

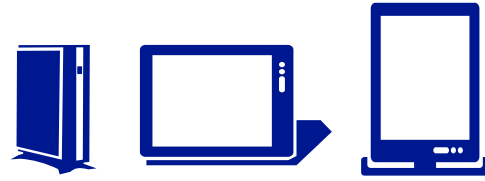
Windows Embedded 8 Standard

Lockdown | Harden your system

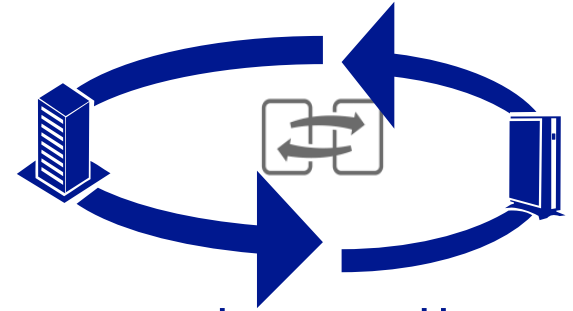
Windows Embedded 8 Standard



One Trusted
Platform

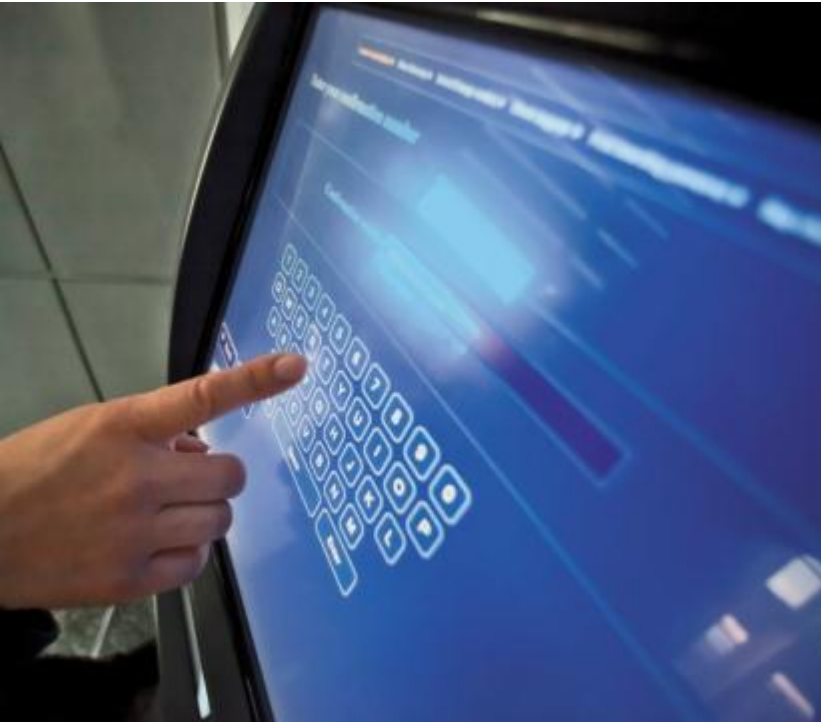


Differentiated
Devices



Extend Intelligent
Systems

User Experiences



Disclaimer



Features described in this section are not representative of the final feature set that will be available at RTM:

Features per SKU are not finalized, and feature availability may change

Features will continue to evolve until RTM

Embedded Market View | Why Lockdown?

Prevent unauthorized access to the device:

Control the experience of your device from boot to shutdown
Limit end user interactions through lockdown features

Custom Branding

Deliver brand
on top of
Microsoft
proven
technology

Provide a
customized end
user experience



Boot screen:
Suppression of
Windows boot UI



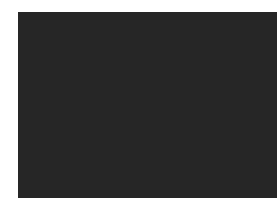
Auto Logon:
Hides all Windows
login UI



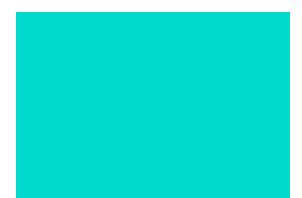
**Embedded
Logon:** Hides
Windows status
messages




