



## **User Management and Security Commands**

# Table of contents

## User Accounts

username

show usernames

show users

show whoami

password

show password hardening

## AAA Methods

aaa accounting

aaa authentication login

aaa authentication attempts fail-delay

aaa authentication attempts track

aaa authentication attempts logout

aaa authentication attempts class-override

aaa authentication attempts reset

clear aaa authentication attempts

aaa authorization

show aaa

show aaa authentication attempts

## RADIUS

radius-server

radius-server host

show radius

## TACACS+

---

tacacs-server

---

tacacs-server host

---

show tacacs

---

## LDAP

---

ldap enable

---

ldap base-dn

---

ldap bind-dn/bind-password

---

ldap group-attribute/group-dn

---

ldap nested-group-search

---

ldap nested-group-depth

---

ldap nested-group-count

---

ldap host

---

ldap hostname-check enable

---

ldap login-attribute

---

ldap port

---

ldap referrals

---

ldap scope

---

ldap ssl

---

ldap timeout

---

ldap version

---

show ldap

---

show ldap crl

---

## System Secure Mode

---

system secure-mode enable

---

show system secure-mode

---

show secure-boot-status

---

## System Secure SSD Wipe

---

system ssd-wipe

---

# User Accounts

## username

	<p>username &lt;username&gt; [capability &lt;cap&gt;   disable [login   password]   disconnect   full-name &lt;name&gt;   nopassword   password [0   7] &lt;password&gt;]</p> <p>no username &lt;username&gt; [capability   disable [login   password]   full-name]</p> <p>Creates a user and sets its capabilities, password and name. The no form of the command deletes the user configuration.</p>	
Syntax Description	username	<p>Specifies a username and creates a user account. New users are created initially with admin privileges but is disabled.</p> <p>Allowed characters for the username:</p> <ul style="list-style-type: none"> <li>• a-z</li> <li>• A-Z</li> <li>• 0-9</li> <li>• period (.), underscore (_), hyphen (-)</li> </ul> <p>Any single character or combination of characters from the above is allowed except for a period "." in a single form.</p>
	capability <cap>	<p>Defines user capabilities.</p> <ul style="list-style-type: none"> <li>• admin—full administrative capabilities</li> <li>• monitor—read only capabilities, can not change the running configuration</li> <li>• unpriv—can only query the most basic information, and cannot take any actions or change any configuration</li> <li>• v_admin—basic administrator capabilities</li> </ul>
	disable [login   password]	<ul style="list-style-type: none"> <li>• Disable—disable this account</li> <li>• Disable login—disable all logins to this account</li> <li>• Disable password—disable login to this account using a local password</li> </ul>
	disconnect	Logs out the specified user from the system.

	name	Full name of the user.														
	nopassword	The next login of the user will not require password.														
	0   7	<ul style="list-style-type: none"> <li>• 0—specifies a login password in cleartext</li> <li>• 7—specifies a login password in encrypted text</li> </ul>														
	password	Specifies a password for the user in string form. If [0   7] was not specified then the password is in cleartext.														
Default	<p>The following usernames are available by default:</p> <ul style="list-style-type: none"> <li>• admin</li> <li>• monitor</li> </ul>															
Configuration Mode	config															
History	<table border="1"> <tr> <td>3.1.000 0</td> <td></td> </tr> <tr> <td>3.4.000 0</td> <td>Updated example</td> </tr> <tr> <td>3.4.110 0</td> <td>Updated example</td> </tr> <tr> <td>3.6.200 2</td> <td>Added “disconnect” parameter</td> </tr> <tr> <td>3.8.100 0</td> <td>Added "username" syntax description (allowed characters)</td> </tr> <tr> <td>3.8.200 0</td> <td>Removed xmladmin and xmluser usernames due to XML depreciation</td> </tr> <tr> <td>3.9.090 0</td> <td>Added note</td> </tr> </table>		3.1.000 0		3.4.000 0	Updated example	3.4.110 0	Updated example	3.6.200 2	Added “disconnect” parameter	3.8.100 0	Added "username" syntax description (allowed characters)	3.8.200 0	Removed xmladmin and xmluser usernames due to XML depreciation	3.9.090 0	Added note
3.1.000 0																
3.4.000 0	Updated example															
3.4.110 0	Updated example															
3.6.200 2	Added “disconnect” parameter															
3.8.100 0	Added "username" syntax description (allowed characters)															
3.8.200 0	Removed xmladmin and xmluser usernames due to XML depreciation															
3.9.090 0	Added note															
Example	switch (config) # username monitor full-name smith															
Related Commands	show usernames show users															
Notes	<ul style="list-style-type: none"> <li>• To enable a user account, just set a password on it (or use the command “username &lt;user&gt; nopassword” to enable it with no password required for login)</li> </ul>															

- Removing a user account does not terminate any current sessions that user has open; it just prevents new sessions from being established
- Encrypted password is useful for the command “show configuration”, since the cleartext password cannot be recovered after it is set
- The command "username <user> password <password>" or "username <user> password 0 <password>" are not security and will leave clear text in user's terminal (log and command history will be treated as sensitive information without clear text password). They are recommended to be replaced as "username <user> password" or "username <user> password" commands.

## show usernames

	show usernames Displays list of users and their capabilities.	
Syntax Description	N/A	
Default	N/A	
Configuration Mode	Any command mode	
History	3.1.0000	
	3.8.1000	Updated example output
	3.8.2000	Updated example output
Example		
<pre>switch (config) # show usernames  USERNAME  FULL NAME          CAPABILITY ACCOUNT STATUS USERID    System Administrator admin    Local password login disabled admin     System Administrator admin    No password required for login monitor   System Monitor       monitor Password set (SHA512) root      Root User            admin    No password required for login</pre>		
Related Commands	username show users	

Notes	
-------	--

## show users

	show users [history] Displays logged in users and related information such as idle time and what host they have connected from.	
Syntax Description	history	Displays current and historical sessions.
Default	N/A	
Configuration Mode	Any command mode	
History	3.1.0000	
Example		
<pre>switch (config) # show users  USERNAME  FULL NAME          LINE  HOST          IDLE ----- admin     System Administrator pts/0  172.22.237.174  0d0h34m4s admin     System Administrator pts/1  172.30.0.127   1d3h30m49s admin     System Administrator pts/3  172.22.237.34  0d0h0m0s  switch (config) #s how users history admin     pts/3 172.22.237.34  Wed Feb 1 11:56  still logged in admin     pts/3 172.22.237.34  Wed Feb 1 11:42 - 11:46 (00:04) wtmpt    begins          Wed Feb 1 11:38:10 2012</pre>		
Related Commands	username show usernames	
Notes		

