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	≡ Profil	es					
DASHBOARD >	_						
DEVICES >	Profile	es Default I	Profiles				
A USERS >	ţ	南			Ē	ГŢ	
CONFIGURATION TEMPLATES	Create	Import	Export Profile	Clone Profile	Delete Profile	Export	
Profiles							
Alerts		US NAME					
Procedures		Securit	y profile				
Monitors							
00 NETWORK MANAGEMENT BETA >		Profiles	s for UI settings				
APPLICATION STORE		[cloned	[cloned] Windows - Security Level 1 Profile v.6.23 vicky				
APPLICATIONS >		[cloned] Windows - Sec	urity Level 1 Pr	ofile v.6.23		
SECURITY SUB-SYSTEMS		hhhh					
LICENSE MANAGEMENT		сссс					
SETTINGS		ccs pro	file				
· · · · · · · · · · · · · · · · · · ·		Wins -	Security				

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



Step [3]: Select virtual desktop option

Endpoint Manager	Profiles / Security profile / Containment	™ 2	요 Logout (stephenrobert778@gmail.com)
DASHBOARD >			
DEVICES >	Security profile		
△ USERS >	ç 🛱 🛱 🛱 🛱		
E CONFIGURATION TEMPLATES 🗸	Add Profile Export Profile Clone Profile Delete Profile Make Default Section		
Profiles			
Alerts	Reneral Attiving Containment		
Procedures			
Monitors	Partitionant		
00 NETWORK MANAGEMENT	Concamment		
APPLICATION STORE	Settings Rules Baseline Virtual Desktop		
APPLICATIONS	Launch Virtual Desktop upon user login CCS 11.e		
SECURITY SUB-SYSTEMS	Automatically reset Virtual Desktop when session is terminated		
LICENSE MANAGEMENT >	Request password when exiting Virtual Desktop		
SETTINGS >	Password *		
	Confirm password *		

• 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

COMODO Virtual Desktop							
1:48 PM	4/4/2019						
Last Session Duration: 00:01:54							
COMODO Enter pass	sword ×						
Password:							
	OK CANCEL						
Switch to Wi	indows View Switch to Windows View						