

How to Shield Your Magento Installation from Password Guessing Attacks?

As we have noticed that password guessing attack on Magento installation is growing worldwide, so we are going to discuss some ways to help you shield your Magento installation from such password guessing attacks.

Every Magento store features two sections for administrative usage (also known as back end or admin panel), and these attacks have led to unauthorized back-end access. So, we recommend you to take following actions in opposition of such attacks:

Note: If it is case associated with Magento 1 installation, it requires shielding “locations/admin” & “/downloader”. Otherwise, you need to protect only the admin panel location in case of Magento 2 installation.

Step 1: You need to review all your admin users (located in System> Permissions> Users) at least once in a month & just do away with any unused entries unknown to you.

Step 2: Be it is your own password or any of your employee passwords utilizing the admin panel – needs to be strong. Always keep in mind that longer & complex passwords are more secure and can't be easily guessed. Also, keep you continue to change admin passwords every three months.

Step 3: Ensure that you are using a user name that you can easily remember, but that is harder for others to guess. So, we recommend you not to use something like “admin”, “admin123”, “admin@123”, etc...

Step 4: Security patches play one of the most significant

roles behind the security of a Magento store. So, make sure that you have patched your Magento store up to the latest Magento security patch, which are accessible on “My Account of Adobe commerce (Magento Commerce)” for Enterprise Edition customers and on the “Community Edition Download Page of Adobe commerce (Magento Commerce)” for the Community Edition.