

IDIRA PLUGIN FOR RDCMAN

IMPLEMENTATION GUIDE

Version: 2.0.0

Last Updated: 7/30/2026



Table of Contents

1 Introduction.....	3
1.1 Guide Background.....	3
1.2 Terms of Use.....	3
2 Solution Overview.....	4
3 Plugin Installation and Configuration.....	5
3.1 Client Prerequisites.....	5
3.2 Plugin Installation.....	5
3.3 First Run Experience.....	6
3.3.1 Quick Start - Secure Infrastructure Access (SIA) with Privilege Cloud.....	6
3.3.2 Quick Start - Privileged Session Manager (PSM) via PAM Self-Hosted.....	6
3.4 Plugin Settings.....	7
3.4.1 Settings Storage (Persistence).....	7
3.4.2 Environment Details.....	7
3.4.3 Secure Infrastructure Access (SIA) Settings.....	8
3.4.4 Privileged Access Manager (PAM) Settings.....	8
3.4.5 Vaulted Accounts – Search Preferences.....	9
3.4.6 Vendor Mode.....	10
3.4.7 Debug Logging.....	11
3.4.8 Applying Settings via Group Policy (Registry).....	11
4 Plugin Interface and Workflows.....	13
4.1 Main Menu.....	13
4.1.1 Privileged Access Management (PAM) Embedded Portal.....	13
4.2 Authentication (Login).....	14
4.3 Idira Connection Properties.....	15
4.3.1 Connection Property Persistence.....	16
4.3.2 Pinned Accounts.....	16
4.4 Connect Server via Idira Menus.....	17
4.4.1 Privileged Session Manager (PSM) Connect - User Parameters.....	17
4.4.2 Connection Guidance.....	18
4.4.3 Account Status Icons.....	19
5 Plugin Behavior.....	20
5.1 Connecting with Local Accounts.....	20
5.2 RemoteApp and HTML5 Gateway PSM Connections.....	20
5.3 File Transfer, Redirection, Custom Ports, and Connect to Console.....	21
5.4 Idle Session Timeout and Max Session Duration.....	22
5.4.1 Customizing Session Limits.....	23
5.5 Session Concurrency (PAM Self-Hosted).....	23
5.6 Secure Infrastructure Access (SIA) RDP MFA Caching Techniques.....	24

1 Introduction

1.1 Guide Background

The contents and works depicted in this guide are derived from a non-production lab environment, aimed solely to provide information on the setup and utilization of this tool. This guide is being presented 'as is' and resources contained within including but not limited to screenshots and website links / URLs, may be subject to change. Individual experiences may vary given the uniqueness across PAM implementations as it pertains to network architecture, Safe design, and Platform design.

1.2 Terms of Use

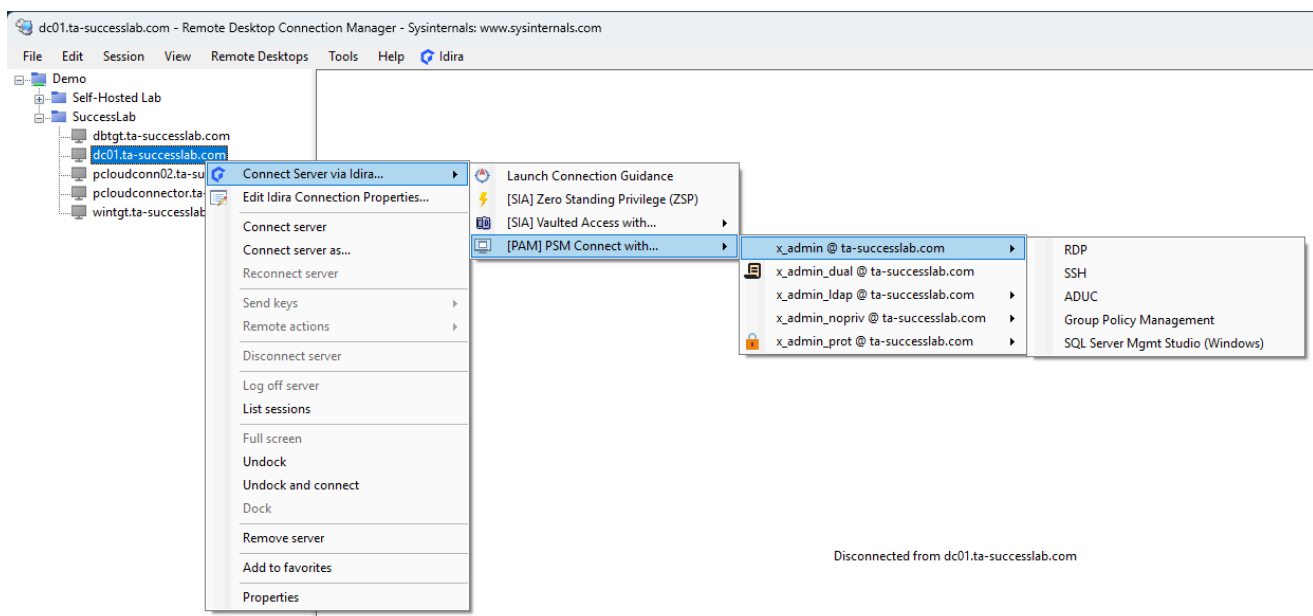
This is a Community tool which is provided 'as is', without warranties. It is not supported by Palo Alto Networks. When downloading or using the tool, users are responsible for ensuring that their environment is secured according to industry security best practices.

2 Solution Overview

Microsoft Remote Desktop Connection Manager (RDCMan) is a free and simple commercial RDP client developed by Microsoft and maintained by the Microsoft Sysinternals team. It empowers system administrators to save, group, organize, share, and simultaneously connect via RDP to a collection of server targets within hierarchical tree navigation via docked/undocked windows.

For environments secured with **Idira's Privileged Session Manager (PSM)** and **Secure Infrastructure Access (SIA)**, RDP connections must be adjusted to route through Idira infrastructure leveraging Vaulted Credentials or **Zero Standing Privilege (ZSP)**. Traditionally to accomplish this within RDCMan it is necessary to permanently alter each server target's connection criteria individually. This added overhead can place undesirable strain on administrative teams.

The Idira Plugin for RDCMan is designed to eliminate this overhead and even further reduce friction through the implementation of single sign-on techniques. The plug-in serves as a bolt-on connection accelerator through the addition of *new* right-click context menus which overlay your existing server targets, providing seamless transparent connection options via the Idira **Privileged Access Management (PAM)** and/or **Secure Infrastructure Access (SIA)** solutions, all without the need to permanently modify any existing connection settings.



This is achieved through plugin integration with **Idira Identity Security Platform (ISP)** and **Password Vault Web Access (PVWA)** RESTful APIs to inventory vaulted accounts, initiate PSM/SIA sessions, and incorporate **MFA Caching (SIA)** techniques employed by the Idira ISP. All the while offering the *entire* array of authentication methods that are supported by the Idira platforms.

3 Plugin Installation and Configuration

3.1 Client Prerequisites

- Microsoft Remote Desktop Connection Manager Version **3.11** (64-bit) or newer
- Windows 11 or newer / Windows Server 2016 or newer
- Microsoft Edge WebView2 Runtime
 - This should be pre-installed and available out of the box on **Windows 11**
 - This may need to be installed for **Windows Server 2016** or newer
- A login with access to one or more of the following Idira platforms:
 - Idira Privileged Access Management (PAM) Self-Hosted v14.0+
 - Idira Privilege Cloud ISPSS
 - Idira Secure Infrastructure Access (SIA)

