How to understand connection and security status of devices from Endpoint Manager device list

Open Endpoint Manager > Click 'Devices' > 'Device List' > 'Device Management'

- The 'Device Management' screen is an inventory of all mobile devices and endpoints enrolled to Endpoint Manager.
- It shows each device's connection, security and patch status, which security components are enabled, recent activity, and more.
- This article explains how to understand the connection, security, patching and virtual desktop activity statuses of an endpoint from the icons in the interface.

The device management interface

- Login to Xcitium
- Click 'Applications' > 'Endpoint Manager'
- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab (if it is not open already)

The interface shows all mobile devices and endpoints added to Endpoint Manager, with their details:

OS - The operating system of the device.

Name - The label assigned to the device by the user. If no name is assigned, the device model number is used as the name.

- The device icon to the left of the name shows the device's connection status. See 'Connectivity status icons' to read more.
- The shield icon to the right of the name indicates the status of Xcitium Client Security (CCS) (Windows only). See Security status icons to read more.

Active Components - Indicates which modules are installed on the device. Possible components are 'Agent',

'Antivirus' (AV), 'Firewall' (FW) and 'Containment'.

- **Android devices** - The agent will automatically install the AV (antivirus) component.
- **iOS devices** - Only the agent (EM client)
- **Windows endpoints** - Available components are - Agent, AV, FW (firewall) and Containment. These components are installed automatically when a profile featuring the components is applied.
- **Mac OS endpoints** - Available components are EM Agent and AV

  The color of the icon shows the status of the component:

  - **Green** - Installed and active
  - **Gray** - Installed but disabled by profile setting
  - **Blue** (only applies to the 'Containment' module) - The containment module is baselining the device. During the baseline period, unknown files are auto-submitted to Valkyrie for analysis, but are not placed in containment. See this wiki for help to configure baseline settings in the 'Containment' section of the security profile applied to a device.
  - **Blank** - Component is not installed.

Virtual Desktop - The status of the virtual desktop on the endpoints. See Virtual desktop status icons to read more

Patch status - The icons indicate whether endpoint is patched up-to-date or any patches are available for it. See Patch status icons to read more.

Customer - The name of the company to which the device is enrolled.

- Xcitium MSP customers can enroll devices to any of the companies they have created in C1.
- Xcitium Enterprise customers / EM standalone customers can only use the 'default company'.

Logged in User - The name of the user currently signed-in to the device.

- The user name is prefixed with the active directory (AD) domain or workgroup that the user is currently logged-in to:

Active Directory - Name is shown as <AD domain name>\<user name>

Workgroup - Name is shown as <workgroup name>\<user name>

No network - Name is shown as <device name>\<user name>

Last Activity - The date and time at which the device last communicated with the EM agent.

Connectivity status icons

 - Device is not reachable. The connection might be down or the endpoint is switched off.

 - Slow connection. The device is connected but commands and messages may take some time to execute since the endpoint is busy.