**App Launcher or
Shell launcher
plus Dialog Filter:**
Kiosk mode



**Automatic
handling of system
errors:** Blank screen
followed by
automatic reboot



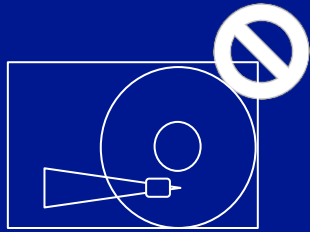
**Shutdown /
Logoff:** All
Windows messages
can be suppressed



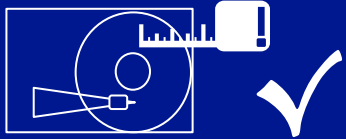
Embedded Lockdown Features

Unified Write Filter (UWF)

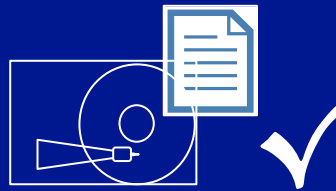
Sector Based Protection



Registry
Exclusion



File
Exclusion



Protect system against write operations
Easily create read only devices
Improve system up-time

Blocking Disk Writes with the Unified Write Filter

Single solution combining features from Enhanced Write Filter, File Based Write Filter, and Registry Filter

Enhanced configuration/management options:

- WMI Interfaces (for local and remote scripting)
- Command line utility
- Integration with Embedded Lockdown Manager (ELM)



System up-time improvement

	Sector-based protection	File Exclusion	Registry Exclusion	Memory Reclaim	ELM Integration
UWF	✓	✓	✓	✓	✓
EWF	✓				
FBWF		✓		✓	

New & Old Options with Unified Write Filter

Old Filters still available

Managed the same way as before & not via the new Embedded Lockdown Manager

Commit changes dynamically

Using UWFmgr.exe . No need to reboot system for changes to take effect. Make permanent changes to a write protected system while it's running.

Disk overlay option

Greater robustness over RAM overlay

Configuration options

Run-time command line utility. UWFmgr.exe
WMI object. Script or code

Servicing option

Get critical Windows updates for a write protected device and apply them to permanent storage

UWF Servicing Mode

One click method to service UWF protected systems

Automatically retrieves and applies updates from

Windows Update (WU)

Windows Server Update Services (WSUS)

Works with Task Scheduler

Flexible architecture

OEMs can configure servicing screen

OEMs can control what is done during servicing

Configurable using

WMI Interfaces (for local and remote scripting)

UWFMGR command line utility

Integration with Embedded Lockdown Manager (ELM)

UWF Commit Functionality

Ability to make permanent changes to a write protected system while the system is running

Service a device without requiring system reboots

Update files and registry values

Commit functionality is accessible using

WMI Interfaces (for local and remote scripting)

UWFMGR command line utility

Only administrators can perform commit operations

Antimalware Modules

Automatically configures UWF file and registry exclusions to help protect a device from viruses and malware

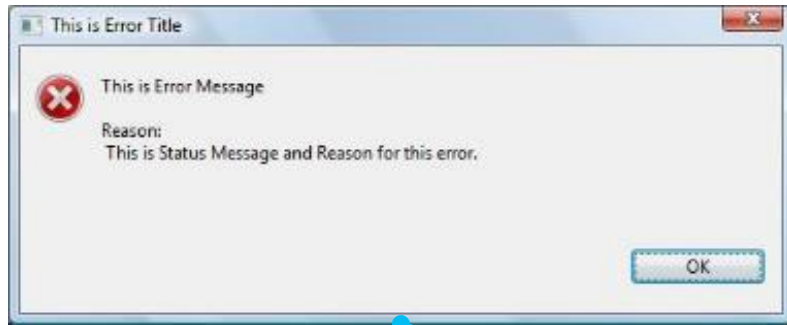
New Modules

 **SCEP Support**
Enables System Center 2012 Endpoint Protection to stay up-to-date

 **UWF AntiMalware**
Enables Windows Defender to stay up-to-date

Dialog Filter

Block Pop-up Dialog Boxes



Provide a consistent user experience

Ensure OS is not visible to users

Lockdown device

Dialog Filter

Extends former dialog filter experience

Management of all desktop windows and dialogs

Blocking of managed code is now supported

Protected processes feature

Allow all windows/dialogs in a processes

Set a default behavior for all other windows and dialogs (e.g. Close, Cancel)

