

mIAG Appliance-Two Factor based Authentication
PINSafe INSTALLATION NOTES

Factory Installed if addon needed.

INTRODUCTION

This document outlines the necessary steps to install PinSafe on a mIAG™ platform. This includes the installation for the required third-party software, eg Java™ and Apache Tomcat.

1. JAVA INSTALLATION

PINsafe requires a Java Runtime Environment (JRE). A JRE may already be installed you can check to see which versions of Java are installed by looking under C:\Program Files\Java. PINsafe will run with Sun's JRE versions 1.5 and 1.6.0. PINsafe will probably work with later version of the JRE, but this cannot be guaranteed. For advice about using other Java Virtual Machines contact support@nappliance.com

If you need in install a JRE you can obtain the latest JRE one from

<http://java.sun.com/javase/downloads/index.jsp>

Previous JREs are available from

<http://java.sun.com/javase/downloads/previous.jsp>

2. APACHE TOMCAT INSTALLATION

Apache Tomcat needs to listen on port 8180 and port 8443 for https. Use netstat -an

to verify that no processes are currently running on port 8180 or 8443.

Note :For the appliance it should not be 8080 as that what ISA is using.

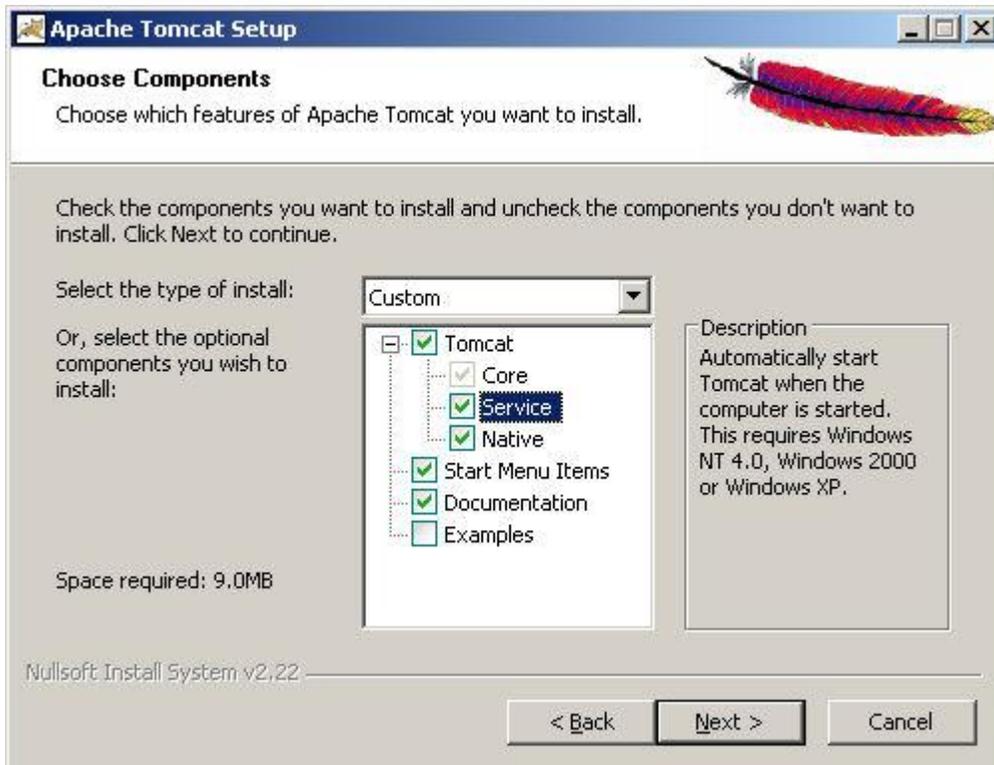
Download the required version of Apache Tomcat from <http://tomcat.apache.org>

