

# How to manage virtual desktop in the Endpoint Manager

## Introduction

- The 'Virtual Desktop' is a sandbox environment in which you can run programs and browse the internet without fear those activities will damage the host computer.
- Applications in the virtual desktop are isolated from other processes on the host computer, write to a virtual file system, and cannot access personal user data. Changes made to files and settings in the virtual desktop do not affect the originals on the host system.
- Similarly, any attacks by internet based malware cannot reach or compromise the host system. This makes the Virtual Desktop a highly secure environment for general workflows, and specifically for surfing the internet.
- Because the desktop can run any Windows program, admins could use the virtual desktop the default login environment for their users. You can also password-protect the virtual desktop. Users and guests will need to enter the password before they can exit the desktop.

This wiki explains how to configure virtual desktop from endpoint manager:

**Step [1]:** Go to Endpoint Manager > CONFIGURATION TEMPLATES > Profiles

Select the profile which needs virtual desktop configuration.

For example: Here we are selecting profile "security profile"

**Endpoint Manager** ☰ Profiles

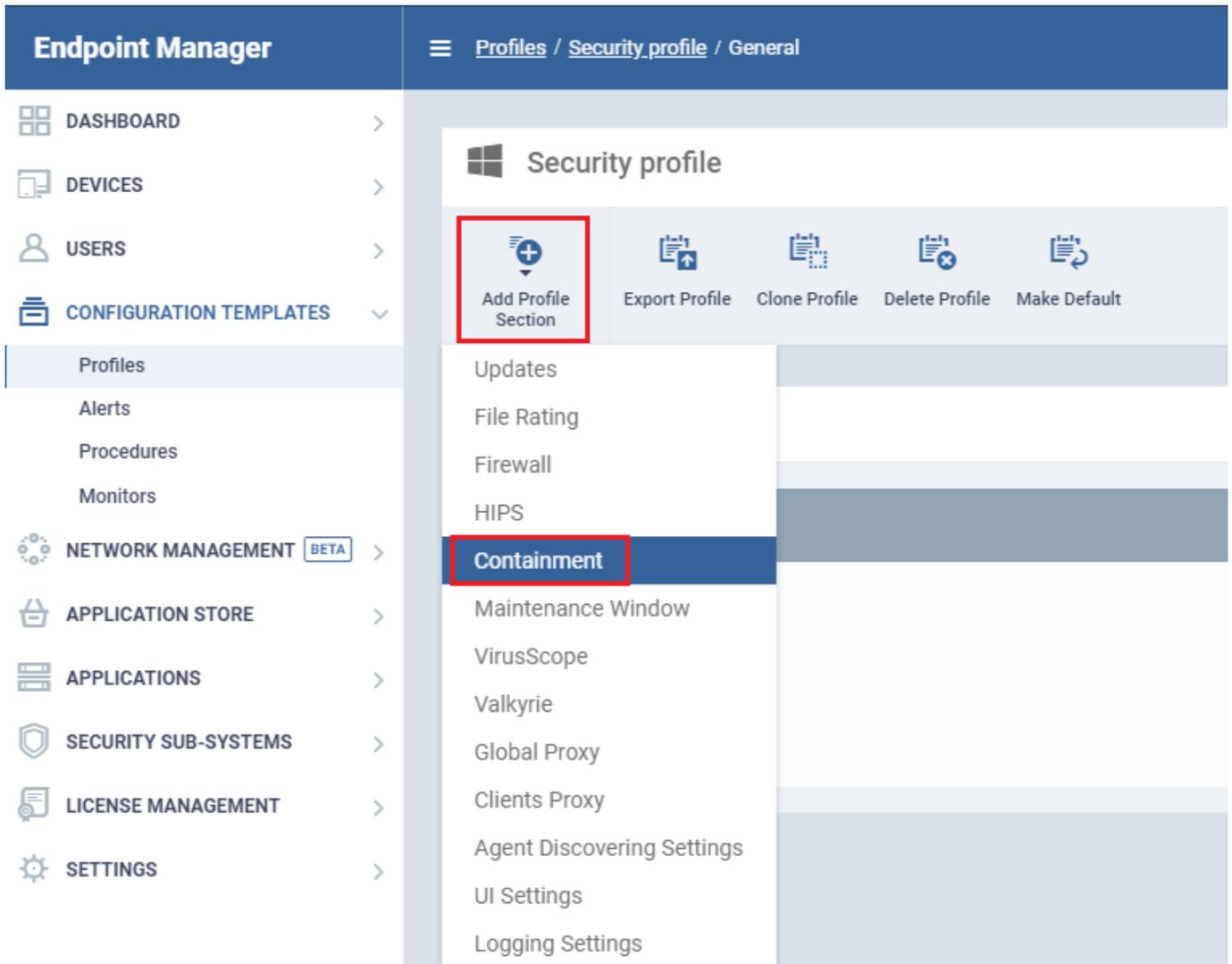
- DASHBOARD >
- DEVICES >
- USERS >
- CONFIGURATION TEMPLATES ▾
- Profiles**
- Alerts
- Procedures
- Monitors
- NETWORK MANAGEMENT BETA >
- APPLICATION STORE >
- APPLICATIONS >
- SECURITY SUB-SYSTEMS >
- LICENSE MANAGEMENT >
- SETTINGS >

