Predict | Protect | Prevent

ARCON|PAM

Privilege Elevation and Delegation Management

arcon

Table of Contents

Disclaimer

The handbook of ARCON PAM solution is being published to guide stakeholders and users. If any of the statements in this document are at variance or inconsistent it shall be brought to the notice of ARCON through the support team. Wherever appropriate, references have been made to facilitate better understanding of the PAM solution. ARCON team has made every effort to ensure that the information contained in it was correct at the time of publishing.

Nothing in this document constitutes a guarantee, warranty, or license, expressed or implied. ARCON disclaims all liability for all such guarantees, warranties, and licenses, including but not limited to: Fitness for a particular purpose; merchantability; non-infringement of intellectual property or other rights of any third party or of ARCON; indemnity; and all others. The reader is advised that third parties can have intellectual property rights that can be relevant to this document and the technologies discussed herein, and is advised to seek the advice of competent legal counsel, without obligation of ARCON.

Copyright Notice

ARCON retains the right to make changes to this document at any time without notice. ARCON makes no warranty for the use of this document and assumes no responsibility for any errors that can appear in the document nor does it make a commitment to update the information contained herein.

Trademarks

Other product and corporate names may be trademarks of other companies and are used only for explanation and to the owners' benefit, without intent to infringe.

Sales Contact

You can directly contact us with sales related topics at the email address <sales@arconnet.com>, or leave us your contact information and we will call you back.

1 Overview

ARCON understands that security is one of the top concerns for business worldwide today, so we have built strong security features into the servers to protect the most valuable assets of organizations. We proactively work with our global ARCON partners and our cross-functional teams to determine the current and future security requirements so that our product security is always inline with the latest security trends.

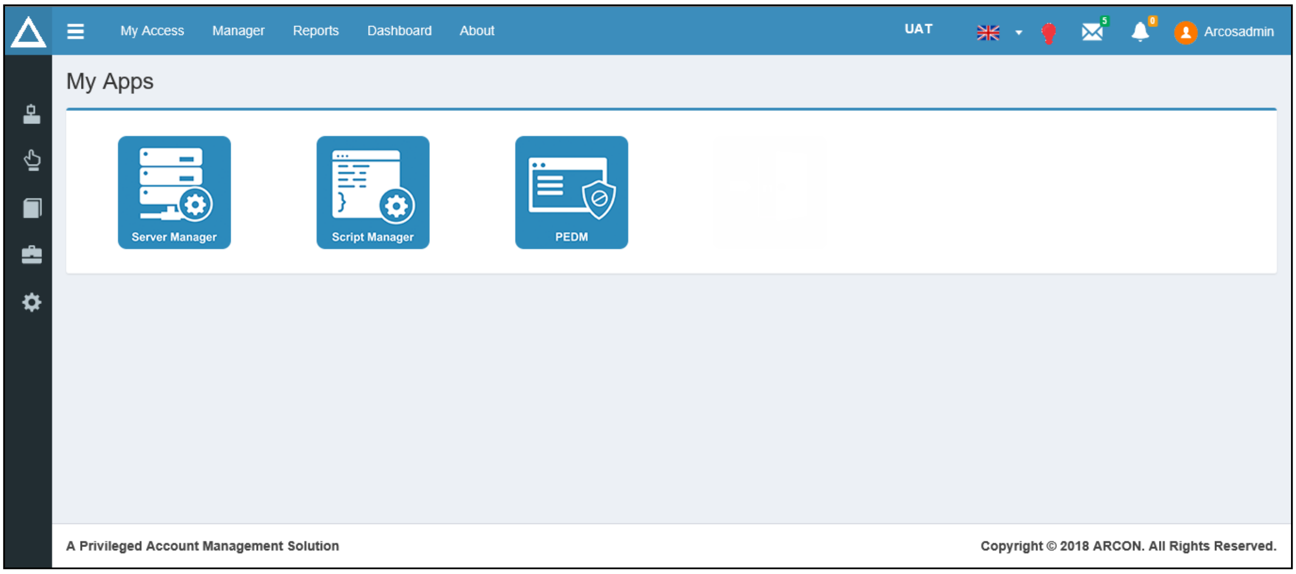
ARCON PEDM overcomes all threats hampering the organization's internal structure; It limits the scope of what administrators can do, or prevent administrators from carrying out unsafe activities that could be a vector for malware or that potentially could do great damage. Privilege Elevation and Delegation Management (PEDM) feature is introduced to elevate or restrict an application or process for an User based on his role or preference. The Users or Groups assigned to the Elevated or Restricted Profile, are those Users who have been onboarded in ARCON PAM. PEDM is supported in both Ubuntu and Windows platform. PEDM is designed to detect and prevent known cyber threats using fixed techniques, protection methodologies. Specific Processes are either elevated or restricted for users based on their job role or their requirements. PEDM will allow certain processes to be executed under elevated privileges and restrict certain process that should be restricted for the particular end user. Administrators can define policies to limit the access levels according to their requirements thus limiting the scope of any unsafe activities that could become a potential threat.

2 How to elevate/restrict an application?

You can elevate / restrict an application by adding it in Client Manager; by creating a profile for application and assigning it to a user or group of users.

To Add Application, Create Profile, Assign Profile, View Profile or View Assigned Profile, use the following path:

Client Manager → Manager → PEDM



⚠

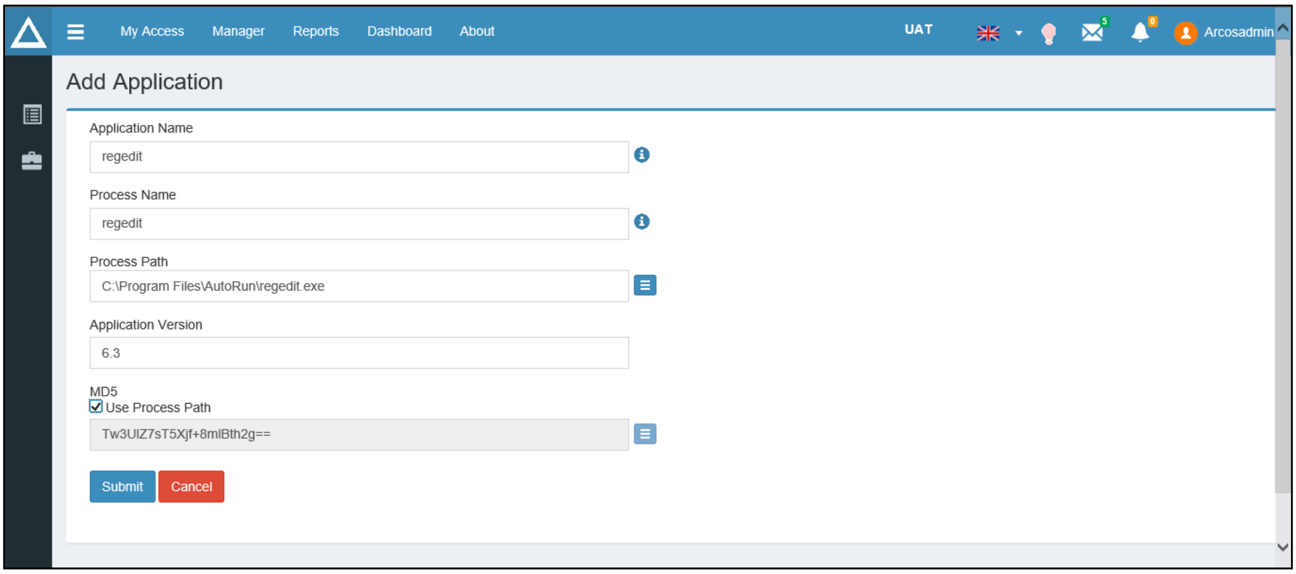
- Client User having **Manager Menu Display** and **Process Elevation & Delegation Management** privilege will be able to view **PEDM** option.
- Whereas, the Administrator having **Process Elevation & Delegation Management** privilege will be able to view **PEDM** option.

2.1 Adding an Application

This section helps you to add application in ARCON PAM by specifying the process name. You can then create profile to elevate/restrict the process.

To Add Application, use the following path:

Application (▤ **)** → Click **Add Application.** The following screen is displayed.