PINsafe has been tested with Version 5.5 and Version 6

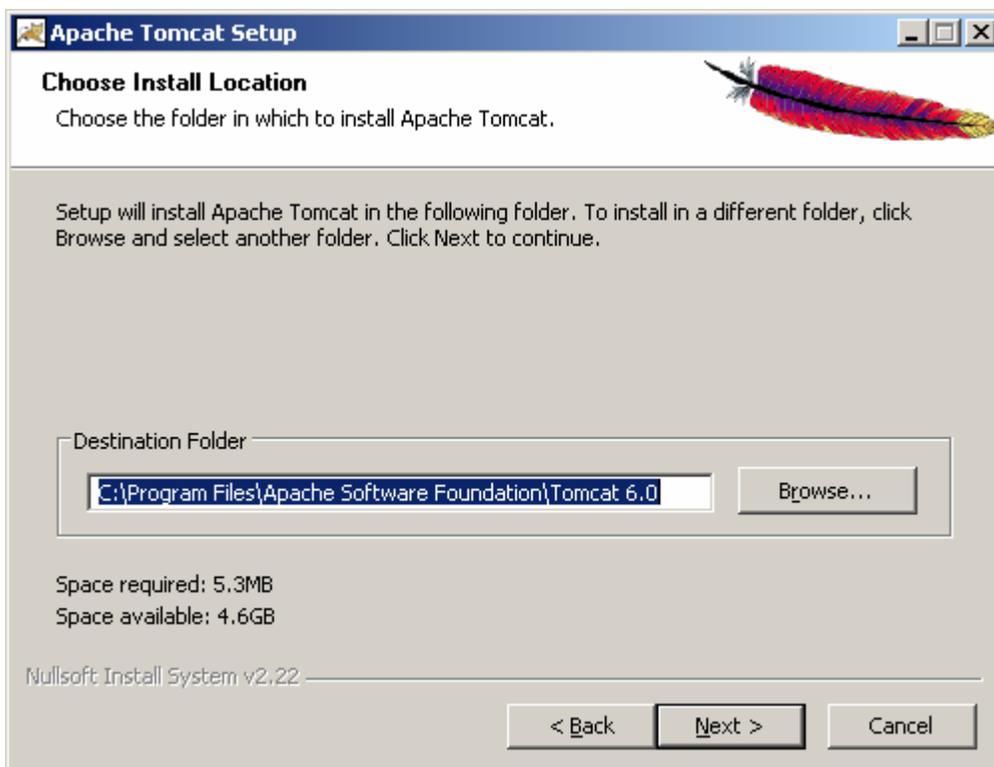
These instructions are to install Apache Tomcat as a service.

Under Download select the version and then under binary distributions select the Windows Service Installer.

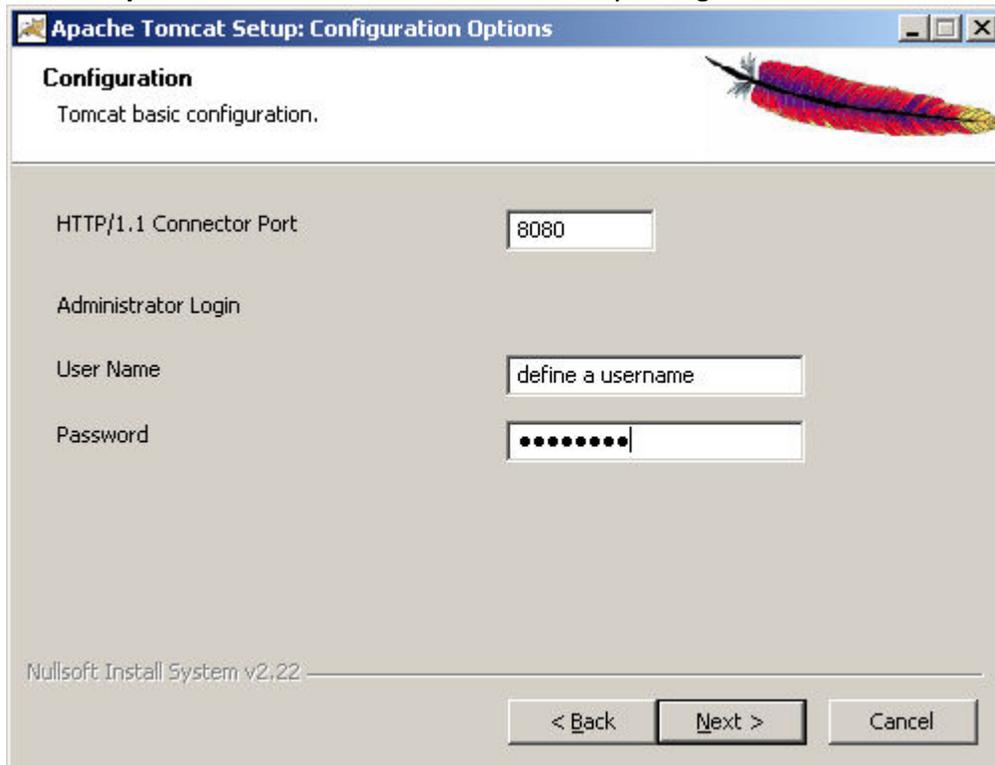
Run the Apache Installer Executable accepting the license agreement and then selecting the components to install, **ensure that service selected**. Native is optional.



