Predict | Protect | Prevent

ARCON|PAM

Windows Thick client Installation and Configuration

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 PAM through the support team. Wherever appropriate, references have been made to facilitate better understanding of the PAM solution. The ARCON PAM 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 PAM 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 PAM; 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 PAM.

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

Privileged Access Management (PAM) is a high level access security solution for managing the privileged accounts in an enterprise. The solution allows organization to secure, control, monitor and audit all the activities associated with all types of Privilege Identities such as Administrators on Windows server, Root on UNIX server, Cisco Enable in Cisco, etc . It is frequently used as an Information Security and Governance tool to help companies prevent data breaches through the use of privileged accounts and meets compliance regulations.

Privileged Access Management (PAM) involves managing privileged individual identities , their authentication, authorization, and privileges/permissions within or across systems and enterprise boundaries with the goal of increasing security and productivity while optimizing the downtime, repetitive task and the cost.

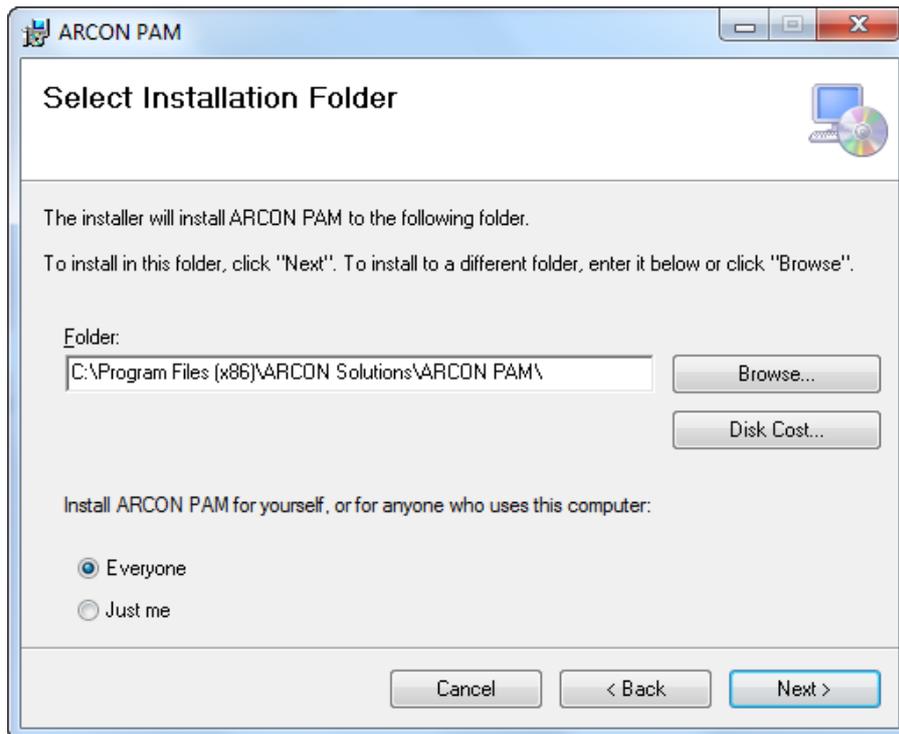## 1.1 Installation Procedures

⚠   1. Users with Administrator rights can only install ARCON PAM
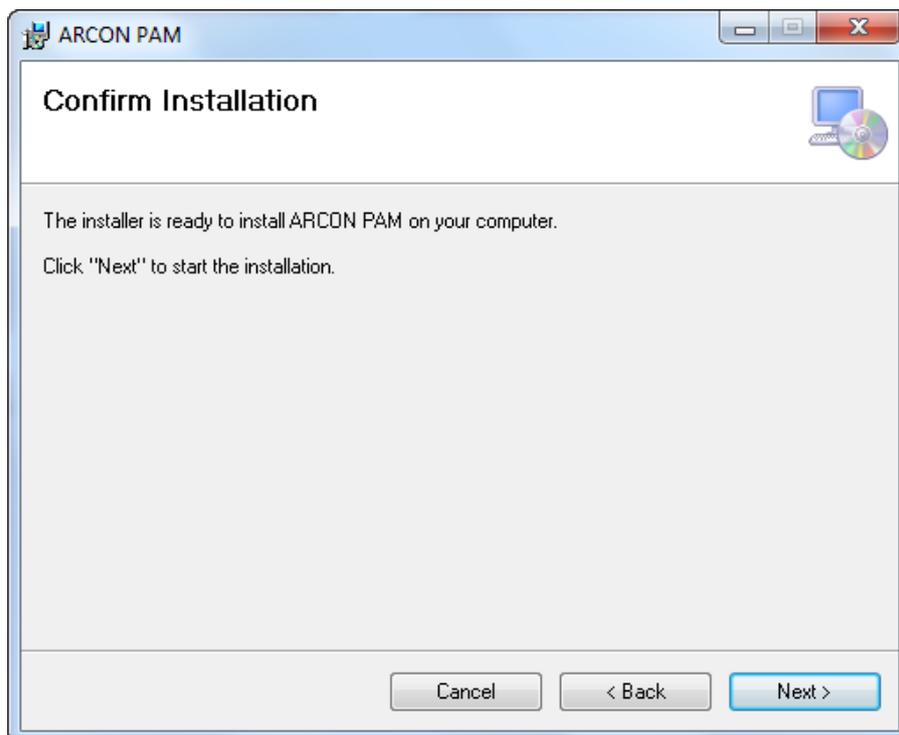
1. Double click on .exe file and following Installer Wizard will start. Click continue to proceed with the installation
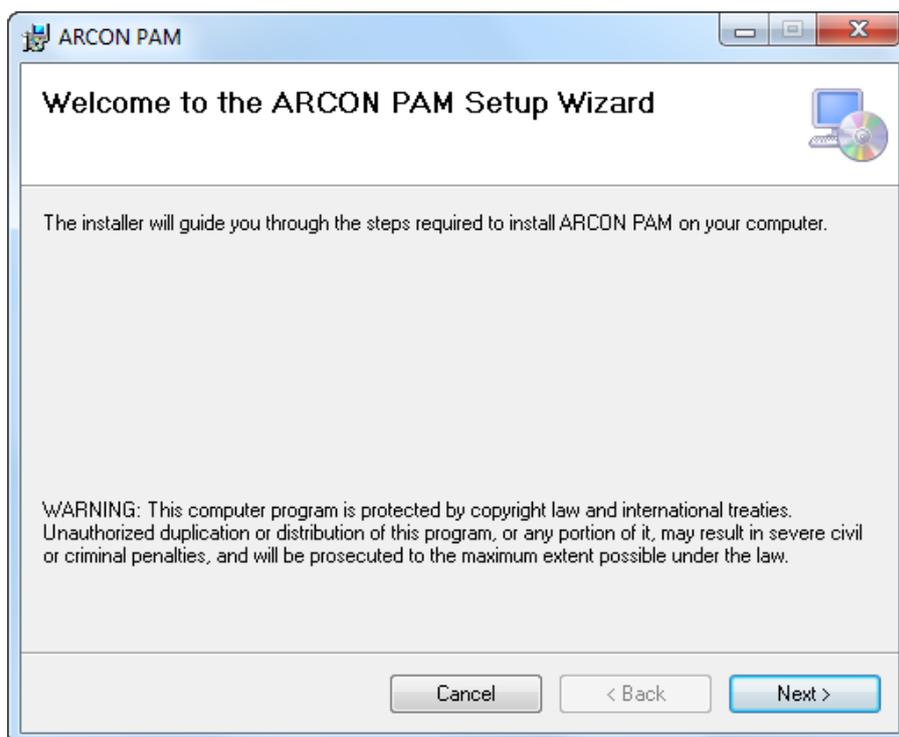
2. Browse and select the folder where the installation files should be placed and click Next.
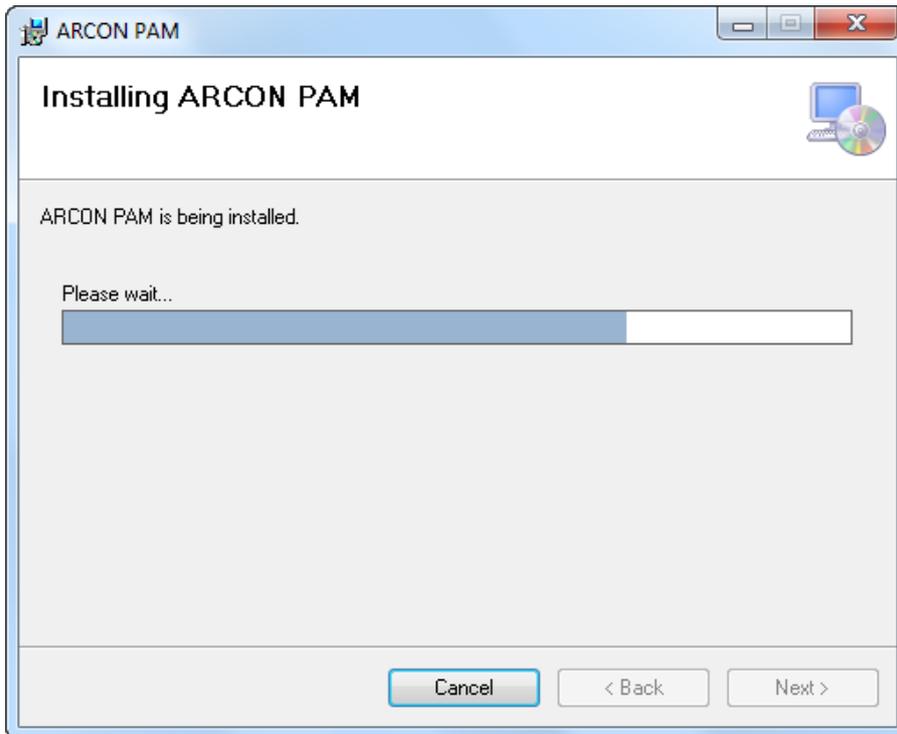
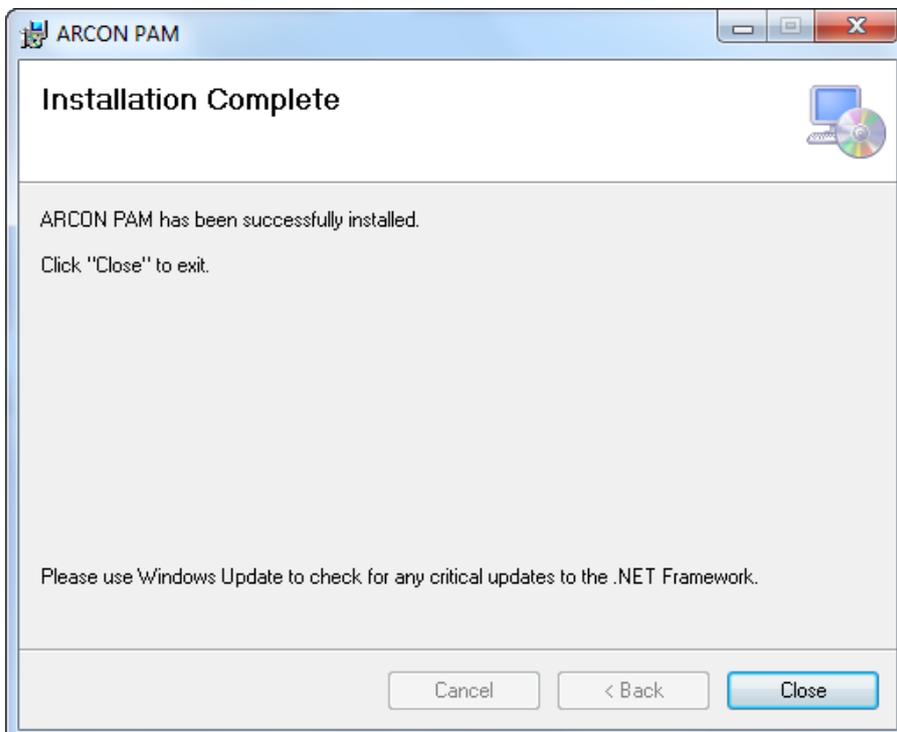3. To continue with the installation process, click Next