Add Application

Application Name: regedit

Process Name: regedit

Process Path: C:\Program Files\AutoRun\regedit.exe

Application Version: 6.3

MD5

☑ Use Process Path

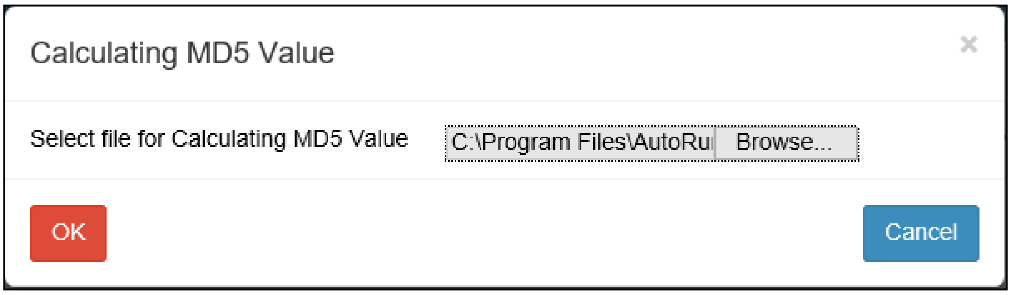
Tw3UlZ7sT5Xjf+8mlBth2g==

Submit Cancel

The **Add Application** screen contains the following fields:

Field Name	Description
Application Name	Enter the application name of the application that should be restricted or elevated.
Process Name	Enter the file name of the process. For Example: Paint.exe
Process Path	Click **Select Path** (☰) icon to browse and select the path of process.
Application Version	Enter the version number of the application.
MD5	Select **User Process Path** checkbox to calculate MD5 value or click **Calculate MD5** (☰) icon to browse and select file.

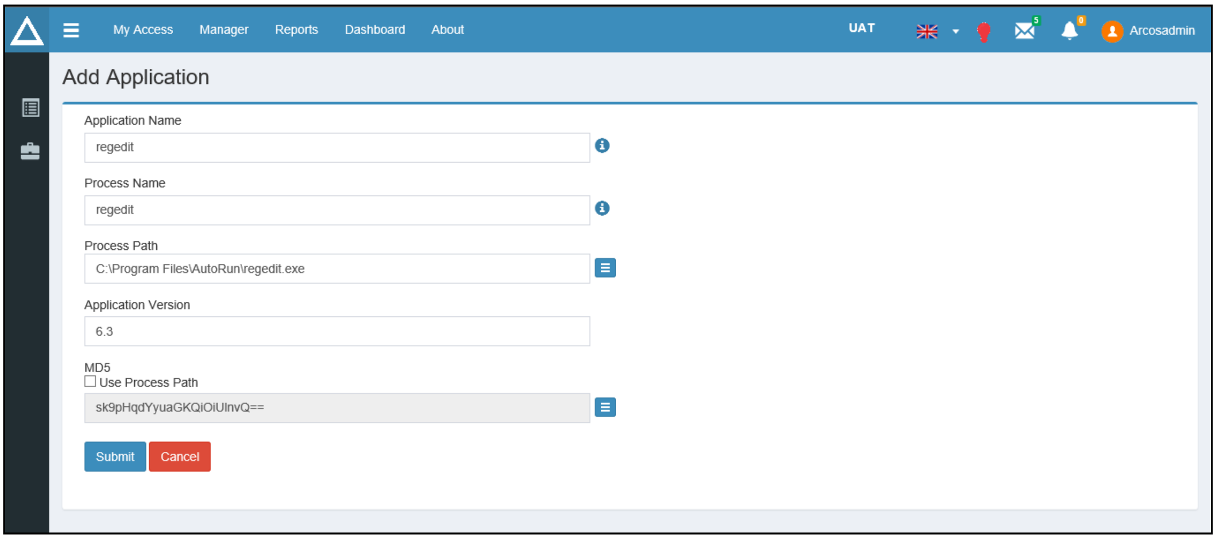
1. Click **Calculate MD5** icon.
2. Click **Browse**.
3. Browse to display value in **Select file for Calculating MD5 Value**
4. Click **OK**.



Calculating MD5 Value

Select file for Calculating MD5 Value: C:\Program Files\AutoRu

5. MD5 value is displayed in MD5 field.



Add Application

Application Name: regedit

Process Name: regedit

Process Path: C:\Program Files\AutoRun\regedit.exe

Application Version: 6.3

MD5
□ Use Process Path
sk9pHqdYyuaGKQiOiUlnvQ==

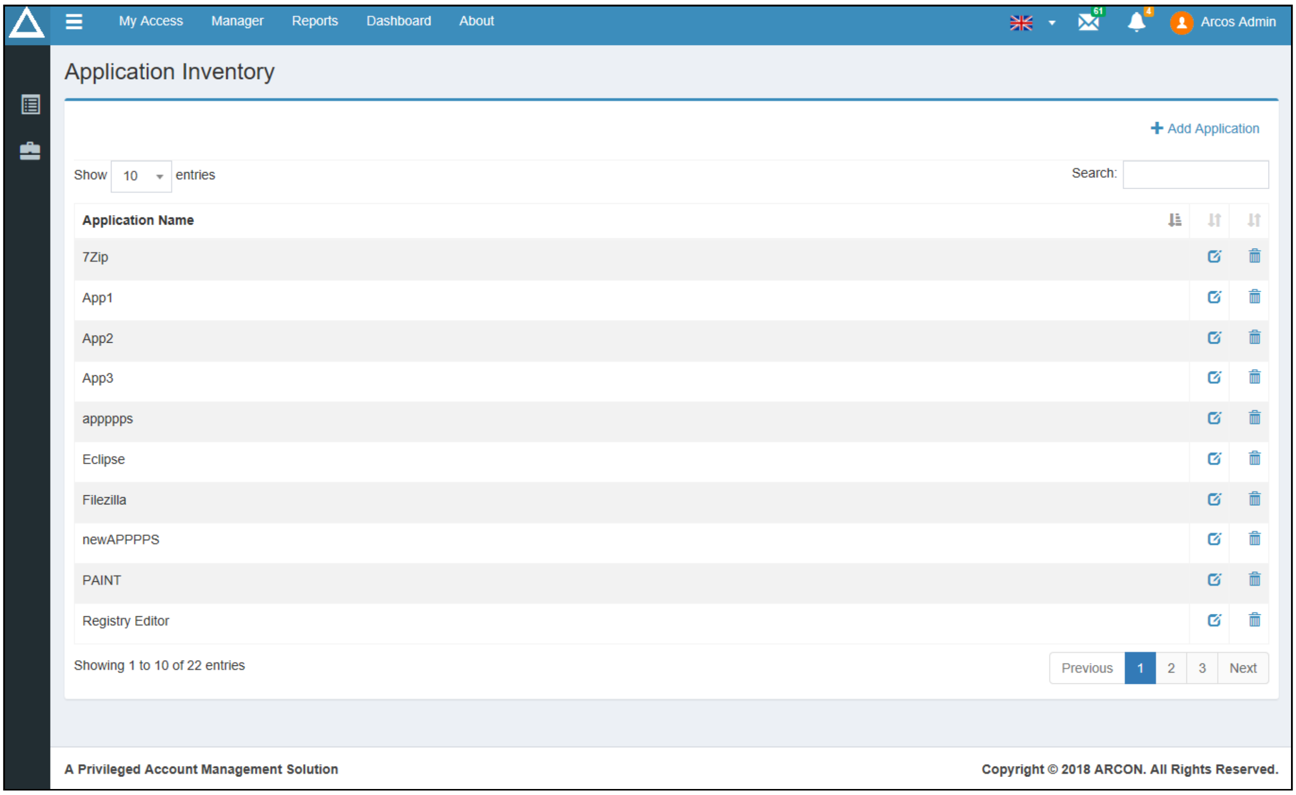
6. Click **Submit**. A window pops up with the following message: **"Application has been Added successfully".**
7. Click **OK**. A new application is added.

2.2 Process to view Application Inventory

This section helps you to view created applications. You can update and delete already created applications. User can also create new application by clicking on the given link.

To view Application Inventory , use the following path:

Application (▤ **)** → Click **Application Inventory**. The following screen is displayed.



Application Inventory

+ Add Application

Show 10 entries

Search:

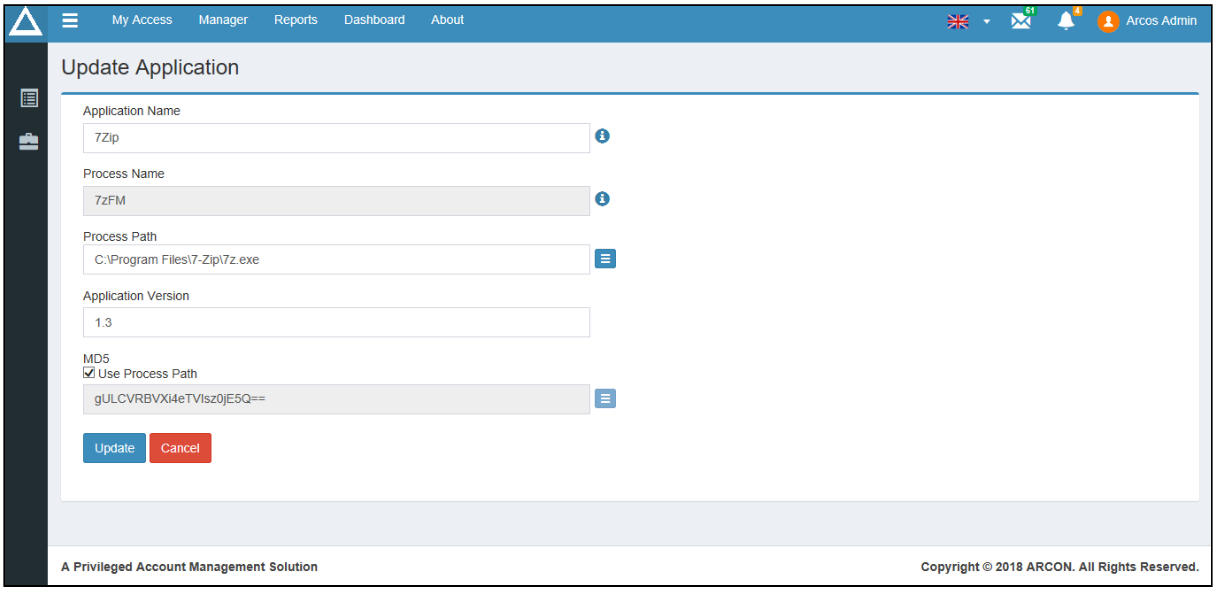
Application Name		
7Zip	✎	🗑
App1	✎	🗑
App2	✎	🗑
App3	✎	🗑
appppps	✎	🗑
Eclipse	✎	🗑
Filezilla	✎	🗑
newAPPPPS	✎	🗑
PAINT	✎	🗑
Registry Editor	✎	🗑

Showing 1 to 10 of 22 entries

A Privileged Account Management Solution

Copyright © 2018 ARCON. All Rights Reserved.

1. User can add new application by clicking **Add Application** link and Edit or Delete existing profiles by selecting respective icons.
2. Click **Delete** 🗑 icon to delete application.
3. Click **Edit** ✎ icon to modify an application. The following screen is displayed for updating profile.



Update Application

Application Name: 7Zip

Process Name: 7zFM

Process Path: C:\Program Files\7-Zip\7z.exe

Application Version: 1.3

MD5

☑ Use Process Path

gULCVRBVXi4eTVlsz0jE5Q==

A Privileged Account Management Solution

Copyright © 2018 ARCON. All Rights Reserved.

The **Update Application** screen contains the following fields:

Field Name	Description
Application Name	Edit application name if required.
Process Name	Process name field cannot be edited.
Process Path	Click **Select Path** (☰) icon to browse and select the path of process.
Application Version	Edit the version number of the application.
MD5	Select **User Process Path** checkbox to calculate MD5 value or click **Calculate MD5** (☰) icon to browse and select file.

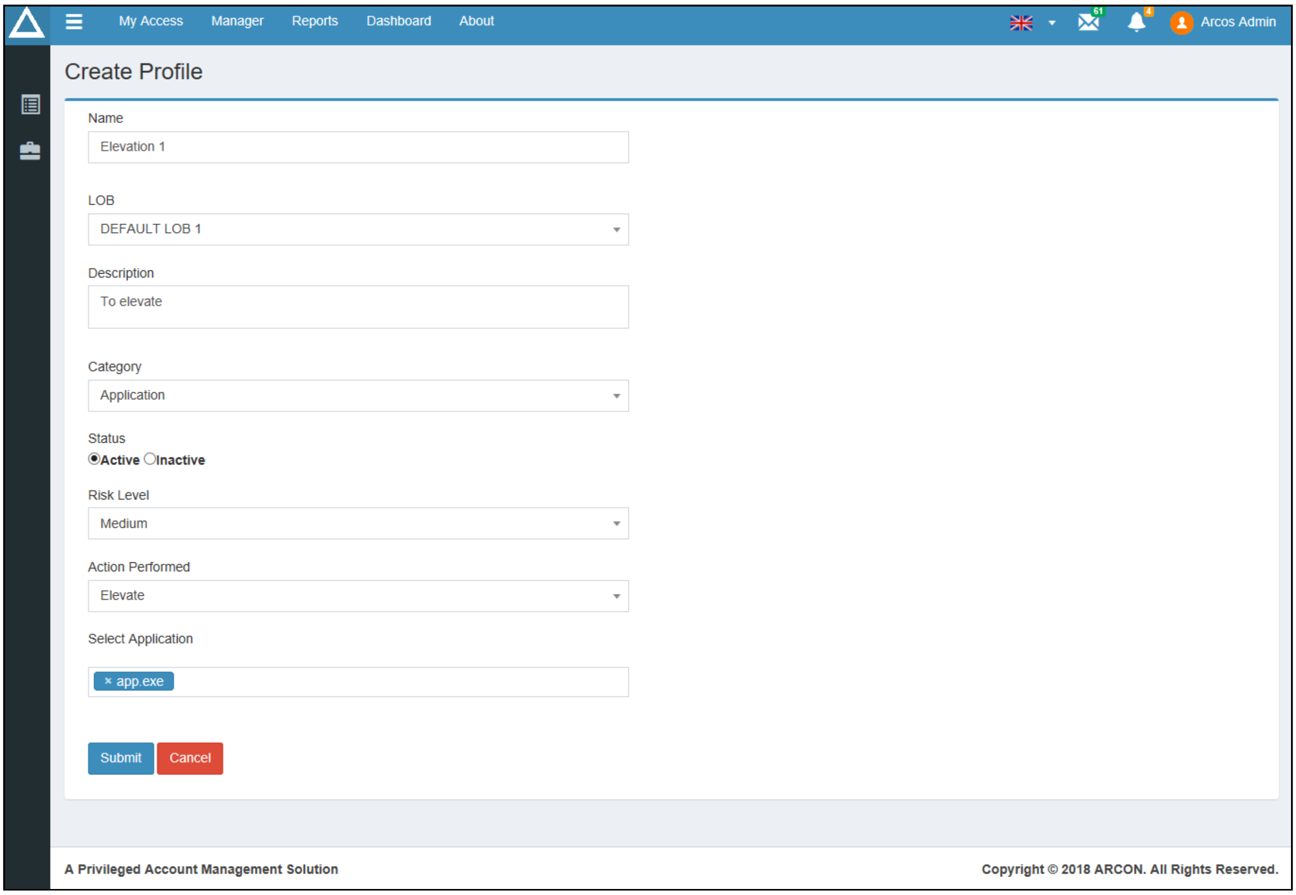
4. Enter or select the required details and click **Update**. A window pops up with the following message: **"Application has been updated successfully"**.
5. Click **OK**. The application is updated.

2.3 Creating an Application Profile

This section helps you to create a profile for the added application. You can configure the profile to restrict/ elevate the process.

To Create Profile, use the following path:

Profiles (💼 **)** → Click **Create Profile.** The following screen is displayed.


My Access
Manager
Reports
Dashboard
About
Arcos Admin

Create Profile

Name: Elevation 1

LOB: DEFAULT LOB 1

Description: To elevate

Category: Application

Status: ● Active ○ Inactive

Risk Level: Medium

Action Performed: Elevate

Select Application: × app.exe

Submit
Cancel
A Privileged Account Management Solution
Copyright © 2018 ARCON. All Rights Reserved.

The **Create Profile** screen contains the following fields:

Field Name	Description
Name	Enter a profile name of the application that should be restricted or elevated.
LOB	Select the LOB.
Description	Enter description for application profile.
Category	Select the category as Application.
Status	Select the profile as Active/Inactive. ⚠ Only active profiles will be restricted/elevated.
Risk Level	Select the risk level as High/Medium/Low.
Actions Performed	Select Restrict for restricting applications and Elevate for elevating applications.

Field Name	Description
Select Application	Select the application to restrict/elevate.