Choose the install location



Ensure a password is set and for added security change the username.

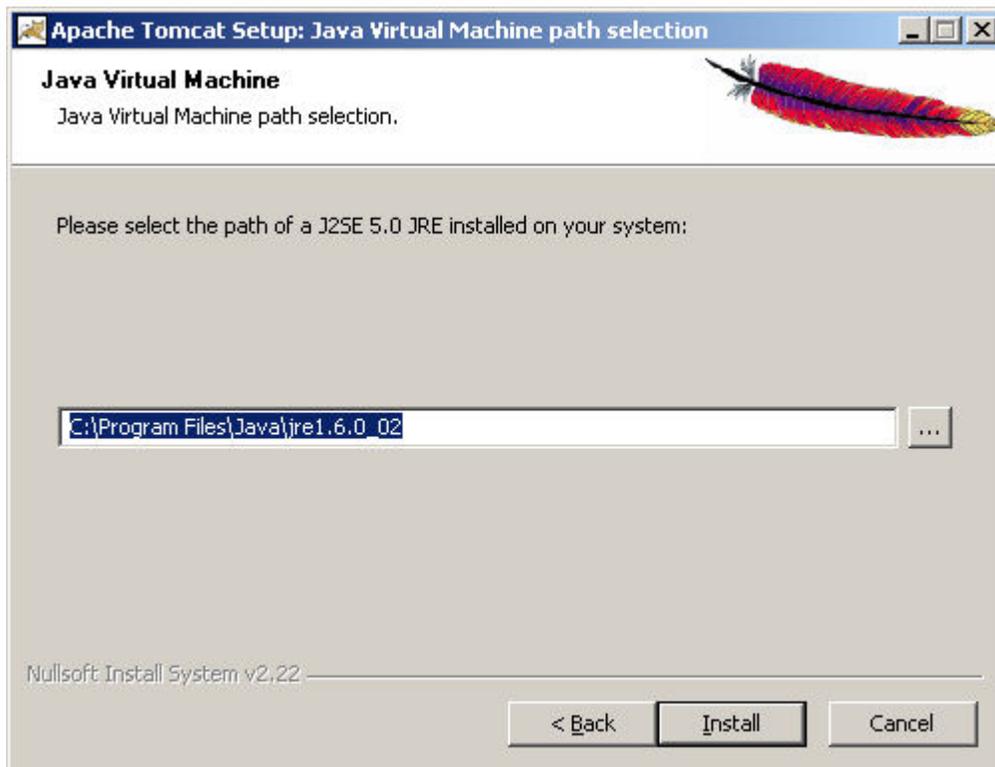


The screenshot shows a Windows-style dialog box titled "Apache Tomcat Setup: Configuration Options". The dialog has a blue title bar with standard window controls (minimize, maximize, close) on the right. Below the title bar, the word "Configuration" is displayed in bold, followed by the text "Tomcat basic configuration." and a colorful feather icon. The main area of the dialog is light gray and contains four configuration fields:

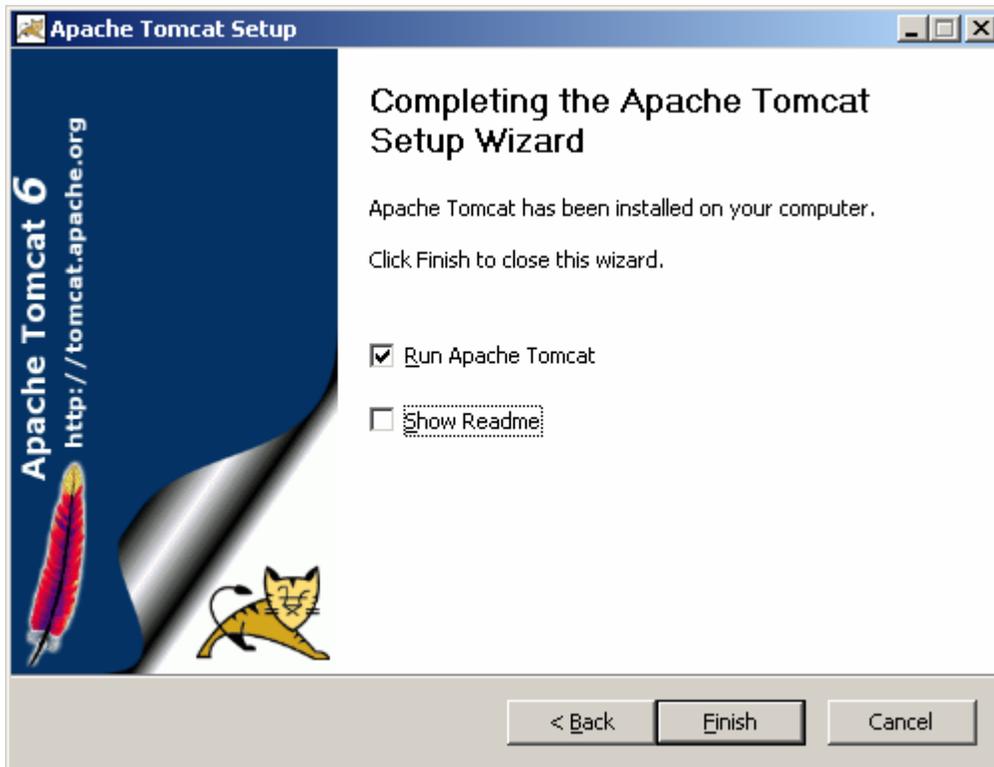
- HTTP/1.1 Connector Port:** A text box containing the value "8080".
- Administrator Login:** A label with no corresponding input field.
- User Name:** A text box containing the placeholder text "define a username".
- Password:** A text box containing ten black dots, indicating a password is being entered.

At the bottom left of the dialog, the text "Nullsoft Install System v2.22" is visible. At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel".

Define the path to the Java Virtual Machine



Apache Tomcat should now be installed and should be run by ensuring the checkbox is selected.



2.1. VERIFYING APACHE TOMCAT INSTALL

An Apache Tomcat icon should appear in the taskbar with the following status:

Started = A green Arrow

Stopped = A red square

Also the services for the system should list an Apache Tomcat service

Verify the administration page can be connected to by connecting to:

<http://127.0.0.1:8180>

and remotely by

<http://<IP Address>:8180>

If Apache Tomcat fails to start check the system logs and the Apache Tomcat logs located under:

C:\Program Files\Apache Software Foundation\Tomcat x.xx\logs

You can start and stop Tomcat from the Computer Management console. Click on start then right click on My Computer and select manage. Click on Services and Applications and then on Services. There will be an Apache Tomcat service that you can start/stop/restart.

3. PINSafe INSTALLATION

Stop Apache Tomcat, if it is running.

Copy the pinsafe.war file to the Apache Tomcat webapps folder:

C:\Program Files\Apache Software Foundation\Tomcat x.x\webapps

Start Apache Tomcat.

A pinsafe folder should appear. If it fails to appear after a few minutes, stop Apache Tomcat then

start the service.

3.1. CONNECTING TO PINSAFE

Connect to the PINsafe server from a web browser using port

http://<IP Address>:8180/pinsafe

<http://127.0.0.1:8180/pinsafe>

4. FIRST STEPS IN PINSAFE

4.1. LOGIN

Enter the default username of admin, then click on Start Session, PINsafe has a default PIN of 1234. Extract the One Time Code, and enter it into the OTC box, from the example below the OTC is 3527.