4. Click Yes to continue with the installation procedure, Click No to discontinue the installation process.

5. On clicking Yes, the following screen will be displayed.
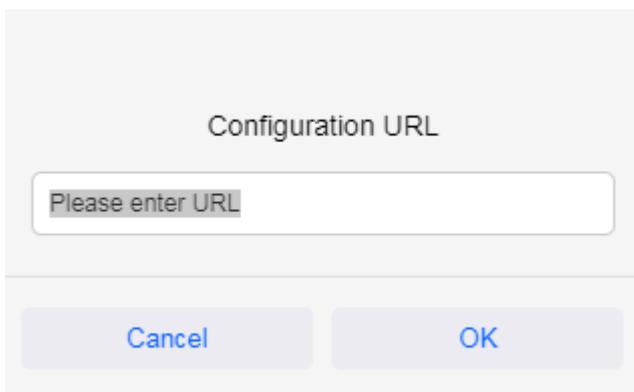

6. The following screen will be displayed on successful installation, click logout to finish the installation
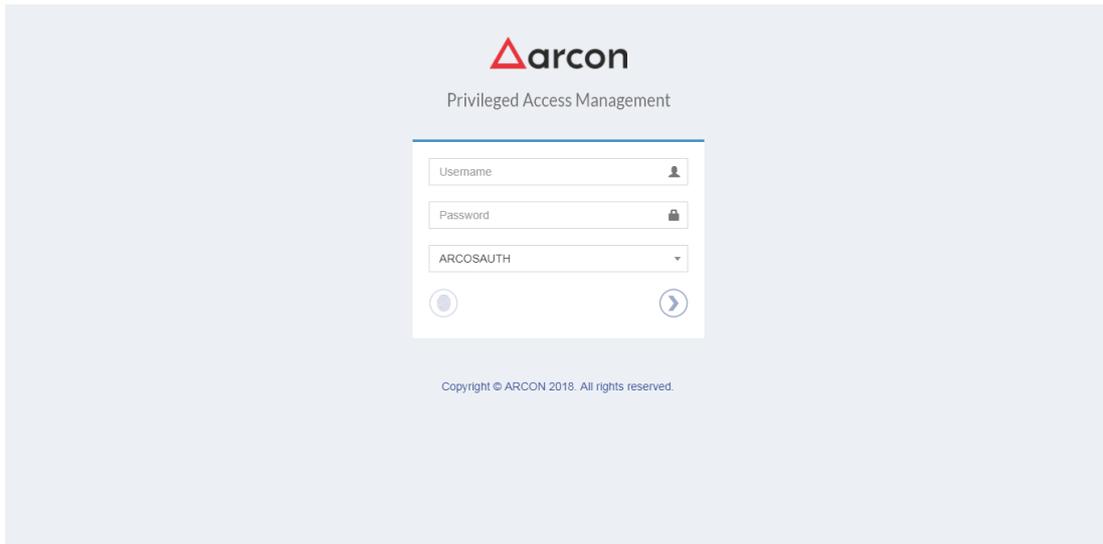
7. Once the installation is complete, go to start, click ARCON PAM to launch the application.