3.2 Plugin Installation

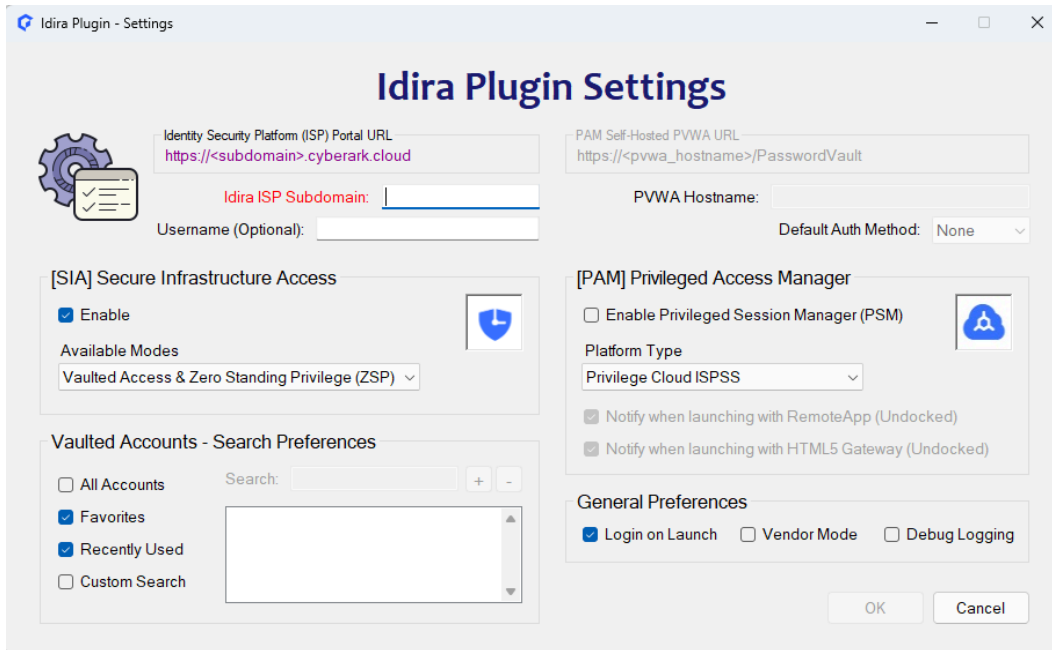
- Download the ZIP package from the Idira Marketplace
- Extract the ZIP package. The package should contain the following files:
 - `Plugin.Idira.dll`
 - `WebView2Loader.dll`
 - `Acknowledgements.txt`
 - `GPOTemplate.zip`
- Copy `Plugin.Idira.dll` and `WebView2Loader.dll` into the same directory as `RDCMan.exe`
- If present from a previous version, delete the legacy `Plugin.CyberArk.dll` file
- Launch `RDCMan.exe`

Name	Date modified	Type	Size
 RDCMan.exe	7/9/2026 8:43 AM	Application	67,035 KB
 Plugin.Idira.dll	7/29/2026 10:03 AM	Application extens...	1,422 KB
 WebView2Loader.dll	6/30/2026 4:24 AM	Application extens...	161 KB
 Acknowledgements.txt	12/17/2025 7:47 AM	Text Document	54 KB

OPTIONAL: Copy `GPOTemplate.zip` to your Domain Controller, extract, and place the `IdiraRDCManPlugin.admx` and `en-US\IdiraRDCManPlugin.adml` files into `C:\Windows\PolicyDefinitions` (or your [Central Store](#)) to manage your plugin settings via Group Policy!

3.3 First Run Experience

Upon first launch, you will be automatically greeted with the Idira Plugin Settings window. The default settings arrangement (shown below) assumes a SIA preference on the Idira ISP / Privilege Cloud platform however these can be freely adjusted as needed. **All settings include a hover tooltip that explains their purpose and behavior.**



3.3.1 Quick Start - Secure Infrastructure Access (SIA) with Privilege Cloud

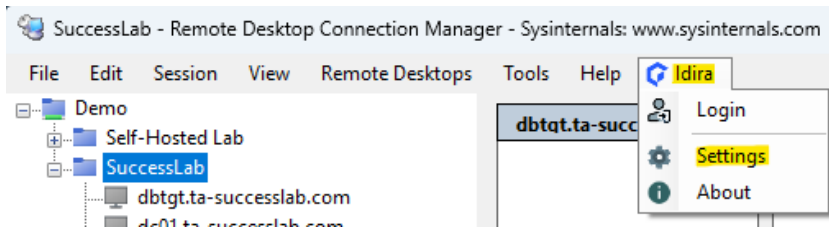
1. Supply your IdiraISP **Subdomain** in the field provided in the top-left
2. **[OPTIONAL]** Adjust the **Vaulted Accounts – Search Preferences** as desired
3. Click **OK**
4. Click the **Idira** menu, then **Login**

3.3.2 Quick Start - Privileged Session Manager (PSM) via PAM Self-Hosted

1. Uncheck the **Enable** checkbox under the **SIA Settings**
2. Check the **Enable Privileged Session Manager (PSM)** checkbox under the **PAM Settings**
3. Select **PAM Self-Hosted** in the **Platform Type** drop-down under the **PAM Settings**
4. Supply your **Password Vault Web Access (PVWA) Hostname** in the top-right field
5. **[OPTIONAL]** Set your desired **Default Auth Method for PAM**
6. **[OPTIONAL]** Adjust your **Vaulted Accounts – Search Preferences** as desired
7. Click **OK**
8. Click the **Idira** menu, then **Login**

3.4 Plugin Settings

The settings page can always be reached from within the new Idira menu:



3.4.1 Settings Storage (Persistence)

Clicking **OK** on the **Settings** window for the first time will generate a new configuration file named `Plugin.Idira.dll.config`. All future adjustments made to the **Settings** window will be written in this file as well. This allows you to standardize on default **environment details** and **available products / modes** by setting them once, then distributing the resultant configuration file along with plugin DLL files to end user and vendor teams. Settings may also be inherited from the Registry (see section [3.4.8](#)).

NOTE: If a legacy `Plugin.CyberArk.dll.config` file exists in the directory, settings will be automatically converted and imported to the `Plugin.Idira.dll.config` file upon startup.

3.4.2 Environment Details

Each section pertaining to the environment details at the top of the **Settings** window, will activate based on what's required for a given configuration state within the plugin.

For the following configuration states which depend upon the Idira ISP platform:

- ✓ SIA is enabled
- ✓ PSM is enabled and Platform Type is set to Privilege Cloud ISPSS

The **left-hand properties** will activate requiring information about your **Idira ISP** tenant:

Identity Security Platform (ISP) Portal URL <code>https://successlab.cyberark.cloud</code>	PAM Self-Hosted PVWA URL <code>https://<PVWA_Hostname>/PasswordVault</code>
Idira ISP Subdomain: successlab	PVWA Hostname:
Username (Optional):	Default Auth Method: None

Idira ISP Subdomain (Mandatory) – Your Idira ISP subdomain

Username (Optional) – If supplied, will automate ISP username entry on the login page. This can be useful for external IdP configurations to enable a more natural authentication flow.

For the following configuration states which depend upon the Idira PAM Self-Hosted platform:

- ✓ PSM is enabled and Platform Type is set to PAM Self-Hosted

The **right-hand properties** will activate requiring information about your **PAM Self-Hosted** system:

Identity Security Platform (ISP) Portal URL https://successlab.cyberark.cloud	PAM Self-Hosted PVWA URL https://pvwa.idra.lab/PasswordVault
Idira ISP Subdomain: successlab	PVWA Hostname: pvwa.idra.lab
Username (Optional):	Default Auth Method: SAML

PVWA Hostname (Mandatory) – The DNS hostname or IP address for your Password Vault Web Access (PVWA) instance or Load Balancer DNS alias or VIP.

Default Auth Method (Optional) – When set to any value other than **None**, will engage the selected authentication method by default. When set to **None**, you will be delivered to the PVWA landing page where you can freely select an authentication method.

And for the following that depend upon *both* the Idira ISP and PAM Self-Hosted platforms:

- ✓ SIA is enabled and Platform Type is set for PAM Self-Hosted

Both property regions will activate, requiring information for both environments.

3.4.3 Secure Infrastructure Access (SIA) Settings

Settings which govern SIA connection options and behavior.

[SIA] Secure Infrastructure Access

☒ Enable

Available Modes

Enable – Enables SIA connection options within the right-click context menus.

Available Modes – Allows specification of *which* SIA connection options should be available:

- ☐ Both Vaulted Access & Zero Standing Privilege (ZSP)
- ☐ Vaulted Access Only
- ☐ Zero Standing Privilege (ZSP) Only

3.4.4 Privileged Access Manager (PAM) Settings

Settings which govern PAM connection options and behavior

[PAM] Privileged Access Manager

☒ Enable Privileged Session Manager (PSM)

Platform Type

☒ Notify when launching with RemoteApp (Undocked)

☒ Notify when launching with HTML5 Gateway (Undocked)

Enable Privileged Session Manager (PSM) – Enables the PSM connection options within the right-click context menus.