SWIVEL[®]
AUTHENTICATION YOU CAN IDENTIFY WITH

PINsafe v3.3.2021 © 2007
ith000144-pinsafe

• [Login](#)

PINsafe Administration Login

Username:

Password:

OTC:

1	2	3	4	5	6	7	8	9	0
3	5	2	7	9	6	8	0	1	4

4.2. ENTER LICENSE KEY

PINsafe comes with a perpetual 5 user evaluation license key. If you have a license key for PINsafe enter it under Server/License.

• [Status](#)

• [Log Viewer](#)

▣ Server

- [Name](#)
- [Language](#)
- [License](#)
- [Jobs](#)
- [SMTP](#)
- [Agents](#)

Server > License

Please enter your PINsafe license key below.

License key:

4.3.SET AN INTERNAL DATABASE

Configure an internal database from Database/General, setting the Database to Internal then apply.

- [Status](#)
- [Log Viewer](#)
- ▣ [Server](#)
- ▣ [Policy](#)
- ▣ [Logging](#)
- ▣ [Transport](#)
- ▣ [Database](#)
 - [General](#)
 - [Internal](#)
 - [Connection Pool](#)
- ▣ [Mode](#)
- ▣ [Repository](#)
- ▣ [RADIUS](#)
- ▣ [Migration](#)
- [User Administration](#)
- [Save Configuration](#)
- [Administration Guide](#)
- [Logout](#)

Database>General

Please select and configure a Database. The selected Database will be used to hold authentication information about users.

Database:	<input type="text" value="Internal"/>
Case sensitive usernames:	<input type="text" value="No"/>
Databases:	
Identifier:	<input type="text" value="Shipping"/>
Class:	<input type="text" value="com.swiveltechnologies.pinsafe.user.database.ShippingDatabase"/>
Driver:	<input type="text"/>
URL:	<input type="text"/>
Username:	<input type="text"/>
Password:	<input type="password"/>
	<input type="button" value="Delete"/>
Identifier:	<input type="text" value="Internal"/>
Class:	<input type="text" value="com.swiveltechnologies.pinsafe.user.database.InternalDatabase"/>
Driver:	<input type="text"/>
URL:	<input type="text"/>
Username:	<input type="text"/>
Password:	<input type="password"/>
	<input type="button" value="Delete"/>

4.4. SET SYNCHRONIZED MODE

Set the Mode to Synchronized under Mode/Synchronized

- [Status](#)
- [Log Viewer](#)
- ▣ Server
- ▣ Policy
- ▣ Logging
- ▣ Transport
- ▣ Database
- ▣ Mode
 - [General](#)
 - [Synchronized](#)
- ▣ Repository
- ▣ RADIUS
- ▣ Migration
- [User Administration](#)
- [Save Configuration](#)
- [Administration Guide](#)
- [Logout](#)

Mode>General

Please select and configure a Mode.

Mode:

Modes:

Identifier:	<input type="text" value="Synchronized"/>	
Class:	<input type="text" value="com.swiveltechnologies.pinsafe.user.mode.SynchronizedMode"/>	<input type="button" value="Delete"/>
Identifier:	<input type="text" value="Slave"/>	
Class:	<input type="text" value="com.swiveltechnologies.pinsafe.user.mode.SlaveMode"/>	<input type="button" value="Delete"/>
Identifier:	<input type="text"/>	
Class:	<input type="text"/>	

4.5. CREATE AN XML REPOSITORY

Configure an XML Repository under Repository/Servers, enter a Repository Name and select Repository type XML, then click on apply.

SWIVEL
AUTHENTICATION YOU CAN IDENTIFY WITH

PINsafe v3.3.2021 © 2007
ith000144-pinsafe

Repository > Servers

Please add and configure the user repository servers.

Repository Servers:

Repository Name:	<input type="text" value="XML"/>	
Repository Type:	XML	<input type="button" value="Delete"/>
Repository Name:	<input type="text"/>	
Repository Type:	XML	<input type="button" value="Delete"/>

Delete users with server:

4.6. SYNC USERS

Under User Administration click on the User Sync button, then click on the user and set a PIN number for the user by clicking on the reset PIN button and entering a new PIN.

5. TROUBLESHOOTING

Check the PINsafe, Windows and Apache Tomcat logs.

6. ADDITIONAL INFORMATION

For assistance in the PINsafe installation and configuration please contact your reseller or email nAppliance support at support@nappliance.com