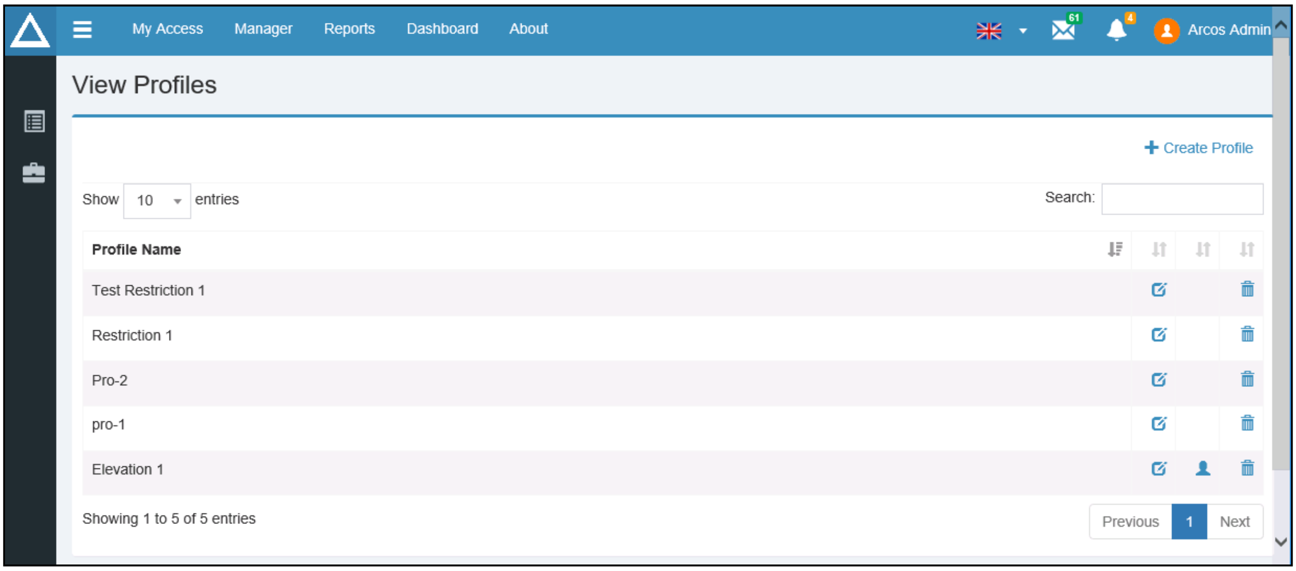
1. Enter or select the details and click **Submit**. A window pops up with the following message: "**Profile for particular user has been created successfully**".
2. Click **OK**. A new profile is created.

2.4 Process to view the profile

This section helps you to view created profile. You can update, assign or delete already created profile. User can also create new profile by clicking on the given link.

To View Profile, use the following path:

Profiles (💼 **)** → Click **View Profile**. The following screen is displayed.



View Profiles

+ Create Profile

Show 10 entries

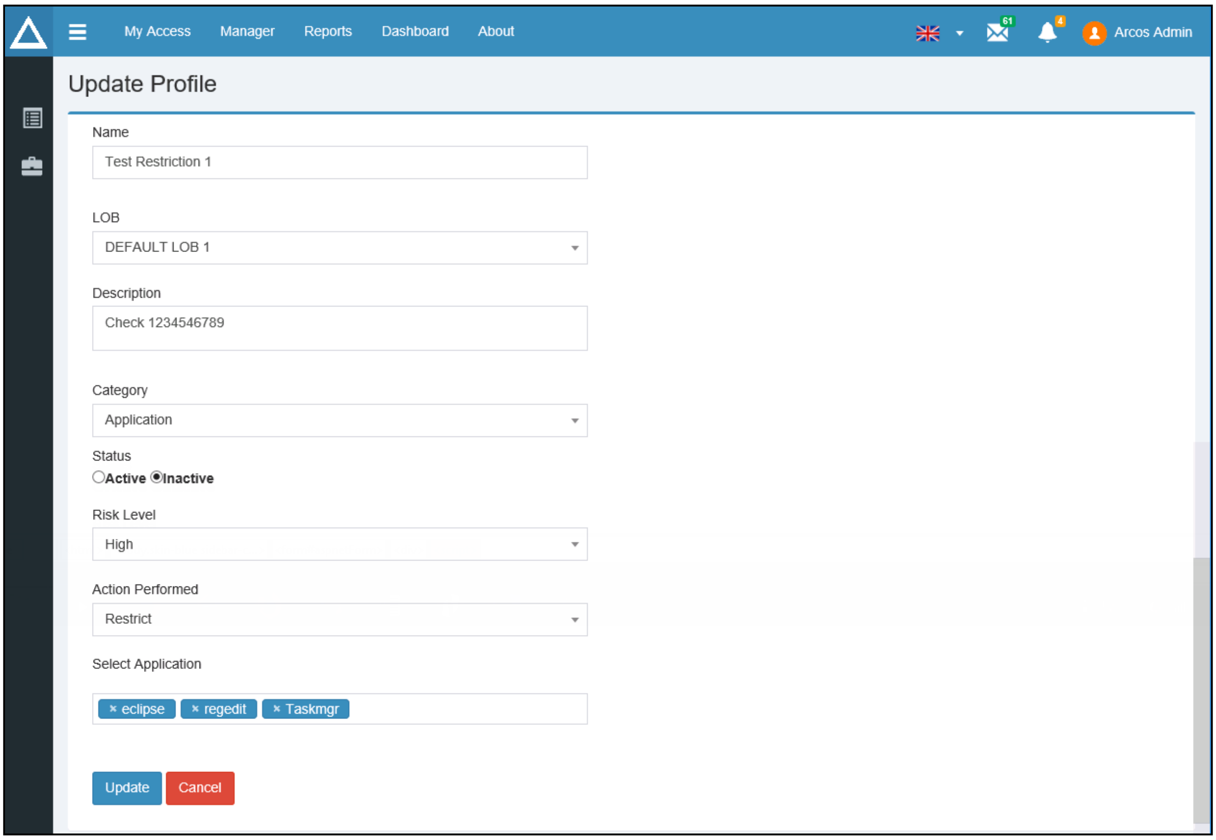
Search:

Profile Name			
Test Restriction 1	✎		🗑
Restriction 1	✎		🗑
Pro-2	✎		🗑
pro-1	✎		🗑
Elevation 1	✎	👤	🗑

Showing 1 to 5 of 5 entries

Previous 1 Next

1. User can create new profile by clicking **Create Profile** link and Edit, Assign or Delete existing profiles by selecting respective icons.
2. Click **Delete** 🗑 icon to delete profile.
3. Click **Assign** 👤 icon to assign profile to user / group of users.
4. Click **Edit** ✎ icon to modify a profile. The following screen is displayed for updating profile.



Update Profile

Name: Test Restriction 1

LOB: DEFAULT LOB 1

Description: Check 1234546789

Category: Application

Status: ○Active ●Inactive

Risk Level: High

Action Performed: Restrict

Select Application: × eclipse × regedit × Taskmgr

The **Update Profile** screen contains the following fields:

Field Name	Description
Name	Enter a profile name of the application that should be restricted or elevated.
LOB	Select the LOB.
Description	Enter description for application profile.
Category	Keep the category as Application.
Status	Select the profile as Active/Inactive. ⚠ Only active profiles will be restricted/elevated.
Risk Level	Select the risk level as High/Medium/Low.
Actions Performed	Select Restrict for restricting applications and Elevate for elevating applications.
Select Application	Select the application to restrict/elevate.

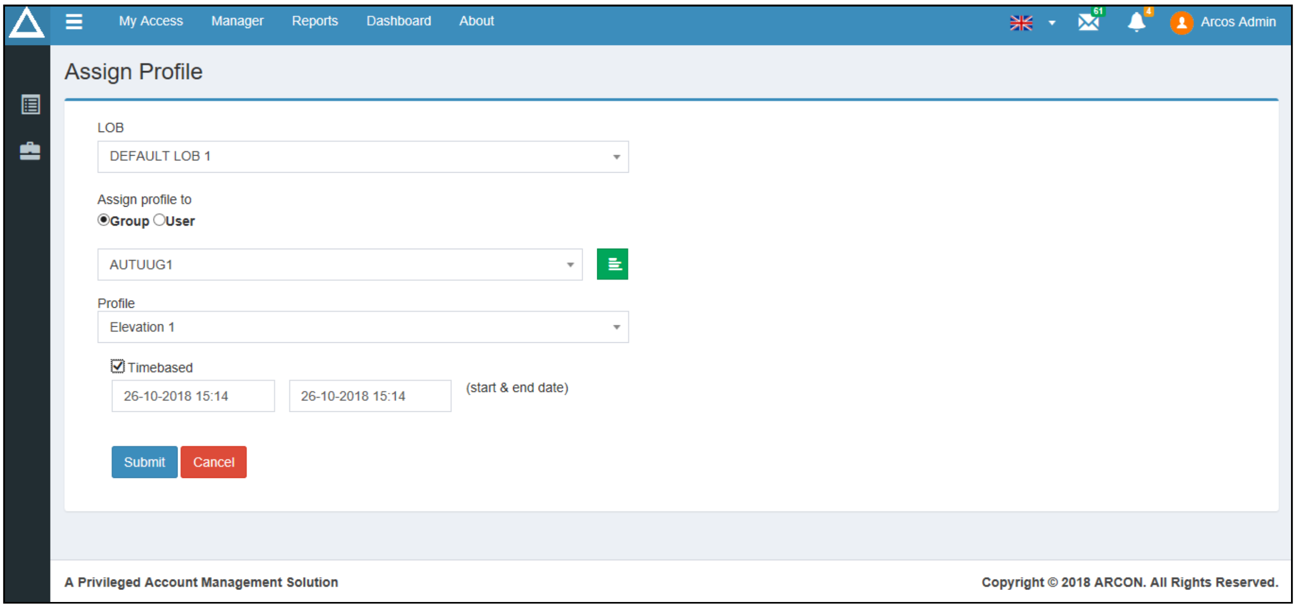
5. Enter or select the required details and click **Update**. A window pops up with the following message: **"Profile for particular user has been updated successfully"**.
6. Click **OK**. The profile is updated.

