Additional WAE CLI Commands

This section contains the following topics:

Commit Flags

Commit flags modify transaction semantics. Use a commit flag when issuing a **commit** command:

```
commit <flag>
```

The following table lists some of commonly used flags.

Command	Description
and-quit	Exits to CLI operational mode after a commit.
bypass-commit-queue	Attempts to commit directly, bypassing the commit queue. This flag is relevant only when the commit queue is used by default (by the configuration item `/devices/global-settings/commit-queue/enabled-bydefault`). The operation fails if the commit queue contains entries that affect the same device(s) as the transaction to be committed.
check	Validates the pending configuration changes. Equivalent to the **validate** command.
comment | **label**	Adds a commit comment or label the is visible in compliance reports, rollback files, and so on.
dry-run	Validates and displays the configuration changes, but does not perform the actual commit. Neither CDB nor devices are affected. Various output formats are supported.
no-networking	Validates the configuration changes and updates the CDB, but does not update the actual devices. This is equivalent to first setting the admin state-state to southbound locked, then issuing a standard commit. In both cases the configuration changes are not committed to actual devices. If the commit implies changes, it makes the device out-of-sync.

no-out-of-sync-check	Commits even if the device is out-of-sync. This flag can be used in scenarios where you know the change is not in conflict with what is on the device, and you don't want to perform a **sync-from** first. Use **device compare-config** to verify the result. If the commit implies changes, it makes the device out-of-sync.
no-revision-drop	Fails if devices have obsolete device models. When WAE connects to a NETCONF device, the version of the device data model is discovered. Different devices in the network might have different versions. When WAE sends configurations to devices, by default it drops any configuration that only exists in later models than the device supports.
through-commit-queue	Although the configuration change is committed to CDB immediately, it is not committed to the actual device. Instead, to increase transaction throughput, the config change is queued for eventual commit. This enables the use of the commit queue feature for individual commit commands without enabling it by default.

All WAE command can have pipe commands. For example, the **details** pipe command provides feedback on the steps performed in the commit:

```
wae% commit | details
```

To enable debugging on all templates, use the **debug** pipe command:

```
wae% commit | debug template
```

If you use many templates during configuration, the debug output can be overwhelming. You can limit debug information to just one template, as shown in the following example for a template named *l3vpn*:

```
wae% commit | debug template l3vpn
```

Device Actions

Actions for devices can be performed globally on the `/devices` path, and for individual devices on `/devices/device/name`. Many actions are also available on device groups and device ranges.

The following table lists device actions.

Command	Description
check-sync	Checks if the WAE copy of the device configuration is in sync with the actual device configuration. This operation compares only a signature of the configuration from the device; it does not compare the entire configuration. The signature is implemented as a transaction-id, time-stamp, or hash-sum. The corresponding NED must support the capability. If the output says unsupported, you must use a full **device compare-config** command.
check-yang-modules	Checks if WAE and the devices have compatible YANG modules.
clear-trace	Clears all trace files.

commit-queues	Displays a list of queued commits.
connect	Sets up sessions to unlocked devices. This action is not used in real operational scenarios, because WAE automatically establishes connections on demand. However, this action is useful for test purposes when installing new NEDs, adding devices, and so on.
disconnect	Closes the session to the device.
sync-from	Synchronizes the WAE copy of the device configuration by reading the actual device configuration. The change is committed immediately to WAE and cannot be rolled back. If any service created a configuration on the device, the corresponding service might be out of sync. To reconcile this discrepancy, use the commands **service check-sync** and **service re-deploy**.
sync-to	Synchronizes the device configuration by pushing the WAE copy to the devices. (This action cannot be rolled back.)

Service Actions

Many of the preceding device operations can be combined with the option **no-networking**, which performs all updates only in the configuration database and makes the devices out of sync. The updates can be pushed to the network later. (This action is the same as setting the devices in admin-state southbound-locked.)

The following table lists service actions.

Command	Description
check-sync	Verifies that the service and the associated device configuration is in sync. Any differences are displayed in a chosen out-format. If configuration changes were made out-of-band, a **deep-check-sync** is required to detect an out-of-sync condition.
deep-check-sync	Validates whether the actual devices are configured according to the service. Use **re-deploy** to reconcile the service.
get-modifications	Gets the configuration data created by the service.
re-deploy	Reruns the service logic—taking into account all service data—and generates a diff using the device configuration in the configuration database. Sends the configuration diff to the devices. This action is useful when: • A **device sync-from** action has been performed to incorporate an out-of-band change. • Data referenced by the service—topology information, QoS policy definitions, and so on—has changed. This action is idempotent. If no configuration diff exists, nothing needs to be done. The WAE general principle of minimum change applies.
un-deploy	Undoes the effects of the service on the network. This action removes the configuration from the actual devices and from the WAE configuration database.

wae.conf Configuration Parameters

The following table lists the `wae.conf` configuration parameters and their type (in parentheses) and default values (in brackets). Parameters are written using a path notation to make it easier to see how they relate to each other.