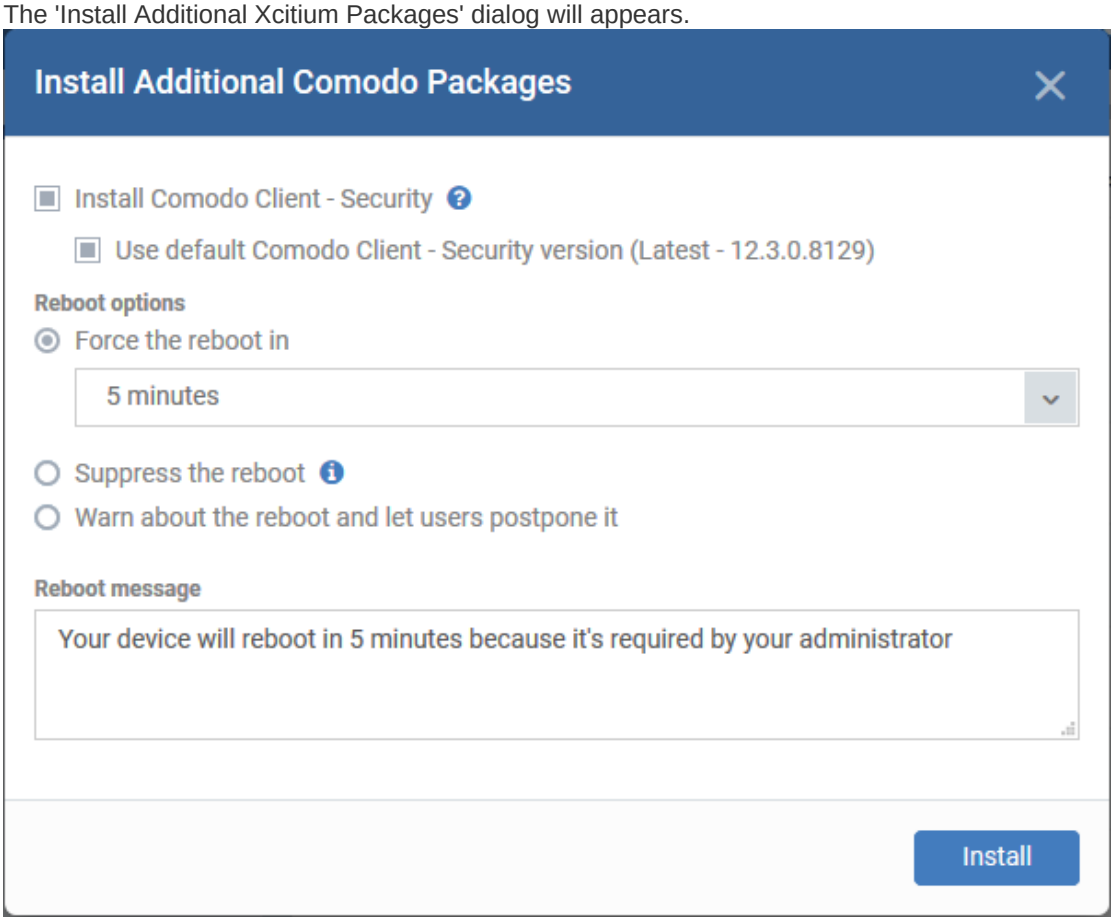
 - Good connection. Commands should be executed in real time.

- A device is marked as 'Old' if it does not connect to EM for a certain number of days.
You can set how many consecutive days of inactivity must pass before EM marks a device as 'Old'.
You can also tell EM to remove devices that do not reconnect for a certain number of days after being marked 'Old'.
See this wiki if you need help to do this.

- The device is a duplicate. Applies to Windows devices only.
A duplicate device is one that has the same name and / or MAC address as one or more other devices. This could be because the same device was enrolled more than once, or because the same name was given to multiple devices.
You can tell EM to auto-remove duplicate devices or to selectively uninstall the clients.
See this wiki if you need help to do this.

Security Status icons

Yellow - CCS is not installed on the endpoint.
Click the shield icon to remotely install CCS on the endpoint.
The 'Install Additional Xcitium Packages' dialog will appears.



- CCS requires the endpoint to be restarted in order for the installation to take effect.

- Configure the 'Restart' options and click 'Install'.

- See this wiki for more help on remote installation of CCS.

Gray - Outdated clients. Communication Client (CC) and/or Xcitium Client Security (CCS) on the endpoint require updates.
Note. This status is only shown on endpoints that have CC 6.16 + and CCS 10.0 + installed.

Red - The endpoint is at risk. One or more of security components (AV, FW or containment) may have been disabled by the user. Place your mouse over the icon to view the warning:

Amber - The endpoint needs attention. The virus signature database might be out-dated or the endpoint needs to be re-started after installation of CCS.
Place your mouse over the icon to view the full message

	Green	-	The endpoint is secure. All installed components are up and running.
	Blue	-	CCS is in 'Silent Mode'. Note: CCS lets users enable 'Silent Mode' if they do not want to be disturbed by product notifications. For example, when running a full-screen presentation. Alerts and notifications are suppressed and operations that could interfere with their work are postponed.
		-	Communication with CCS on the endpoint has been lost.

Virtual Desktop Status icons

The 'Virtual Desktop' column shows whether the virtual desktop feature is supported on the endpoint and whether it is currently running:

	Running	-	The virtual desktop is open on the endpoint
	Not Running	-	The virtual desktop is not open on the endpoint
	Un supported	-	The version of the security and/or communication client on the endpoint does not support the virtual desktop. Alternatively, it can mean the security client is not installed at all.

Patch Status icons

The icon in the 'Patch status' column indicate whether any patches are to be installed on the device. If so, it also shows the number of patches available for the device.

	-	No patches required. All patches are up-to-date.
	-	Critical patches are available. The number to the right shows how many are pending. Click the number to view and manage the patches. See this wiki for help to remotely install patches on the device.
	-	Optional patches are available. Click the number to the right to view and manage the patches.

Further Reading:

How to enroll devices using the on-boarding wizard

How to install xcitium Client Security on Windows, Linux and Mac devices

How to check patch status on individual devices

How to run a browser in the virtual desktop

How to configure removal options for inactive and duplicate devices