config user setting

Configure user authentication setting.

```
config user setting
    Description: Configure user authentication setting.
    set auth-blackout-time {integer}
    set auth-ca-cert {string}
    set auth-cert {string}
    set auth-http-basic [enable|disable]
    set auth-invalid-max {integer}
    set auth-lockout-duration {integer}
    set auth-lockout-threshold {integer}
    set auth-on-demand [always|implicitly]
    set auth-portal-timeout {integer}
    config auth-ports
        Description: Set up non-standard ports for authentication with HTTP, HTTPS, FTP, and
TELNET.
        edit <id>
            set type [http|https|...]
            set port {integer}
        next
    end
    set auth-secure-http [enable|disable]
    set auth-src-mac [enable|disable]
    set auth-ssl-allow-renegotiation [enable|disable]
    set auth-ssl-max-proto-version [sslv3|tlsv1|...]
    set auth-ssl-min-proto-version [default|SSLv3|...]
    set auth-ssl-sigalgs [no-rsa-pss|all]
    set auth-timeout {integer}
    set auth-timeout-type [idle-timeout|hard-timeout|...]
    set auth-type {option1}, {option2}, ...
    set per-policy-disclaimer [enable|disable]
    set radius-ses-timeout-act [hard-timeout|ignore-timeout]
end
```

config user setting

Parameter	Description	Type	Size	Default
auth-blackout-time	Time in seconds an IP address is denied access after failing to authenticate five times within one minute.	integer	Minimum value: 0 Maximum value: 3600	0
auth-ca-cert	HTTPS CA certificate for policy authentication.	string	Maximum length: 35	
auth-cert	HTTPS server certificate for policy authentication.	string	Maximum length: 35	
auth-http-basic	Enable/disable use of HTTP basic authentication for identity-based firewall policies.	option	-	disable
	Option	**Description**		
	enable	Enable setting.		
	disable	Disable setting.		
auth-invalid-max	Maximum number of failed authentication attempts before the user is blocked.	integer	Minimum value: 1 Maximum value: 100	5
auth-lockout-duration	Lockout period in seconds after too many login failures.	integer	Minimum value: 0 Maximum value: 4294967295	0
auth-lockout-threshold	Maximum number of failed login attempts before login lockout is triggered.	integer	Minimum value: 1 Maximum value: 10	3
auth-on-demand	Always/implicitly trigger firewall authentication on demand.	option	-	implicitly
	Option	**Description**		
	always	Always trigger firewall authentication on demand.		
	implicitly	Implicitly trigger firewall authentication on demand.		
auth-portal-timeout	Time in minutes before captive portal user have to re-authenticate.	integer	Minimum value: 1 Maximum value: 30	3
auth-secure-http	Enable/disable redirecting HTTP user authentication to more secure HTTPS.	option	-	disable
	Option	**Description**		
	enable	Enable setting.		
	disable	Disable setting.		
auth-src-mac	Enable/disable source MAC for user identity.	option	-	enable
	Option	**Description**		
	enable	Enable source MAC for user identity.		
	disable	Disable source MAC for user identity.		
auth-ssl-allow-renegotiation	Allow/forbid SSL re-negotiation for HTTPS authentication.	option	-	disable
	Option	**Description**		
	enable	Allow SSL re-negotiation.		
	disable	Forbid SSL re-negotiation.		
auth-ssl-max-proto-version	Maximum supported protocol version for SSL/TLS connections.	option	-	
	Option	**Description**		
	sslv3	SSLv3.		
	tlsv1	TLSv1.		
	tlsv1-1	TLSv1.1.		
	tlsv1-2	TLSv1.2.		
	tlsv1-3	TLSv1.3.		
auth-ssl-min-proto-version	Minimum supported protocol version for SSL/TLS connections.	option	-	default
	Option	**Description**		
	default	Follow system global setting.		
	SSLv3	SSLv3.		
	TLSv1	TLSv1.		
	TLSv1-1	TLSv1.1.		
	TLSv1-2	TLSv1.2.		
auth-ssl-sigalgs	Set signature algorithms related to HTTPS authentication.	option	-	all
	Option	**Description**		
	no-rsa-pss	Disable RSA-PSS signature algorithms for HTTPS authentication.		
	all	Enable all supported signature algorithms for HTTPS authentication.		
auth-timeout	Time in minutes before the firewall user authentication timeout requires the user to re-authenticate.	integer	Minimum value: 1 Maximum value: 1440	5
auth-timeout-type	Control if authenticated users have to login again after a hard timeout, after an idle timeout, or after a session timeout.	option	-	idle-timeout
	Option	**Description**		
	idle-timeout	Idle timeout.		
	hard-timeout	Hard timeout.		
	new-session	New session timeout.		
auth-type	Supported firewall policy authentication protocols/methods.	option	-	http https ftp telnet
	Option	**Description**		
	http	Allow HTTP authentication.		
	https	Allow HTTPS authentication.		
	ftp	Allow FTP authentication.		
	telnet	Allow TELNET authentication.		
per-policy-disclaimer	Enable/disable per policy disclaimer.	option	-	disable
	Option	**Description**		
	enable	Enable per policy disclaimer.		
	disable	Disable per policy disclaimer.		
radius-ses-timeout-act	Set the RADIUS session timeout to a hard timeout or to ignore RADIUS server session timeouts.	option	-	hard-timeout
	Option	**Description**		
	hard-timeout	Use session timeout from RADIUS as hard-timeout.		
	ignore-timeout	Ignore session timeout from RADIUS.		

config auth-ports

Parameter	Description	Type	Size	Default
id	ID.	integer	Minimum value: 0 Maximum value: 4294967295	0
type	Service type.	option	-	http
	Option	**Description**		
	http	HTTP service.		
	https	HTTPS service.		
	ftp	FTP service.		
	telnet	TELNET service.		
port	Non-standard port for firewall user authentication.	integer	Minimum value: 1 Maximum value: 65535	1024