TECH TIP: Transparent Login Basics

# RDP Applications

The starting point in PAM for Transparent Login(TL) is the creation of an RDP Application service. The service points at the location, on the target server, of the program you wish to run as an RDP application.

# Published Applications

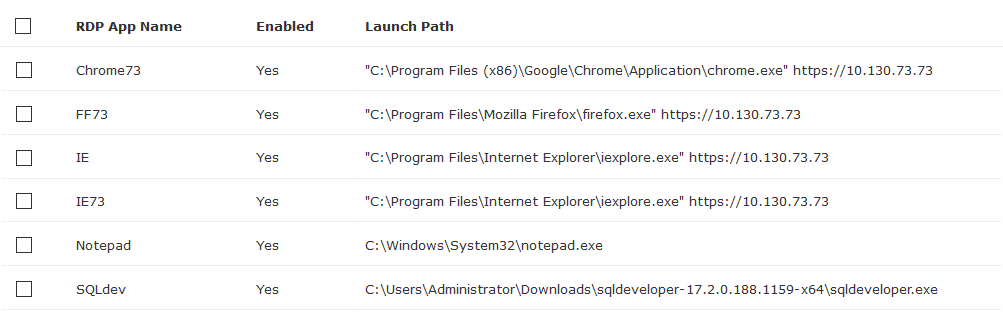
In order for a server program to be run as an RDP Application it must be published in the Active Directory(AD). Please check the PAM documentation wiki for the details regarding the publishing of programs, <https://docops.ca.com/ca-privileged-access-manager/2-8-3/EN/implementing/provision-your-server/provisioning-devices/set-up-transparent-login/rdp-connections>.

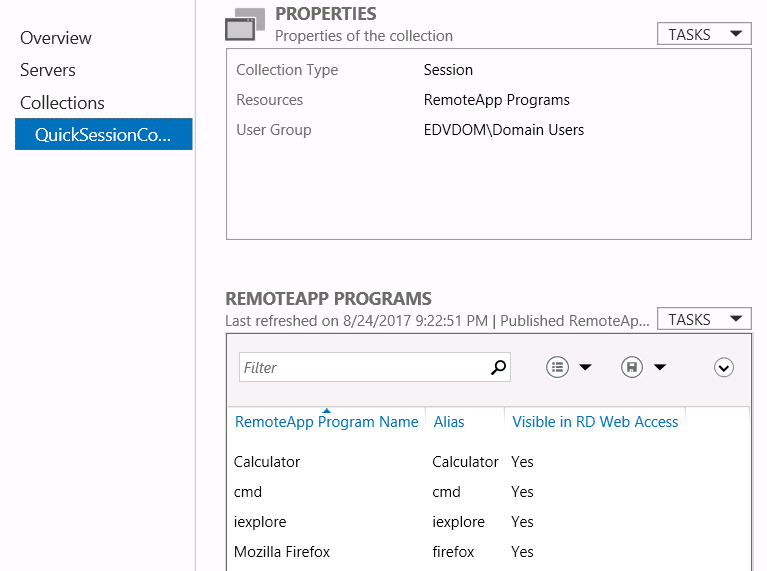
# Add Service to Device

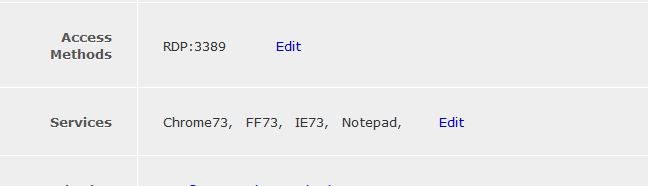
Next configure a new device, or open an existing device, that is in your domain and contains published applications. Select the RDP Application from the list of Services.

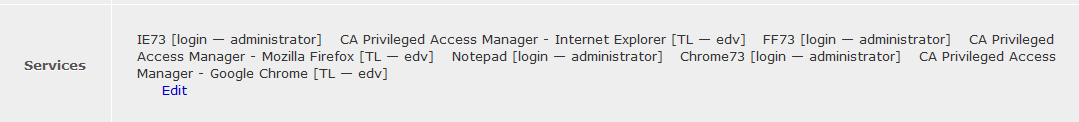
# Add Service to Policy

Create or modify a policy so that the service is selectable on the Access page. If you’ve already configured the credentials to be used they may be associated with the service. If not, configure the Target Application and Target Account before configuring the policy. At this point you will be able to launch the service by clicking its link on the Access page.