Protected processes are allowed to run overriding defaults settings

Dialogs in protected processes can be blocked explicitly

Easily configurable using ELM tool and NEW:
WMI interfaces

Hiding System / Application Windows with Dialog Filter

Replaces Message Box Interception

Works on all architectures

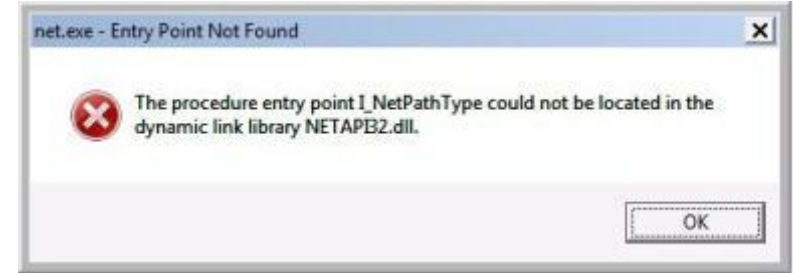
Protected processes list
(new for WES8)

Allow all windows/dialogs from an OEM-configured list of processes.

Disallow all other windows/dialogs...

Supports blocking of managed code

Configurable using ICE or Embedded
Lockdown Manager (ELM)

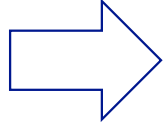


Shell & App Launcher

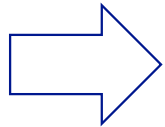
App Launcher | WinRT Apps



Users



Admins

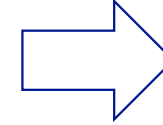


Launch directly into new Windows 8 apps

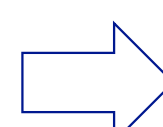
Shell Launcher | Desktop Apps



Users



Admins



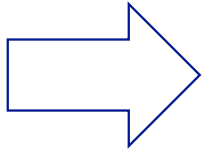
Launch Desktop apps as a custom shell

Shell Launcher

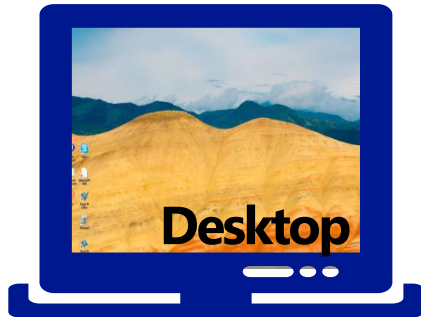
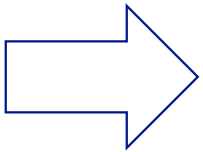
Launch Desktop apps as a custom shell



Users



Admins



Control device
experience

Lockdown device
for users

Provide full access
for admins

Shell Launcher

Launches an application as a custom shell

Supports different shells for different users

(or groups of users)

NEW: WMI interface

Robustness

Shell Launcher restarts the shell, if something goes wrong

Acts similar to a watchdog process

Embedded Lockdown Manager (ELM)

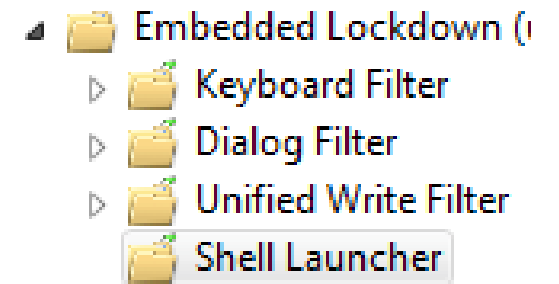
Enables local and remote management of embedded features

