

Configure Security Policies

(WHM >> Home >> Security Center >> Configure Security Policies)

- [Overview](#)
- [Security Policy Items](#)
- [Security Policy Extensions](#)
- [Disable security questions via SSH](#)
- [Additional documentation](#)

Overview

The *Configure Security Policies* interface allows you to configure your security policy options and security policy extensions.

Notes:

- When you attempt to log in from an unverified IP address and successfully answer your security questions, the system automatically adds the IP address to the list of verified IP addresses.
- If you configure your own security questions, and then immediately enable the *Limit logins to verified IP addresses* setting in this interface, the system automatically adds your IP address to the list of verified IP addresses.

Security Policy Items

Select the following checkboxes to help secure your server:

Option	Description
<i>Limit logins to verified IP addresses</i>	<p>This option determines whether to require users to answer security questions when they log in to their cPanel, Webmail, and WHM accounts from unverified IP addresses.</p> <p>Notes:</p> <ul style="list-style-type: none">• When a user successfully answers the required security questions, the system automatically adds the user's current IP address to the list of verified IP addresses.• WHM users can add verified IP addresses and configure security questions in WHM's <i>Security Questions</i> interface (<i>WHM >> Home >> Security Center >> Security Questions</i>).• After you enable this option, cPanel users can add verified IP addresses and configure security questions in cPanel's <i>Security Policy</i> interface (<i>cPanel >> Home >> Security >> Security Policy</i>).
<i>Two-Factor Authentication: Google Authenticator</i>	<p>This option determines whether to require users additionally enter a generated security code provided by a time-based one-time password (TOTP) app on a smartphone.</p> <p>Note:</p> <p>To configure the two-factor authentication settings, use WHM's <i>Two-Factor Authentication</i> interface (<i>WHM >> Home >> Security Center >> Two-Factor Authentication</i>).</p>

<i>Password Strength</i>	<p>This option enforces a minimum password strength for cPanel, Webmail, and WHM users.</p> <div style="border: 1px solid #f0e68c; padding: 5px; margin-top: 10px;"> <p>Note: To modify the minimum password strength, use WHM's Password Strength Configuration interface (<i>WHM >> Home >> Security Center >> Password Strength Configuration</i>).</p> </div>
<i>Password Age</i>	<p>This option allows you to specify the number of days to allow cPanel, Webmail, and WHM users to use the same password.</p> <p>When you select this checkbox, the <i>Maximum password age (in days)</i> text box appears. Enter the maximum number of days to allow users to use the same password.</p>

Security Policy Extensions

The *Security Policy Extensions* options apply your security policy to WHM API requests and DNS cluster requests.

Enable the following options to help secure your server:

Option	Description
<i>API requests</i>	Select this checkbox to apply the <i>Security Policy Items</i> settings to WHM API requests. If you enable this option, the policies that you set apply to any user who attempts to call a WHM API function.
<i>DNS Cluster requests</i>	Select this checkbox to apply the <i>Security Policy Items</i> settings to DNS cluster requests. If you enable this option, the policies that you set apply to any user who attempts to make a DNS cluster request.

Disable security questions via SSH

To disable security questions via the command line, perform the following steps:

1. Use SSH to log in to your server as the `root` user.
2. Open the `/var/cpanel/cpanel.config` file in your preferred text editor.
3. Change the value of the `SecurityPolicy::SourceIPCheck` option to `0`.
4. Save and exit the file.
5. Run the `/scripts/restartsrv cpanel` command to restart cPanel & WHM.

Additional documentation

Suggested documentation [For cPanel users](#) [For WHM users](#) [For developers](#)

- [Configure Security Policies](#)
- [Security Questions](#)
- [Two-Factor Authentication for WHM](#)
- [The failurls File](#)
- [Tweak Settings - Display](#)
- [Two-Factor Authentication for cPanel](#)
- [Password and Security](#)
- [SSH Access](#)

- [SSL TLS Wizard](#)
- [Security Policy](#)

- [Configure Security Policies](#)
- [Basic Security Concepts](#)
- [Security Questions](#)
- [Two-Factor Authentication for WHM](#)
- [The failurls File](#)

- [Guide to cPanel Interface Customization - Login Templates](#)
- [Guide to cPanel Interface Customization - Login Images](#)
- [WHM API 1 Functions - setminimumpasswordstrengths](#)
- [Guide to API Authentication - API Tokens in WHM](#)
- [UAPI Modules - LastLogin](#)