Platform Type – Allows for selection of the given PAM Platform Type for the environment:

- ☐ Privilege Cloud ISPSS
- ☐ PAM Self-Hosted

Notify when launching with RemoteApp – Some PSM connection components will have RemoteApp enabled and these cannot be launched inside of the RDCMan docked stage. Instead, these connections will launch externally to RDCMan, providing the complete RemoteApp experience.

When this checkbox is **enabled**, you will receive an informational notification that an external RemoteApp launch is about to occur, giving you the option to proceed or abort the connection.

Disable this checkbox to suppress these notifications.

Notify when launching with HTML5 Gateway – When HTML5 Gateway is opted into (or forced by a given connection component or PAM configuration state), the HTML5 Gateway session must launch via your default web browser, externally to the RDCMan client.

When this checkbox is **enabled**, you will receive an informational notification that this is about to occur. When this checkbox is **disabled**, you will suppress these notifications.

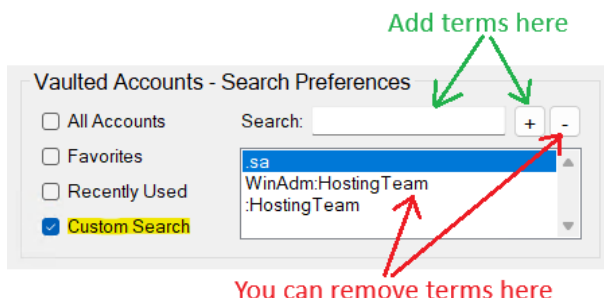
3.4.5 Vaulted Accounts – Search Preferences

The **Vaulted Accounts – Search Preferences** section of the **Settings** window allows you to tailor the PAM vaulted accounts you wish to make available for use via the plugin connection menus. The default selection assumes **Favorites** and **Recently Used** however, consider the following scenarios:

- ✓ If you have limited access to a small and precise quantity of vaulted accounts, it might be suitable to simplify by selecting **All Accounts** instead
- ✓ If you have broader account visibility within PAM – common to Vault Admins and Auditors - it might be more suitable to use **Custom Search** terms to attain specific inventory results

When specifying **Custom Search** terms, you can specify that the term is to be searched generally across all Safes, or for the term to be applied to a *specific* Safe within PAM. This can be achieved by delimiting the **Search Term** and the **Safe Name** with a **colon** character as follows:

<search_term>:<safe_name>



Examples Explained:

To search for all accounts in the entire Vault that contain **.sa** simply supply that as the search term:

.sa

To search for all accounts that contain **WinAdm** in a specific Safe called **HostingTeam** then supply:

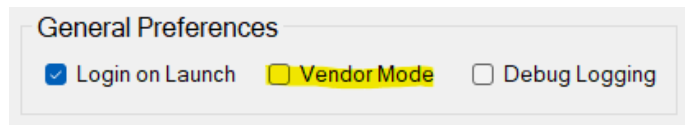
WinAdm:HostingTeam

This technique can also be applied to return **all** accounts within a particular Safe. Continuing from the example above, if you instead wished to return all results in the **HostingTeam** Safe, then supply:

:HostingTeam

Terms can also be added with the **Enter** key and removed (after highlight) with the **Backspace** key and can be further combined with **Favorites** and **Recently Used** if so desired. Finally, you can generally exclude local accounts from this search criteria as these are natively retrieved just in time.

3.4.6 Vendor Mode



For Idira ISP (SIA-ZSP and Privilege Cloud) environments ONLY, this plugin provides the option to utilize the vendor authentication flow through Idira Remote Access!

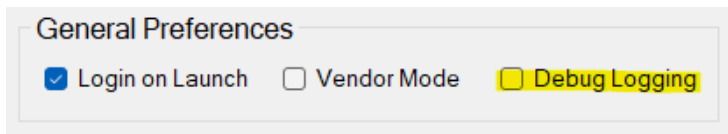
Engaging the Vendor Mode check box will automatically make the following Settings adjustments:

- The Idira ISP **Subdomain** is no longer required and grayed out
- The PAM **Platform Type** is set and locked to **Privilege Cloud ISPSS**
- The **Idira ISP login URL** is automatically set to <https://portal.alero.io>
- The **Vaulted Accounts – Search Preferences** are automatically set to **All Accounts**
 - *This can still be adjusted as desired, it's just a default state*

When login to the plugin is initiated in this mode, you will be greeted with the familiar Remote Access screen where you would scan the QR code with your Idira Mobile App and proceed through the authentication flow into the desired company and tenant, just as you normally would.

NOTE: If the tenant is affiliated with a Remote Access datacenter that is different than **US & Worldwide**, you can freely switch to the intended datacenter from the top-right drop-down at the beginning of the authentication flow.

3.4.7 Debug Logging



Recommended State under Normal Conditions – Disabled (Unchecked)

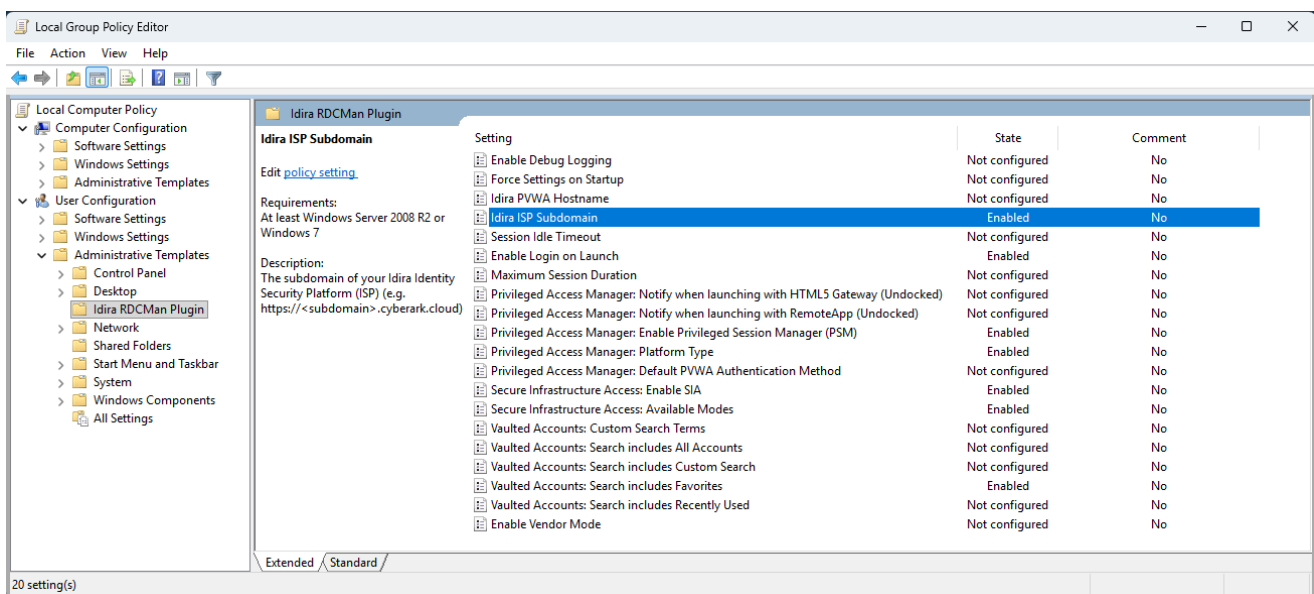
This plugin is equipped with an information rich logging implementation which under normal circumstances, should remain disabled. Should an unexpected issue or behavior be encountered with the plugin, these logs can be a great help towards identifying the root cause.

Regardless of the debug logging setting state, a log file named `Plugin.Idira.log` will be automatically generated in the same directory as the RDCMan client and DLL files when the plugin is loaded for the first time. When debug logging is disabled, only plugin startup and shutdown events will be written to this log file.

CAUTION: When Debug Logging is enabled, the log may contain information considered to be **sensitive** to include tenant names/IDs, Idira environment URLs, hostnames, domain names, IP addresses, and usernames. Never post the debug log file to public discussion boards or Discord channels. The log file should only ever be shared to trusted parties and transmitted through secure means. Verbose debug logs should be promptly deleted or otherwise securely stowed when no longer needed.