# Add TL to Service

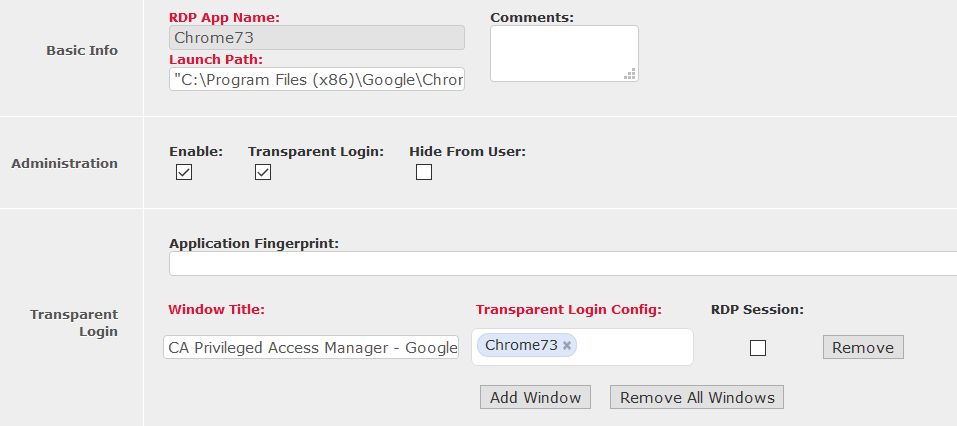
One you have the RDP application working you can add Transparent Login to it by checking the box. You will now see several additional fields. The Window Title and Transparent Login Config fields are required. The Title is what appears in the window when the program is launched on the target server. The Config is the name of the script you create in order to inject the username and password into program, so that it may be used.

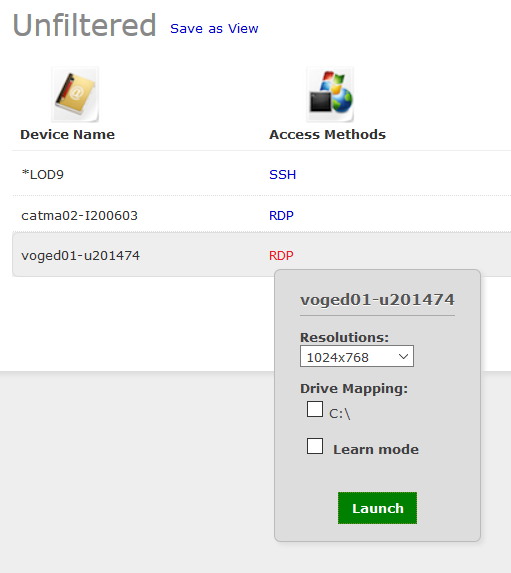
# TL Learn tool

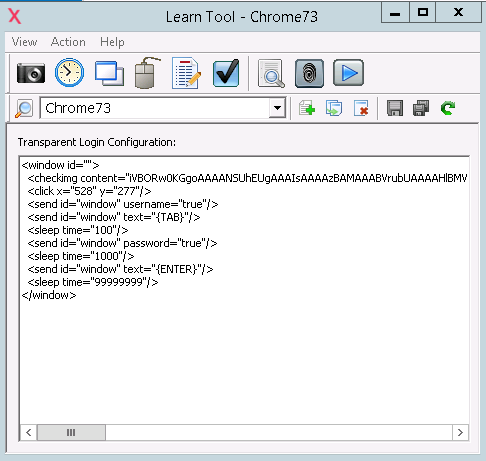
One you have the RDP application working you can add Transparent Login to it by checking the box. You will now see several additional fields. The Window Title and Transparent Login Config fields are required. The Title is what appears in the window when the program is launched on the target server. The Config is the name of the script you create in order to inject the username and password into program, so that it may be used. You run the learn tool by hovering your mouse over the RDP link for the AD device and clicking the Learn mode box and the Launch button. You will not see this if you have not configured Drive Mapping under Global Settings. The Learning tool will not launch if it has not been properly configured as a Published Application.

