Activation Type Comparison

Privilege Manager provides different ways for activating temporary access on a client. This documents describes activation types and lists common benefits and limitations of each type. By default, only the Credential provider activation types are usable on clients because in these types, the user can handle the whole activation process in the Windows login window or UAC (User Account Control) window.

Activation type	**User interface**	**Benefits**	**Limitations**
Legacy request password (disabled by default)	Recast Agent icon in Windows notification area	• User gets local user account and password so user can use login to computer and use Run as Administrator functionality without Carillon credential provider • Service Desk can select how long time user can use the user account/password combination • Works offline • Works in Windows XP and older • Local account used so no access to other devices on network	• User need to use Request activation code functionality (disabled by default) or contact Service Desk to get activation code • Password hard to remember (random generated password) and Windows 10 does not allow copy/paste in UAC window
Use activation code	Credential provider in login screen and/or UAC window	• Service Desk can select how long time same activation code can be used • Works in offline • Local account used so no access to other devices on network	• User need to use Request activation code functionality (disabled by default) or contact Service Desk to get activation code • Activation code (20 characters) must be typed in Windows 10 UAC window (copy/paste does not work when UAC in Secure Desktop)

Activation type	User interface	Benefits	Limitations
Run with local account	Credential provider in UAC window	• User can perform without contacting Service Desk by typing reason • Local account used so no access to other devices on network • Alternative credentials can be used when logged on user does not have permissions to use this activation type • Privilege Manager administrator can configure who and where this can be used (for example all users on their primary devices)	• Requires connection to Privilege Manager server
Run with domain account	Credential provider in UAC window	• User can perform without contacting Service Desk by typing reason • Network resources can be accessed (because using domain account) • Privilege Manager administrator can configure who and where this can be used (for example Service Desk users on workstations)	• Requires connection to Privilege Manager server • Requires connection to On-Premises domain controller or used account must exist in cached credentials