Keyboard Filter

Dialog Filter

Unified Write Filter

Shell Launcher



Embedded Lockdown

Snap-in into MMC

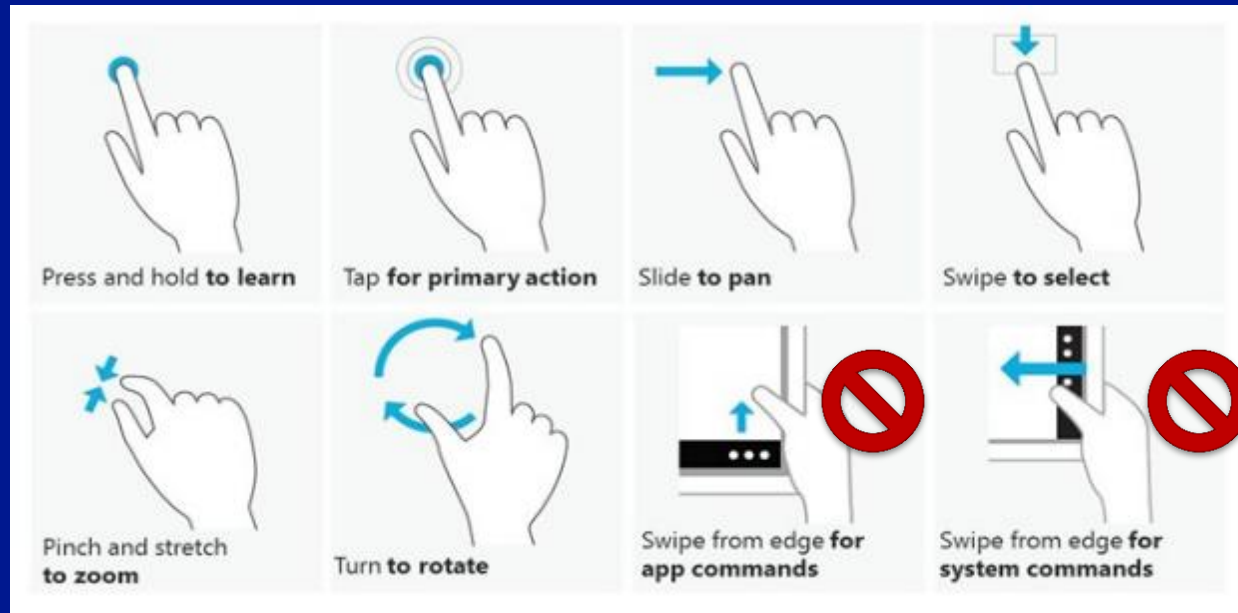
Integrated into security infrastructure including:

Directory services - Active Directory

Secure file access (ACL) - NTFS Security

Gesture Filter

Block edge gestures



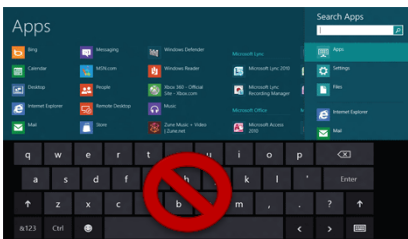
Ensuring Windows settings are not accessible by user
Lockdown device