3.4.8 Applying Settings via Group Policy (Registry)

Most named settings found within `Plugin.Idira.dll.config` can be alternatively read in from the client's Registry. This allows you to proactively seed environmental settings and preferences for your teams via Group Policy (using the provided ADMX template, see section [3.2 Plugin Installation](#) for details) or Microsoft Intune.



Registry Key: [HKCU>HKLM]\SOFTWARE\Policies\Palo Alto Networks\Idira\RDCManPlugin

REG Value Name	REG Value Type
DebugLogging	REG_DWORD
IdiraSubdomain	REG_SZ
IdiraPvwaHostname	REG_SZ
LoginOnLaunch	REG_DWORD (Decimal)
NotifyHtml5	REG_DWORD (Decimal)
NotifyRemoteApp	REG_DWORD (Decimal)
PAMEnabled	REG_DWORD (Decimal)
PAMType	REG_DWORD (Decimal)
PVWAAuthMethod	REG_SZ
SIAEnabled	REG_DWORD (Decimal)
SIAModes	REG_DWORD (Decimal)
VaultSearchIncludeAll	REG_DWORD (Decimal)
VaultSearchIncludeFavorites	REG_DWORD (Decimal)
VaultSearchIncludeRecently	REG_DWORD (Decimal)
VaultSearchIncludeCustom	REG_DWORD (Decimal)
VaultSearchCustomTerms	REG_SZ
VendorMode	REG_DWORD (Decimal)

By default, settings that are pre-existing in the local config file will take precedence even if the same setting is configured in the Registry. If you wish to override local config file settings on plugin startup, you may force one-time application of settings from the Registry by optionally defining the following additional Value:

Value Name: ForceSettingsOnStartup

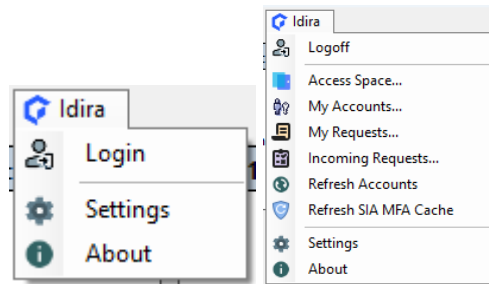
Value Type: REG_DWORD (Decimal)

Value Data: 1

4 Plugin Interface and Workflows

4.1 Main Menu

The plugin's main menu serves as the primary interface for plugin settings, login/logoff, along with the ability to directly visit your PAM portal(s) post-login when the configuration state includes Vaulted access options. The status and available options in this menu will change depending on plugin settings and login state.

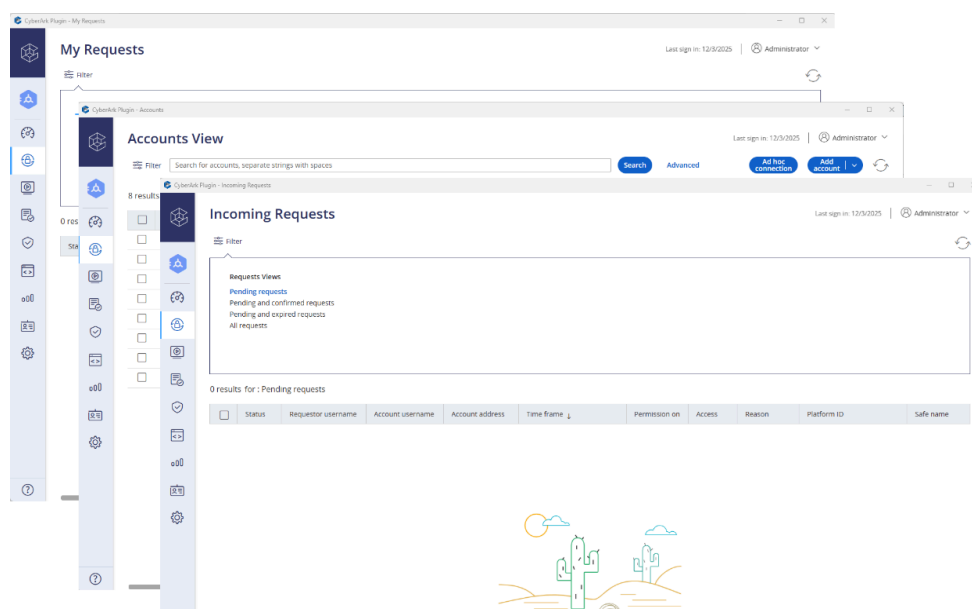


4.1.1 Privileged Access Management (PAM) Embedded Portal

When a configuration state which involves Vaulted Access is set within plugin settings, the post-login main menu will contain items for **Access Space (ISP-Only)**, **My Accounts**, **My Requests**, and **Incoming Requests**. These launch a modern embedded web browser that is based on Microsoft Edge, navigating to your respective ISP or Password Vault Web Access (PVWA) portal environment.

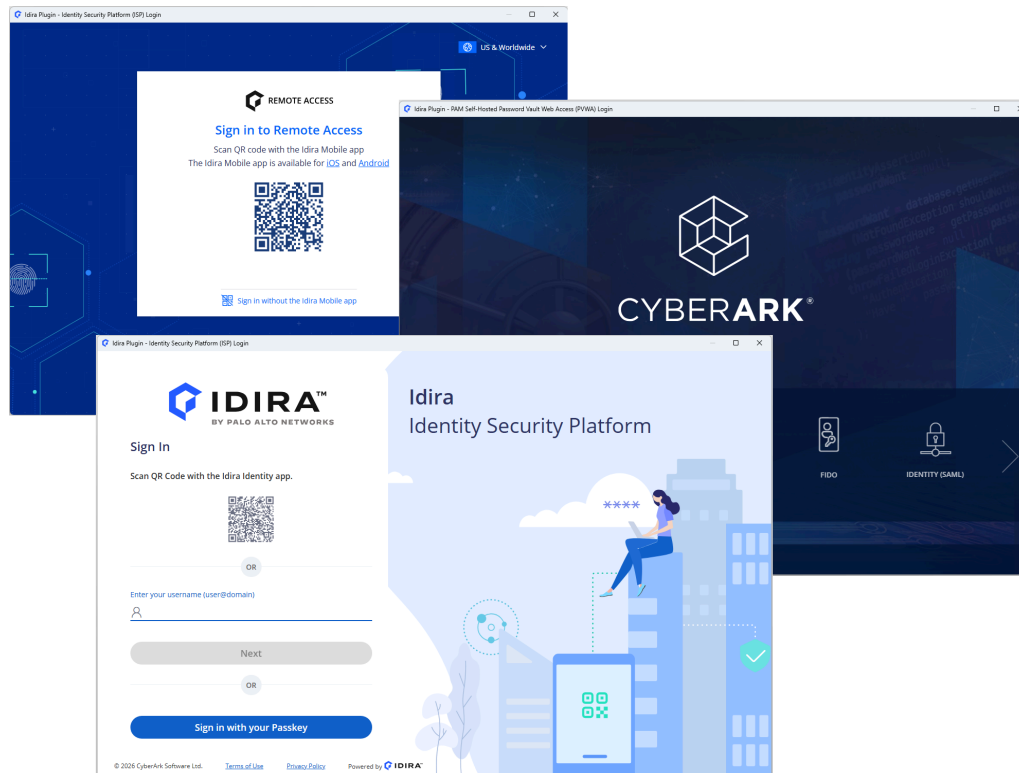
These are designed to provide you with the optional yet direct means to conveniently search and browse accounts you have access to, designate favorite accounts, check-in exclusive accounts, submit Dual Control requests, approve Dual Control requests, or other administrative tasks.

This window is tethered to RDCMan and a maximum of one (1) window can be held open at a time.