# Using the learn tool

The Learn Tool has many options. The ones you will need will depend on your application. From left to right the icons are Screen Verification, Sleep, Activate window, Mouse click, Text input, Element Verification, Run Control Viewer, Get Application Fingerprint and Debug. This document will not explain all of these icons in detail. It will also not cover all of the options for each.







# Using screen verification

Screen Verification is used to insure that the username and password are injected on the right page. Clicking the Screen Verification button opens a clipping tool. You should select an area that is unique to the desired page. In this case, this was done after opening a browser and entering the url of a PAM instance. To make it more unique, Script Verification was not clicked until after the username field was clicked. You can see in the clipping that there is a blue border around that field. This insures that the injection won’t start until after that field is clicked. This line should be at the beginning of the script, so move it up if necessary.

# Using Sleep

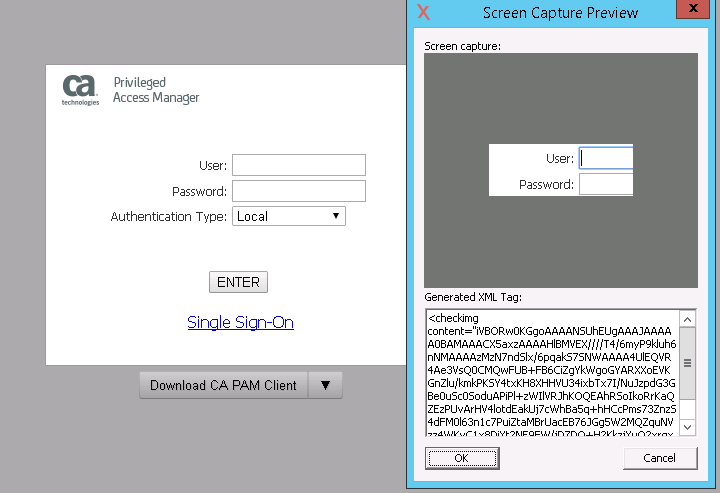
Clicking the Sleep icon will open a window prompting you to enter the duration. This field is in milliseconds. You might need this to account for the time needed to open another window.

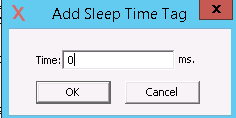
# Using Activate

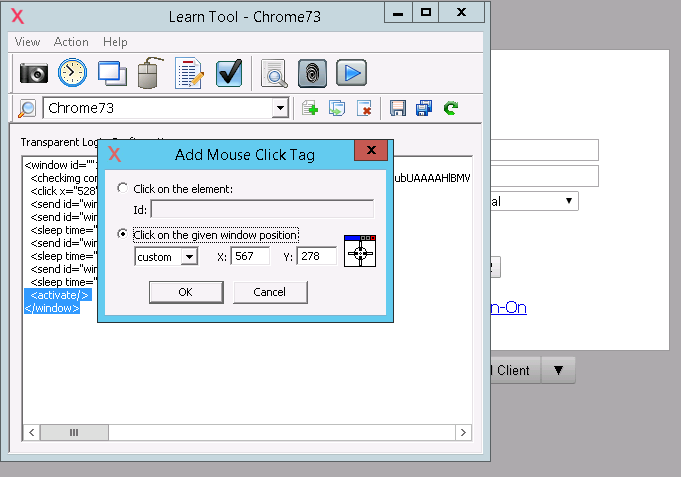
Clicking the Activate icon brings a window into focus.

# Using Mouse click

Clicking the Mouse Click icon opens a window which lets you generate a click. With “Click on the given window selection” the crosshairs icon is activated. Drag it to the position in the target window where you want the data be injected, for example the username. You might use this technique if want to use a web page that uses plugins not compatible with PAM.







# Using Text Input

Clicking Text Input icon opens a window with several options. First is the Element Type, which can be set to Text Field, Combobox, Checkbox, Radio Button or Keystrokes. Depending on what you select you may select the Value Type. In this case the Value Type is set to username. For all of these, you will have to enter the Element ID. You get this using the Control Viewer. Drag the Browse Tool over to the field you wish to identify. Copy the contents of the ID field to the Element ID and click OK. If the application you are using supports field selection using Alt-key combinations, you will be able to move to a desired field with the appropriate AutoIT string. For example, if you want to go to a field using Alt-A insert %a as keystrokes.