## show whoami

	show whoami Displays username and capabilities of user currently logged in.	
Syntax Description	N/A	



Default	N/A
Configuration Mode	Any command mode
History	3.1.0000
Example	switch (config) # show whoami Current user: admin Capabilities: admin
Related Commands	username show usernames show users
Notes	

## password

	password [age expiration <days>   age warning <days>   history <length >   length minimal <length>   length maximal < length >   username-password-match enable   complexity-class <char class>   hardening enable] Configures restrictions for new passwords.	
Syntax Description	age expiration <days>	Specifies validity period of any password configured. Range: 0-365 days (0=password will not expire) Default: 365 days
	age warning <days>	Specifies how many days before expiration a warning message should be printed while logging in. Range: 0-30 days (0 indicates that a warning message will not be printed) Default: 15 days
	history <length >	Specifies how many passwords are saved per user. New password will be compared to previous passwords and will not be allowed if it is the same as an old one. Range: 0-20 passwords Default: 5 passwords
	length minimal <length>	Specifies minimal length of allowed password. Range: 1-32 characters Default: 8 characters

	length maximal < length>	Specifies maximal length of allowed password. Range: 64-80 characters Default: 64 characters
	username-password-match enable	Restricts user from having password identical to its username. Default: enabled The no form of this command will allow this.
	complexity-class <char class>	Specifies what characters must be used while configuring password.  <ol style="list-style-type: none"> <li>1. none—no restrictions</li> <li>2. lower</li> <li>3. lower-upper</li> <li>4. lower-upper-digit</li> <li>5. lower-upper-digit-special</li> </ol> Special characters allowed are: `~!@#\$\$%^&*()-_+= [{}];',<.> Default: lower-upper-digit
	hardening enable	Enable password restrictions. If enabled, all the above will be checked upon every new password that is being configured. Password that does not meet the requirements will be rejected. The no form will disable any password restrictions and every password will be allowed.
Default	Enabled. After upgrade, the feature will be disabled by default.	
Configuration Mode	Config	
History	3.9.2000	
Example	switch (config) # password hardening enable	
Related Commands	show password hardening	
Notes		

## show password hardening

	show password hardening Displays all the configured password restrictions settings.
--	--

Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.9.2000
Example	<pre>switch (config) # show password hardening Password settings:   Password hardening      : enabled   Min password length    : 8 (characters)   Max password length    : 64 (characters)   Character class        : Lowercase, uppercase and digits   Password history length : 5   Different username and password: yes   Password aging         : enabled   Expiration warning message : 15 (days)   Password age           : 365 (days) switch (config) # show password hardening Password settings:   Password hardening      : disabled</pre>
Related Commands	password
Notes	<ul style="list-style-type: none"> <li>• Wizard will prompt for enabling/disabling password hardening</li> <li>• Configuring password 7 while password hardening is enabled, will disable it</li> </ul>

## AAA Methods

### aaa accounting

	<p>aaa accounting changes default stop-only tacacs+</p> <p>no aaa accounting changes default stop-only tacacs+</p> <p>Enables logging of system changes to an AAA accounting server. The no form of the command disables the accounting.</p>
Syntax Description	N/A
Default	N/A

Configuration Mode	config
History	3.1.0000
Example	switch (config) # aaa accounting changes default stop-only tacacs+
Related Commands	show aaa
Notes	<ul style="list-style-type: none"> <li>• TACACS+ is presently the only accounting service method supported</li> <li>• Change accounting covers both configuration changes and system actions that are visible under audit logging, however this feature operates independently of audit logging, so it is unaffected by the commands “logging level audit mgmt” or “configuration audit”</li> <li>• Configured TACACS+ servers are contacted in the order in which they appear in the configuration until one accepts the accounting data, or the server list is exhausted</li> <li>• Despite the name of the “stop-only” keyword, which indicates that this feature logs a TACACS+ accounting “stop” message, and in contrast to configuration change accounting, which happens after configuration database changes, system actions are logged when the action is started, not when the action has completed</li> </ul>

## aaa authentication login

	aaa authentication login default <auth method> [<auth method> [<auth method> [<auth method> [<auth method>]]]] no aaa authentication login Sets a sequence of authentication methods. Up to four methods can be configured. The no form of the command resets the configuration to its default.	
Syntax Description	auth-method	<ul style="list-style-type: none"> <li>• local</li> <li>• radius</li> <li>• tacacs+</li> <li>• ldap</li> </ul>
Default	local	

Configuration Mode	Any command mode
History	3.1.0000 3.7.1102—Updated notes
Example	switch (config) # aaa authentication login default radius tacacs+ ldap local
Related Commands	show aaa
Notes	<ul style="list-style-type: none"> <li>• The order in which the methods are specified is the order in which the authentication is attempted. It is recommended that “local” is one of the methods selected.</li> <li>• When defining a remote server that to authenticate users against, once a connection is established with it, it does not go through other authentication methods. Meaning, if local is defined first, it will not go to other methods.</li> </ul> <p>If a remote server is defined first and then local (radius → local), then if the radius server is reachable, the response from this server will dictate whether the switch can be accessed or not (regardless of whether the user exists on any other authentication method).</p>

## aaa authentication attempts fail-delay

	aaa authentication attempts fail-delay <time> no aaa authentication attempts fail-delay Configures delay for a specific period of time after every authentication failure. The no form of the command resets the fail-delay to its default value.	
Syntax Description	time	Range: 0-60 seconds
Default	0	
Configuration Mode	config	
History	3.5.0200	
Example	switch (config) # aaa authentication attempts fail-delay 1	