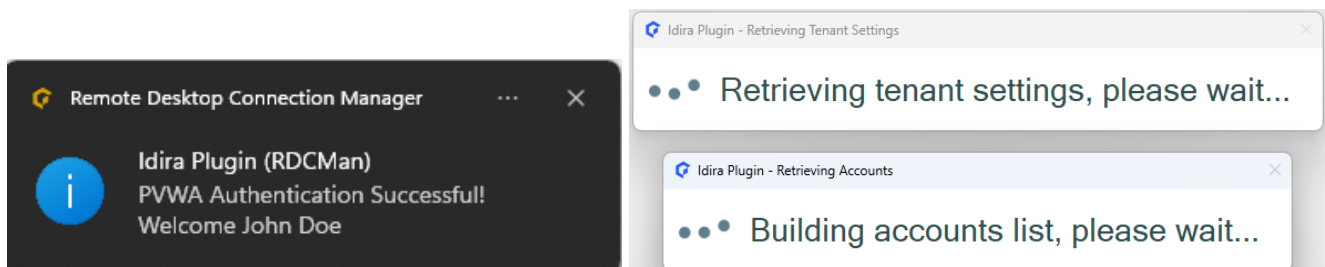
4.2 Authentication (Login)

Clicking **Login** from the main menu or right-click context menus, will launch the plugin authentication flow. This flow leverages a modern embedded browser experience based on Microsoft Edge, designed to navigate your configured auth portal. This would be Idira Identity for Privilege Cloud and Secure Infrastructure Access (SIA), the Password Vault Web Access (PVWA) for PAM Self-Hosted, or Remote Access for Vendor Mode.



All authentication methods that are configured or enabled for your given platform and Idira login are viable through the plugin. Upon successful authentication, the embedded browser window will automatically close, and a **toast notification** (example shown below) will appear indicating so.

Plugin session initialization will automatically begin following authentication. This involves building the vaulted accounts list based on your **Vaulted Accounts – Search Preferences** (if applicable) as well as the retrieval of tenant settings for SIA MFA Caching (if applicable), both also shown below.

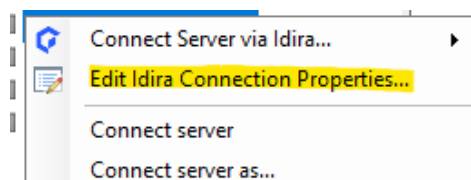


4.3 Idira Connection Properties

There will often be occasions where it's desirable or otherwise necessary to specify certain PSM or SIA connection settings that should apply over the entire environment, just a group of server targets, or specific individual server targets.

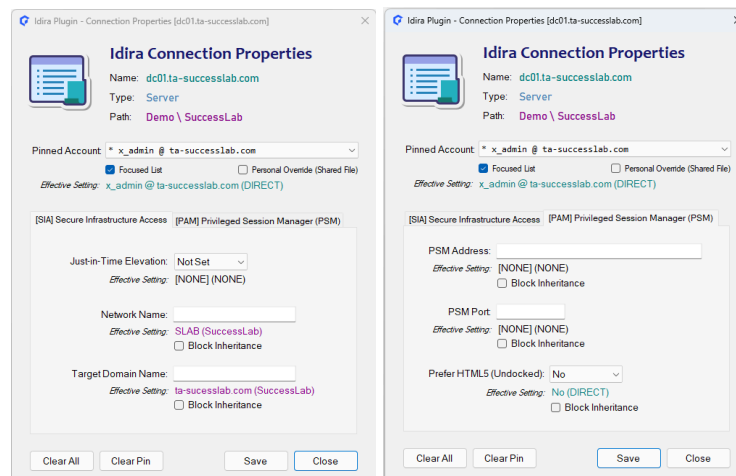
To address all scenarios, this plugin is equipped with a hierarchical settings scheme that allows you to define connection properties at the root, group, or target server levels. Settings defined at the root or a group level, will *propagate* to all child groups and sever targets underneath it. Settings defined closest to the server target will always take precedence, and inheritance can be strategically blocked.

Right clicking the RDG root, a group (excluding smart group), or server target node, will present an **Edit Idira Connection Properties...** menu option.



This dialog window that is shown provides information on the node being edited, the current value for any properties that have been defined *directly* on that node, along with the *effective settings* that might be applying to that node as inherited from a *parent node in its path*. The effective settings are color coded for quick visual reference of their setting source.

In the example shown below, a server target node named **dc01.ta-successlab.com** has the **x_admin** pinned account set directly on this node, inheriting the SIA Network Name of **SLAB** from a parent node (SuccessLab), inheriting the SIA domain name of **ta-successlab.com** from the root node (**Demo**), and PSM HTML5 preference of **No** is also set directly on this node.



The respective settings **tabs** shown above for **[SIA] Secure Infrastructure Access** or **[PAM] Privileged Session Manager (PSM)** will only be visible when their underlying product is functionally enabled from within plugin settings. In other words, if you disable SIA in plugin settings, you will not see the SIA tab within the connection properties dialog window, and vice-a-versa.

4.3.1 Connection Property Persistence

Settings defined on a node via the **Edit Idira Connection Settings** dialog window are appended to the node's comment property in the following format:

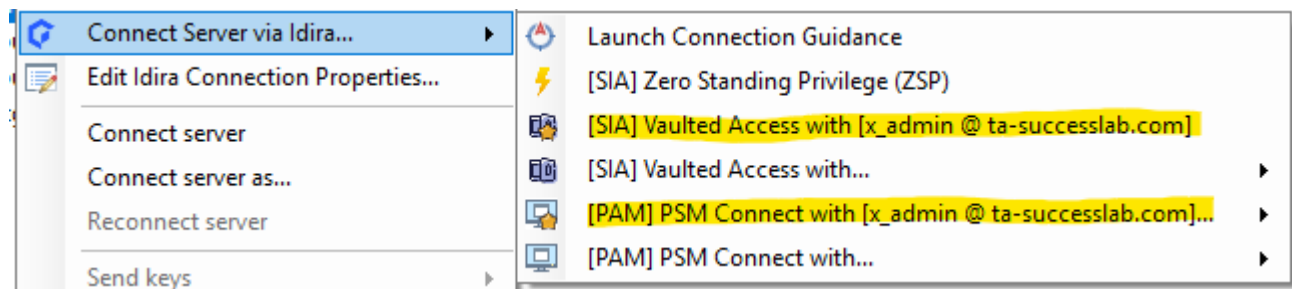
```
idira:<setting_name>:<setting_value>
```

As a result, to save any changes made via this dialog window, you should save the underlying **.rdg** file by going to **File > Save Filename.rdg**. This also means that RDG files can be shared amongst a team, or to a Vendor, and its Idira connection properties will remain intact.

NOTE: Although these raw comment values *may* be manipulated directly, it is best to keep within the connection settings dialog window for making edits, and more easily observing the effective settings.

4.3.2 Pinned Accounts

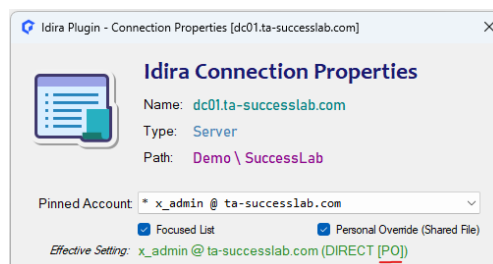
In situations where there is a specific account that is preferred or frequently utilized for connections to a given target or group of targets, you can establish that account as a **Pinned Account** on the node. Doing so will introduce new quick-connect options (denoted with a star icon) from the right-click context menu that allow you to rapidly launch sessions and save on sub-menu fatigue.



Particularly for team-shared RDG files, it may become useful or necessary to set *individual* account pins (such as for a personal privileged account) that you would not want to be written to the shared RDG file. In these scenarios, individual members can check the **Personal Override (Shared File)** checkbox which will apply the pin through their individual plugin configuration file instead.

Hierarchical precedence applies, so pins set at a server target level have precedence over pins set at a parent group or root level. And **Personal Override** pins have precedence over standard pins.

You can visually identify a Personal Override pin by effective setting trailing with the designation of **[PO]** (and be colored **green** if set direct) as shown here:



The **Clear Pin** button at the bottom of the **Connection Properties** form will prompt individually for options to clear a Personal Override (config file) pin, and a standard (RDG file) pin, when present.

4.4 Connect Server via Idira Menus

The right-click context menu on a server or group target will supply different sub-menu options depending on which products are enabled in the plugin settings, and the node type that is selected.

Server nodes may include one or more sub-menus for **Connection Guidance**, **[SIA] Zero Standing Privilege**, **[SIA] Vaulted Access**, and **[PAM] PSM Connect**.

