



## 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 on 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:

A screenshot of the 'Admin &gt; Documents' configuration page. The left sidebar shows a navigation menu with 'DOCUMENTS' (Manage documents list), 'UTILITIES' (Documents import, Documents export, Trash can, Documents reports, Documents permissions report), and 'CONFIGURATION'. The main content area is titled 'ERMS features' and lists several options with toggle switches. The option 'Use security levels in permission system (ERMS\_CONFIG\_SECURITY\_LEVEL)' is highlighted with a red box and has its toggle switch turned 'On'. Other options include 'Use ERMS records', 'Use ERMS markers', 'Use record types', 'Use multi-component documents', 'Use MD5 signature for documents', 'Use export/import for ERMS objects', 'Use ERMS schedules', 'Use Google drive links', and 'Use Microsoft OneDrive links'. At the bottom, there is a 'Statistics' section showing 'Number of Documents' as 49.

### 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.

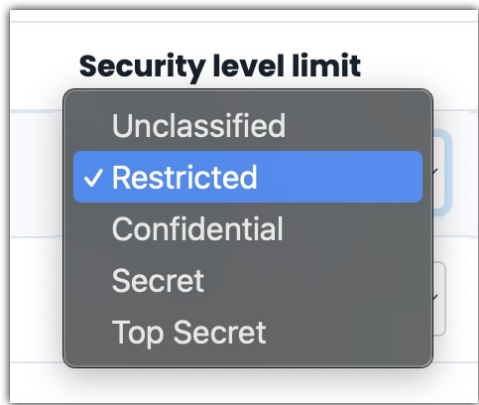
Your team will also need to decide how they wish to restrict access (e.g. which IPs) and to which levels.

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)

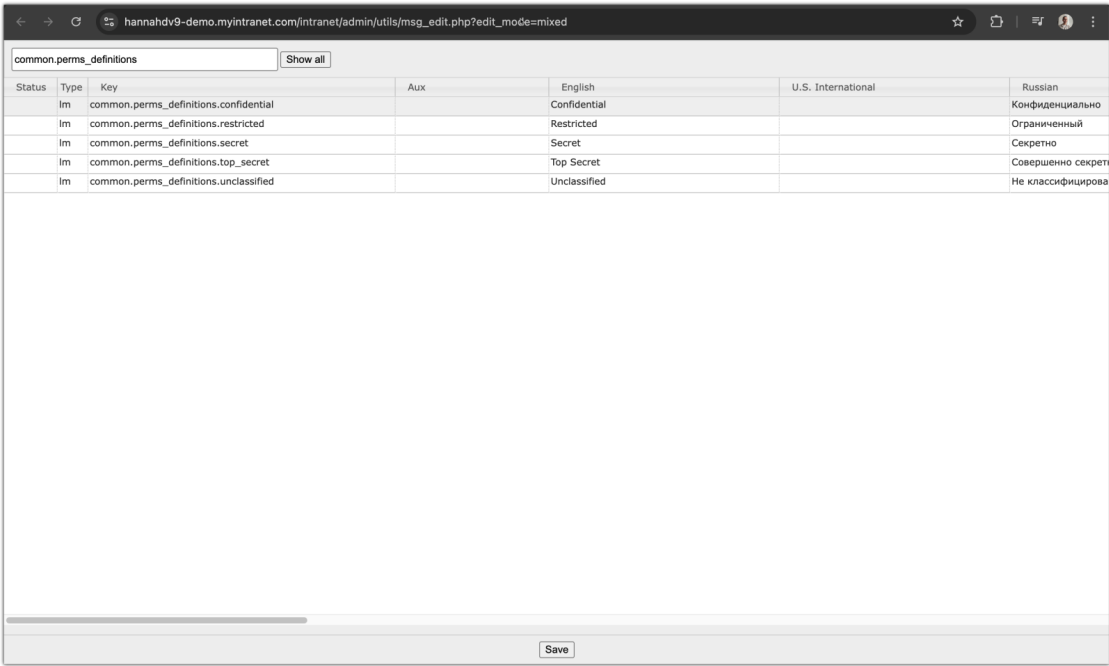
## Set up

### 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:



common.perms_definitions						
Show all						
Status	Type	Key	Aux	English	U.S. International	Russian
Im		common.perms_definitions.confidential		Confidential		Конфиденциально
Im		common.perms_definitions.restricted		Restricted		Ограниченный
Im		common.perms_definitions.secret		Secret		Секретно
Im		common.perms_definitions.top_secret		Top Secret		Совершенно секретно
Im		common.perms_definitions.unclassified		Unclassified		Не классифицировано
Save						

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:

Admin > Documents > Documents list > Edit folder properties > Edit permissions

## View/edit permissions

Location: Root > Document Library

Permissions:  [Browse](#) [Remove](#)

All registered

Owner

Role: Administrators

☒ View  
☐ Create Draft  
☐ Edit & Approve  
☐ Move/delete  
☐ Edit Metadata  
☐ Edit permissions

Security level

Restricted

[View effective permissions...](#)

[Apply permissions](#) [Close](#)

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.

Admin > People Control Panel > Edit user info

[Edit user information](#) [Role](#) [Group](#) [Org chart](#) [Other settings](#)

Access level

Unclassified

Restricted

Confidential

Secret

Top Secret

User code

Last time login

Account state: ☒ Enabled ☐ Disabled

Assign user to extranet area: Primary Area

Username: abigail

Password

☐ Generate random password

Change image

Delete image

☐ Email log-in details

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:

The screenshot shows the 'Admin > People Control Panel' interface. The left sidebar contains a 'CONFIGURATION' section with 'Configure user profile fields' highlighted. The main area displays a table of users with columns: Photo, Full name, Job Title, Role, Group, and Last time login. The table lists four users: Abigail Clark, Alan Metcalfe, Alison Kelly, and Amelia Jackson.

Photo	Full name	Job Title	Role	Group	Last time login
	Abigail Clark	Human Resources Assistant	none	Company, Human Resources, Learning and Development	22-04-2025 10:02
	Alan Metcalfe	Sales Assistant	none	Company, Sales	17-04-2025 17:17
	Alison Kelly	Human Resources Assistant	none	Company, Human Resources	26-05-2020 15:45
	Amelia Jackson	Human Resources Assistant	none	Company, Human Resources	24-07-2020 15:50

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.

The screenshot shows the 'Admin > People Control Panel > Configure IP ranges' page. It includes instructions on how to restrict IP ranges to certain security levels. Below the instructions is a table with two entries:

Description	Security level limit	IP range
<input type="checkbox"/> Office Only	Top Secret	67.186.21.173 - 67.186.21.173
<input type="checkbox"/> Entire world	Unclassified	0.0.0.0 - 255.255.255.255

Buttons for 'Save' and 'Delete selected' are at the bottom.

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 [a support ticket](#) for us to assist with this.

---

---

Created on 16 May 2025 by [Hannah Door](#). Last modified on 6 November 2025

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