Application Rights Management for Windows Desktops

Liquidware ProfileUnity's Application Rights Management features enable Administrators to securely modify and/or elevate "standard user" rights in Windows to allow or deny applications from being executed, delivered, or installed on select users' desktops. Application Rights Management is included within the ProfileUnity User Environment Management feature set for no extra cost, adding great value for organizations.

Two feature modules within ProfileUnity enable organizations to accomplish Application Rights Management: (1) Privilege Elevation; and (2) Application Restrictions. These two modules empower Administrators to limit or enable user rights to execute, receive, or install any type of application, including virtualized and layered applications.

ProfileUnity Application Rights Management processes user rights from an Administrator level, securely preventing Standard Users from executing or launching applications where permissions do not exist.

ProfileUnity Application Rights Management solves the following use cases:

Deliver Specific Applications to Only Select Users

Administrators can minimize base image builds or deliver an application that can't be virtualized with VMware ThinApp, Microsoft App-V, or layered with ProfileUnity FlexApp. Simply add challenging applications to a base image and then restrict unauthorized users from launching the application with ProfileUnity's Application Restrictions feature.

Elevate Privileges for Standard Users to Run an Application

Elevate a Standard User to be an Administrator to run and/or install select applications. Simply elevate privileges for a specific user or user group to run the select application by using context-aware filters in ProfileUnity.

Make Administrator Required Applications Compatible with Microsoft RDSH or Citrix XenApp

Certain applications require Administrative privileges, making them a non-starter for server-based computing. ProfileUnity enables desktop administrators to easily elevate users or groups to Administrative privileges for select applications.

Lockdown Applications on a Select Desktop for Kiosk or Call Center Mode

ProfileUnity's Application Restrictions feature can be set to only "allow" certain select applications; the user will then be denied access to all other applications.

Elevate Privileges for a User to Install Applications in Virtual or Physical Desktops/Laptops

ProfileUnity can be set to automatically raise the credentials of a user to an Administrator for select application installers by using Privilege Elevation.

Location-Aware Application Restrictions

ProfileUnity's Application Restrictions feature can be utilized with context-aware filter to make application(s) available to only certain users who meet select criteria.

Focus on Security

ProfileUnity enables Application Rights Management while keeping the environment secure. Variables such as a SHA-1 Hash specific to the application can be added to ensure the exact application is being enabled and nothing more. ProfileUnity also enables or restricts a user's rights and profile settings with Administrator rights at a system level that Standard Users cannot modify.

Privilege Elevation

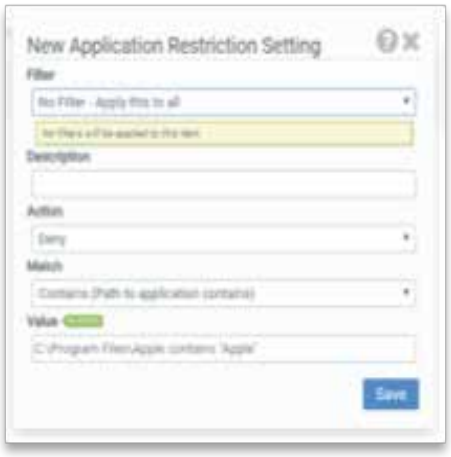
The Privilege Elevation feature module in ProfileUnity allows standard users to securely install and run applications needing elevated rights without making the user an administrator. The Allow and Deny policy rules defined by the administrator determine how the privileges are applied to users.

Using this module along with the Application Restrictions module provides Application Rights Management that enables administrators to securely grant specific users with detailed application rights without making them a Windows Administrator.

The Privilege Elevation features Allows or Denies applications to be Installed or Run elevated (as Administrator) based on selected criteria. Options include if the path contains certain value (equals, contains, ends, starts with), the SHA256 hash of the installer, or the fact that the installer is Signed (has a digital signature). Any of these can also be used along with a context aware filter (covered below).

Application Restrictions

The Privilege Elevation feature module in ProfileUnity allows standard users to securely install and run applications needing elevated The Application Restrictions feature module in ProfileUnity allows or denies users access to applications providing allow/deny options for installed applications per user.



Use this feature along with the Privilege Elevation to provide Application Rights Management which enables administrators to securely grant specific users detailed application rights without making them a Windows Administrator. More specifically, the Application Restrictions module allows organizations to minimize their number of base images while ensuring they are compliant with licensing and imaging agreements. Applications can be added to the base image of an end user workspace then restricted with Application Restrictions.

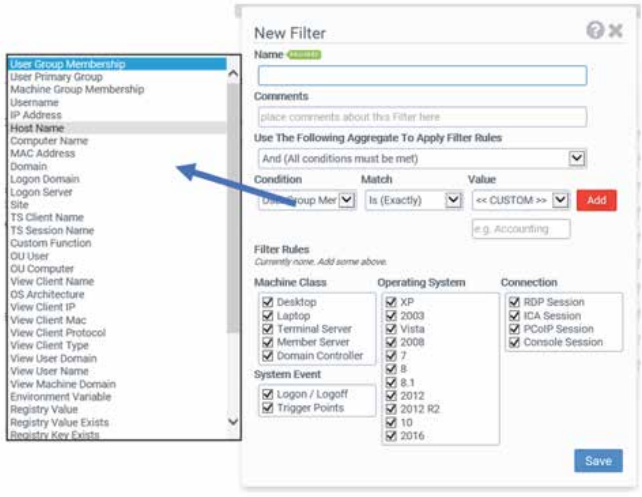
Administrators can add any number of both Allow and Deny rules in the Application Restriction feature module. The rules are evaluated sequentially starting with the first one at the top of the list. When a filter returns true for an individual user, then that rule sets whether the Application Restriction module becomes an "all allow" or "all deny" list for that user. If that first true rule has an Allow Action, then any of the remaining Allow rules in the module list where the filter is also true will apply. If instead the first true filter rule has a Deny Action, then it will become an "all deny" list for that user.

The application access policy will be applied based on whether the rules evaluate to create an Allow List or a Deny List. If the rules evaluate to create a Deny List for a user, then the user can run any applications except for those specified in the deny rules. If the rules evaluate to create an Allow List for a user, then the user can only run applications that are specified by the allow rules. Access to other applications will be denied. By default, the following processes are automatically allowed:

- ProfileUnity processes
- All system processes
- Processes from C:\Windows and subdirectories
- Processes signed by VMware or Citrix

Filters (Conditional Settings)

Context aware filters greatly control how features and configurations are applied within ProfileUnity including all Application Rights Management features. You can apply a feature's ruleset based on hundreds of criteria (including existing Microsoft Active Directory values) with a single filter or by "stacking" filters. For example, you may want to limit users to be able to open applications from within a certain IP address range. To accomplish this task, you can an application restriction or allowance based on the IP address range that corresponds to where the Windows session is to be connected. Writing a filter is as simple as filling in the boxes and selecting your options on the screen.



For more information about Application Rights Management features in ProfileUnity download the full ProfileUnity Help Manual on the ProfileUnity Documentation Support web page.