



## **Central Desktop Enterprise Edition (Security Pack)**

The Central Desktop Security Pack is included in the Enterprise Edition of Central Desktop. The Enterprise Edition is for companies and organizations that require deeper and more granular security features to comply to internal, corporate or 3<sup>rd</sup> party compliance codes (Corporate Governance, HIPAA, etc).

The Enterprise Edition is a pre-requisite for companies and organizations that wish to integrate a Single Sign-On experience between Central Desktop and a third party application (additional configuration may be required).

To learn more about Central Desktop's security and infrastructure please download the [Security Document here](#). More information about Central Desktop security can be accessed at:

<http://www.centraldesktop.com/security>

The key security features and functions available with the Enterprise Edition include the following:



## Advanced Password Security Settings

Central Desktop already provides customizable permissions and rights management to accommodate a variety of customer needs. User Permissions are managed at both the Company Level and at the Workspace Level – allowing access to specified Workspaces only and allowing the Administrator to further restrict user permissions at the Workspace Level.

Additionally, user authentication is controlled via unique and valid username and password combination that is encrypted using a one way hash. (When users submit their username and password via this one-way hash to Central Desktop, a unique digital signature (or fingerprint) is created, which in turn identifies and authenticates the sender and the contents of the message.)

## Enhanced Password Complexity

The Security Pack adds an additional layer of Password Security by allowing the Administrator to adjust a range of password options such as:

### ➤ **Minimum Password Length**

The Administrator can determine what the minimum password length must be for all users within the Company. To ensure a minimum level of password security, Central Desktop natively requires a minimum of 6 characters but can support up to a 50 character minimum password length.

### ➤ **Password Save Option**

The Administrator can determine whether or not to enable the “Remember Me” function at the point of login for all users within the Company. This option should be disabled if Administrators are concerned about users accessing Central Desktop from public terminals and locations and want to ensure that login credentials are not saved. (Note: Whether or not this feature is enabled, users can still save their username and password locally via their web browser.)

### ➤ **Password Complexity**

Administrators can require users to use ‘complex’ password credentials. Enabling this feature will require all users to include the following details in their passwords:

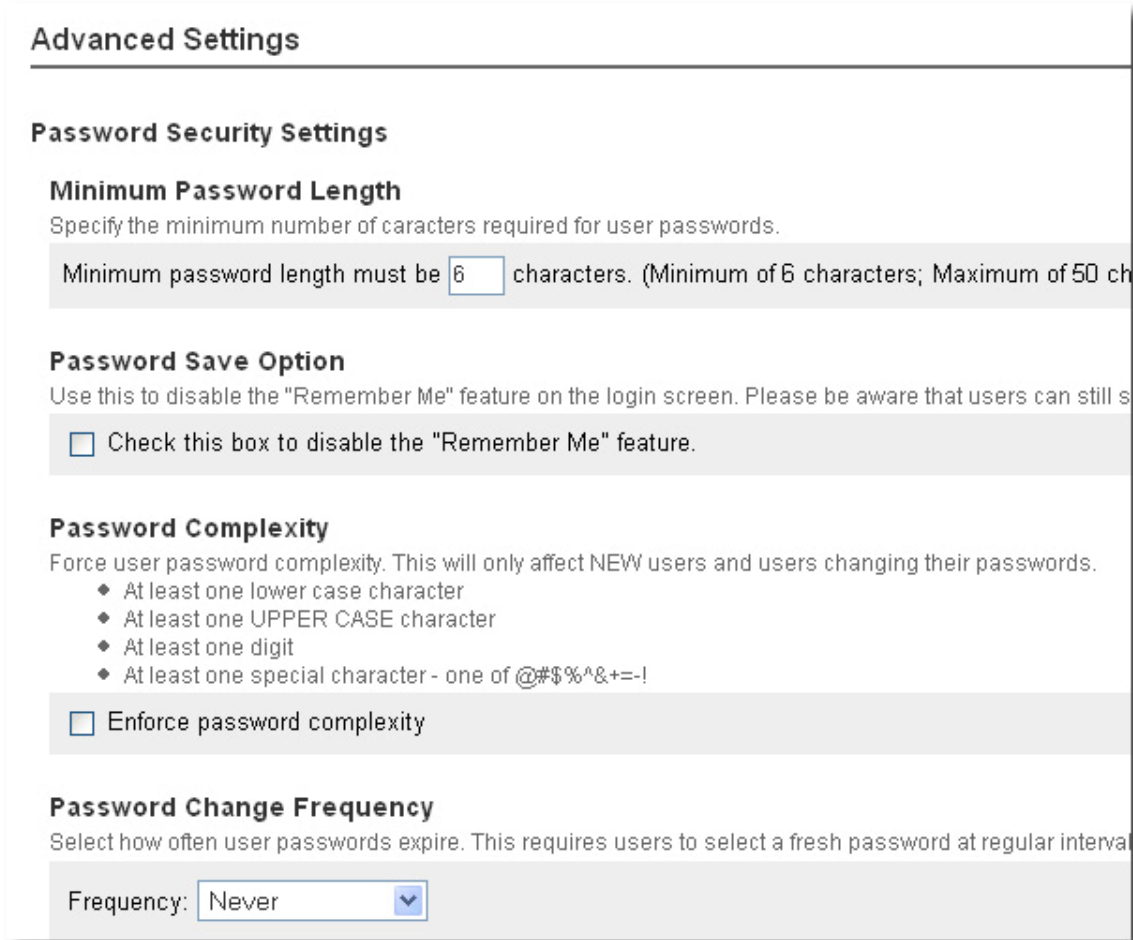
- At least one lower case character
- At least one UPPER CASE character
- At least one digit (numeral)
- At least one special character – one of the following characters: @#\$%^&+==!