Connect with... options will contain a list of accounts which were collected post-authentication based on your configured **Vaulted Accounts – Search Preferences**. The immediate sub-menu will favor a **focused list** of accounts that were identified as being local (matching address) or of the same domain as the target address. For server targets entered with an IP address, this accounts list will be flat.

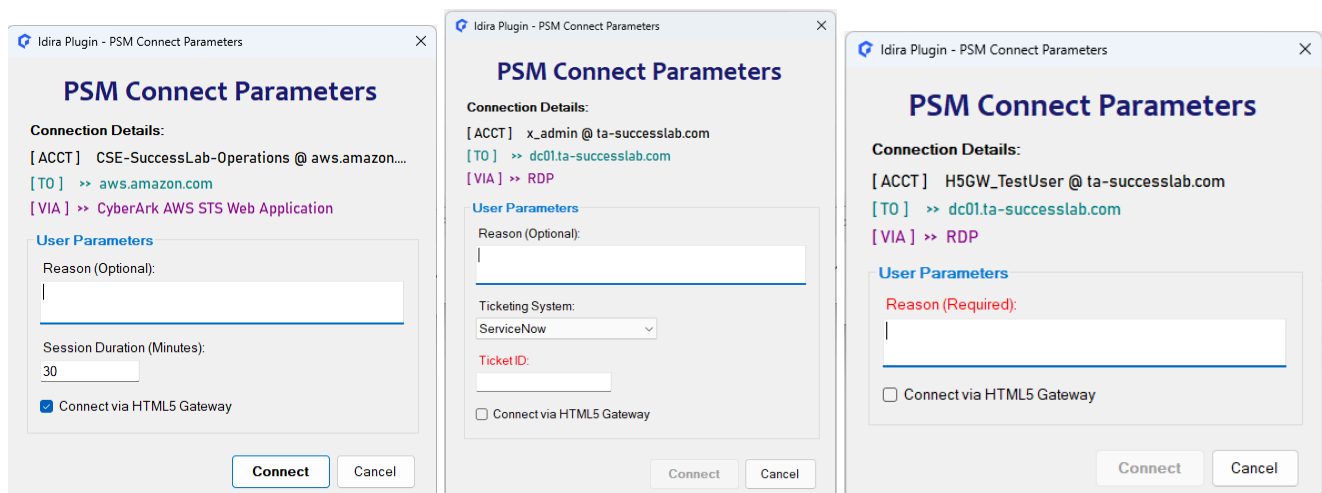
Group nodes (including Root, Virtual Groups, and Smart Groups) also offer the ability to launch a **group** connection to all child server targets under that node. For group connections, you can select an account to utilize for all server targets or infer the **effective pinned** account that would resolve on each child server target. And for **effective pinned** group launches, if a target lacks an account pin or the pinned account does not have the selected PSM Connection Component assigned to it (for PSM group connections), the target's connection will be skipped.

CAUTION: Group connections may not be aborted once committed! You will be warned of the target count before proceeding. Particularly for PSM, it is recommended to test with a smaller group to ensure your settings are effective before expanding to larger sets and connection types.

4.4.1 Privileged Session Manager (PSM) Connect - User Parameters

As when connecting via Privilege Cloud / Password Vault Web Access (PVWA), certain Connection Components may prompt the end user for additional input. This might include things such as **Ticketing System Integration**, **Mandatory Reason**, the toggle for connecting via **HTML5 Gateway**, or any other bespoke user parameter that are applied through Idira PAM configuration.

When such required parameters are present on a connection component (or otherwise required by Master Policy or Platform configuration), the plugin will prompt the end user for more information, and required fields will be highlighted red. Various examples of this prompt can be seen below:



The image displays three examples of the 'Idira Plugin - PSM Connect Parameters' dialog box. Each window has a title bar with the Idira logo and the text 'Idira Plugin - PSM Connect Parameters'. The main content area is titled 'PSM Connect Parameters'.

- Left Window:** Shows 'Connection Details' with fields for [ACCT] (CSE-SuccessLab-Operations @ aws.amazon...), [TO] (aws.amazon.com), and [VIA] (CyberArk AWS STS Web Application). Under 'User Parameters', there is a 'Reason (Optional):' text box, a 'Session Duration (Minutes):' spinner set to 30, and a checked checkbox for 'Connect via HTML5 Gateway'. 'Connect' and 'Cancel' buttons are at the bottom.
- Middle Window:** Shows 'Connection Details' with [ACCT] (x_admin @ ta-successlab.com), [TO] (dc01.ta-successlab.com), and [VIA] (RDP). Under 'User Parameters', there is a 'Reason (Optional):' text box, a 'Ticketing System:' dropdown set to 'ServiceNow', a 'Ticket ID:' text box, and an unchecked checkbox for 'Connect via HTML5 Gateway'. 'Connect' and 'Cancel' buttons are at the bottom.
- Right Window:** Shows 'Connection Details' with [ACCT] (H5GW_TestUser @ ta-successlab.com), [TO] (dc01.ta-successlab.com), and [VIA] (RDP). Under 'User Parameters', the 'Reason (Required):' text box is highlighted in red, and the 'Connect via HTML5 Gateway' checkbox is unchecked. 'Connect' and 'Cancel' buttons are at the bottom.

Depending on your environment and connection type, there may be no User Parameters prompt at all. And in situations where HTML5 Gateway selection might be the *only* parameter which would trigger a prompt, your preemptive HTML5 Gateway preference can be installed via the **Edit Idira Connection Properties** dialog, which will supersede (and effectively allow you to bypass) the prompt.

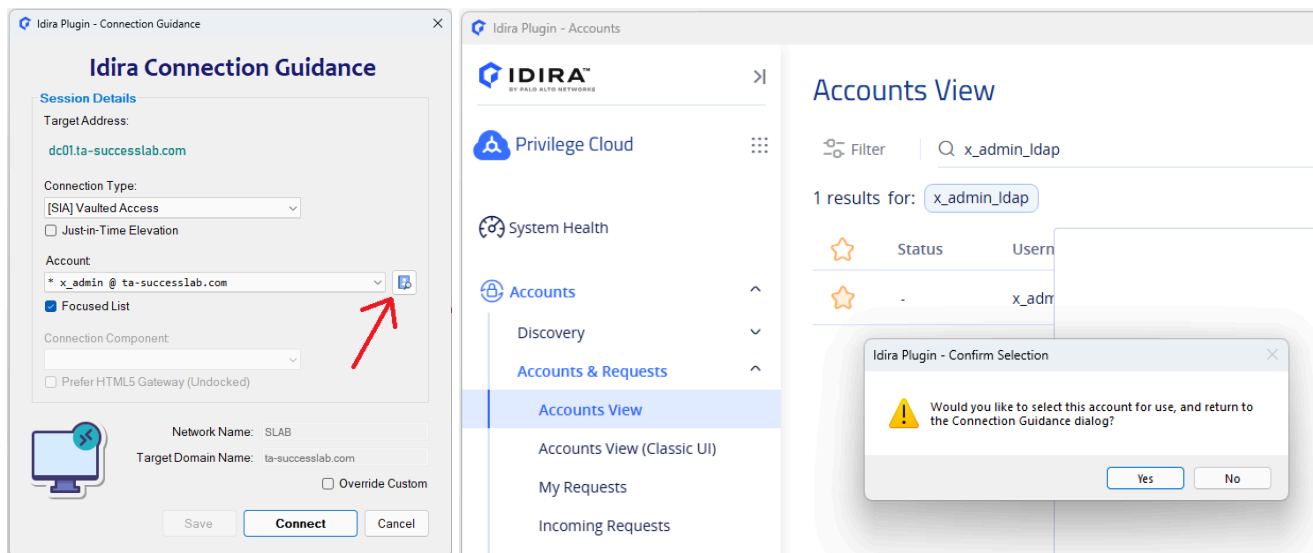
4.4.2 Connection Guidance

Between **Idira Connection Properties** and the other quick connect menus, there is a good degree of flexibility for how to leverage the plugin. A **Launch Connection Guidance** option exists in the sub-menus mostly out of convenience, primarily to help facilitate a couple of possible scenarios:

1. Certain products and connection modes may require special connection criteria that are foreign to you. **Connection Guidance** can help with visualizing the required data points.
2. There may be “one-off” or less frequent needs to connect with different accounts (perhaps ones not normally in your accounts list), and/or while using different connection criteria, and you don’t want the inconvenience of having to edit (and revert) **Idira Connection Properties** each time you need to do so.