Parameter	Description
/ncs-config	WAE configuration.
/ncs-config/db-mode (running) [running]	This feature is deprecated; WAE supports only running db-mode. It is not a requirement to set this leaf; it is retained only for backward compatibility.
/ncs-config/ncs-ipc-address	WAE listens by default on 127.0.0.1:4569 for incoming TCP connections from WAE client libraries, such as CDB, MAAPI, the CLI, the external database API, as well as commands from the ncs script (such as 'ncs --reload'). The IP address and port can be changed. If they are changed, all clients using MAAPI, CDB, and so on must be recompiled to handle this. **Caution** There are severe security implications involved if WAE is instructed to bind(2) to anything but localhost. Use the IP 0.0.0.0 if you want WAE to listen(2) on all IPv4 addresses.
/ncs-config/ncs-ipc-address/ip (ipv4-address | ipv6-address) [127.0.0.1]	The IP address that WAE listens on for incoming connections from the Java library.
/ncs-config/ncs-ipc-address/port (port-number) [4569]	The port number that WAE listens on for incoming connections from the Java library.
/ncs-config/ncs-ipc-extra-listen-ip (ipv4-address | ipv6-address)	This parameter can be given multiple times. It lists additional IPs to which to bind the WAE IPC listener. This is useful if you don't want to use the wildcard 0.0.0.0 address in order to never expose the WAE IPC to certain interfaces.
/ncs-config/ncs-ipc-access-check	WAE can be configured to restrict access for incoming connections to the IPC listener sockets. The access check requires that connecting clients prove possession of a shared secret.
/ncs-config/ncs-ipc-access-check/enabled (boolean) [false]	If 'true', the access check for IPC connections is enabled.
/ncs-config/ncs-ipc-access-check/filename (string)	This parameter is mandatory. *filename* is the full path to a file containing the shared secret for the IPC access check. The file should be protected via OS file permissions, such that it can only be read by the WAE daemon and client processes that are allowed to connect to the IPC listener sockets.
/ncs-config/enable-shared-memory-schema (boolean) [true]	*enabled* is either true or false. If true, a C program starts and loads the schema into shared memory (which can then be accessed by Python, for example).
/ncs-config/load-path	—

Parameter	Description
/ncs-config/load-path/dir (string)	This parameter can be given multiple times. The *load-path* element contains any number of *dir* elements. Each *dir* element points to a directory path on disk that is searched for compiled and imported YANG files (.fxs files) and compiled clispec files (.ccl files) during daemon startup. WAE also searches the load path for packages at initial startup, or when requested by the /packages/reload action.
/ncs-config/state-dir (string)	This parameter is mandatory. This is where WAE writes persistent state data. It stores a private copy of all packages found in the load path, in a directory tree rooted at 'packages-in-use.cur' (also referenced by a symlink 'packages-in-use'). It is also used for the state file 'running.invalid', which exists only if the running database status is invalid, which occurs if one of the database implementations fails during the two-phase commit protocol. It is also used for 'global.data', which is used to store data that needs to be retained across reboots.
/ncs-config/commit-retry-timeout (xs:duration | infinity) [infinity]	Commit timeout in the WAE back plane. This timeout controls how long the commit operation in the CLI and the JSON-RPC API try to complete the operation when another entity is locking the database; for example, when another commit is in progress or when a managed object is locking the database.
/ncs-config/max-validation-errors (uint32 | unbounded) [1]	Controls how many validation errors are collected and presented to the user at a time.
/ncs-config/notifications	Defines NETCONF northbound notification settings.
/ncs-config/notifications/event-streams	Lists all available notification event streams.
/ncs-config/notifications/event-streams/stream	Parameters for a single notification event stream.
/ncs-config/notifications/event-streams/stream/name (string)	The name attached to a specific event stream.
/ncs-config/notifications/event-streams/stream/description (string)	This parameter is mandatory. Descriptive text attached to a specific event stream.
/ncs-config/notifications/event-streams/stream/replay-support (boolean)	This parameter is mandatory. Signals if replay support is available for a specific event stream.
/ncs-config/notifications/event-streams/stream/builtin-replay-store	Parameters for the built-in replay store for this event stream. If replay support is enabled, WAE automatically stores all notifications on disk, ready to be replayed if a NETCONF manager asks for logged notifications. The replay store uses a set of wrapping log files on disk (of a certain number and size) to store the notifications. To achieve fast replay of notifications in a certain time range, the max size of each wrap log file should not be too large. If possible, use a larger number of wrap log files instead. If in doubt, use the recommended settings (see below).

