Mario Enrico Ragucci

SailPoint Technologies GmbH

TinyMFA

a multifactor-authentication plugin for IdentityIQ

Table of Contents

[Versioning 2](#_Toc497429997)

[Introduction 3](#_Toc497429998)

[Installation 3](#_Toc497429999)

[Pre-requisites 3](#_Toc497430000)

[Installation 3](#_Toc497430001)

[Post-Installation 3](#_Toc497430002)

[Plugin Settings 3](#_Toc497430003)

[Assigning Capabilities 4](#_Toc497430004)

[Administrative Setup 4](#_Toc497430005)

[Usage 5](#_Toc497430006)

[Generate QR-Code 5](#_Toc497430007)

[Test your token 6](#_Toc497430008)

[Plugin Uninstall Instructions 6](#_Toc497430009)

## Versioning

| **Version** | **Autor** | **Review** | **Comment** | **Datum** |
| --- | --- | --- | --- | --- |
| 1.0 | Mario Enrico Ragucci | - | Initial version | 02.11.2017 |
|  |  |  |  |  |

# Introduction

IdentityIQ 7.2 introduced a new functionality for multifactor authentication. To leverage this functionality without having the need of owning a RSA- or DUO account, the TinyMFA Plugin was created.

This plugin implements the RFC for TOTP based tokens, so (in theory) it is compatible with any app that can register QR-Codes and calculate TOTP tokens (tested with google-authenticator, DUO mobile and FreeOTP). To maximize security, each user gets a unique 128bit key assigned that will be used to calculate the token.

Also, it ships with a MFA configuration, a DynamicScope and assignable Capabilities to grant users access to their personalized token (via QR-Code) as well as forcing users to authenticate with a token.

# Installation

## Pre-requisites

This plugin makes usage of the new multifactor features introduces with IdentityIQ 7.2. Therefore, its usage is limited to this version (or its successors).

## Installation

As an administrator, go to the plugin administration page. Click on the “new” button on the topright corner of the administration page. Drag & Drop the tiny-mfa-plugin.zip on the page.

This concludes the installation.

## Post-Installation

### Plugin Settings

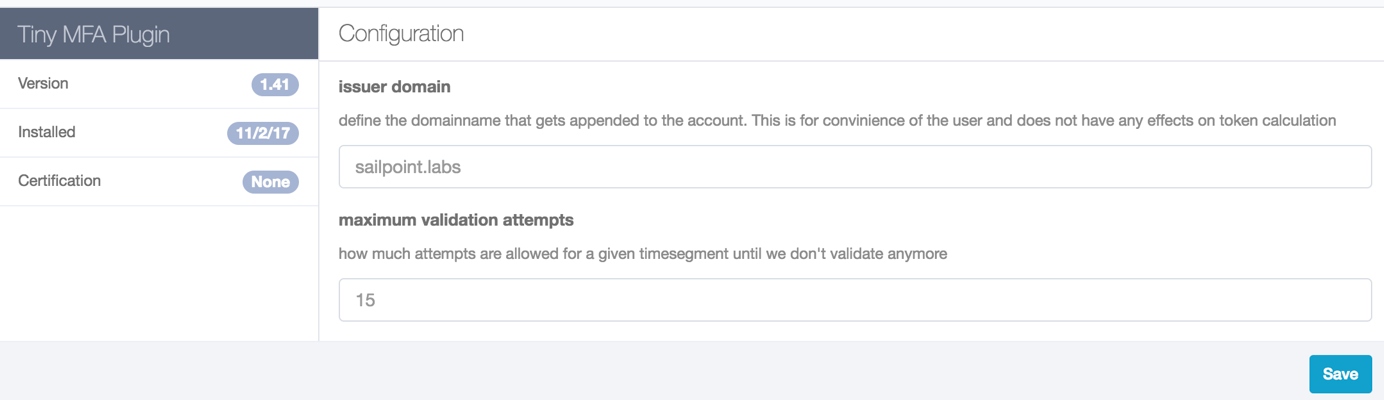


Figure : Plugin Settings

There are two settings on the Plugin Settings page that can be changed according to your needs.

#### Issuer Domain

This will define how the authenticator app will present your account. The format will be %identity.getName()%@%issuerDomain%

Example: [spadmin@sailpoint.labs](mailto:spadmin@sailpoint.labs)

#### Maximum validation attempts

How many validation-attempts per 30 seconds to accept until we don’t allow this certain token to authenticate. This will defeat brute-force attacks.

### Assigning Capabilities

After installing the plugin, a new Capability “TinyMFA Plugin Access” is introduced. This grants access to the plugin page, where you can see your personalized QR Code as well as checking whether your authenticator was registered successfully.

Another Capability “TinyMA activated Identity” can be assigned that results in every user having this capability assigned being part of the Dynamic Scope “TinyMFA Authenticated”.

Also, each identity having this capability assigned are forced to authenticate via a multifactor token.

## Administrative Setup

To review the changes made to the login Login Configuration, go to **Global Settings 🡪 Login Configuration 🡪 MFA Configuration**

You should find an activated Configuration “MFA TinyMFA” with a Population “TinyMFA Authenticated”.