➤ **Password Change Frequency**

Administrators can determine how often user passwords expire; forcing users to create a new password every 30, 60, 90, 180 or 365 days.

Below is a screenshot of the Advanced Password Security Settings:



The screenshot shows a web interface for 'Advanced Settings' with a sub-section for 'Password Security Settings'. It includes three main sections: 'Minimum Password Length' with a text input set to '6', 'Password Save Option' with an unchecked checkbox, and 'Password Complexity' with a list of requirements and an unchecked checkbox. The 'Password Change Frequency' section at the bottom has a dropdown menu set to 'Never'.

**Advanced Settings**

---

**Password Security Settings**

**Minimum Password Length**  
Specify the minimum number of characters required for user passwords.

Minimum password length must be  characters. (Minimum of 6 characters; Maximum of 50 characters)

**Password Save Option**  
Use this to disable the "Remember Me" feature on the login screen. Please be aware that users can still save their passwords manually.

Check this box to disable the "Remember Me" feature.

**Password Complexity**  
Force user password complexity. This will only affect NEW users and users changing their passwords.

- ◆ At least one lower case character
- ◆ At least one UPPER CASE character
- ◆ At least one digit
- ◆ At least one special character - one of @#\$%^&+=-!

Enforce password complexity

**Password Change Frequency**  
Select how often user passwords expire. This requires users to select a fresh password at regular intervals.

Frequency:  ▼



## TLS Encryption and Trusted Email Domain Support

The TLS (Transport Layer Security) Encryption and Trusted Email Domain feature allows you to control access and send encrypted emails to trusted users.

Email domains that are listed as Trusted Domains will receive a TLS encrypted email with all of the contents of the discussion, comment or documents available for the user to read.

Email domains that are NOT listed as a Trusted Email Domain will only receive a generic email notification with a direct link to login to Central Desktop.

NOTE: Additional TLS software configuration and setup is required by the company to support TLS Encryption.

Below is a screenshot of a Trust Email Domain feature.

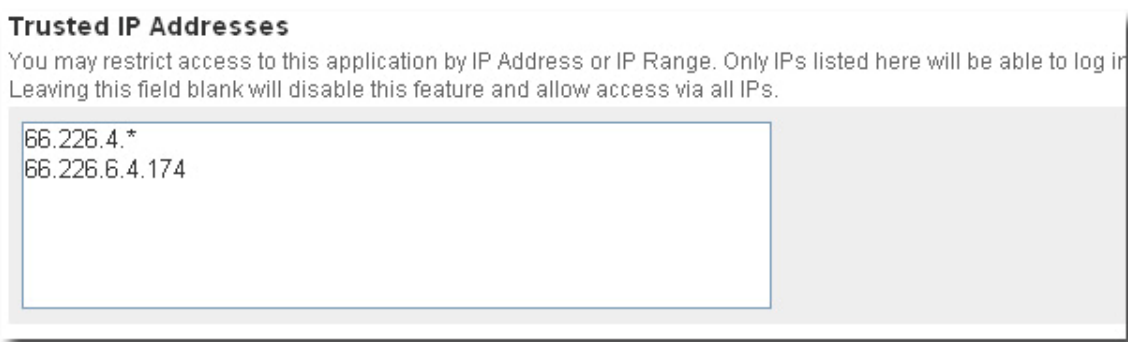


## Trusted IP Addresses

The Trusted IP Address feature allows Administrators to restrict access to Central Desktop by IP Address or IP Range. Only listed IP addresses will be allowed access to Central Desktop.

This is ideal for companies and organizations that need to restrict access to Central Desktop via a VPN or office location IP address. This feature can be configured at the Company level and at the individual User level.