Related Commands	
Notes	

## aaa authentication attempts track

	aaa authentication attempts track {downcase   enable} no aaa authentication attempts track {downcase   enable} Configure tracking for failed authentication attempts. The no form of the command clears configuration for tracking authentication failures.	
Syntax Description	downcase	Does not convert all usernames to lowercase (for authentication failure tracking purposes only).
	enable	Disables tracking of failed authentication attempts.
Default	N/A	
Configuration Mode	config	
History	3.5.0200	
Example	switch (config) # aaa authentication attempts track enable	
Related Commands		
Notes	<ul style="list-style-type: none"> <li>• This is required for the lockout functionality described below, but can also be used on its own for informational purposes.</li> <li>• Disabling tracking does not clear any records of past authentication failures, or the locks in the database. However, it does prevent any updates to this database from being made: no new failures are recorded. It also disables lockout, preventing new lockouts from being recorded and existing lockouts from being enforced.</li> </ul>	

## aaa authentication attempts lockout

	aaa authentication attempts lockout {enable   lock-time   max-fail   unlock-time}
--	---

	<p>no aaa authentication attempts logout {enable   lock-time   max-fail   unlock-time}</p> <p>Configures lockout of accounts based on failed authentication attempts.</p> <p>The no form of the command clears configuration for lockout of accounts based on failed authentication attempts.</p>	
<p>Syntax Description</p>	<p>enable</p>	<p>Enables locking out of user accounts based on authentication failures.</p> <p>This both suspends enforcement of any existing lockouts, and prevents any new lockouts from being recorded. If lockouts are later re-enabled, any lockouts that had been recorded previously resume being enforced; but accounts which have passed the max-fail limit in the meantime are NOT automatically locked at this time. They would be permitted one more attempt, and then locked, because of how the locking is done: lockouts are applied after an authentication failure, if the user has surpassed the threshold at that time. Lockouts only work if tracking is enabled. Enabling lockouts automatically enables tracking. Disabling tracking automatically disables lockouts.</p>
	<p>lock-time</p>	<p>Sets maximum permitted consecutive authentication failures before locking out users.</p> <p>Unlike the “max-fail” setting, this does take effect immediately for all accounts.</p> <p>If both unlock-time and lock-time are set, the unlock-time must be greater than the lock-time.</p> <p>This is not based on the number of consecutive failures, and is therefore divorced from most of the rest of the tally feature, except for the tracking of the last login failure.</p>
	<p>max-fail</p>	<p>Sets maximum permitted consecutive authentication failures before locking out users.</p> <p>This setting only impacts what lockouts are imposed while the setting is active; it is not retroactive to previous logins. So if max-fail is disabled or changed, this does not immediately cause any users to be changed from locked to unlocked or vice versa.</p>
	<p>unlock-time</p>	<p>Enables the auto-unlock of an account after a specified number of seconds if a user account is locked due to authentication failures, counting from the last valid login attempt.</p>

	<p>Unlike the “max-fail” setting, this does take effect immediately for all accounts.</p> <p>If both unlock-time and lock-time are set, the unlock-time must be greater than the lock-time.</p> <p>Careful with disabling the unlock-time, particularly if you have max-fail set to something, and have not overridden the behavior for the admin (i.e. they are subject to lockouts also). If the admin account gets locked out, and there are no other administrators who can aid, the user may be forced to boot single-user and use the pam_tallybyname command-line utility to unlock your account manually. Even if one is careful not to incur this many authentication failures, it makes the system more subject to DOS attacks.</p>
Default	N/A
Configuration Mode	config
History	3.2.3000
Example	switch (config) # aaa authentication attempts lockout enable
Related Commands	
Notes	

## aaa authentication attempts class-override

	<pre>aaa authentication attempts class-override {admin [no-lockout]   unknown {no-track   hash-username}}</pre> <pre>no aaa authentication attempts class-override {admin   unknown {no-track   hash-username}}</pre> <p>Overrides the global settings for tracking and lockouts for a type of account.</p> <p>The no form of the command removes this override and lets the admin be handled according to the global settings.</p>	
Syntax Description	admin	Overrides the global settings for tracking and lockouts for the admin account. This applies only to the single account with the username “admin”. It does not apply to any other users with administrative privileges.



	no-lockout	Prevents the admin user from being locked out though authentication failure history is still tracked (if tracking is enabled overall).
	unknown	<p>Overrides the global settings for tracking and lockouts for unknown accounts. The “unknown” class here contains the following categories:</p> <ul style="list-style-type: none"> <li>• Real remote usernames which simply failed authentication</li> <li>• Mis-typed remote usernames</li> <li>• Passwords accidentally entered as usernames</li> <li>• Bogus usernames made up as part of an attack on the system</li> </ul>
	hash-username	Applies a hash function to the username and stores the hashed result in lieu of the original
	no-track	Does not track authentication for such users (which of course also implies no-lockout)
Default	N/A	
Configuration Mode	config	
History	3.2.3000	
Example	switch (config) # aaa authentication attempts class-override admin no-lockout	
Related Commands		
Notes		

## aaa authentication attempts reset

	<pre>aaa authentication attempts reset {all   user &lt;username&gt;} [{no-clear-history   no-unlock}]</pre> <p>Clears the authentication history for and/or unlocks specified users.</p>	
Syntax Description	all	Applies function to all users
	user	Applies function to a specific user
	no-clear-history	Leaves the history of login failures but unlocks the account

	no-unlock	Leaves the account locked but clears the history of login failures
Default	N/A	
Configuration Mode	config	
History	3.2.3000	
Example	switch (config) # aaa authentication attempts reset user admin all	
Related Commands		
Notes		

## clear aaa authentication attempts

	clear aaa authentication attempts {all   user <username>} [no-clear-history   no-unlock] Clears the authentication history for and/or unlocks specified users.	
Syntax Description	all	Applies function to all users.
	user	Applies function to a specific user.
	no-clear-history	Clears the history of login failures.
	no-unlock	Unlocks the account.
Default	N/A	
Configuration Mode	config	
History	3.2.3000	
Example	switch (config) # aaa authentication attempts reset user admin no-clear-history	
Related Commands		
Notes		