**Profiles** Default Profiles

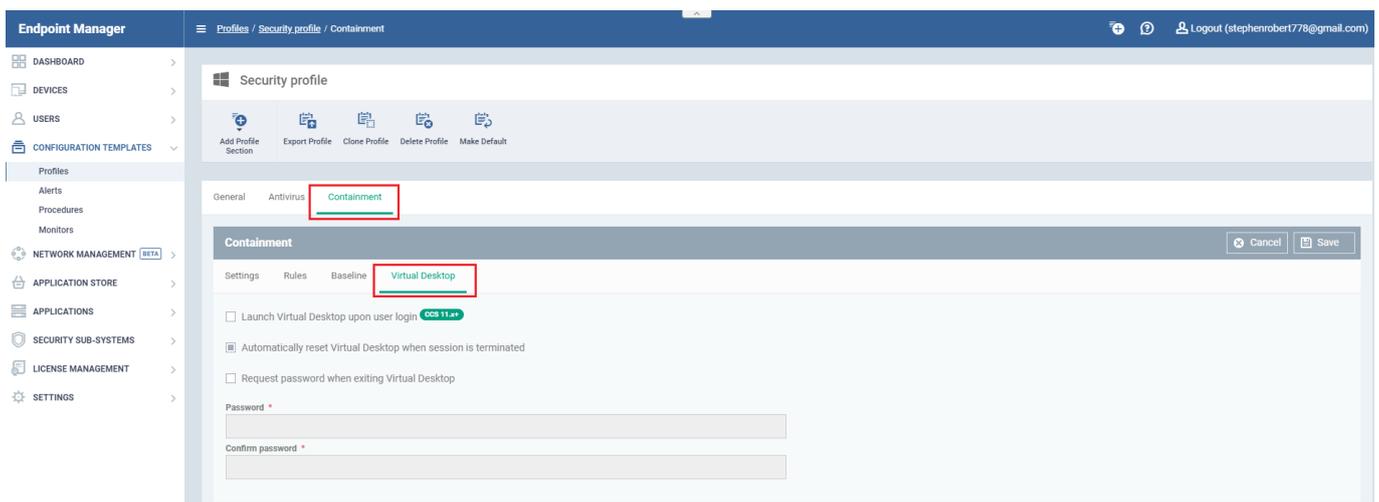
Create Import Export Profile Clone Profile Delete Profile Export

| <input type="checkbox"/> | OS      | NAME   |
|--------------------------|---------|--|
| <input type="checkbox"/> | Windows | Security profile   |
| <input type="checkbox"/> | Windows | Profiles for UI settings                                 |
| <input type="checkbox"/> | Windows | [cloned] Windows - Security Level 1 Profile v.6.23 vicky |
| <input type="checkbox"/> | Windows | [cloned] Windows - Security Level 1 Profile v.6.23       |
| <input type="checkbox"/> | Windows | hhhh   |
| <input type="checkbox"/> | Windows | cccc   |
| <input type="checkbox"/> | Windows | ccs profile  |
| <input type="checkbox"/> | Windows | Wins - Security  |

**Step [2]:** Click Add Profile Section and select Containment



**Step [3]:** Select virtual desktop option



- **Launch Virtual Desktop upon user login** - Will automatically run the Virtual Desktop when a user logs in to the system. (Default = Disabled).

- **Automatically reset Virtual Desktop when session is terminated** - Resetting the virtual desktop will remove all user data and undo all system changes made during virtual session.
- **Request password when exiting Virtual Desktop** - Configure an exit password. The exit password prevents guests or users from closing the virtual desktop and accessing the host, potentially exposing the computer to danger. (Default = Disabled)

These actions will be reflected in the endpoint after the profile is added.

For example : Here we are showing ccs requesting password when exiting virtual desktop

