
Tokenize User Authentication - User Manual

Nickolas Burr
2019-01-05
Version 1.1.0
Magento 1.x CE

Abstract

This user manual describes the process of configuring and utilizing Tokenize User Authentication, a Magento extension that provides passwordless authentication for administrators and customers.

Contents

1	Introduction	2
1.1	Background	2
1.2	Description	2
2	Configuration	2
2.1	Fields	2
2.1.1	General Settings	2
2.1.2	Administrator Settings	2
2.1.3	Customer Settings	3
3	Usage	4
3.1	Tokenized URLs	4
3.2	Examples	4
4	Feedback	4
4.1	Contact	4
4.2	Reviews	4

1 Introduction

1.1 Background

By default, Magento 1.x password requirements are weak and susceptible to brute-force attacks. There are many ways to mitigate the problem, such as increasing the minimum password length, but even then, this does not eliminate the possibility of a successful brute-force attack, it only slows it down a bit.

1.2 Description

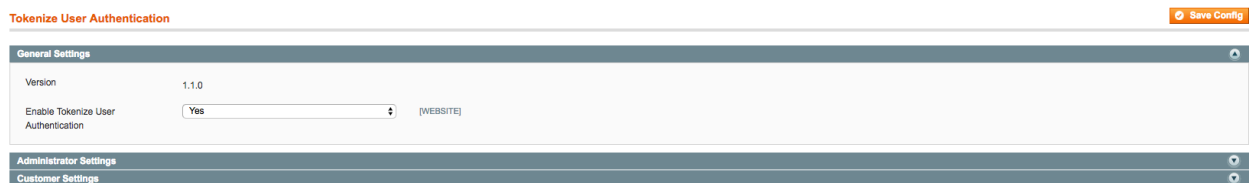
Tokenize User Authentication provides passwordless authentication for administrators and customers alike. Through single-use, tokenized hyperlinks sent via email, a user is able to authenticate quicker, and without the need for username and password input, eliminating the brute-force attack vector.

2 Configuration

2.1 Fields

2.1.1 General Settings

Enable Tokenize User Authentication: Enable the extension. By default, it is disabled.



The screenshot shows the 'Tokenize User Authentication' configuration page with the 'General Settings' tab selected. The page has a 'Save Config' button in the top right corner. The 'General Settings' section includes a 'Version' field showing '1.1.0' and an 'Enable Tokenize User Authentication' checkbox that is currently checked (Yes). There is a '[WEBSITE]' link next to the checkbox.

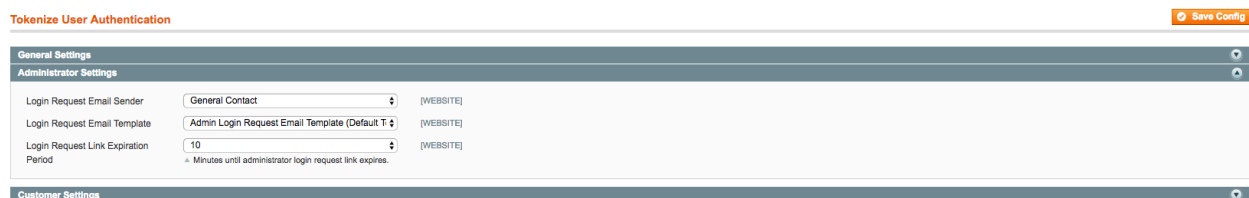
Figure 1: General Settings

2.1.2 Administrator Settings

Login Request Email Sender: The **From** email address for admin login requests.

Login Request Email Template: The email template used for admin login requests. You can customize this template, or add a new one.

Login Request Link Expiration Period: The amount of minutes until the admin login request link expires and is no longer usable. Defaults to **10 minutes**.