2.5 Process to assign the profile

This section helps you to assign profile of added application to group of users / a particular user.

To Assign Profile, use the following path:

Profiles (💼 **)** → Click **Assign Profile**. The following screen is displayed.



Assign Profile

LOB
DEFAULT LOB 1

Assign profile to
● **Group** ○ **User**

AUTUUG1

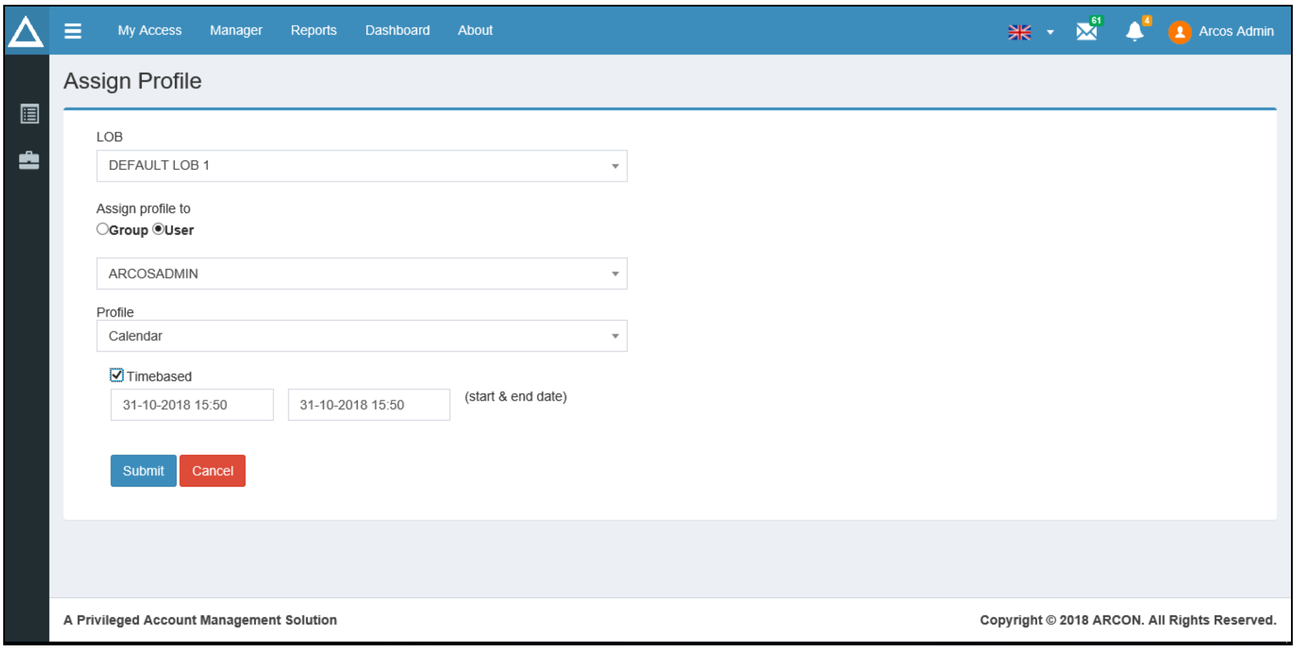
Profile
Elevation 1

☑ Timebased
26-10-2018 15:14 | 26-10-2018 15:14 (start & end date)

A Privileged Account Management Solution

Copyright © 2018 ARCON. All Rights Reserved.

The **Group** radio button is by default selected. When you select **User** radio button, following screen is displayed.



Assign Profile

LOB
DEFAULT LOB 1

Assign profile to
○ **Group** ● **User**

ARCOSADMIN

Profile
Calendar

☑ Timebased
31-10-2018 15:50 | 31-10-2018 15:50 (start & end date)

A Privileged Account Management Solution

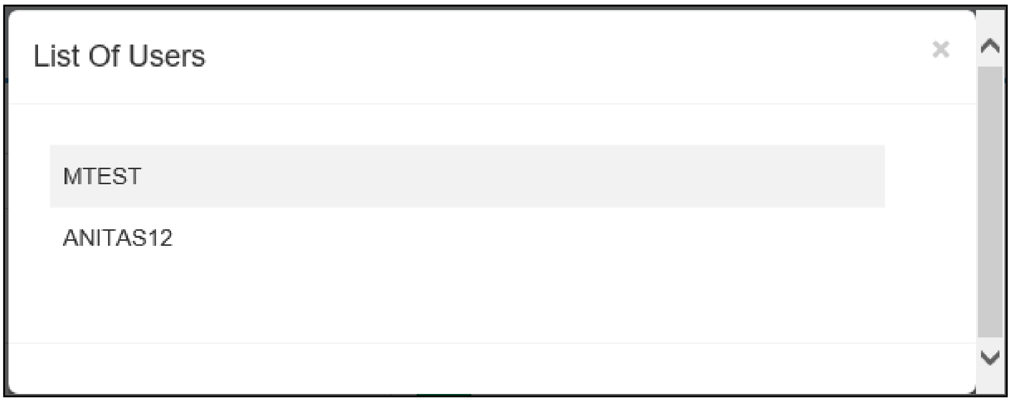
Copyright © 2018 ARCON. All Rights Reserved.

The **Assign Profile** screen contains the following fields:

Field Name	Description
LOB	Select the LOB.
Assign Profile to	Select the radio button of Group /User for whom the profile is to be assigned.
Groups	Name of the group for which the the profile is assigned; Group name can be selected from an existing list. ⚠ This field will be disabled if User is selected.
User	Select the user name of the user/admin. ⚠ This filed will be disabled if Group is selected.
Profile	Select the Profile name. ⚠ Ensure to give the same description when you created the application profile.
Timebased	Select the checkbox and configure from and to date and time for which you want the configuration to be active. ⚠ • The application will be restricted/elevated only for the set time. • If you do not want to restrict/elevate process for particular time period then do not select this checkbox.

To Assign Profile to Group of users

1. Select **Group** radio button.
2. The group name will be displayed. Click 🟩 icon. The following list of users in selected group screen is displayed.



List Of Users

MTEST

ANITAS12

3. Select or enter details on **Assign Profile** screen and click **Submit**. A window pops up with the following message: “**Profile Assigned Successfully**”.
4. Click **OK**. The profile is assigned to users in selected user group.

To Assign Profile to User

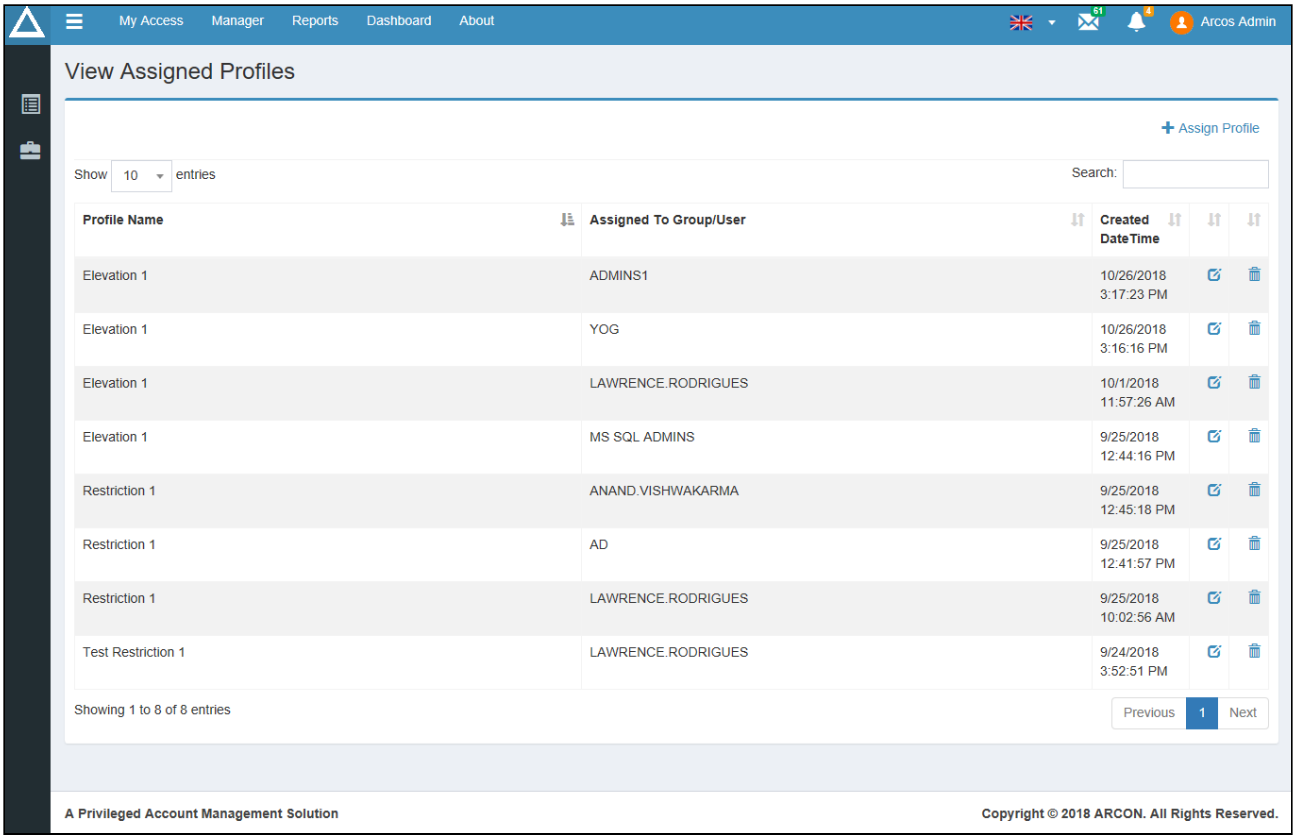
1. Select **User** radio button, select details and click **Submit**. A window pops up with the following message: “**Profile Assigned Successfully**”.
2. Click **OK**. The profile is assigned to selected user.