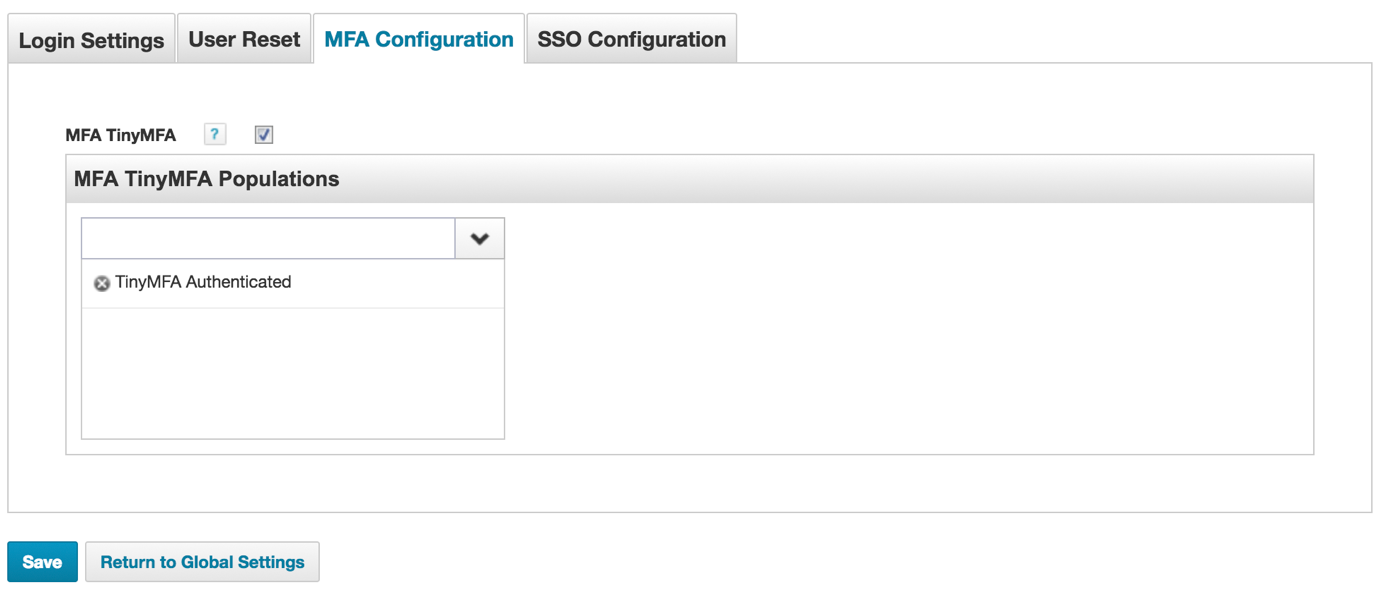


Figure : Login Configuration

# Usage

/Users/mario.ragucci/Desktop/Screen Shot 2017-11-02 at 23.37.43.png

Once entitled to plugin usage, you will find a new icon on your menubar:

By clicking on this icon, you will be transferred to the TinyMFA Plugin page, where you will have several options:

* Generate a QR-Code
* Test your token

## Generate QR-Code



Figure : Generated QR-Code

A QR-Code is generated for your identity that contains all information needed by a multifactor app like google authenticator or DUO mobile.

## Test your token

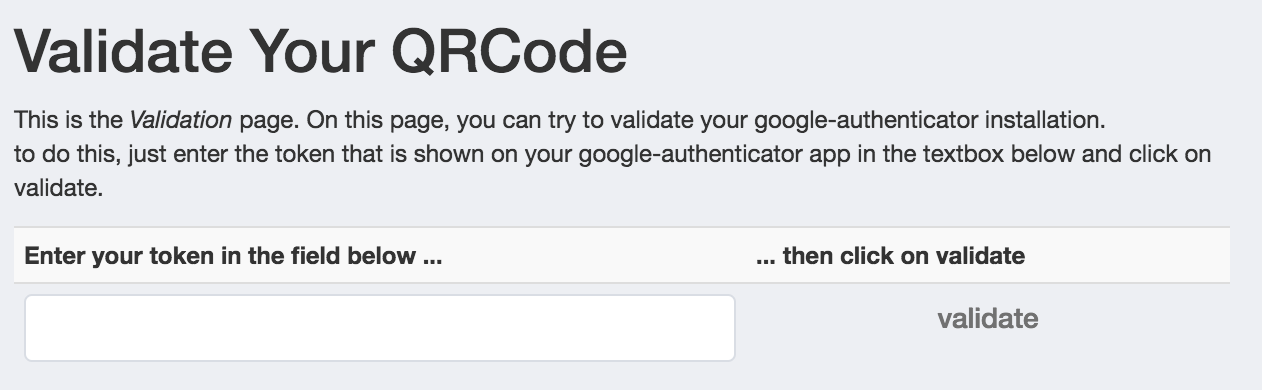


Figure : Test token

On this page, you can test your token generator. Enter the token that your device/app generated, and click on validate. You will receive either success- or errormessage depending on the outcome.

# Plugin Uninstall Instructions

After uninstalling the plugin via the plugin administration page, there are several leftovers that need to be uninstalled manually. You can do this via the debug pages.

* SPRight: TinyMfaPluginIcon
* SPRight: TinyMfaPluginActivatedIdentity
* Capability: TinyMFAActivatedIdentity
* Capability: TinyMFAPluginAccess
* DynamicScope: TinyMFA Authenticated
* Form: TinyMFA Token Form
* Workflow: MFA TinyMFA
* Configuration: MFAConfiguration