Keyboard Filter

Alt + F4

Disable or enable for Admin accounts

Ctrl + Alt + Del



Works on screen keyboards as well

Admin access mode

Disable Keyboard Filter for Admins

Force Off Accessibility

Block users from enabling Ease of Access feature

New & Enhanced Functionality for Keyboard Filter

Block special key combinations on system level

NEW: Layout detection

NEW: Admin account

NEW: Works for on-screen keyboards

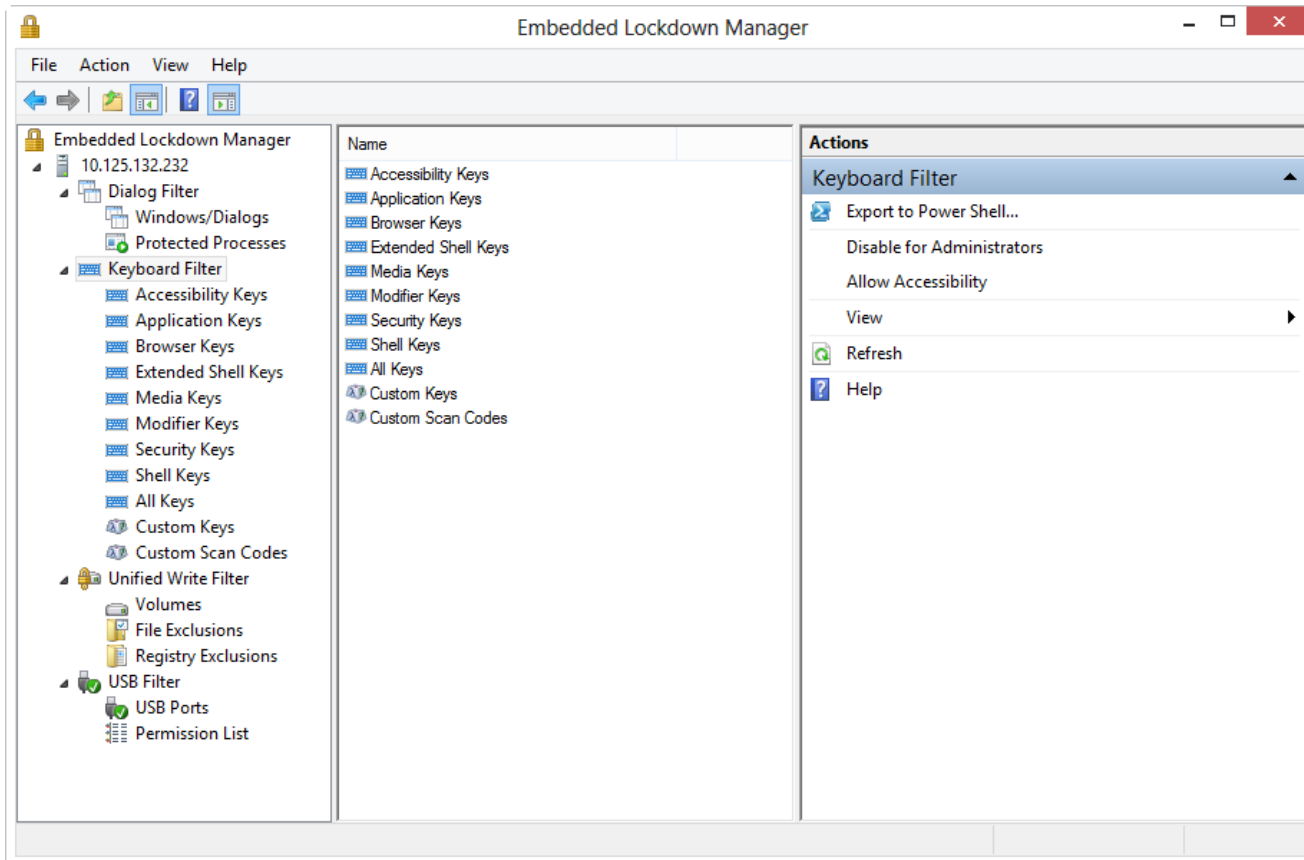
As well as standard keyboards

Flexible configuration options regarding custom key combinations and scan codes

Granular filtering on different levels offered

Shell keys, Browser keys, Media Player keys, Security keys, etc...

