

---

# Recommended Security Settings

Copyright © 2009 cPanel, Inc.

Revision 1	Revision History
Revision 2	Sept. 28, 2009
Revision 3	Oct. 16, 2009
Revision 4	Nov. 30, 2009
	Dec. 9, 2009

## Table of Contents

1. Recommended Security Settings .....	1
2. Recommended Security Settings Checklist .....	1
3. Authentication Method .....	1
4. Cookies .....	2
5. Require SSL .....	2
6. Security Token .....	3
6.1. Referrer Checking .....	3
7. Password Strength .....	4

## 1. Recommended Security Settings

This document describes security settings cPanel recommends as of cPanel version 11.25. The scope of the discussion is limited to the cPanel/WHM product. Operating System and Network security is only addressed where applicable.

## 2. Recommended Security Settings Checklist

The following tables summarize the recommended security settings discussed in this document.

**Table 1. Tweak Settings Checklist**

Setting	Recommendation
Disable HTTP Authentication for cPanel/WebMail/WHM Logins (forces cookie authentication).	<b>Enabled</b>
Validate the IP addresses used in all cookie based logins.	<b>Enabled</b>
Automatically create cpanel, webmail, webdisk and whm proxy subdomain DNS entries for new accounts	<b>Disabled</b>
Require SSL for all remote logins to cPanel, WHM and Webmail	<b>Enabled</b>
Require security tokens for all interfaces.	<b>Enabled</b>

**Table 2. Security Center Checklist**

Setting	Recommended Value
Default Password Strength	<b>50+</b>

## 3. Authentication Method

Setting	Recommendation
Disable HTTP Authentication for cPanel/WebMail/WHM Logins (forces cookie authentication).	Enabled

The design of HTTP Authentication does not allow for logging out of an authenticated session. Once a HTTP Authentication session is established, the credentials are cached by the browser until the browser application is terminated. Some browsers allow a method to flush the credentials, but this method is not reliable nor available in all browsers. Because the authentication credentials are cached they are a likely target for cross-site request forgery attacks, often known as XSRF or CSRF.

Due to the inherent weaknesses of HTTP Authentication cPanel recommends disabling its use with the product. This is done by checking the box of the Tweak Setting labeled:

*Disable Http Authentication for cPanel/WebMail/WHM Logins (forces cookie authentication.) This will help prevent certain types of XSRF attacks that rely on cached Http Auth credentials.*

As noted in the Tweak Setting description, disabling HTTP Authentication forces use of Cookie based logins.

## 4. Cookies

Setting	Recommendation
Validate the IP addresses used in all cookie based logins. This will limit the ability of attackers who capture cPanel session cookies to use them in an exploit of the cPanel or WebHost Manager interfaces. For this setting to have maximum effectiveness, proxydomains should also be disabled.	Enabled

Malicious users can steal cookies for use in CSRF and XSS attacks. There is little to no protection provided by browsers to mitigate this attack vector. To prevent malicious use of cookies used by cPanel, version 11.25 allows recording of the originating IP address as part of the cookie during authentication. On subsequent requests the remote IP address is compared to the original value in the cookie. Mismatches cause an error and result in a request for re-authentication. It is recommended this protection be enabled.



### Proxy Access with Cookie IP Validation

When using this feature it is **strongly** recommended that Proxy domains be disabled. Access via the proxy domains will record the IP address for localhost ( typically 127.0.0.1 ) in the cookie rendering the IP validation check moot.