Parameter	Description
/ncs-config/notifications/event-streams/ stream/builtin-replay-store/ enabled (boolean) [false]	If 'false', the application must implement its own replay support.
/ncs-config/notifications/event-streams/ stream/builtin-replay-store/dir (string)	This parameter is mandatory. The disk location for the wrapping log files.
/ncs-config/notifications/event-streams/ stream/builtin-replay-store/ max-size (tailf:size)	This parameter is mandatory. The max size of each log wrap file. The recommended setting is approximately S10M.
/ncs-config/notifications/event-streams/ stream/builtin-replay-store/ max-files (int64)	This parameter is mandatory. The max number of log wrap files. The recommended setting is around 50 files.
/ncs-config/opcache	Controls the behavior of the operational data cache.
/ncs-config/opcache/enabled (boolean) [false]	If 'true', the cache is enabled.
/ncs-config/opcache/timeout (uint64)	This parameter is mandatory. The amount of time to keep data in the cache, in seconds.
/ncs-config/hide-group	Lists any hide groups that can be unhidden. There can be zero, one, or many hide-group entries in the configuration. If a hide group does not have a hide-group entry, it cannot be unhidden using the CLI 'unhide' command. However, it is possible to add a hide-group entry to the ncs.conf file and then use **ncs -- reload** to make it available in the CLI. This can be useful to enable, for example, a diagnostics hide group that you do not want accessible even using a password.
/ncs-config/hide-group/name (string)	Name of the hide group, which should correspond to a hide group name defined in a YANG module with 'tailf:hidden'.
/ncs-config/hide-group/ password (tailf:md5-digest-string) []	A password can optionally be specified for a hide group. If no password or callback is given, the hide group can be unhidden without giving a password. If a password is specified, the hide group cannot be enabled unless the password is entered. To completely disable a hide group (that is, make it impossible to unhide it), remove the entire hide-group container for that hide group.
/ncs-config/hide-group/ callback (string)	A callback can optionally be specified for a hide group. If no callback or password is given, the hide group can be unhidden without giving a password. If a callback is specified, the hide group cannot be enabled unless a password is entered and verified. The callback receives the name of the hide group, the name of the user issuing the unhide command, and the password. Callbacks make it possible to have short-lived unhide passwords and per-user unhide passwords.

Parameter	Description
/ncs-config/cdb	—
/ncs-config/cdb/db-dir (string)	*db-dir* is the directory on disk that CDB uses for its storage and any temporary files. It is also the directory where CDB searches for initialization files.
/ncs-config/cdb/init-path	—
/ncs-config/cdb/init-path/dir (string)	This parameter can be given multiple times. The *init-path* can contain any number of *dir* elements. Each *dir* element points to a directory path that CDB searches for .xml files before looking in *db-dir*. The directories are searched in the order in which they are listed.
/ncs-config/cdb/client-timeout (xs:duration | infinity) [infinity]	Specifies how long CDB waits for a response before considering a client unresponsive. If a client fails to call Cdb.syncSubscriptionSocket() within the timeout period, CDB logs a syslog of this failure and then, considering the client dead, closes the socket and proceeds with the subscription notifications. If set to infinity, CDB never times out waiting for a response from a client.
/ncs-config/cdb/subscription-replay	—
/ncs-config/cdb/subscription-replay/enabled (boolean) [false]	If enabled, it is possible to request a replay of the previous subscription notification to a new CDB subscriber.
/ncs-config/cdb/replication (async | sync) [sync]	When CDB replication is enabled (which it is when high-availability mode is enabled; see /ncs-config/ha), the CDB configuration stores can be replicated asynchronously or synchronously. With asynchronous replication, a transaction updating the configuration is allowed to complete as soon as the updates are sent to the connected secondary nodes. With the default synchronous replication, the transaction is suspended until the updates are completely propagated to the secondary nodes, and the subscribers on the secondary nodes (if any) have acknowledged their subscription notifications.
/ncs-config/cdb/journal-compaction (automatic | manual) [automatic]	Controls the way the CDB configuration store does its journal compaction. Never set to anything but the default 'automatic' unless there is an external mechanism that controls the compaction using the cdb_initiate_journal_compaction() API call.
/ncs-config/cdb/operational	Operational data can either be implemented by external callbacks, or stored in CDB (or a combination of both). The operational data store is used when data is to be stored in CDB.
/ncs-config/cdb/operational/ db-dir (string)	*db-dir* is the directory on disk that CDB operational uses for its storage and any temporary files. If left unset (default), the same directory as *db-dir* for CDB is used.
/ncs-config/encrypted-strings	*encrypted-strings* defines keys used to encrypt strings that adhere to the types tailf:des3-cbc-encryptedstring and tailf:aes-cfb-128-encrypted-string.
/ncs-config/encrypted-strings/DES3CBC	With DES3CBC, three 64-bit (8-byte) keys and a random initial vector are used to encrypt the string. The initVector leaf is only used when upgrading from earlier versions, but is retained for backward compatibility.