## aaa authorization

	<p>aaa authorization map [default-user &lt;username&gt;   order &lt;policy&gt;   fallback]</p> <p>no aaa authorization map [default-user   order   fallback]</p> <p>Sets the mapping permissions of a user in case a remote authentication is done.</p> <p>The no form of the command resets the attributes to default.</p>	
Syntax Description	username	<p>Specifies what local account the authenticated user will be logged on as when a user is authenticated (via RADIUS or TACACS+ or LDAP) and does not have a local account. If the username is local, this mapping is ignored.</p>
	order <policy>	<p>Sets the user mapping behavior when authenticating users via RADIUS or TACACS+ or LDAP to one of three choices. The order determines how the remote user mapping behaves. If the authenticated username is valid locally, no mapping is performed. The setting has the following three possible behaviors:</p> <ul style="list-style-type: none"> <li>• local-only—maps all remote users to the user specified by the command “aaa authorization map default-user &lt;user name&gt;”. Any vendor attributes received by an authentication server are ignored.</li> <li>• remote-first—if a local-user mapping attribute is returned and it is a valid local username, it maps the authenticated user to the local user specified in the attribute. Otherwise, it uses the user specified by the default-user command.</li> <li>• remote-only—maps a remote authenticated user if the authentication server sends a local-user mapping attribute. If the attribute does not specify a valid local user, no further mapping is tried.</li> </ul>
	fallback	<p>Sets the authenticating fallback behavior via RADIUS or TACACS+ or LDAP. This option attempts to authenticate username through the next authentication method listed in case of an error.</p> <ul style="list-style-type: none"> <li>• server-err—performs fallback if an error occurs while connecting to remote AAA</li> </ul>

	server (e.g., server is down, not responding, and so forth)
Default	Default user—admin Map order—remote-first Order fallback—server-err
Configuration Mode	config
History	3.1.0000 3.7.1000—Added “fallback” parameter 3.7.1000—Updated syntax
Example	switch (config) # aaa authorization map default-user admin
Related Commands	show aaa username
Notes	<ul style="list-style-type: none"> <li>• If, for example, the user is locally defined to have admin permission, but in a remote server such as RADIUS the user is authenticated as monitor and the order is remote-first, then the user is given monitor permissions.</li> <li>• The user must be careful when disabling AAA authorization map fallback server-err, because if the remote server stops working then the user may lock themselves out.</li> <li>• If AAA authorization order policy is configured to remote-only, then when upgrading to 3.4.3000 or later from an older version, this policy is changed to remote-first.</li> </ul>

## show aaa

	show aaa Displays the AAA configuration.
Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.1.0000

	3.7.0020—Example updated
Example	<pre>switch (config) # show aaa  AAA authorization:   Default User: admin   Map Order: remote-first   Fallback on server-err: yes Authentication method(s):   local Accounting method(s):   tacacs+</pre>
Related Commands	<pre>aaa accounting aaa authentication aaa authorization show aaa show usernames username</pre>
Notes	

## show aaa authentication attempts

	<pre>show aaa authentication attempts [configured   status user &lt;username&gt;]]</pre> <p>Displays the current authentication, authorization and accounting settings.</p>	
Syntax Description	authentication attempts	Displays configuration and history of authentication failures.
	configured	Displays configuration of authentication failure tracking.
	status user	Displays status of authentication failure tracking and lockouts for specific user.
Default	N/A	
Configuration Mode	Any command mode	
History	3.2.1000 3.5.0200—Updated example	
Example		
<pre>switch (config) # show aaa authentication attempts</pre>		

Configuration for authentication failure tracking and locking:

Track authentication failures: yes  
 Lock accounts based on authentication failures: yes  
 Override treatment of 'admin' user: (none)  
 Override treatment of unknown usernames: hash-usernames  
 Convert usernames to lowercase for tracking: no  
 Delay after each auth failure (fail delay): none

Configuration for lockouts based on authentication failures:

Lock account after consecutive auth failures: 5  
 Allow retry on locked accounts (unlock time): after 15 second(s)  
 Temp lock after each auth failure (lock time): none

Username	Known	Locked	Failures	Last fail time	Last fail from
0Q72B43EHBKT8CB5AF5PGRX3U3B3TUL4CYJP93N(*)	no	no	1	2020/05/20 14:29:19	ttyS0

(\*) Hashed for security reasons

Related Commands	
Notes	

## RADIUS

### radius-server

	radius-server {key <secret>  retransmit <retries>   timeout <seconds>}	
	no radius-server {key   retransmit   timeout}	
	Sets global RADIUS server attributes. The no form of the command resets the attributes to their default values.	
Syntax Description	secret	Sets a secret key (shared hidden text string), known to the system and to the RADIUS server.
	retries	Number of retries (0-5) before exhausting from the authentication.
	seconds	Timeout in seconds between each retry (1-60).
Default	3 seconds, 1 retry	
Configuration Mode	config	
History	3.1.0000	

Example	switch (config) # radius-server retransmit 3
Related Commands	aaa authorization radius-server host show radius
Notes	Each RADIUS server can override those global parameters using the command “radius-server host”.

## radius-server host

	<p>radius-server host &lt;IP address&gt; [enable   auth-port &lt;port&gt;   key &lt;secret&gt;   prompt-key   retransmit &lt;retries&gt;   timeout &lt;seconds&gt;   cipher &lt;none   eap-peap&gt; ]</p> <p>no radius-server host &lt;IP address&gt; [auth-port   enable   cipher]</p> <p>Configures RADIUS server attributes. The no form of the command resets the attributes to their default values and deletes the RADIUS server.</p>	
Syntax Description	IP address	RADIUS server IP address
	enable	Administrative enable of the RADIUS server
	auth-port	Configures authentication port to use with this RADIUS server
	port	RADIUS server UDP port number
	key	Configures shared secret to use with this RADIUS server
	prompt-key	Prompt for key, rather than entering on command line
	retransmit	Configures retransmit count to use with this RADIUS server
	retries	Number of retries (0-5) before exhausting from the authentication
	timeout	Configures timeout between each try
	seconds	Timeout in seconds between each retry (1-60)
	cipher	Configures which cipher to use for communication encryption <none   eap-peap>
Default	3 seconds, 1 retry Default UDP port is 1812	

Configuration Mode	config
History	3.1.0000 3.8.1000—Updated command description, syntax description & example
Example	switch (config) # radius-server host fe80::202:b3ff:fe1e:8329 switch (config) # radius-server host 40.40.40.40
Related Commands	aaa authorization radius-server show radius
Notes	<ul style="list-style-type: none"> <li>• RADIUS servers are tried in the order they are configured</li> <li>• If you do not specify a parameter for this configured RADIUS server, the configuration will be taken from the global RADIUS server configuration. Refer to the command “radius-server”.</li> </ul>

