IMPERVA®

Imperva Incapsula Two-Factor Authentication

DATASHEET

Incapsula Login Protectv lets online businesses implement strong two-factor authentication on any website or application without integration, coding or software changes. Activated with a single click, Two-Factor Authentication lets you instantly protect administrative
access to any page or URL, secure remote access to corporate web applications, and restrict access to a particular webpage. With Two-Factor Authentication, you can manage and control multiple logins across several websites in a centralized manner. Two-factor authentication is supported using either email, SMS or Google Authenticator. Login Protect is provided with all Incapsula plans. The number of users and authentication methods vary, depending on your service plan.

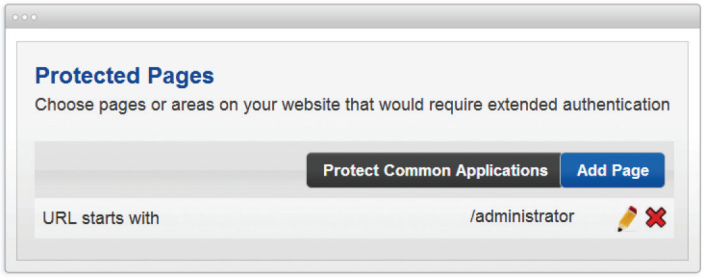
What You Get

- Two-factor authentication for website access
- Protect login to administrative areas (e.g., WordPress or Joomla admin)
- Secure remote access to corporate applications (e.g., employee portal, web mail)
- Restrict access to sites or parts of a site (e.g., staging or invitation-only areas)

Simple Setup & Activation

Two-Factor Authentication is designed for fast and easy implementation. Once Incapsula has been activated on your website, setting up Two-Factor Authentication consists of three easy steps:

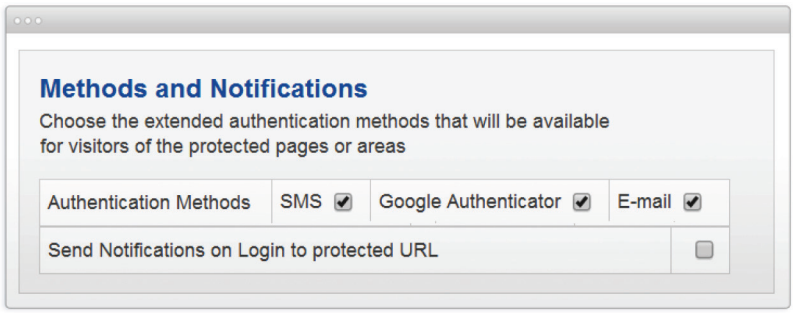
1. Select the URLs or folders you wish to protect, using either exact match or one of the wildcard options



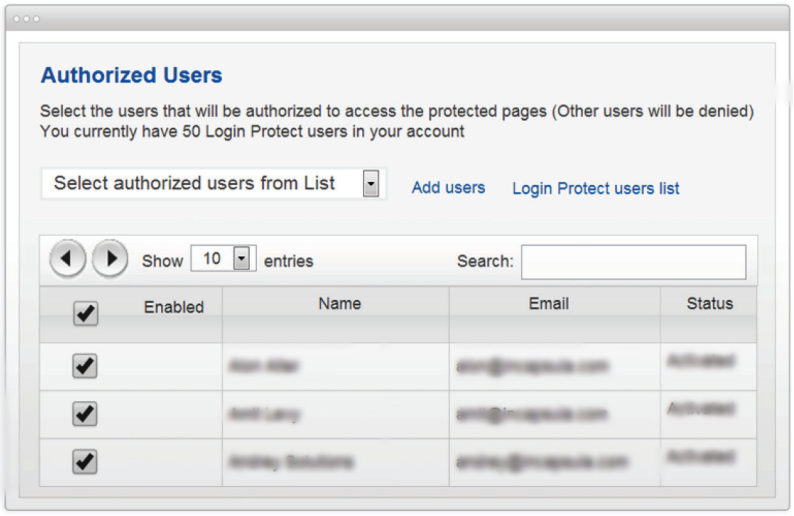
Why Incapsula?