2.6 Process to View the Assigned Profile

The profiles are created and are assigned to a group of users / a particular user. This section helps you to edit profile to user / group of users mapping.

To View Assigned Profile, use the following path:

Profiles (💼**)** → Click **View Assigned Profile**. The following screen is displayed.



View Assigned Profiles

Show 10 entries Search:

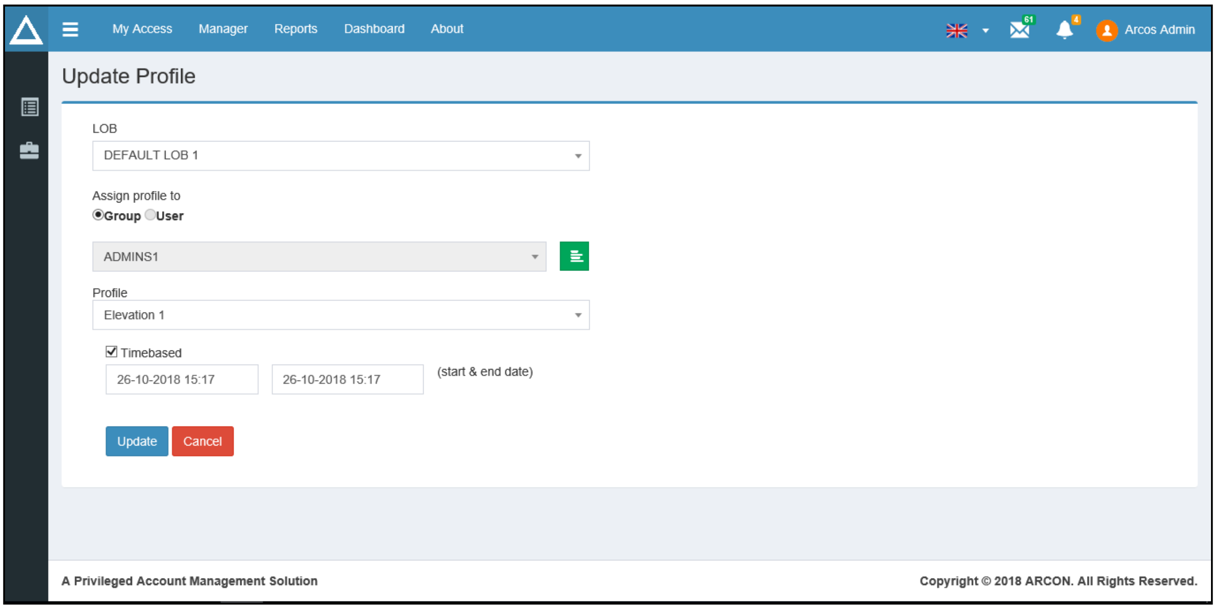
Profile Name	Assigned To Group/User	Created DateTime		
Elevation 1	ADMINS1	10/26/2018 3:17:23 PM	✎	🗑
Elevation 1	YOG	10/26/2018 3:16:16 PM	✎	🗑
Elevation 1	LAWRENCE.RODRIGUES	10/1/2018 11:57:26 AM	✎	🗑
Elevation 1	MS SQL ADMINS	9/25/2018 12:44:16 PM	✎	🗑
Restriction 1	ANAND.VISHWAKARMA	9/25/2018 12:45:18 PM	✎	🗑
Restriction 1	AD	9/25/2018 12:41:57 PM	✎	🗑
Restriction 1	LAWRENCE.RODRIGUES	9/25/2018 10:02:56 AM	✎	🗑
Test Restriction 1	LAWRENCE.RODRIGUES	9/24/2018 3:52:51 PM	✎	🗑

Showing 1 to 8 of 8 entries

A Privileged Account Management Solution

Copyright © 2018 ARCON. All Rights Reserved.

1. Click **Edit** ✎ icon to update details. The following screen is displayed.



Update Profile

LOB: DEFAULT LOB 1

Assign profile to
● Group ○ User

ADMINS1

Profile: Elevation 1

☑ Timebased
26-10-2018 15:17 26-10-2018 15:17 (start & end date)

A Privileged Account Management Solution

Copyright © 2018 ARCON. All Rights Reserved.

The **Update Profile** screen contains the following fields:

Field Name	Description
LOB	Select the required LOB.
Assign Profile to	Select the radio button of Group /User for whom the profile is to be assigned.
Groups	Name of the group for which the the profile is assigned; Group name can be selected from an existing list.
User	Edit the user name of the user/admin.
Profile	Edit the Profile name if required.
Timebased	Select to set this profile to user mapping time based.

2. Select the required details and click **Update**. The Assigned Profile is updated.

> ⚠ Click **Delete** icon 🗑 to delete details.

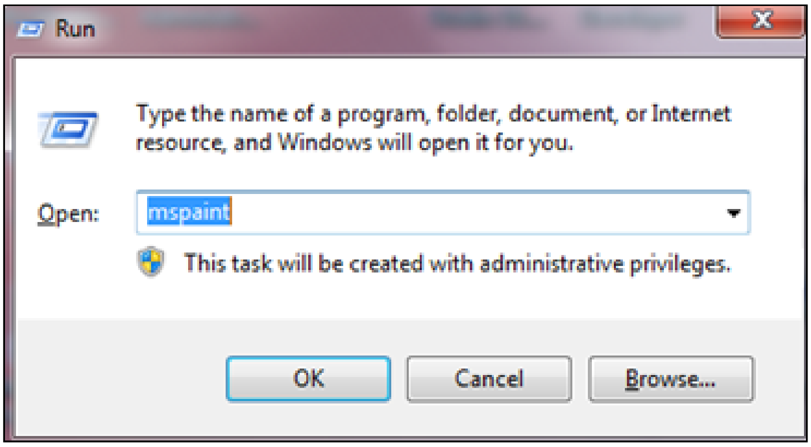
2.7 Accessing Restricted/Elevated application

Application can be elevated/restricted in ARCON PAM by adding the application, then creating a profile and assigning it to a user or group of user.

When the user tries to execute the process elevated for his User ID, process is executed. When the user tries to execute the process restricted for his User Id, process is not executed and an error message is displayed.

Consider an example for accessing a restricted application, MS Paint and accessing an elevated application, Registry Editor.

1. MS Paint is a restricted application. User tries to access MS Paint using Run.

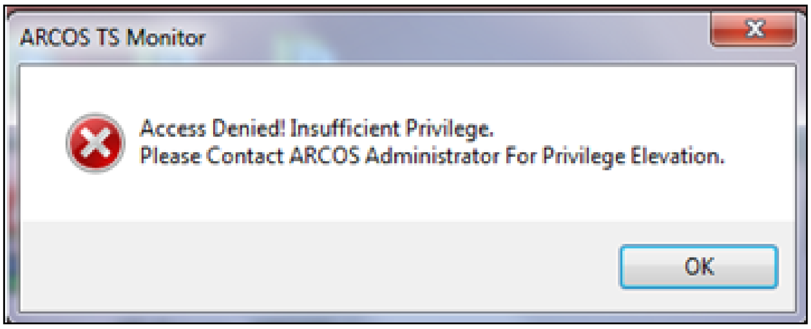


Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: mspaint

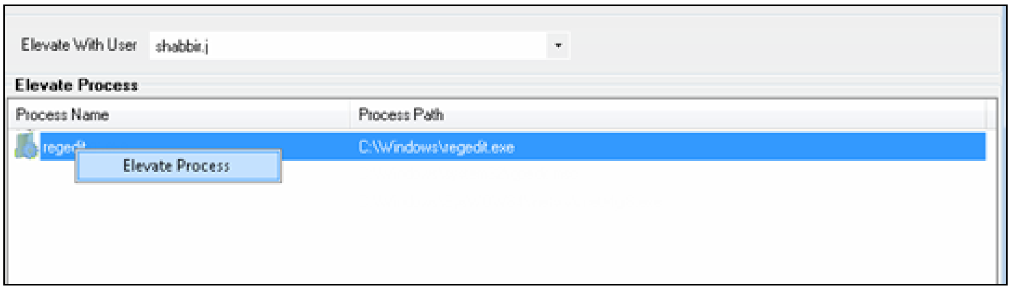
This task will be created with administrative privileges.

