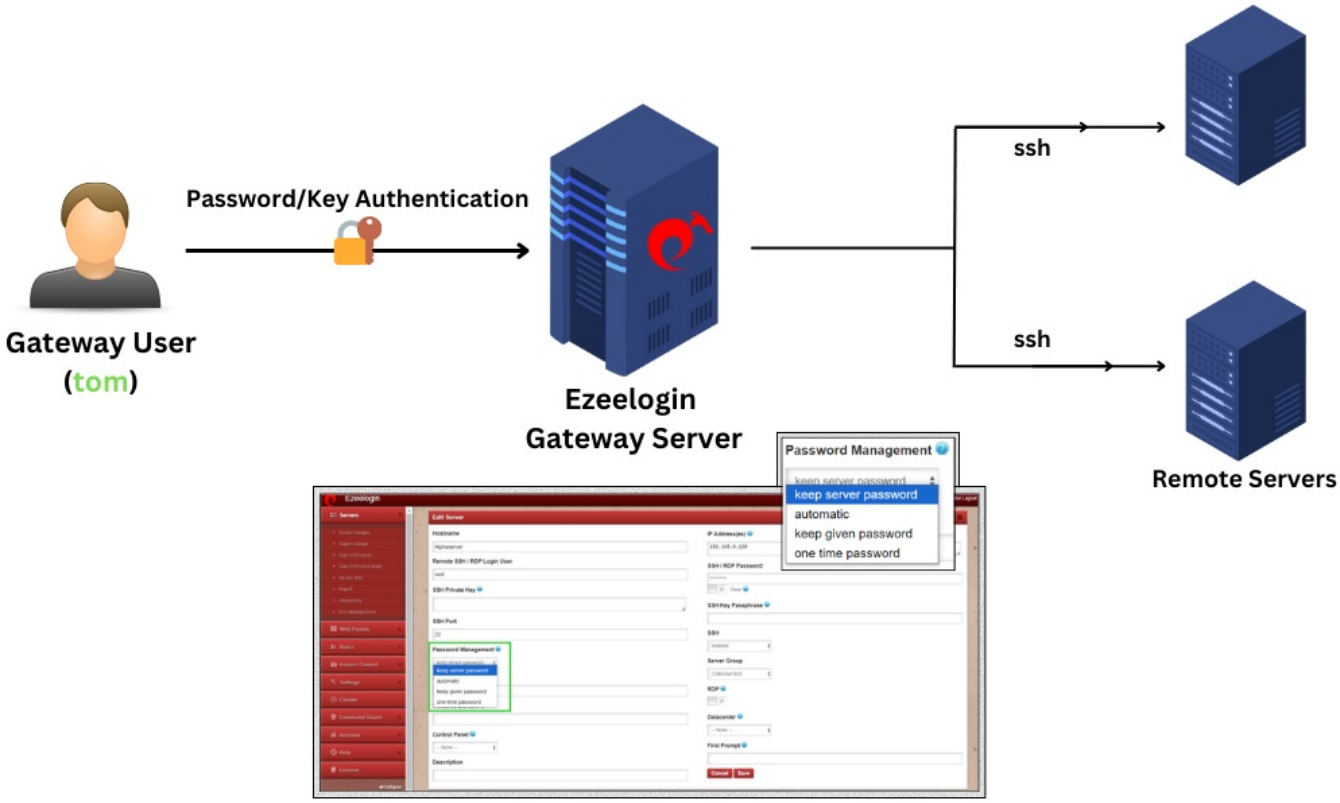
Password management and the different options

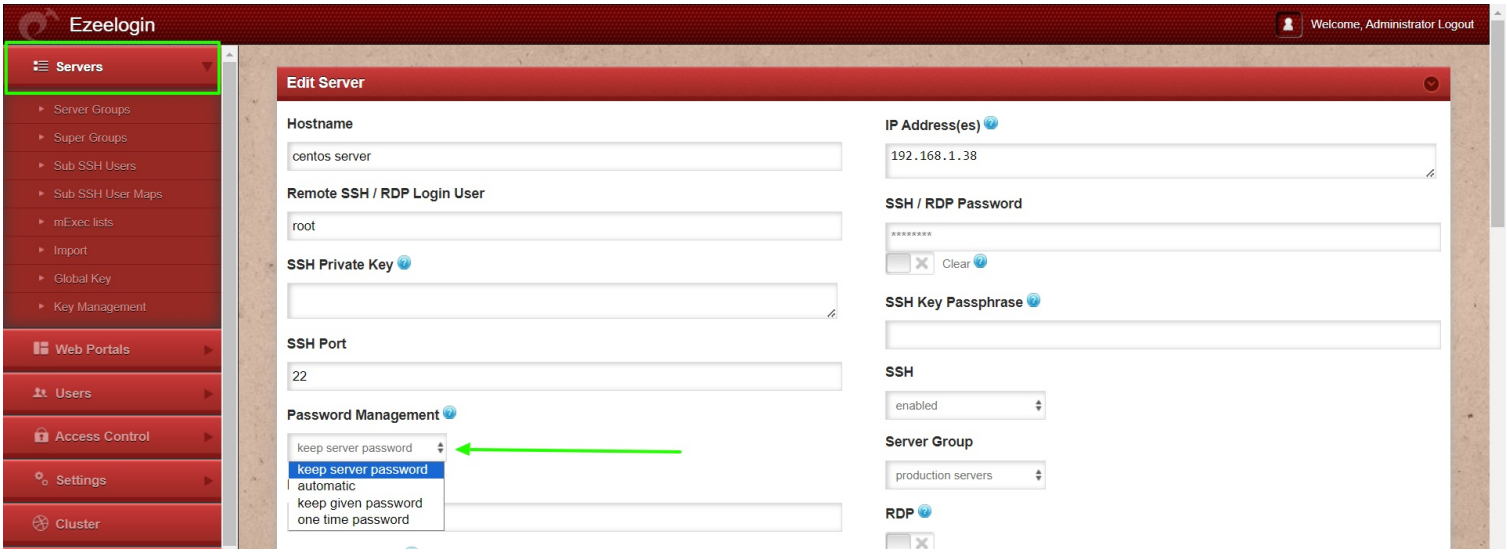
14 admin September 26, 2024 Features & Functionalities 17493