- Activated with a single click, without installing any plugins, making code changes or having to integrate with 3rd party authentication products
- Zero disruption to application functionality and existing username/password management
- Centralized control and management of multiple logins, across several websites

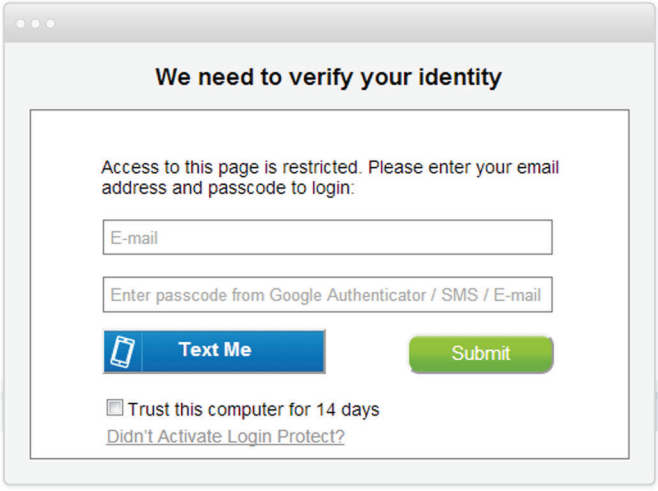
2. Choose the preferred methods of authentication for this URL



3. Define the list of users that can access this URL



Once the setup is complete, anyone trying to access the protected page will first receive an Incapsula Two-Factor Authentication page where they'll be asked to enter a one-time passcode received through one of the pre-defined methods of authentication.



Transparent Integration with Your Application

Using Two-Factor Authentication as an additional layer of authentication for a webpage requires zero integration and zero changes to the way you manage users and passwords on your own application. For example, let's say you want to protect the admin area of an internal HR application. Two-Factor Authentication setup for this area is performed outside of the HR application and is completely transparent to the existing user management functionality.

Authentication Methods

Two-Factor Authentication supports a variety of methods for authenticating the identity of your users, prior to enabling them access to protected pages. Complementing username and password which are based on "something you know", these methods are based on "something you have". Users may choose to use one or more of the following methods (the exact methods available are determined by the site admin during Two-Factor Authentication setup for each site):

- **Email:** user receives an email with the one-time login code
- **Google Authenticator:** user receives the one-time login code via the Google Authenticator App
- **SMS:** user receives an SMS with the one-time login code

When users try to access the protected pages or areas on your site, they will be asked to authenticate using their one-time passcode. After filling in their passcode, they gain access to the application, where in most cases they are asked to enter their username and password.

User Management

An easy-to-use management tool lets you easily define who will be able to access Two-Factor Authentication protected pages after authentication. Users may be selected from the Two-Factor Authentication List of users, which encompasses all users of all sites covered by the specific Incapsula account. New users may be added to this list as needed. Incapsula auto-dispatches an activation email to all selected users.

Application-Aware CMS Integration

Two-Factor Authentication streamlines integration with popular CMS applications through application-aware integration. Incapsula recognizes your connected applications and optimizes its security and acceleration processes for their use. Upon enabling Two-Factor Authentication, Incapsula auto-detects your CMS platform and provides a basic set of two-factor authentication deployment settings. For example, in the case of WordPress, Incapsula identifies the platform and suggests a wildcard rule to protect all pages starting with '/wp-admin', which secures the WordPress default admin area. Currently, the Application Awareness option supports WordPress, Joomla and phpBB, and will be extended to more platforms in the future.

IMPERVA INCAPSULA

Incapsula vs. Other Two Factor Authentication Solutions

FEATURE	INCAPSULA	OTHERS
Integration	5 minute setup, no integration or coding required	Requires time-consuming integration and coding
Flexible protection options	Choose the parts of a web application you wish to protect	Protect login pages only
Security approach	Appears before the protected page, blocking access to it	Appears on or after the protected page is accessed, exposing the login page itself to attacks and hacking attempts
Login management	Centralized control over multiple logins across several websites	Requires separate integration for each website or application
User management	No disruption to the site's existing user/password protection and user database	Requires changes and adds complexity to existing user/password protection and user database