The screenshot shows the 'Tokenize User Authentication' configuration page with the 'Administrator Settings' tab selected. The page has a 'Save Config' button in the top right corner. The 'Administrator Settings' section includes three fields: 'Login Request Email Sender' with a dropdown menu showing 'General Contact' and a '[WEBSITE]' link; 'Login Request Email Template' with a dropdown menu showing 'Admin Login Request Email Template (Default T)' and a '[WEBSITE]' link; and 'Login Request Link Expiration Period' with a dropdown menu showing '10' and a '[WEBSITE]' link. Below the 'Expiration Period' field, there is a note: 'Minutes until administrator login request link expires.'

Figure 2: Administrator Settings

2.1.3 Customer Settings

<i>Login Request Email Sender:</i>	The From email address for customer login requests.
<i>Login Request Email Template:</i>	The email template used for customer login requests.
<i>Login Request Link Expiration Period:</i>	The amount of minutes until the customer login request link expires and is no longer usable. Defaults to 30 minutes .
<i>Account Registration Email Sender:</i>	The From email address for customer account registration emails.
<i>Account Registration Email Template:</i>	The email template used for customer account registration emails.
<i>Account Confirmed Email Sender:</i>	The From email address for customer account confirmation notice emails. This is only applicable when customer email verification is enabled.
<i>Account Confirmed Email Template:</i>	The email template used for customer account confirmation emails.
<i>Confirm Account Email Sender:</i>	The From email address for customer confirmation required emails. This is only applicable when customer email verification is enabled.
<i>Confirm Account Email Template:</i>	The email template used for customer confirmation required emails.

Tokenize User Authentication Save Config

General Settings		
Administrator Settings		
Customer Settings		
Login Request Email Sender	General Contact	[WEBSITE]
Login Request Email Template	Customer Login Request Email Template (Default)	[WEBSITE]
Login Request Link Expiration Period	30	[WEBSITE]
	Minutes until customer login request link expires.	
Account Registration Email Sender	General Contact	[WEBSITE]
Account Registration Email Template	Customer Registration Email Template (Default)	[WEBSITE]
Account Confirmed Email Sender	General Contact	[WEBSITE]
Account Confirmed Email Template	Customer Account Confirmed Email Template (C)	[WEBSITE]
Confirm Account Email Sender	General Contact	[WEBSITE]
Confirm Account Email Template	Customer Confirm Account Email Template (Def)	[WEBSITE]

Figure 3: Customer Settings

3 Usage

3.1 Tokenized URLs

For each login request, a 128-character token is generated and associated with the user. The user receives an email containing a one-time magic link, and after authentication, the token is expired. Tokenized URLs can never be used more than once.

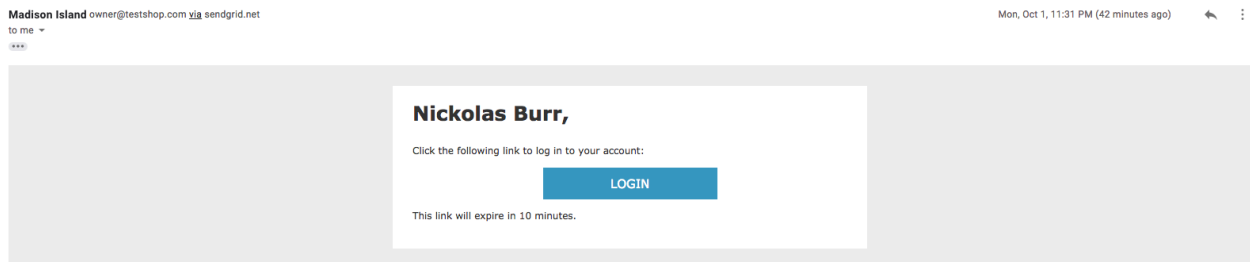


Figure 4: Email Example

3.2 Examples

For a comprehensive list of examples, visit the Tokenize User Authentication wiki.

4 Feedback

4.1 Contact

To get in touch, send an email to **nickolasburr@gmail.com** with the subject line **Tokenize User Authentication Magento 1.x - Customer Inquiry**.

Please allow 48 hours for an inquiry response.

4.2 Reviews

If you find Tokenize User Authentication to be valuable to your business, please consider reviewing the extension on Magento Marketplace.