Setting Time Limits for Temporary Unlock and Suspending Restrictions

In some scenarios you will want to allow temporary unlock. However that unlock may require a restriction to the elements that can be unlocked or the time in which it can be done.

When connected to an endpoint via the Managment Console:

You will have the option of Unlock Wizard.



You are presented with a number of options on the unlock process.

Temporarily unlock Agent	×
Temporarily unlock Agent Select which type of drive or device you want to unlock.	\mathbf{r}
Temporarily unlock Agent 10.0.0.49	
Select the drives or devices to unlock:	
Floppy disk drives	^
CD-ROM drives	
USB bus connected drives	
Firewire (1394) bus connected devices	
SD card drives (SD-bus)	
Fixed disks (eSATA and other non-removable, non-sy	
Encrypted volumes	
Other removable drives	
Network drives and shares	v
Unlock all Indrive types Indevice types	
< <u>B</u> ack <u>N</u> ext >	Cancel

Page 1 / 4 (c) 2025 Adam Gurrie <support@sectiontechnologies.com.au> | 2025-07-01 03:30 URL: https://kb.sectiontechnologies.com.au/index.php?action=artikel&cat=15&id=31&artlang=en

You can define the period or time until which this temporary unlock is valid. The unlock is even maintained during a computer restart, e.g. if you temporarily unlock USB drives for the next three days, the computer can be rebooted in between.

Temporarily unlock Agent	×
Temporarily unlock Agent Select unlocking behavior and other options	\bigcirc
Device control options Disable file filtering during the unlock period Unlock unencrypted portions of encrypted drives Force accepting usage policy before drive can be accessed	_
Other module options Disable web security (URL filtering) during the unlock period	-
< Back Next > 0	Cancel

When you unlock drives, you can select the following options to temporarily additional restrictions:

 \cdot Disable file filtering and auditing during unlock period: Users can read and copy files that would normally be blocked based on file filtering rules. No auditing of file access is performed.

• Unlock encrypted portions of encrypted drives: Allow access to unencrypted portions of drives that are encrypted using Encryption 2-Go. Commonly the Mobile Encryption Application (MEA) is stored on an unencrypted portion of such a drive.

 Force accepting usage policy before drive can be accessed : The user must agree to a configured usage policy before the drive is unlocked.

These options are available for other modules:

•Disable web security (URL filtering) during the unlock period: Disables the Web Security module during an unlock (if licensed).

Click Next.

Femporarily unlock Agent Select unlocking behavior and	d other options		
Application control options			
Disable application control dur	ing the unlock	period	
Add applications launched hash database (learning m	during the unl iode)	ock period to the	local
Executable files to add to t	the local hash o	database:	
 Files written to the com 	puter during th	e unlock period	
Executables (and DLLs)	s) launched dur	ing the unlock pe	riod
Both files written and e	xecutables lau	nched)	
Require user approval f	for all files after	unlock period en	ds

If you are using application control, you can specify settings here so applications can be disabled during unlock. You also specify whether and which application files are added to the local hash database during this unlock period.

Use the "Require user approval for all files after unlock period ends" option to check the "learned" applications manually after the unlock is finished before they are added to the local application database and thus unlocked.

Click Next.

nporarily unlock Agent		×
Select for how long p	ent blicy settings are disabled.	b
Calaat faa haw laa - th - t	unat annua tao udi ba unia alcad	
Select for now long the t	arget computer will be unlocked	
Time span	30 min (ends with reboot)	
O Until date	22:17:37 🗘 04.07.2018 🗸	
Reason for unlocking (fo	reporting purposes)	
documentation		
	c Paole Daiah	annel
	< back Finish C	ancel

Finally, select the required unlock period, either in minutes or up to a specific date and time.

As administrator, you can also enter a text (for example, the reason for unlocking) at this point. This text is also stored in the event and can be evaluated via reporting.

Unique solution ID: #1030 Author: Adam Gurrie Last update: 2019-10-24 07:42