Parameter	Description
/ncs-config/encrypted-strings/ DES3CBC/key1 (hex8-value-type)	This parameter is mandatory.
/ncs-config/encrypted-strings/ DES3CBC/key2 (hex8-value-type)	This parameter is mandatory.
/ncs-config/encrypted-strings/ DES3CBC/key3 (hex8-value-type)	This parameter is mandatory.
/ncs-config/encrypted-strings/ DES3CBC/initVector (hex8-value-type)	—
/ncs-config/encrypted-strings/ AESCFB128	With AESCFB128, one 128-bit (16-byte) key and a random initial vector are used to encrypt the string. The initVector leaf is only used when upgrading from earlier versions, but is retained for backward compatibility.
/ncs-config/encrypted-strings/ AESCFB128/key (hex16-value-type)	This parameter is mandatory.
/ncs-config/encrypted-strings/ AESCFB128/initVector (hex16-value-type)	—
/ncs-config/crypt-hash	*crypt-hash* specifies how clear-text values should be hashed for leafs of the types ianach:crypt-hash, tailf:sha-256-digest-string, and tailf:sha-512-digest-string.
/ncs-config/crypt-hash/algorithm (md5 | sha-256 | sha-512) [md5]	*algorithm* can be set to one of the values 'md5', 'sha-256', or 'sha-512', to choose the corresponding hash algorithm for hashing of clear-text input for the ianach:crypt-hash type.
/ncs-config/crypt-hash/rounds (crypt-hash-rounds-type) [5000]	For the 'sha-256' and 'sha-512' algorithms for the ianach:crypt-hash type, and for the tailf:sha-256-digest-string and tailf:sha-512-digest-string types, *rounds* specifies how many times the hashing loop should be executed. If a value other than the default 5000 is specified, the hashed format has 'rounds=N$', where N is the specified value, prepended to the salt. This parameter is ignored for the 'md5' algorithm for ianach:crypt-hash.
/ncs-config/logs	—
/ncs-config/logs/syslog-config	Shared settings for how to log to syslog. Logs can be configured to log to file or syslog. If a log is configured to log to syslog, the settings under /ncs-config/logs/syslog-config are used.
/ncs-config/logs/syslog-config/version (bsd | 1) [bsd]	*version* is either 'bsd' (traditional syslog) or '1' (new IETF syslog format: RFC 5424). '1' implies that /ncs-config/logs/syslog-config/udp/enabled must be set to true.