## show radius

	show radius Displays RADIUS configurations.
Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.1.0000 3.6.6000—Updated example 3.8.1000—Updated command description, syntax description & example
Example	<pre>switch (config) # show radius RADIUS defaults: Key       : ***** Timeout   : 3 Retransmit : 1  RADIUS servers: 1.1.1.1:1812 : Enabled   : yes Key       : *****</pre>



	Timeout : 3 (default) Retransmit : 1 (default) Cipher : none 40.40.40.40:1812: Enabled : yes Key : ***** Timeout : 3 (default) Retransmit : 1 (default)
Related Commands	aaa authorization radius-server radius-server host
Notes	

## TACACS+

### tacacs-server

	tacacs-server {key <secret>  retransmit <retries>   timeout <seconds>} no tacacs-server {key   retransmit   timeout} Sets global TACACS+ server attributes. The no form of the command resets the attributes to default values.	
Syntax Description	secret	Set a secret key (shared hidden text string), known to the system and to the TACACS+ server.
	retries	Number of retries (0-5) before exhausting from the authentication.
	seconds	Timeout in seconds between each retry. Reang: 1-60
Default	3 seconds, 1 retry	
Configuration Mode	config	
History	3.1.0000	
Example	switch (config) # tacacs-server retransmit 3	
Related Commands	aaa authorization show radius show tacacs tacacs-server host	

Notes	Each TACACS+ server can override those global parameters using the command “tacacs-server host”.
-------	--

## **tacacs-server host**

	<p>tacacs-server host &lt;IP address&gt; {enable   auth-port &lt;port&gt;   auth-type &lt;type&gt;   key &lt;secret&gt;   prompt-key   retransmit &lt;retries&gt;   timeout &lt;seconds&gt;}</p> <p>no tacacs-server host &lt;IP address&gt; {enable   auth-port}</p> <p>Configures TACACS+ server attributes. The no form of the command resets the attributes to their default values and deletes the TACACS+ server.</p>	
Syntax Description	IP address	TACACS+ server IP address.
	enable	Administrative enable for the TACACS+ server.
	auth-port	Configures authentication port to use with this TACACS+ server.
	port	TACACS+ server UDP port number.
	auth-type	Configures authentication type to use with this TACACS+ server.
	type	Authentication type. Possible values are: <ul style="list-style-type: none"> <li>• ASCII</li> <li>• PAP (Password Authentication Protocol)</li> </ul>
	key	Configures shared secret to use with this TACACS+ server.
	secret	Sets a secret key (shared hidden text string), known to the system and to the TACACS+ server.
	prompt-key	Prompts for key, rather than entering key on command line.
	retransmit	Configures retransmit count to use with this TACACS+ server.
	retries	Number of retries (0-5) before exhausting from the authentication.
	timeout	Configures timeout to use with this TACACS+ server.

	seconds	Timeout in seconds between each retry. Range: 1-60
Default	3 seconds, 1 retry Default TCP port is 49 Default auth-type is PAP	
Configuration Mode	config	
History	3.1.0000	
Example	switch (config) # tacacs-server host 40.40.40.40  switch (config) # tacacs-server host fe80::202:b3ff:fe1e:8329	
Related Commands	aaa authorization show tacacs tacacs-server	
Notes	<ul style="list-style-type: none"> <li>• TACACS+ servers are tried in the order they are configured</li> <li>• A PAP auth-type similar to an ASCII login, except that the username and password arrive at the network access server in a PAP protocol packet instead of being typed in by the user, so the user is not prompted</li> <li>• If the user does not specify a parameter for this configured TACACS+ server, the configuration will be taken from the global TACACS+ server configuration. Refer to the command “tacacs-server”.</li> </ul>	

## show tacacs

	show tacacs Displays TACACS+ configurations.
Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.1.0000 3.6.6000—Updated example
Example	TACACS+ servers: 1.1.1.1:49:

	Enabled : yes Auth Type : pap Key : ***** Timeout : 3 (default) Retransmit: 1 (default)
Related Commands	aaa authorization tacacs-server tacacs-server host
Notes	

## LDAP

### ldap enable

	ldap [vrf <vrf-name>] enable [force] no ldap [vrf <vrf-name>] enable Enables LDAP in VRF. The no form of the command disables LDAP in a specified VRF.	
Syntax Description	force	Enables LDAP in the specified VRF while setting all relevant LDAP options to default.
Default	LDAP enabled	
Configuration Mode	config	
History	3.9.2000	
Example	switch (config) # ldap vrf mgmt enable	
Related Commands		
Notes	If VRF mgmt exists, LDAP will be enabled on VRF mgmt. If there is no VRF mgmt, LDAP will be enabled on the "default" VRF.	

### ldap base-dn

	ldap base-dn <string> no ldap base-dn
--	--

	Sets the base distinguished name (location) of the user information in the schema of the LDAP server. The no form of the command resets the attribute to its default values.	
Syntax Description	string	A case-sensitive string that specifies the location in the LDAP hierarchy where the server should begin searching when it receives an authorization request. For example: "ou=users,dc=example,dc=com", with no spaces. Where: <ul style="list-style-type: none"> <li>• ou—Organizational unit</li> <li>• dc—Domain component</li> <li>• cn—Common name</li> <li>• sn—Surname</li> </ul>
Default	ou=users,dc=example,dc=com	
Configuration Mode	config	
History	3.1.1000 3.4.0000—Updated example	
Example	switch (config) # ldap base-dn ou=department,dc=example,dc=com	
Related Commands	show ldap	
Notes		

## ldap bind-dn/bind-password

	ldap {bind-dn   bind-password} <string> no ldap {bind-dn   bind-password} Gives the distinguished name or password to bind to on the LDAP server. This can be left empty for anonymous login (the default). The no form of the command resets the attribute to its default values.	
Syntax Description	string	A case-sensitive string that specifies distinguished name or password to bind to on the LDAP server.
Default	""	

Configuration Mode	config
History	3.1.1000 3.4.0000—Updated example
Example	switch (config) # ldap bind-dn my-dn switch (config) # ldap bind-password my-password
Related Commands	show ldap
Notes	For anonymous login, bind-dn and bind-password should be empty strings "".

