

Understand How Application Launcher Can Integrate with Your Applications

Application Launcher performs a few layers of functionality, which one can use all at once or only in pieces. In its simplest form, an Application Launcher scenario is used to launch an application using the correct rights and then pass the authenticated session with that application over to the end user. In some cases, this will simply mean launching the application with some parameters or using an explicit *run as* like call. For example, when launching PuTTY, one of the applications that is configured out of the box, you execute the application along with some command line parameters to specify the connection details, which come from the Privileged Identity secure library, and then the session running that application is passed to the user to use as if they had done it from their own desktop. This means there is no need for other scripting or mechanisms to make this work. Another example is something like PowerShell, which uses the credential context from its execution. Using the run as options offered at launch time, one can execute PowerShell on the Jump Server or locally as any user with rights to launch it. Again, no scripting is required. For many applications administrators wish to access, that will be how they are configured. The ones supplied out of the box serve as examples on how to make this work.

For many other applications, there is more interaction required. When you launch the application there may be a dialog box that displays, asking for username, password, and possibly more information. There are also web applications that require launching the browser and then interacting with the web pages through the Document Object Model (DOM) to navigate as if the system was a user to enter the authentication data. In those cases, a script is required to be used in conjunction with the passing of the data Privileged Identity has. The script acts as an automation layer, taking the data passed and getting it to where it needs to go in the application UI or web page. We have delivered a number of those out of the box as well. Like the applications that would use the command line parameters or run as method, the scripts are able to be modified and extended to allow for many other similar and even more complex applications to be launched by the system. This does not require any changes to our product, only configuration at deployment time.

All this goes to say that the applications that can be managed by Privileged Identity are limited only by the ability of scripts to interact with applications and passing data needed by applications from what Privileged Identity knows. The ones we do manage out of the box were never intended to act as a limit for what is possible. The intention has always been that the people deploying the solution should be able to add applications as easily as possible in order to meet the business needs they have.