Embedded Lockdown Manager

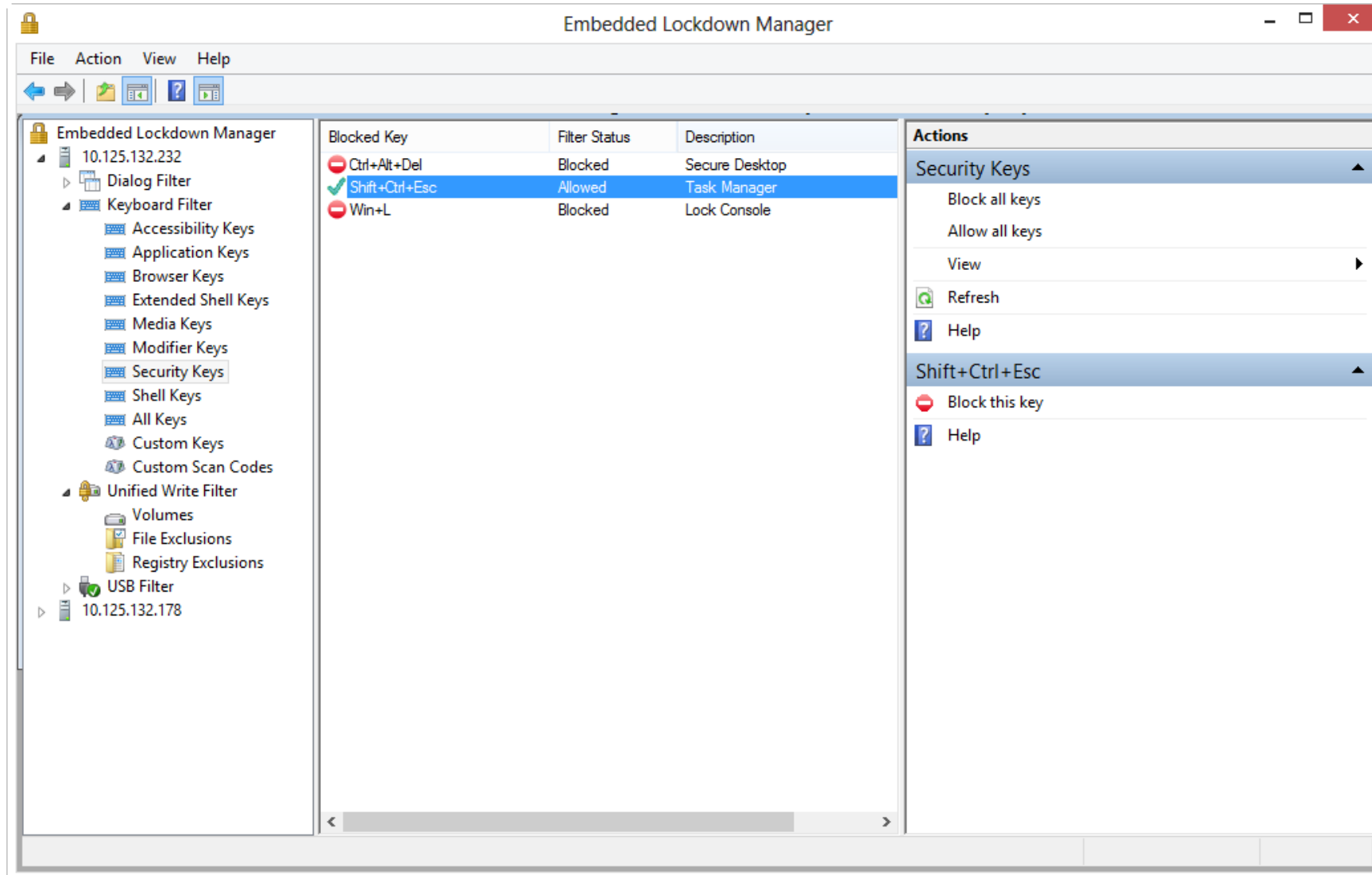


Remotely configure lockdown on a device

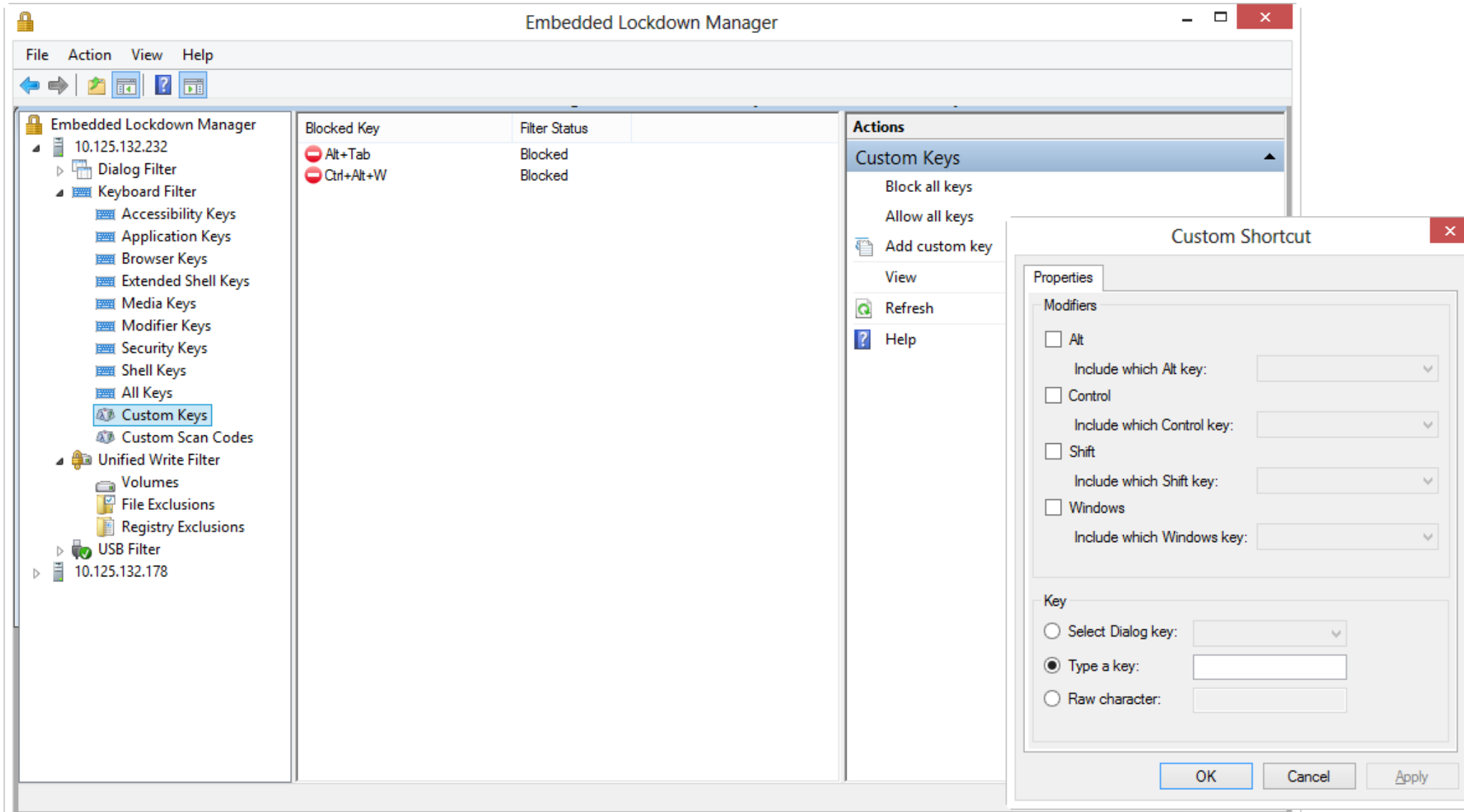
Connect to multiple devices to simplify device lockdown management

Export configuration setting to PowerShell scripts

Keyboard Filter | Blocking Standard Keys



Keyboard Filter | Custom keys



Keyboard Filter | Custom scan codes

The screenshot displays the Embedded Lockdown Manager application. The left sidebar shows a tree view with the following structure:

- Embedded Lockdown Manager
 - 10.125.132.232
 - Dialog Filter
 - Keyboard Filter
 - Accessibility Keys
 - Application Keys
 - Browser Keys
 - Extended Shell Keys
 - Media Keys
 - Modifier Keys
 - Security Keys
 - Shell Keys
 - All Keys
 - Custom Keys
 - Custom Scan Codes
 - Unified Write Filter
 - Volumes
 - File Exclusions
 - Registry Exclusions
 - USB Filter
 - 10.125.132.178

The main pane shows a table of blocked keys:

Blocked Key	Filter Status
Alt+0x30	Blocked
Ctrl+0x30	Blocked
Ctrl+Alt+0x0E	Blocked

The right pane shows the 'Actions' menu with the following options:

- Custom Scan Codes
- Block all keys
- Allow all keys
- Add custom scan code
- View
- Refresh
- Help

A 'Custom Shortcut' dialog box is open in the foreground. It has a 'Properties' tab and the following settings:

- Modifiers:**
 - ☒ Alt
 - Include which Alt key: Either Key
 - ☐ Control
 - Include which Control key:
 - ☒ Shift
 - Include which Shift key: Either Key
 - ☐ Windows
 - Include which Windows key:
- Scan Code:**
 - ☒ Type the key to reveal its Scan Code
 - ☐ Enter Scan Code by number
 - Scan Code (Hex): 09

Buttons at the bottom: OK, Cancel, Apply.

Summary

Granular and sophisticated lockdown options

New features - taking lockdown to the next level

E.g. protected processes

Consistent, familiar lockdown configuration and management via MMC snap-in (ELM)

Introducing a WMI API for scripts and servicing applications

Microsoft