To enable this protection, check the box for the following **Tweak Setting**:

- *Validate the IP addresses used in all cookie based logins. This will limit the ability of attackers who capture cPanel session cookies to use them in an exploit of the cPanel or WebHost Manager interfaces. For this setting to have maximum effectiveness, proxydomains should also be disabled.*

To disable Proxy domains, uncheck the boxes for the following **Tweak Settings**:

- *Add proxy VirtualHost to httpd.conf to automatically redirect unconfigured cpanel, webmail, webdisk and whm subdomains to the correct port (requires mod\_rewrite and mod\_proxy)*
- *Automatically create cpanel, webmail, webdisk and whm proxy subdomain DNS entries for new accounts. When this is initially enabled it will add appropriate proxy subdomain DNS entries to all existing accounts. (Use /scripts/proxy-domains to reconfigure the DNS entries manually)*

## 5. Require SSL

Setting	Recommendation
Require SSL for all remote logins to cPanel, WHM and Webmail.	Enabled

Whether using HTTP or Cookie based authentication, if the authentication happens on ports 2082, 2086 or 2095 the login credentials are sent in plain text. Requiring authentication to happen via SSL or TLS is a basic way of improving system security. In the past System Administrators were required to block the non-SSL cPanel ports using a firewall.

cPanel 11.25 and newer allow disabling use of ports 2082, 2086 and 2095 for remote authentication. Requests that originate from localhost may still use these ports for authentication. To disable use of ports 2082, 2086 and 2095 for remote authentication purposes check the box for the following **Tweak Setting**:

*Require SSL for all remote logins to cPanel, WHM and Webmail. This setting is recommended.*

When the **Tweak Setting** is enabled, remote authentication requests to ports 2082, 2086 and 2095 will encounter a page redirecting the user to the proper port. The redirection is not automatic.

## 6. Security Token

Setting	Recommendation
Require security tokens for all interfaces.	Enabled

Cross-site request forgery, often abbreviated as CSRF or XSRF, exploits the trust a website has in a user's browser. By exploiting that trust a malicious user can execute unauthorized commands on a website. CSRF attacks rely upon two items to accomplish a successful attack:

- Access to authentication credentials
- Surreptitious execution of a command ( url )

To prevent CSRF attacks cPanel can insert into the URL a token unique to the login session. Requests without the token produce an error and a request for authentication. This effectively thwarts CSRF attacks as the attacking URL will not contain the token.

To activate the security token feature, check the box for the following **Tweak Setting**

- *Require security tokens for all interfaces. This will greatly improve the security of cPanel and WHM against XSRF attacks, but may break integration with other systems, login applications, billing software and third party themes.*



### Caution

Use of the security token feature may cause usability problems with custom scripts and third-party applications that integrate with cPanel or WHM. It is recommended to verify that the third party application is compatible with security tokens. For applications that are not compatible it is recommended the URL Referrer checks be enabled.

### 6.1. Referrer Checking



### Caution

It is **strongly** recommended to use the security token feature rather than the Referrer checks. The Referrer checks are not as dependable a security mechanism. These checks are only dependable when the "blank referer" check is enabled and enabling the "blank referer" check will result in an unacceptable number of false positives.

The security token works even when the browser is hiding its referrer.

The HTTP Referrer, commonly misspelled referer, identifies the address of the webpage that links to a web page. The identification is performed from the point of view of the requested web page.

### Example 1. Referer

A hyperlink on www.example.com that points to www.example.org will set the referrer to www.example.com

If use of Security Tokens is not possible it is recommended the following settings be enabled in Tweak Settings:

1. *Only permit cpanel/whm/webmail to execute functions when the browser provides a referrer*
2. *Only permit cpanel/whm/webmail to execute functions when the browser provided referrer (Domain/IP and Port) exactly matches the destination URL.*

## 7. Password Strength

Setting	Recommendation
Default Required Password Strength	50+

Weak passwords provide little protection against brute force attacks. Within Web Host Manager's Security Center you can use the **Password Strength Configuration** interface to require new passwords meet a minimum threshold. cPanel recommends setting the minimum threshold to **50** as a starting point.

The Default threshold may be inherited by the granular thresholds, or overridden.

The minimum password strength requirement only applies to passwords created and modified by the product. The feature does not configure PAM to enforce the requirements. Thus a user with shell access may be able to change his password to a weaker one using the **passwd** system utility.