Below is a screenshot of the Trusted IP Address feature:



## Custom Terms of Service & Privacy Policy

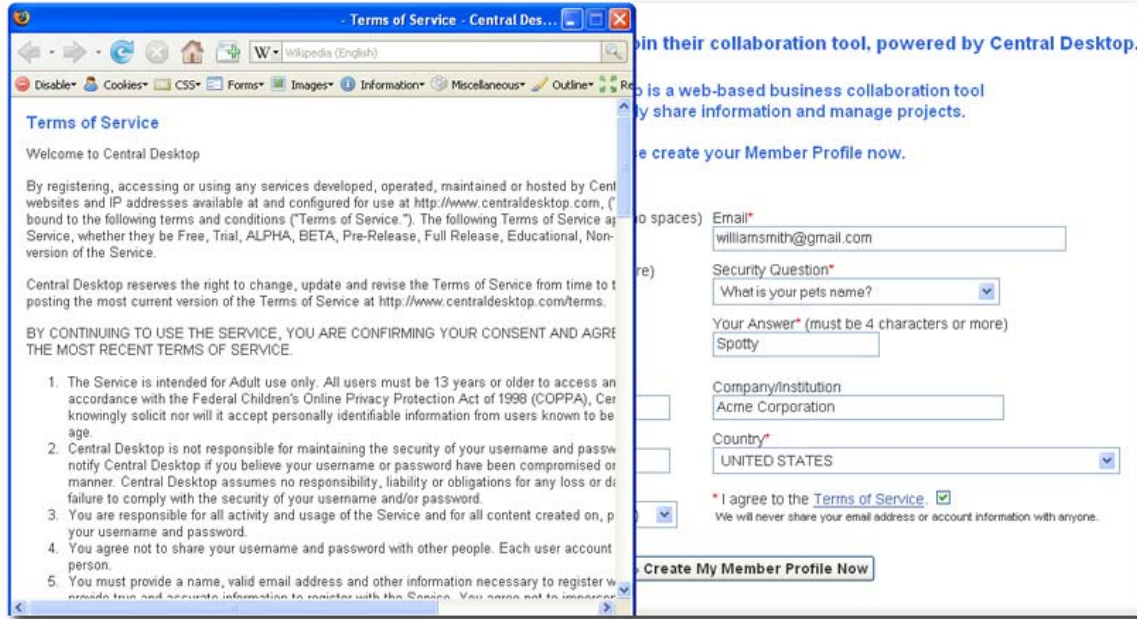
The Custom Terms of Service & Privacy Policy feature allows Administrators to force Internal Members and External Members to agree to custom Terms of Service and Privacy Policy when they register with Central Desktop.

This feature enables companies to comply with certain confidentiality or terms of use required under certain corporate policies or statutory requirements.

Below are screenshots of the Custom Terms of Service & Privacy Policy features:

The screenshot shows a web interface for configuring custom terms of service and privacy policies. The page title is "Custom Terms of Service & Privacy Policy". Below the title, there is a brief description: "Central Desktop allows you to modify the Terms of Service and Privacy Policy for your users. These policies are notified and your request to change your policies will go into a queue. Typical turn around time for policy notification is 24 hours." The "Current Status" section shows two items: "Terms of Service: Using Central Desktop [Terms of Service](#)" and "Privacy Policy: Using Central Desktop [Privacy Policy](#)". The "Custom Terms of Service" section has a text area with a rich text editor toolbar. The text in the area reads: "Welcome to Central Desktop  
By registering, accessing or using any services developed, operated, maintained or hosted by Central Desktop ("Service"), you agree to be bound to the following terms and conditions ("Terms of Service."). The Service is provided on an Educational, Non-Profit, Complete or any Paying version of the Service.  
Central Desktop reserves the right to change, update and revise the Terms of Service from time to time. BY CONTINUING TO USE THE SERVICE, YOU ARE CONFIRMING YOUR CONSENT AND AGREEMENT TO THESE TERMS.  
1. The Service is intended for Adult use only. All users must be 13 years or older to access any part of the Service. Central Desktop never knowingly solicit nor will it accept personally identifiable information from users known to be under the age of 13."





## Single Sign-On Redirect

The Single Sign-On (SSO) Redirect feature allows companies and organizations a secure way to create a Single Sign-On experience from Central Desktop to 3<sup>rd</sup> applications, so that users don't have to login twice when clicking from Central Desktop to another application.

The Single Sign-On Redirect will require additional configuration and support to fully integrate into another application.

Please visit this link for more technical information on how to utilize this feature:  
<http://cd.centraldesktop.com/adn/SingleSignInFromCentralDesktopToAnother3rdPartyApplication>