## ldap group-attribute/group-dn

	ldap {group-attribute {<group-att>  member   uniqueMember}   group-dn <group-dn>} no ldap {group-attribute   group-dn} Sets the distinguished name or attribute name of a group on the LDAP server. The no form of the command resets the attribute to its default values.	
Syntax Description	group-att	Specifies a custom attribute name.
	member	groupOfNames or group membership attribute.
	uniqueMember	groupOfUniqueNames membership attribute.
	group-dn	DN of group required for authorization.
Default	group-att: member group-dn: ""	
Configuration Mode	config	
History	3.1.1000 3.4.0000—Updated example	
Example	switch (config) # ldap group-attribute member switch (config) # ldap group-dn my-group-dn	
Related Commands	show ldap	

Notes	<ul style="list-style-type: none"> <li>• The user's distinguished name must be listed as one of the values of this attribute, or the user will not be authorized to log in</li> <li>• After login authentication, if the group-dn is set, a user must be a member of this group or the user will not be authorized to log in. If the group is not set (""—the default) no authorization checks are done.</li> </ul>
-------	---

## ldap nested-group-search

	ldap nested-group-search no ldap nested-group-search Enable LDAP nested-group search mechanism for user-authentication group matching. The no form of the command resets the attribute to its default values.
Syntax Description	N/A
Default	Disabled
Configuration Mode	config
History	3.10.2000
Example	switch (config) # ldap nested-group-search switch (config) # no ldap nested-group-search
Related Commands	ldap nested-group-depth ldap nested-group-count show ldap
Notes	

## ldap nested-group-depth

	ldap nested-group-depth <1-9> no ldap nested-group-depth Sets LDAP maximum depth for nested-group search. The no form of the command resets search depth to default (3).
--	---

Syntax Description	N/A
Default	3
Configuration Mode	config
History	3.10.2000
Example	switch (config) # ldap nested-group-depth 6 switch (config) # no ldap nested-group-depth
Related Commands	ldap nested-group-search ldap nested-group-count show ldap
Notes	

## ldap nested-group-count

	ldap nested-group-count <1-10000> no ldap nested-group-count Sets LDAP maximum number of queried nested-groups. The no form of the command resets search depth to default (1000).
Syntax Description	N/A
Default	1000
Configuration Mode	config
History	3.10.2000
Example	switch (config) # ldap nested-group-count 500 switch (config) # no ldap nested-group-count
Related Commands	ldap nested-group-depth ldap nested-group-search show ldap
Notes	

## ldap host



	ldap host <ip-address> [order <number> last] no ldap host <ip-address> Adds an LDAP server to the set of servers used for authentication. The no form of the command deletes the LDAP host.	
Syntax Description	ip-address	IPv4 or IPv6 address.
	number	The order of the LDAP server.
	last	The LDAP server will be added in the last location.
Default	No hosts configured	
Configuration Mode	config	
History	3.1.1000 3.4.0000—Updated example	
Example	switch (config) # ldap host 10.10.10.10	
Related Commands	show aaa show ldap	
Notes	<ul style="list-style-type: none"> <li>• The system will select the LDAP host to try according to its order</li> <li>• New servers are by default added at the end of the list of servers</li> </ul>	

## ldap hostname-check enable

	ldap hostname-check enable no ldap hostname-check enable Enables LDAP hostname check. The no form of the command disables LDAP hostname check.	
Syntax Description	N/A	
Default	No hosts configured	
Configuration Mode	config	
History	3.6.8008	
Example	switch (config) # ldap hostname-check enable	

Related Commands	show aaa show ldap
Notes	

## ldap login-attribute

	ldap login-attribute {<string>   uid   sAMAccountName} no ldap login-attribute Sets the attribute name which contains the login name of the user. The no form of the command resets this attribute to its default.	
Syntax Description	string	Custom attribute name.
	uid	LDAP login name is taken from the user login username.
	sAMAccountName	SAM Account name, active directory login name.
Default	sAMAccountName	
Configuration Mode	config	
History	3.1.1000 3.4.0000—Updated example	
Example	switch (config) # ldap login-attribute uid	
Related Commands	show aaa show ldap	
Notes		

## ldap port

	ldap port <port> no ldap port Sets the TCP port on the LDAP server to connect to for authentication. The no form of the command resets this attribute to its default value.	
Syntax Description	port	TCP port number

Default	389
Configuration Mode	config
History	3.1.1000 3.4.0000—Updated example
Example	switch (config) # ldap port 1111
Related Commands	show aaa show ldap
Notes	

## ldap referrals

	ldap referrals no ldap referrals Enables LDAP referrals. The no form of the command disables LDAP referrals.
Syntax Description	N/A
Default	LDAP referrals are enabled
Configuration Mode	config
History	3.1.1000 3.4.0000—Updated example
Example	switch (config) # no ldap referrals
Related Commands	show aaa show ldap
Notes	Referral is the process by which an LDAP server, instead of returning a result, will return a referral (a reference) to another LDAP server which may contain further information.

## ldap scope

	ldap scope <scope>
--	--------------------

	no ldap scope Specifies the extent of the search in the LDAP hierarchy that the server should make when it receives an authorization request. The no form of the command resets the attribute to its default value.	
Syntax Description	scope	<ul style="list-style-type: none"> <li>• one-level—searches the immediate children of the base dn</li> <li>• subtree—searches at the base DN and all its children</li> </ul>
Default	subtree	
Configuration Mode	config	
History	3.1.1000 3.4.0000—Updated example	
Example	switch (config) # ldap scope subtree	
Related Commands	show aaa show ldap	
Notes		

## ldap ssl

	ldap ssl {ca-list <options>   cert-verify   ciphers {all   TLS1.2}   crl-check {enable   file fetch all [vrf <vrf-name>] <path>}   mode <mode>   port <port-number>} no ldap ssl {cert-verify   ciphers   crl-check enable   mode   port} Sets SSL parameter for LDAP. The no form of the command resets the attribute to its default value.	
Syntax Description	options	<p>This command specifies the list of supplemental certificates of authority (CAs) from the certificate configuration database that is to be used by LDAP for authentication of servers when in TLS or SSL mode. The options are:</p> <ul style="list-style-type: none"> <li>• default-ca-list—uses default supplemental CA certificate list</li> <li>• none—no supplemental list, uses the built-in one only</li> </ul>