2. The user / group of users will get the following message on accessing MS Paint.



Access Denied! Insufficient Privilege.
Please Contact ARCOS Administrator For Privilege Elevation.

3. Registry Editor is an elevated application. User has to right click on the process name to elevate the application.

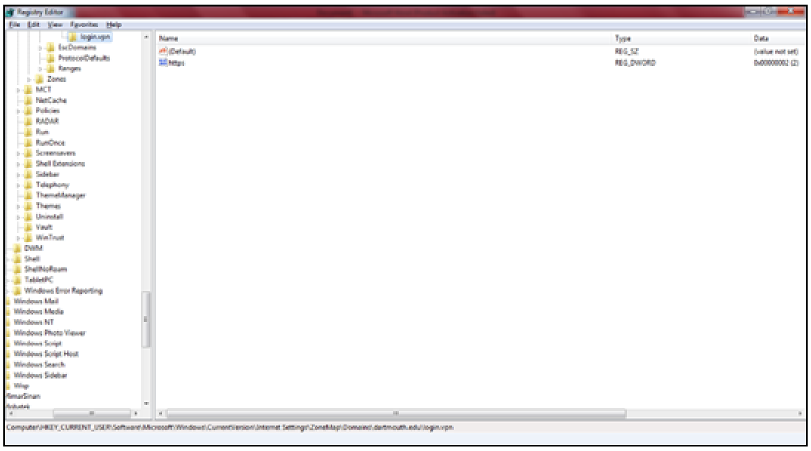


Elevate With User: shabbir.j

Elevate Process

Process Name	Process Path
regedit	C:\Windows\regedit.exe

4. The user or group of users can access the elevated application.



Name	Type	Data
(Default)	REG_SZ	(value not set)
https	REG_DWORD	0x00000002 (2)

Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains\dartmouth.edu\login.vpn

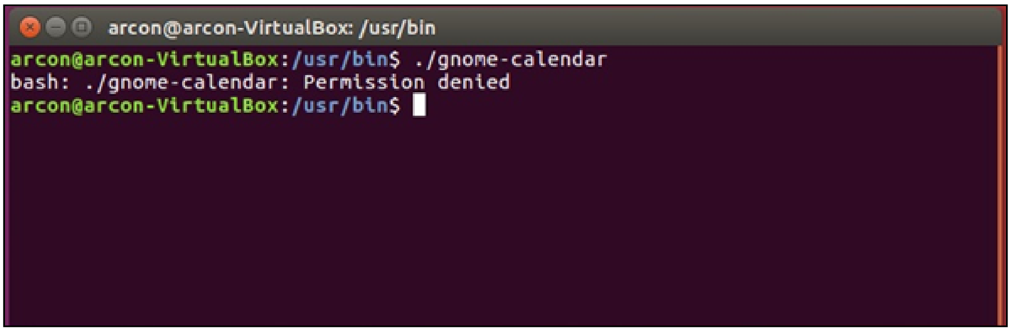
3 Accessing Restricted/Elevated application in Ubuntu/Windows

Applications can be elevated/restricted in Ubuntu/Windows.

When a process is restricted for a user and he tries to execute it, Access Denied message is displayed. When a user wants to execute a process and it is restricted for his ID, he needs to add application in ARCON PAM, create a profile and assign it to user or group of users. The requested process is then elevated for the user for the given date and time.

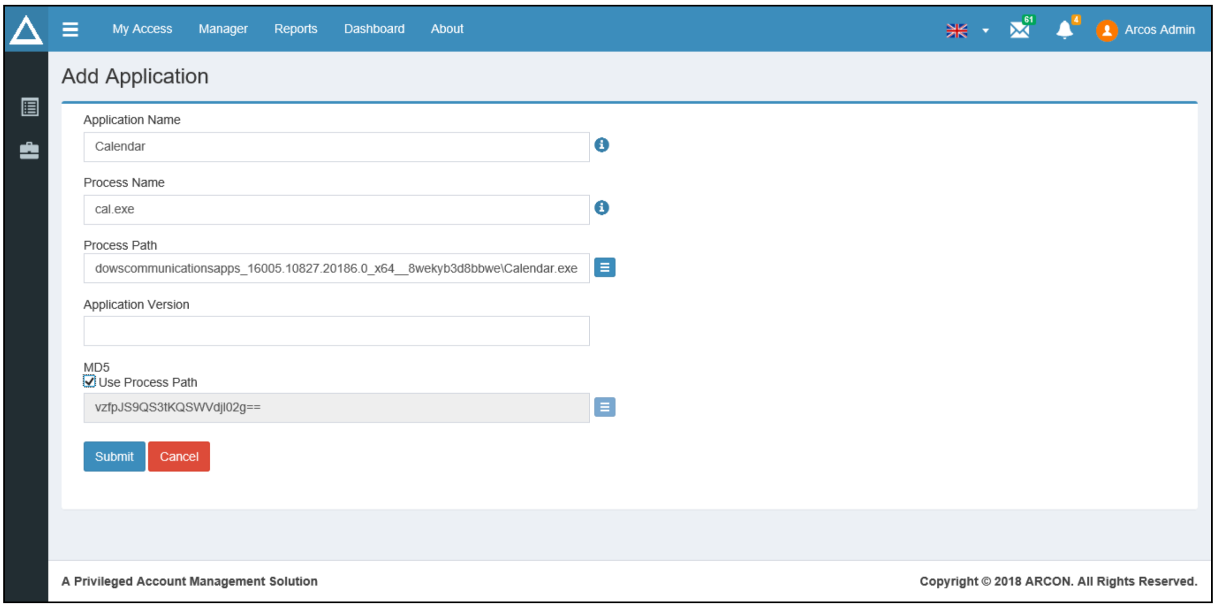
Consider an example for accessing a restricted application, Calendar. This application is then elevated for user.

1. Calendar is a restricted application. User tries to access this application. The following message will be displayed for the user.



```
arcon@arcon-VirtualBox:/usr/bin$ ./gnome-calendar
bash: ./gnome-calendar: Permission denied
arcon@arcon-VirtualBox:/usr/bin$ 
```

2. The user adds required application in Add Application screen as follows.



Add Application

Application Name: Calendar

Process Name: cal.exe

Process Path: dowscommunicationsapps_16005.10827.20186.0_x64__8wekyb3d8bbwe\Calendar.exe

Application Version:

