Link to article: https://discover.claromentis.com/knowledgebase/articles/675/security-level-in-documents

Security Level in Documents

Overview

It is possible to add an extra layer of security to files and folders in the Documents application that goes beyond the standard permissions that are already set, and gives or restricts access to users/roles/groups.

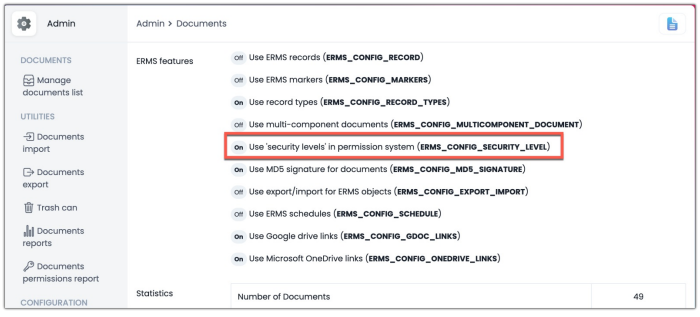
This is achieved by applying classification levels to files, folders and users, then restricting certain levels to only be accessible from specific IP addresses/ranges. e.g. documents classified as 'Top Secret' can only be accessed when users (with standard permissions already to view these items) are an the office IP.

Please note: Application administrators of the Documents application will always be able to see all files and folders from the admin side, regardless of their classification level on the front end or the IP they are accessing from.

Request security level is enabled

The Document security level feature is disabled by default (as it is optional), so if you want to try this out, please raise a support ticket requesting this, and we will enable it for your site.

Once this is enabled, it will display as 'ON' in Admin > Documents:



Considerations before set-up

There are several elements involved in setting up the security levels.

To ensure this achieves your goal, your team will need to confirm what you are trying to achieve by applying the levels to your documents and consider on what scale this is necessary for your directory.

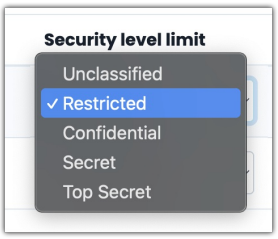
Your team will also need to decide how they wish to restrict access (e.g. which IPs) and to which levels.

This will require collaboration between your site's application administrators of both Documents and People to ensure the changes you want to make can be applied (as these users have the right access to do so)

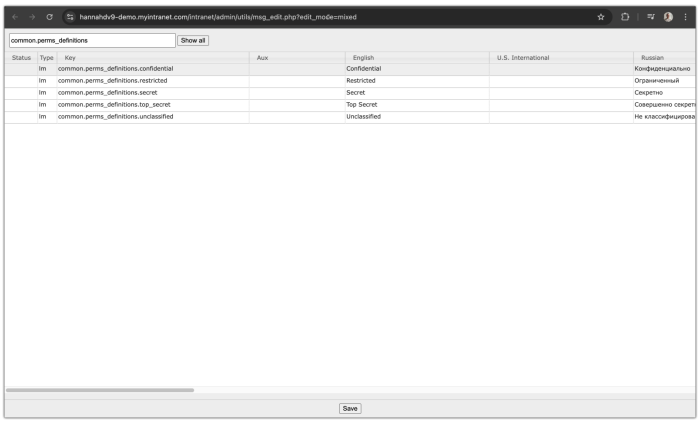
Set up

Classification labels

There are 5 labels, from low to high 'security', they are:



Your team can change the phrasing of each level in the localisation if you so wish in Admin > System > Localisation > Core apps and update each:

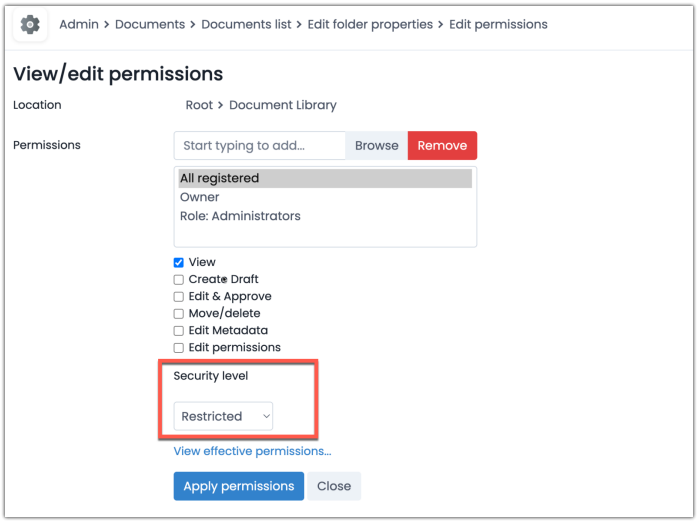


Clear the site cache from Admin > System > Labs to ensure your changes apply.

