unticked the annotation would not appear to other users, while unticking the 'print' option means that the annotation will not appear when the document is printed.



The 'execute' annotation option is for the hyperlink capability while unticking the option prevents the linking or launching of a hyperlinked object.

If the document already has annotations applied under the 'Simple Security' method, the extended options can be enabled for them by programmatically adding the 'SECURITYMODEL = 2' line to each annotation definition at retrieval time, using the server object.



Extended Annotations Security Screenshots

Annotation Passwords

Another pair of parameters that can be used to control annotations editing or removal are 'annotationEditPasswordModify' and 'annotationEditPasswordSecurity': <param name="annotationEditPasswordModify" value="true"><param name="annotationEditPasswordSecurity" value="true">. When set to 'true' as in the example above, then it is possible to set a password that must be entered before users are allowed to modify an annotation or its security settings. The passwords themselves are encrypted using private-key 32-bit encryption, so that they are not viewable or editable outside of ViewONE. The properties they are saved under in the annotations file are PASSWORDMODIFY and PASSWORDSECURITY. If a user wishes to amend an annotation, but doesn't know or forgets a password assigned to a particular annotation, they must either be the annotation 'owner' or an 'admin' user in order to clear and re-enter a new password. Otherwise, they are prevented from editing the annotation. Passwords themselves are never displayed, always being replaced during entry or in dialog boxes by the "*" character.

3. INTEGRATION INTO BACK-END SECURITY

To achieve a much greater level of annotation security control, it is recommended to extract the individual annotation field data to XML through an XSLT parser on the web server, (you will need to create your own schema) and feed it into a database. In addition to the fact that annotations can then be searchable within your ECM system, when the annotations data is recompiled for document serving to the client, whatever security information you select can be applied to the annotations data before the XML is parsed back into its '.ini' format (the format of '.ant' annotations files).

The annotations file format was specifically developed to be open and flexible to allow just this sort of tailoring to your individual needs. Instead of forcing administrators to abide by a restrictive format, we have utilized an open format which offers complete configurability. Security can consequently be applied at serving time at a group, user, document, annotation set or individual annotation level.

4. CUSTOM DIALOG INTEGRATION

For deeper integration into your existing security structure, to incorporate greater definition of your user and group privileges, it is possible for Daeja to implement your own custom security dialogs within ViewONE and ViewONE Pro. This option requires specific development effort by Daeja to tailor the viewer, which is chargeable, but offers the greatest level of annotation security integrated within existing security structure.

For more information about ViewONE and ViewONE Pro, please contact sales@daeja.com

For full pricing information on our all products please visit www.daeja.com

Daeja Image Systems - UK
18 London House
Swinfens Yard
Stony Stratford
Milton Keynes,
MK11 1SY
Tel: +44 1908 563007
Fax: +44 1908 567833

Daeja Image Systems – New York
48 Bi-State Plaza
#125
Old Tappan, NJ 07675-7079
USA
Tel: 201-822-4343
Fax: 617-249-1888