	<p>CA certificates are ignored if “ldap ssl mode” is not configured as either “tls” or “ssl”, or if “no ldap ssl cert-verify” is configured.</p> <p>The default-ca-list is empty in the factory default configuration. Use the command: “crypto certificate ca-list default-ca-list name” to add trusted certificates to that list.</p> <p>The “default-ca-list” option requires LDAP to consult the system’s configured global default CA-list for supplemental certificates.</p>
cert-verify	Enables verification of SSL/TLS server certificates. This may be required if the server's certificate is self-signed, or does not match the name of the server.
ciphers {all   TLS1.2}	Sets SSL mode to be used
crl-check enable	Enables LDAP CRL check
crl-check file fetch	Fetches CRL from remote server. CRL must be a valid PEM file unless a proper message shown. Supported formats: SCP, HTTP, HTTPS, FTP, and FTPS.
mode	<p>Sets the security mode for connections to the LDAP server.</p> <ul style="list-style-type: none"> <li>• none—requests no encryption for the LDAP connection</li> <li>• ssl—the SSL-port configuration is used, an SSL connection is made before LDAP requests are sent (LDAP over SSL)</li> <li>• start-tls—the normal LDAP port is used, an LDAP connection is initiated, and then TLS is started on this existing connection</li> </ul>
vrf-name	VRF to be affected. If "vrf-name" parameter is not specified, "default" VRF will be used.
port-number	Sets the port on the LDAP server to connect to for authentication when the SSL security mode is enabled (LDAP over SSL)
Default	<p>cert-verify—enabled</p> <p>mode—none (LDAP SSL is not activated)</p> <p>port-number—636</p> <p>ciphers—all</p>

Configuration Mode	config
History	3.1.1000 3.2.3000—Added ca-list argument 3.4.0000—Added “ssl ciphers” parameter and Updated example 3.6.8008—Added the parameter “crl-check” 3.9.2000—Added VRF option 3.10.6000—Added note
Example	switch (config) # ldap ssl crl-check file fetch scp://root:pass@1.1.1.1/etc/pki/crl.pem 100.0% [#####] #####]
Related Commands	show aaa show ldap
Notes	<ul style="list-style-type: none"> <li>• If available, the TLS mode is recommended, as it is standardized, and may also be of higher security</li> <li>• The port number is used only for SSL mode. If the security mode selected is TLS, the LDAP port number is used.</li> <li>• To use SSL option in LDAP, the server must support this accordingly. Enable SSL option on the LDAP server by editing the following: Add the following string on customer LDAP server "ldaps:///" to the SLAPD_SERVICES in the ldap config file.</li> </ul>

## ldap timeout

	ldap {timeout-bind   timeout-search} <seconds> no ldap {timeout-bind   timeout-search} Sets a global communication timeout in seconds for all LDAP servers to specify the extent of the search in the LDAP hierarchy that the server should make when it receives an authorization request. The no form of the command resets the attribute to its default value.	
Syntax Description	timeout-bind	Sets the global LDAP bind timeout for all LDAP servers.
	timeout-search	Sets the global LDAP search timeout for all LDAP servers.
	seconds	Number of seconds.

	Range: 1-60
Default	5 seconds
Configuration Mode	config
History	3.1.1000 3.4.0000—Updated example
Example	switch (config) # ldap timeout-bind 10
Related Commands	show aaa show ldap
Notes	

## ldap version

	ldap version <version> no ldap version Sets the LDAP version. The no form of the command resets the attribute to its default value.	
Syntax Description	version	Sets the LDAP version Available values: 2, 3
Default	3	
Configuration Mode	config	
History	3.1.1000 3.4.0000—Updated example	
Example	switch (config) # ldap version 3	
Related Commands	show aaa show ldap	
Notes		

## show ldap

	show ldap
--	-----------

	Displays LDAP configurations.
Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.1.1000 3.4.0000—Updated example 3.6.8008—Updated example 3.10.2000—Updated example to reflect the following added fields: "Nested-group search," "nested-group search depth," and "nested-search maximum group count"
Example	<pre>switch (config) # show ldap      administratively                : enabled VRF name:                          : mgmt User base DN                       : ou=users,dc=example,dc=com User search scope                  : subtree Login attribute                    : sAMAccountName Bind DN                            : Bind password                      : ***** Group base DN                      : Group attribute                    : member Nested-group search                : disabled Nested-group search depth          : 3 Nested-search maximum group count: 1000 LDAP version                       : 3 Referrals                          : yes Server port                        : 389 Search Timeout                    : 5 Bind Timeout                       : 5 Server Hostname check              : no SSL mode                           : none Server SSL port                    : 636 (not active)</pre>



	<pre> SSL ciphers                : all (not active) SSL cert verify            : yes SSL ca-list                : default-ca-list SSL CRL check              : no  LDAP servers:   No LDAP servers configured. </pre>
Related Commands	<pre> show aaa show ldap </pre>
Notes	

## show ldap crl

	<pre> show ldap crl Displays current CRL configured by the user. </pre>
Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.6.8008
Example	<pre> switch (config) # show ldap crl -----BEGIN CERTIFICATE----- MIIDVzCSd..... -----END CERTIFICATE----- </pre>
Related Commands	<pre> show aaa show ldap </pre>
Notes	

## System Secure Mode

## system secure-mode enable

	<p>system secure-mode enable  no system secure-mode enable  Enables secure mode on the switch.  The no form of the command disables secure mode.</p>
Syntax Description	N/A
Default	Disabled
Configuration Mode	config
History	3.5.0200 3.10.2000: Added note
Example	<pre>switch (config) # system secure-mode enable Warning! Configuration is about to be saved and the system will be reloaded. Type 'YES' to confirm the change in secure mode: YES</pre>
Related Commands	<pre>user &lt;username&gt; password &lt;password&gt; ssh server min-version ssh server security strict snmp-server user no neighbor &lt;ip-address&gt; password ntp server disable ntp server keyID router bgp neighbor password router bgp peer-group password</pre>
Notes	<ul style="list-style-type: none"> <li>• Before enabling secure mode, the command performs the following configuration checks: <ul style="list-style-type: none"> <li>◦ NTP Key ID cannot be MD5 when secure mode is enabled</li> <li>◦ SSH min-version cannot be 1 when enabling secure mode</li> <li>◦ SSH security must be set to strict security</li> <li>◦ SNMPv3 user auth cannot be md5 when enabling secure mode</li> <li>◦ SNMPv3 user priv cannot be des when enabling secure mode</li> <li>◦ SNMPv3 trap auth cannot be md5 when enabling secure mode</li> <li>◦ SNMPv3 trap priv cannot be des when enabling secure mode</li> <li>◦ Router BGP neighbor password cannot be set when enabling secure mode</li> </ul> </li> </ul>