Connection Guidance will provide a dialog window where you can make the single-use selections for which product / method you wish to use to connect with, which vaulted account (when applicable), and which PSM Connection Component (when applicable).

Connection Guidance will pre-populate any settings that are applied through **Idira Connection Properties** (as shown below), and offers a **Save** button in case there are connection properties you *do* want to save on the target server node. It also provides a means of performing **an ad hoc lookup of a vaulted account** that is not in the plugin’s compiled account list (based on your plugin settings search criteria). This launches your PAM portal (My Accounts); simply click an account entry and the plugin will interpret the selection prompting for confirmation.



4.4.3 Account Status Icons

Accounts within **connect/access with...** menus will visually indicate special status icons:

Pinned accounts are designated with 

Exclusive accounts which are checked out by another user are designated with 

- **NOTE:** The mouse-over tooltip for these accounts will also indicate *who* has it checked out

Exclusive accounts which are checked out by *you* are designated with 

Dual Control protected accounts which **require an access request** are designated with 

Dual Control protected accounts with an access request **pending approval**, are designated with 

Dual Control protected accounts which you **have an active approval** to use, are designated with 

Local Accounts – vaulted account's address matches the server target - are designated with 

These account status icons (except for pinned) will not automatically update once the accounts list has been established. If you expect the status for one or more of the accounts in your list to have changed (i.e. you were just approved via Dual Control for access), you can refresh the status of all accounts by selecting the main **Idira Menu > Refresh Accounts**.

5 Plugin Behavior

5.1 Connecting with Local Accounts

Connecting with local accounts is functionally identical to all others. The fundamental difference, and primary challenge, is the factor of scale. It would provide for a practically unworkable experience if the plugin's **Connect/Access With...** menus were populated with hundreds or thousands of arbitrary local accounts. And for this reason, your **Vaulted Accounts – Search Preferences** should also generally **exclude** local accounts wherein possible.

To facilitate the use of local accounts, this plugin features an automatic local account lookup and listing within the menus. At the time of a server target right click, the plugin will automatically trigger an inexpensive asynchronous background task that does the following:

- Conducts a best-effort DNS forward/reverse lookup of the target server address
- Adds all DNS results (if any) to a search list
- Checks an established **local account cache** for each result in the search list
- If cached results exist, add them to the **Connect/Access With...** menus
- If cached results do not exist, conduct an API lookup for accounts whose address property matches any term in the search list, add these accounts to the local account cache, and add these accounts to the **Connect/Access With...** menus

In simpler terms, the plugin will automatically conduct a cache-optimized, DNS-enhanced, just in time look up, presenting your local account options for a given server target, in real time.

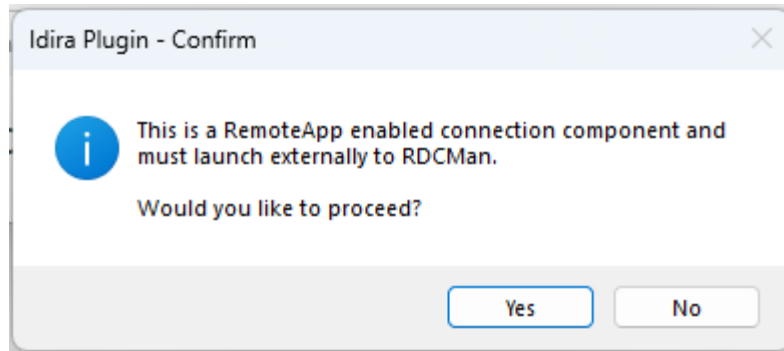
NOTE: An accounts list refresh from **Idira Menu > Refresh Accounts**, will clear the local accounts cache. This is perfectly fine and will result in a local accounts cache rebuild over time.

5.2 RemoteApp and HTML5 Gateway PSM Connections

RemoteApp is a Microsoft technology provided through **Remote Desktop Services (RDS)**, that allows applications to be virtualized and presented to an end user over an RDP session. This provides a look and feel experience as though the application were running on the local desktop, wherein in reality it's being hosted remotely via an RDS server.

For **non-RDP based** Connection Components, **Idira Privileged Session Manager (PSM)** implements RemoteApp to provide these components with the same native app experience. Due to limitations with the RemoteApp implementation, connection components which are RemoteApp enabled *cannot* be launched within the docked stage of RDCMan and **must be launched externally** to the RDCMan client, just as they would be if initiated directly from the respective PAM Portal.

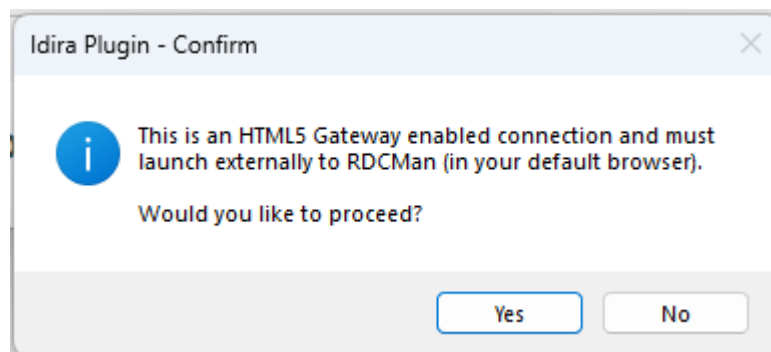
This plugin will facilitate the external launch and will present an informational notice to the end user that they may accept or decline, when this external launch is about to take place.



NOTE: If you wish for RemoteApp enabled connection components to be usable within the docked stage in RDCMan, contact your **Idira Administrator** to have the connection component (or platform level override) modified with the **DisableRemoteApp** component parameter set to **Yes**.

Your PAM environment may employ an HTML5 Gateway which allows connections through the Idira PSM via a web browser. For connection components which are enabled for **HTML5 Gateway** and engaged, the session cannot be launched inside of the docked stage of RDCMan and must be launched externally to the RDCMan client.

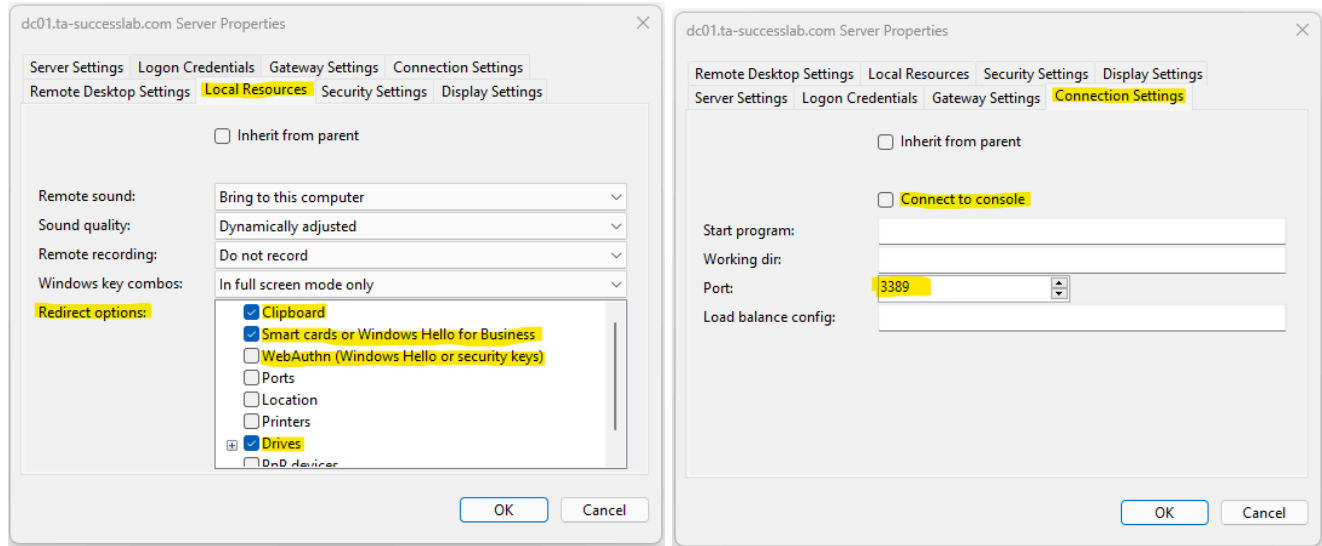
This plugin provides this ability and will **automatically facilitate launch of the HTML5 Gateway session in your default web browser**. And given this is an external launch, the end user will also receive an informational notice which they can accept or decline.