MD5

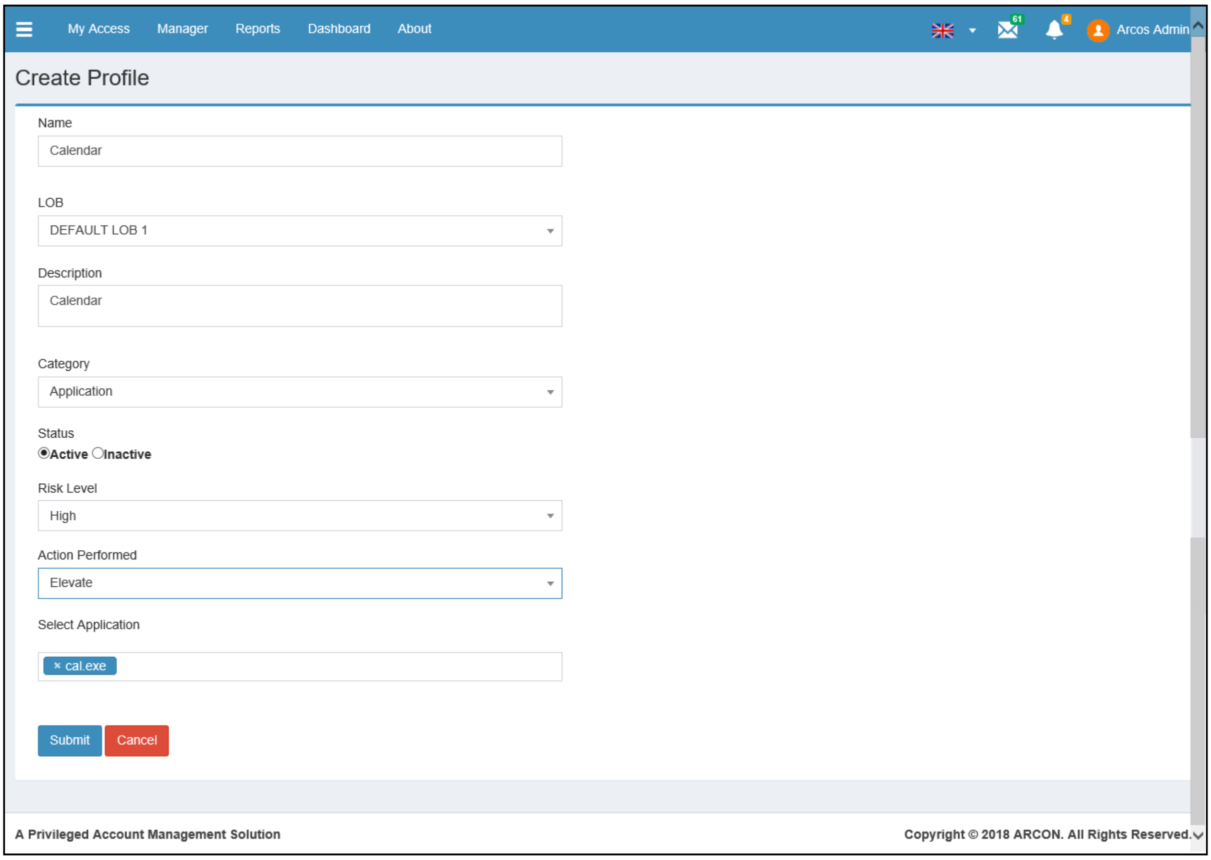
☑ Use Process Path

vzfpJS9QS3tKQSWVdjl02g==

A Privileged Account Management Solution

Copyright © 2018 ARCON. All Rights Reserved.

3. Create a profile with “Elevate” Action Performed for the added application.



Create Profile

Name
Calendar

LOB
DEFAULT LOB 1

Description
Calendar

Category
Application

Status
● Active ○ Inactive

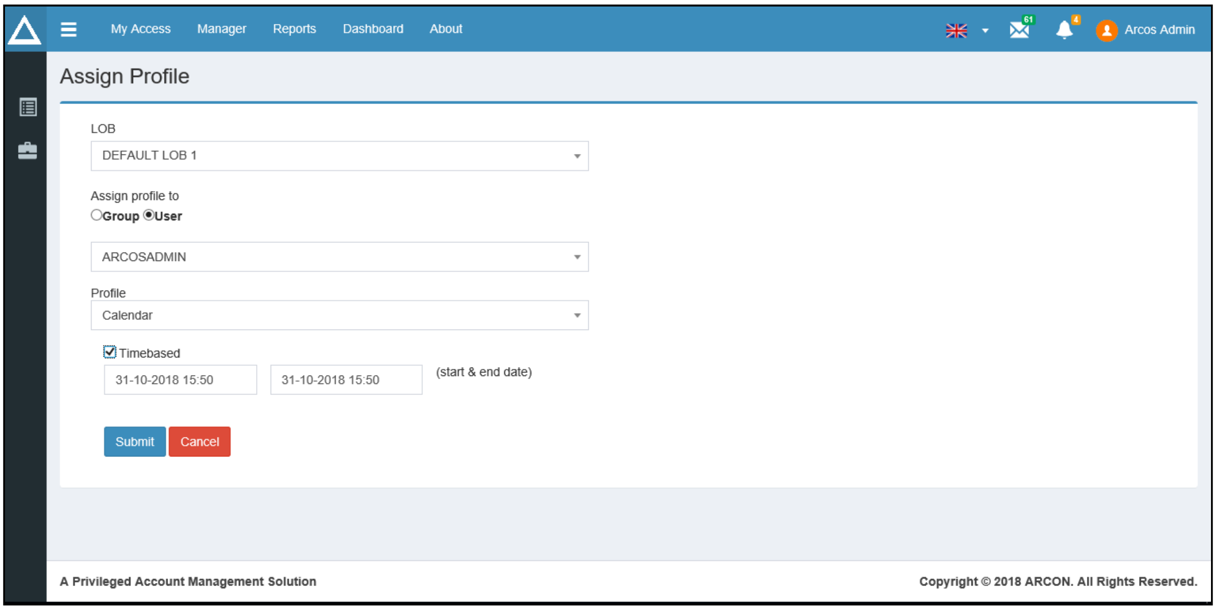
Risk Level
High

Action Performed
Elevate

Select Application
× cal.exe

A Privileged Account Management Solution

4. Assign the created profile to group of users / a particular user.



Assign Profile

LOB
DEFAULT LOB 1

Assign profile to
○ Group ● User

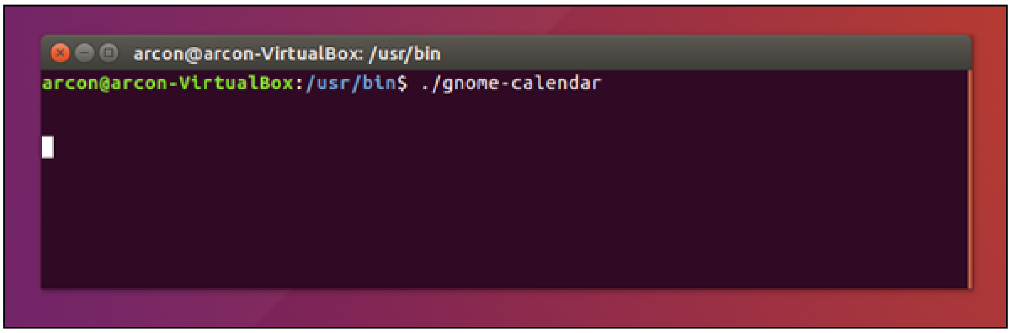
ARCOSADMIN

Profile
Calendar

☑ Timebased
31-10-2018 15:50 31-10-2018 15:50 (start & end date)

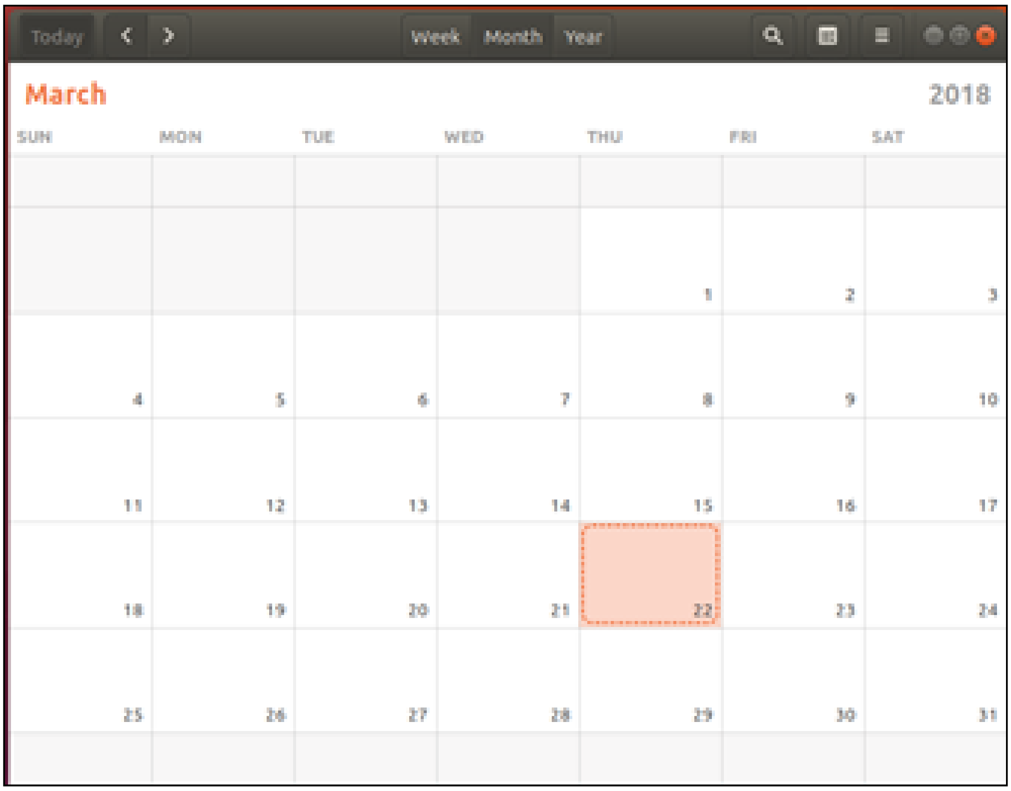
A Privileged Account Management Solution

5. The process Calendar is now Elevated for the users in selected group / selected User for the given Date and Time in Assign Profile. The user tries to execute the process.



```
arcon@arcon-VirtualBox:/usr/bin$ ./gnome-calendar
```

6. The process Calendar is elevated in the following screen.



SUN	MON	TUE	WED	THU	FRI	SAT
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Privileged Access Management Suite

arcon

Predict | Protect | Prevent