8. Configuration URL pop up will be displayed, enter the URL in the format <https://ip-address:port> in the field.
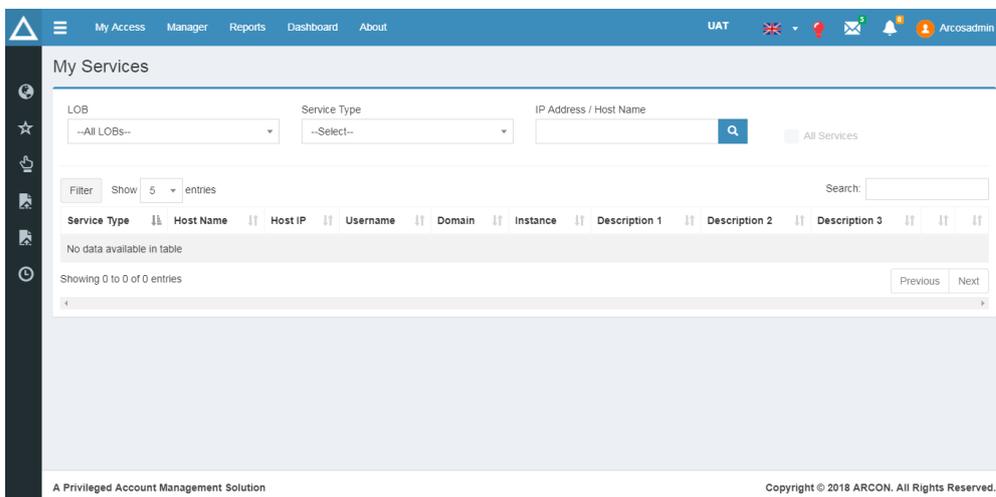

9. On entering the URL, the ARCON PAM login screen will be displayed, enter the login id and password.

10. The login screen contains the following fields

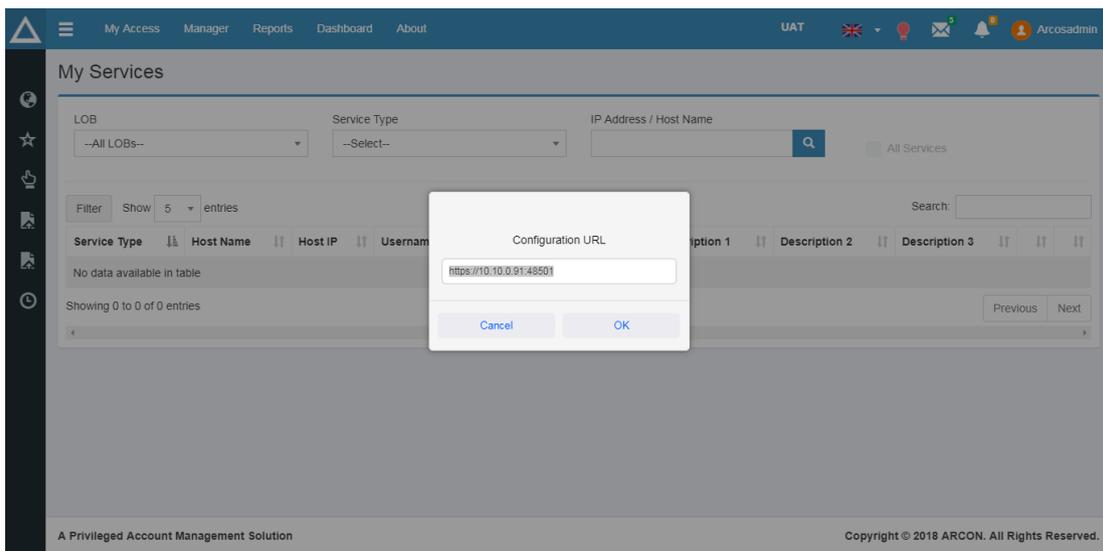| Field Name	Description
Username	Enter the username
Password	Enter the password
Domain	Select the particular domain

11. Enter all the above details and click the

button. My Access page will be displayed.

12. Users can Click on Edit option on the left corner of the screen, and click configure URL option to change URL

13. This option will allow to change the configuration URL

Privileged Access Management Suite

arcon

Predict | Protect | Prevent