5.3 File Transfer, Redirection, Custom Ports, and Connect to Console

The **Idira Privileged Session Manager (PSM)** and **Secure Infrastructure Access (SIA)** both provide capabilities for file transfer, clipboard redirection, and other select resource redirections. Additionally, PSM provides the ability to connect to the RDP console session, and SIA provides the ability to specify a custom RDP port for the target server.

To utilize any of these features, **simply enable them in RDCMan just as you normally would** by opening the standard properties of your server target (or a parent group node), and configuring your redirect options on the **Local Resources** tab or console/port options on the **Connection Settings** tab:

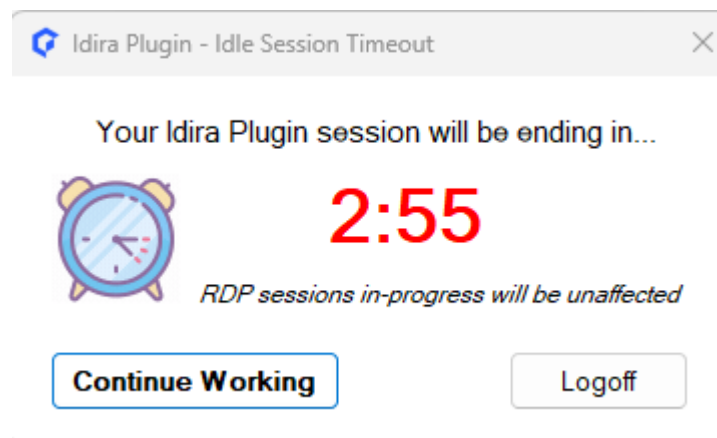


NOTE: The Idira PSMs and their Connection Components must still be configured to allow drive redirection and console access! Drive redirection is enabled through the **AllowMappingLocalDrives** user parameter. Console access is enabled through the **AllowConnectToConsole** user parameter.

5.4 Idle Session Timeout and Max Session Duration

This plugin implements an independent session timeout feature which tracks general activity within the RDCMan client window and transparently keeps the plugin session alive so long as you remain active within the RDCMan client window.

Should you become inactive for **20 minutes** (by default), a **3-minute countdown** will appear, providing one final opportunity to keep the session alive.



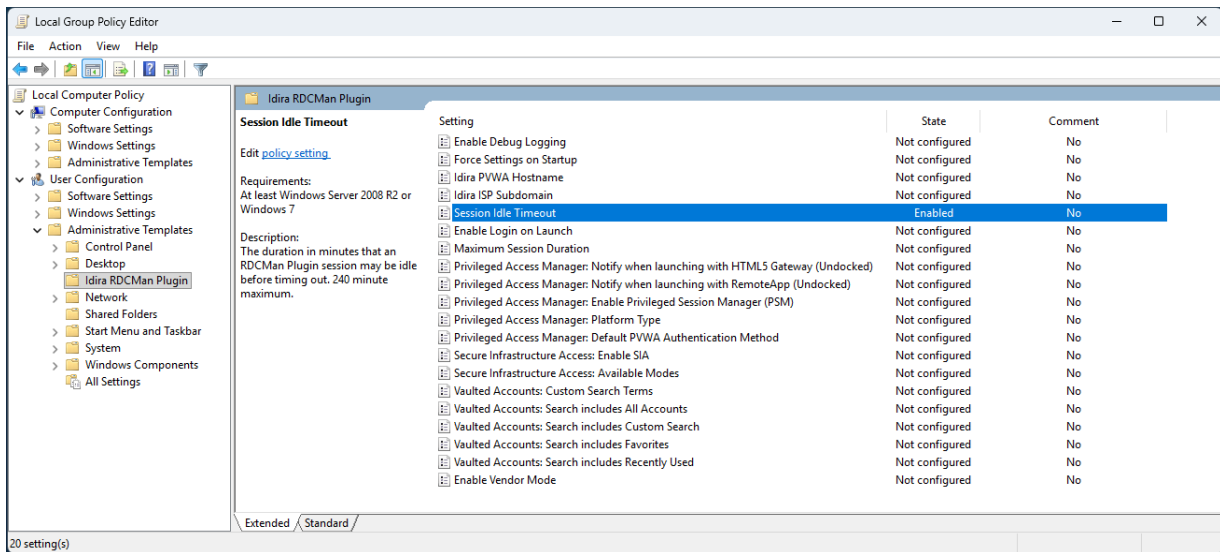
Clicking **Continue Working** will maintain the plugin session and reset the idle timer. Clicking **Logoff** or otherwise letting the countdown timer expire, will result in a logoff of the plugin session.

An active plugin session can endure a maximum contiguous timespan of **16 hours** (by default) before being forced to re-authenticate to the plugin, regardless of activity.

5.4.1 Customizing Session Limits

Both Idle session timeout and max session duration can be customized, allowing alignment with individual security teams and operational comfort. This is accomplished through Registry values under either the HKEY_CURRENT_USER (User Configuration) or the HKEY_LOCAL_MACHINE (Computer Configuration) Registry hives, in that order of precedence. This enables per-user or per-device governance through Group Policy (using the provided ADMX template, see section [3.2 Plugin Installation](#) for details) or Microsoft Intune.

Example of the User Configuration policy tree in Group Policy Editor with the provided custom ADMX template, is shown below:



Registry Key: [HKCU>HKLM]\SOFTWARE\Policies\Palo Alto Networks\Idira\RDCManPlugin

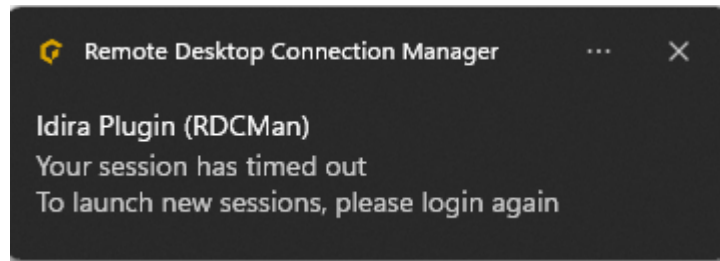
REG Value Name	REG Value Type	REG Value Data
IdleTimeout	REG_DWORD (Decimal)	1-240 (minutes)
MaxSessionDuration	REG_DWORD (Decimal)	1-2880 (minutes)

Values that exceed the maximum of **240 (4 hours)** for [IdleTimeout](#) and **2880 (48 hours)** for [MaxSessionDuration](#) will be ignored. The plugin continuously polls these registry values **every 5 minutes**, and applies all value updates immediately, including to active sessions.

5.5 Session Concurrency (PAM Self-Hosted)

The technique employed by this plugin does not allow for concurrent sessions to be taken on the PAM Self-Hosted platform. While logged into the plugin, any subsequent attempts to login to PAM Self-Hosted platform outside of the plugin, as the same user, will immediately invalidate both the plugin's session and the external session.

Occurrences of a collision will become generally apparent in the plugin upon its next API-bound activity which will fail and result in a session timeout toast notification as shown below.



It is advisable to utilize the PAM Portals (embedded browser) from within the plugin's Main Menu to conduct the intended activities, or to otherwise logoff of your RDCMan session when it's not in use.

5.6 Secure Infrastructure Access (SIA) RDP MFA Caching Techniques

This plugin will transparently optimize the best possible experience based on SIA RDP MFA Caching settings that are configured on the SIA tenant, in the following order of precedence:

RDP MFA Caching – When enabled, the plugin will automatically retrieve and maintain (background refresh) an RDP MFA Caching token for establishing SIA connections. This is the most performant option as individual session launches do not need to be preceded by an API call.

RDP File without a need to re-authenticate – When enabled, and only wherein **RDP MFA Caching** is also *disabled*, the plugin will automatically retrieve RDP files for establishing SIA connections. This is slightly less performant, as each individual session launch is preceded by an API call.

For most, RDP MFA Caching will remain out of mind as it's managed automatically by the plugin. If SSO token errors are encountered however, simply select **Refresh SIA MFA Cache** from the Idira menu to immediately refresh the cached token.