	<ul style="list-style-type: none"> <li>◦ Router BGP peer-group password cannot be set when enabling with secure mode</li> <li>◦ User password hash cannot be MD5 when secure mode is enabled Only if the check passes, secure mode is enabled on the switch system.</li> </ul> <ul style="list-style-type: none"> <li>• When secure mode is enabled extra reboot may happen after next steps: install new image and boot to newly installed image.</li> </ul>
--	---

## show system secure-mode

	<pre>show system secure-mode</pre> Displays the security mode of the switch system.
Syntax Description	N/A
Default	N/A
Configuration Mode	Any command mode
History	3.4.2300
Example	<pre>switch (config) # show system secure-mode Secure mode configured: yes Secure mode enabled : yes</pre>
Related Commands	system secure-mode enable
Notes	<ul style="list-style-type: none"> <li>• “Secure mode configuration” describes the user configuration</li> <li>• “Secure mode enabled” describes the system state</li> </ul>

## show secure-boot-status

	<pre>show secure-boot-status</pre> Displays the state of the secure boot: enable or disable.
Syntax Description	N/A

Default	N/A
Configuration Mode	Any command mode
History	3.10.1000
Example	Switch # show secure-boot-status SecureBoot disabled
Related Commands	
Notes	This command is only available for NDR platforms and above

## System Secure SSD Wipe

### system ssd-wipe

	system ssd-wipe Wipe all data from SSD hard disk including user data, NOS and ONIE.
Syntax Description	N/A
Default	N/A
Configuration Mode	Config
History	3.11.4000
Example	switch (config)# system ssd-wipe WARNING - This action is IRREVERSIBLE and will wipe the whole SSD, are you sure? Type 'YES' to confirm SSD wipe: YES
Related Commands	show cpld
Notes	<ul style="list-style-type: none"> <li>• This command is only available for NDR platforms (QM9700).</li> <li>• In order to execute this command, be sure CPLD Version is 4 or higher and PN = 0x144</li> <li>• Supported SSD models: <ul style="list-style-type: none"> <li>◦ VSFCM4XC016G-B201</li> <li>◦ StorFly VSFBM4XC016G-MLX2</li> <li>◦ SFSA016GM3AA1TO-I-LB-12P-STD</li> </ul> </li> </ul>



## Notice

This document is provided for information purposes only and shall not be regarded as a warranty of a certain functionality, condition, or quality of a product. NVIDIA Corporation (“NVIDIA”) makes no representations or warranties, expressed or implied, as to the accuracy or completeness of the information contained in this document and assumes no responsibility for any errors contained herein. NVIDIA shall have no liability for the consequences or use of such information or for any infringement of patents or other rights of third parties that may result from its use. This document is not a commitment to develop, release, or deliver any Material (defined below), code, or functionality.

NVIDIA reserves the right to make corrections, modifications, enhancements, improvements, and any other changes to this document, at any time without notice.

Customer should obtain the latest relevant information before placing orders and should verify that such information is current and complete.

NVIDIA products are sold subject to the NVIDIA standard terms and conditions of sale supplied at the time of order acknowledgement, unless otherwise agreed in an individual sales agreement signed by authorized representatives of NVIDIA and customer (“Terms of Sale”). NVIDIA hereby expressly objects to applying any customer general terms and conditions with regards to the purchase of the NVIDIA product referenced in this document. No contractual obligations are formed either directly or indirectly by this document.

NVIDIA products are not designed, authorized, or warranted to be suitable for use in medical, military, aircraft, space, or life support equipment, nor in applications where failure or malfunction of the NVIDIA product can reasonably be expected to result in personal injury, death, or property or environmental damage. NVIDIA accepts no liability for inclusion and/or use of NVIDIA products in such equipment or applications and therefore such inclusion and/or use is at customer’s own risk.

NVIDIA makes no representation or warranty that products based on this document will be suitable for any specified use. Testing of all parameters of each product is not necessarily performed by NVIDIA. It is customer’s sole responsibility to evaluate and determine the applicability of any information contained in this document, ensure the product is suitable and fit for the application planned by customer, and perform the necessary testing for the application in order to avoid a default of the application or the product. Weaknesses in customer’s product designs may affect the quality and reliability of the NVIDIA product and may result in additional or different conditions and/or requirements beyond those contained in this document. NVIDIA accepts no liability related to any default, damage, costs, or problem which may be based on or attributable to: (i) the use of the NVIDIA product in any manner that is contrary to this document or (ii) customer product designs.

No license, either expressed or implied, is granted under any NVIDIA patent right, copyright, or other NVIDIA intellectual property right under this document. Information published by NVIDIA regarding third-party products or services does not constitute a license from NVIDIA to use such products or services or a warranty or endorsement thereof. Use of such information may require a license from a third party under the patents or other intellectual property rights of the third party, or a license from NVIDIA under the patents or other intellectual property rights of NVIDIA.

Reproduction of information in this document is permissible only if approved in advance by NVIDIA in writing, reproduced without alteration and in full compliance with all applicable export laws and regulations, and accompanied by all associated conditions, limitations, and notices.

THIS DOCUMENT AND ALL NVIDIA DESIGN SPECIFICATIONS, REFERENCE BOARDS, FILES, DRAWINGS, DIAGNOSTICS, LISTS, AND OTHER DOCUMENTS (TOGETHER AND SEPARATELY, “MATERIALS”) ARE BEING PROVIDED “AS IS.” NVIDIA MAKES NO WARRANTIES, EXPRESSED, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO THE MATERIALS, AND EXPRESSLY DISCLAIMS ALL IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE. TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL NVIDIA BE LIABLE FOR ANY DAMAGES, INCLUDING WITHOUT LIMITATION ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF

ANY USE OF THIS DOCUMENT, EVEN IF NVIDIA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Notwithstanding any damages that customer might incur for any reason whatsoever, NVIDIA's aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms of Sale for the product.

## **Trademarks**

NVIDIA and the NVIDIA logo are trademarks and/or registered trademarks of NVIDIA Corporation in the U.S. and other countries. Other company and product names may be trademarks of the respective companies with which they are associated.

© Copyright 2024, NVIDIA. PDF Generated on 11/18/2024