



Security Level in Documents

Overview

It is possible to further restrict access to a certain document or folder based on the IP range of the users. For instance, you may want to allow unrestricted access when the user is accessing a document from the office building and known IP address but block access when the user is accessing the same document from outside the office or known IPs.

How to enable:

Firstly security level must be enabled in the configuration, so if it is not on your site [please submit a support ticket](#) so we can enable this for you.

Once it is enabled you can check under [Admin/Documents](#) under Security Level with status ON.

The screenshot shows the 'Admin / Documents' configuration page. Under 'ERMS features', the option 'Use security levels in permission system (ERMS_CONFIG_SECURITY_LEVEL)' is highlighted with a red box and is currently set to 'Off'. Other features include ERMS records, markers, record types, multi-component documents, MD5 signatures, export/import, schedules, Google Drive links, and Microsoft OneDrive links. A 'Statistics' table is also visible, showing document counts and sizes.

Feature	Status
Use ERMS records (ERMS_CONFIG_RECORD)	Off
Use ERMS markers (ERMS_CONFIG_MARKERS)	On
Use record types (ERMS_CONFIG_RECORD_TYPES)	On
Use multi-component documents (ERMS_CONFIG_MULTICOMPONENT_DOCUMENT)	Off
Use security levels in permission system (ERMS_CONFIG_SECURITY_LEVEL)	Off
Use MD5 signature for documents (ERMS_CONFIG_MD5_SIGNATURE)	Off
Use export/import for ERMS objects (ERMS_CONFIG_EXPORT_IMPORT)	Off
Use ERMS schedules (ERMS_CONFIG_SCHEDULE)	Off
Use Google drive links (ERMS_CONFIG_GDOC_LINKS)	On
Use Microsoft OneDrive links (ERMS_CONFIG_ONEDRIVE_LINKS)	On

Statistics	Value
Number of Documents	89
Number of all versions of documents	94
Number of checked out documents	0
Total space occupied by documents	401.99 Mb
Number of deleted documents and folders	0
Size of deleted documents	0 Bytes

Navigate to [Admin/People/Configure IP Ranges](#) (Under Configuration) to configure the IP range:



Each ip range (intranet, office, employee's home, campus, etc) can be restricted to certain security level.

For example, company intranet has "Top secret" level, some department restricted to "Confidential" level, entire world has "Restricted" level.

When user logs in from some computer, their security level will be calculated as lower of their own security level and security level of computer's ip.

NB: if there are firewall or proxy between intranet webserver and user's computer, firewall ip will be taken.

	Description	Security level limit	IP range
<input type="checkbox"/>	<input type="text" value="Claromentis Office"/>	Top Secret	<input type="text"/>
<input type="checkbox"/>	<input type="text" value="Entire world"/>	Unclassified	0.0.0.0 - 255.255.255.255

Add

IP range can be specified as range (10.2.0.0-10.2.255.255), single IP (10.1.0.1) or network with mask (10.3.0.0/255.255.0.0 or 10.3.0.0/16).

Each IP range (intranet, office, employee's home, campus, etc) can be restricted to a certain security level.

For example, the company intranet has a "Top secret" level, some departments may be restricted to a "Confidential" level, and all others outside this "Restricted".

When a user logs in from some computer, their security level will be calculated as lower than their own security level and the security level of the computer's IP.

NB: if there are firewalls or proxies between the intranet web server and the user's computer, the firewall IP will be used.

Last modified on 30 November 2023 by [Hannah Door](#)

Created on 16 December 2019 by [Michael Christian](#)

Tags: [user guide](#), [security](#), [level](#)