Regardless, the default label titles selections cover the security levels that could be needed to complete the set up your company wants to implement.

- Applying classification labels to documents

An application administrator of Documents can set the security level for a folder or file by editing its permissions on the admin side, changing the field for this and saving:



If permissions are set to inherit, the security level will be inherited.

The security level can only be changed at sub-levels if permissions are not set to inherit.

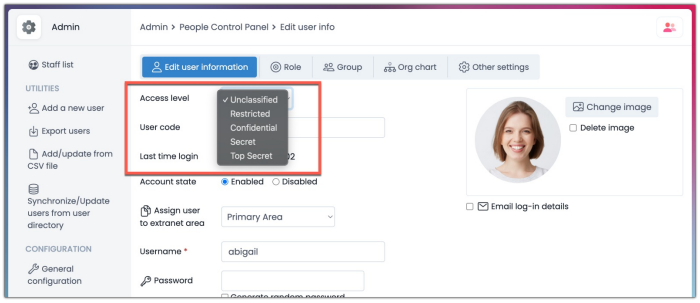
To make the implementation efficient, start with the folder and file classification levels that will be restricted to IPs.

Once the security level feature is enabled, all folders and files are given the 'unclassified' label by default.

So, start updating the folders and files that will be the highest level restriction to this first and update the rest over time.

- Applying classification labels to users

An application administrator of People can access individual profiles from Admin > People, update their classification level in the field for this, and save.



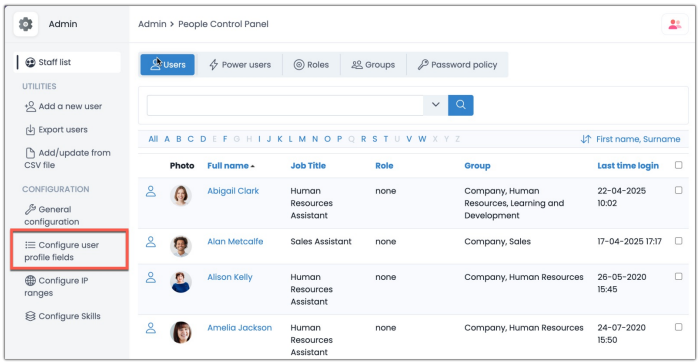
To make the implementation efficient, start with the user classification levels that will be restricted to IPs.

Once the security level feature is enabled, all users are given the 'unclassified' label by default.

So, start updating the users who will be the highest level restriction to this first and update the others over time.

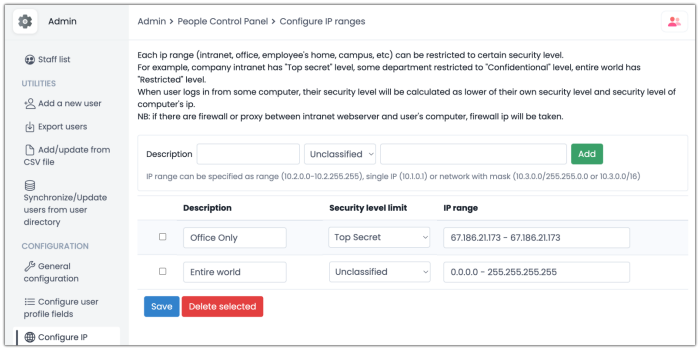
- Applying classification labels to IP addresses

An application administrator of People can navigate to Admin > People > Configure IP ranges:



Here, they can enter the desired IP ranges and choose the security level of documents that will be accessible when on that IP.

e.g. in the below example, users that have 'Top Secret' classification (the highest level) set on their profile will only be able to open files/folders with that classification when on the Office IP. Whereas all documents that are 'unclassified' (the lowest level, which is applied by default after the feature has been enabled) are accessible on any IP.



Standard permissions applied to folders and files still apply; a user will only be able to see documents they have permissions for.

The document security level is simply another layer on top that can prevent access to the content from IPs outside those configured.

Test

Once the security levels have been set across your folders and files, and the IP configuration area has the desired ranges entered against each level, you are ready to test.

Have a user access your Intranet from certain IPs to check what they can/can't access in Documents is in line with the configuration you have created.

Tweak the IP configuration area based on this.

Edit or remove the configuration

An application administrator of People can edit the configuration at any time from Admin > People > Configure IP ranges.

The levels and IP ranges they are restricted to can be changed freely or deleted.

They can also update the user classification level on their profiles.

An application administrator of Documents can update and manage the classification level of files and folders over time.

If you wish to turn the security level feature off entirely (rather than just removing all the configuration in the IP area) please raise asupport ticket for us to assist with this.

Created on 16 May 2025 by Hannah Door. Last modified on 23 May 2025
Tags: user guide, security, level