# Using element Verification

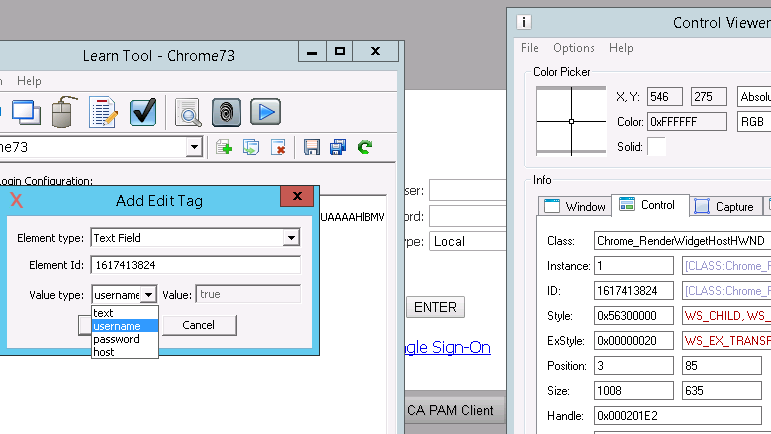
Allows insertion of a tag that confirms or denies existence of an element, and optionally that element in a specified state (for example, a text field containing a particular string). It opens a window in which you will select the Element Type, enter the Element ID and the Value.

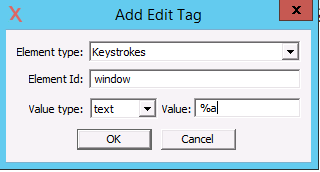
# Using the control viewer

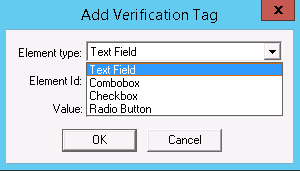
The Control Viewer was mentioned already. Here you can see the full Window Title.

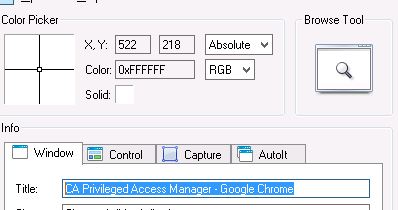
# Application Verification

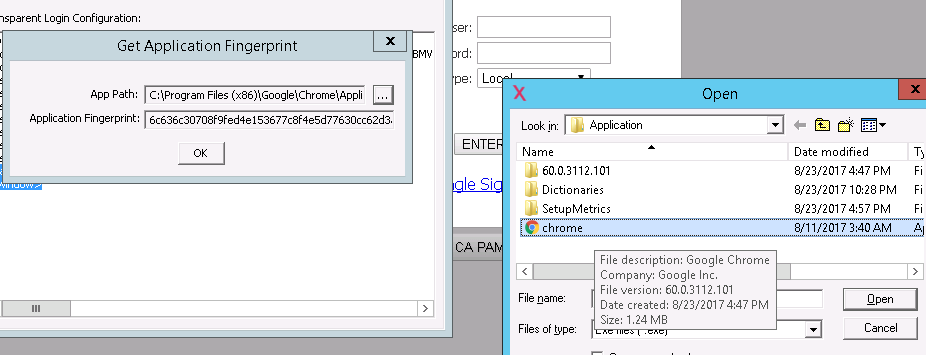
Clicking the Application Verification icon opens a window in which you will browse to the application you will be running. Selecting the program and clicking OK will populate both the App Path and Application Fingerprint.











# DEbug

Clicking Debug opens a window where you’ll browse to the program to be run. Next enter the appropriate values in the Title, Username and Password fields. You may also have to enter the IP address or FQDN in the Host field. That was not done here because this example requires https. The browser had to be opened separately and then the correct url entered , so the login screen would appear. After clicking in the username field the username and password were injected, following which the login completed.

# Transparent Login Config

You can select and edit the TL script from PAM. The Manage Transparent Login Configs window is opened from the RDP Application page. Select the one you want and make the necessary changes. It would be difficult to create a script from scratch, but simple edits are possible.

# Closing

As mentioned at the start this is document does not cover everything about Transparent Login. It should give you enough to get started with your own applications. Please contact Support if you need assistance.