How do Automatic, Keep Given, and Keep Server Password Options Differ?

Overview: This article will provide a better understanding of how password management works and explain various options such as automatic, keep server password, keep given password, and OTP.



You can choose the following password management options by *editing any user under the Server section* menu.



1. Keep server password:

This option allows the gateway user to **add the target server to the Ezeelogin system without confirming whether the entered password is correct**. If an incorrect password is provided, the target server will still be added, but the gateway user will not be able to log in to the target server via the SSH gateway.

This option is typically chosen when the user does not know the current password set on the target server but does not want to change it to add the system to the SSH gateway. We recommend copying the Servers -> Global Key into the target server's /root/.ssh/authorized_keys file to enable login to the target server via SSH in the Ezeelogin shell (ezsh).

2. Automatic:

This option allows the gateway user to add the target server, after which the **password is automatically reset to a new one**. The password entered in the target server add form is used to log in and verify that it works before the target server is added to the system. Once verified, a new password is auto-generated and set for the added target server. We recommend this option for optimal security, as it enables automatic password resets with a single click.

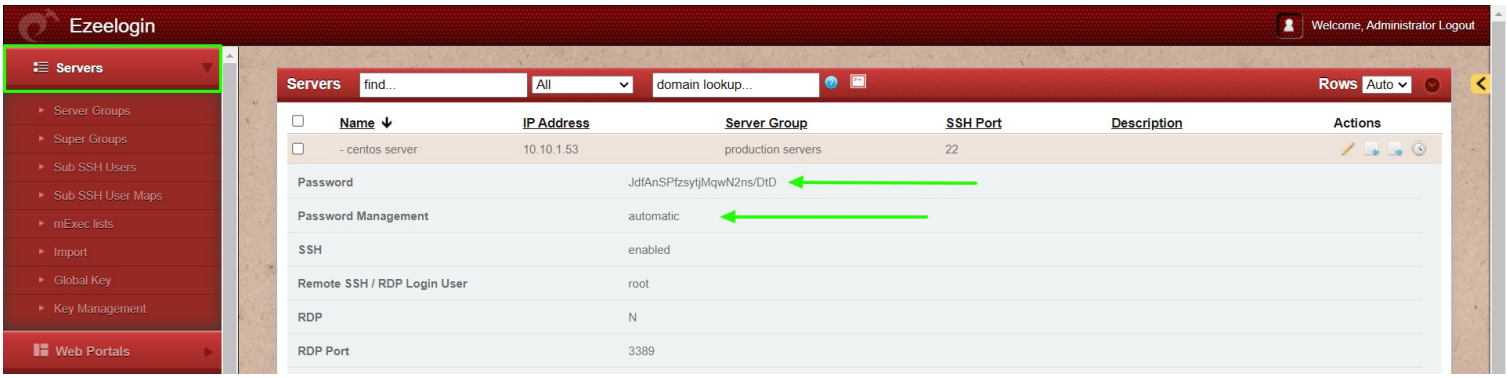
3. Keep given password:

This option allows the gateway user to preserve the **current password set on the server, ensuring that it will not be changed on the target server** during an automatic password reset across all target servers. The password entered in the server add form is used to log in and verify its validity. The target server is added only if the login succeeds with the given password.

4. One-time password:

This option allows the gateway user to enter the corresponding **one-time password at the password prompt**. This is useful when you have servers with OTP authentication that require manual entry of random codes.

Ex: The following image shows an example of a remote server displaying a password in Ezeelogin GUI.



Make sure to access the Ezeelogin software GUI with 2FA and enable HTTPS to display the password of the remote server.

Related Articles:

How to add target servers to Ezeelogin?

How to prompt for a username and password while logging into the remote device?

How do we manage SSH access to Routers and Switch with Ezeelogin?

Online URL: https://www.ezeelogin.com/kb/article/password-management-and-the-different-options-14.html