Parameter	Description
/ncs-config/logs/syslog-config/facility (daemon | authpriv | local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7 | uint32) [daemon]	This facility setting is the default facility. It is also possible to set individual facilities in the different logs.
/ncs-config/logs/syslog-config/udp	—
/ncs-config/logs/syslog-config/udp/enabled (boolean) [false]	If 'false', messages are sent to the local syslog daemon.
/ncs-config/logs/syslog-config/udp/host (string | ipv4-address | ipv6-address)	This parameter is mandatory. *host* is either a domain name or an IPv4/IPv6 network address. UDP syslog messages are sent to this host.
/ncs-config/logs/syslog-config/udp/port (port-number) [514]	*port* is a valid port number to be used in combination with /ncs-config/logs/syslog-config/udp/host.
/ncs-config/logs/syslog-config/syslog-servers	This is an alternative way of specifying UDP syslog servers. If you configure the /ncs-config/logs/syslog-config/udp container, any configuration in this container is ignored.
/ncs-config/logs/syslog-config/syslog-servers/server	A set of syslog servers that get a copy of all syslog messages.
/ncs-config/logs/syslog-config/syslog-servers/server/host (string | ipv4-address | ipv6-address)	*host* is either a domain name or an IPv4/IPv6 network address. UDP syslog messages are sent to this host.
/ncs-config/logs/syslog-config/syslog-servers/server/port (port-number) [514]	*port* is the UDP port number where this syslog server is listening.
/ncs-config/logs/syslog-config/syslog-servers/server/version (bsd | 1) [bsd]	*version* is either 'bsd' (traditional syslog) or '1' (new IETF syslog format: RFC 5424).
/ncs-config/logs/syslog-config/syslog-servers/server/facility (daemon | authpriv | local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7 | uint32) [daemon]	—
/ncs-config/logs/syslog-config/syslog-servers/server/enabled (boolean) [true]	If 'false', this syslog server does not get any UDP messages.
/ncs-config/logs/ncs-log	ncs-log is WAE's daemon log. Check this log for startup problems of the WAE daemon itself. This log is not rotated; use logrotate(8).

Parameter	Description
/ncs-config/logs/ncs-log/ enabled (boolean) [true]	If 'true', the log is enabled.
/ncs-config/logs/ncs-log/file	—
/ncs-config/logs/ncs-log/ file/name (string)	*name* is the full path to the actual log file.
/ncs-config/logs/ncs-log/file/ enabled (boolean) [false]	If 'true', file logging is enabled.
/ncs-config/logs/ncs-log/syslog	—
/ncs-config/logs/ncs-log/ syslog/enabled (boolean) [false]	If 'true', syslog messages are sent.
/ncs-config/logs/ncs-log/ syslog/facility (daemon | authpriv | local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7 | uint32)	This optional value overrides the /ncs-config/logs/syslog-config/facility for the specified log.
/ncs-config/logs/developer-log	*developer-log* is a debug log for troubleshooting user-written Java code. Enable and check this log for problems with validation code. This log is enabled by default. In all other regards it can be configured as ncs-log. This log is not rotated; use logrotate(8).
/ncs-config/logs/developer-log/ enabled (boolean) [true]	If 'true', the log is enabled.
/ncs-config/logs/developer-log/ file	—
/ncs-config/logs/developer-log/ file/name (string)	*name* is the full path to the actual log file.
/ncs-config/logs/developer-log/ file/enabled (boolean) [false]	If 'true', file logging is enabled.
/ncs-config/logs/developer-log/ syslog	—
/ncs-config/logs/developer-log/ syslog/enabled (boolean) [false]	If 'true', syslog messages are sent.
/ncs-config/logs/developer-log/ syslog/facility (daemon | authpriv | local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7 | uint32)	This optional value overrides the /ncs-config/logs/syslog-config/facility for the specified log.

Parameter	Description
/ncs-config/logs/developer-log-level (error | info | trace) [info]	Controls the level of developer messages to print in the developer log.
/ncs-config/logs/audit-log	*audit-log* is an audit log that records successful and failed logins to the WAE back plane. This log is enabled by default. In all other regards it can be configured as /ncs-config/logs/ncs-log. This log is not rotated; use logrotate(8).
/ncs-config/logs/audit-log/ enabled (boolean) [true]	If 'true', the log is enabled.
/ncs-config/logs/audit-log/file	—
/ncs-config/logs/audit-log/ file/name (string)	*name* is the full path to the actual log file.
/ncs-config/logs/audit-log/ file/enabled (boolean) [false]	If 'true', file logging is enabled.
/ncs-config/logs/audit-log/ syslog	—
/ncs-config/logs/audit-log/ syslog/enabled (boolean) [false]	If 'true', syslog messages are sent.
/ncs-config/logs/audit-log/ syslog/facility (daemon | authpriv | local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7 | uint32)	This optional value overrides the /ncs-config/logs/syslog-config/facility for the specified log.
/ncs-config/logs/audit-log-commit (boolean) [false]	Controls whether the audit log should include messages about the resulting configuration changes for each commit to the running data store.
/ncs-config/logs/netconf-log	*netconf-log* is a log for troubleshooting northbound NETCONF operations, such as checking why a filter operation didn't return the data requested. This log is enabled by default. In all other regards it can be configured as /ncs-config/logs/ncs-log. This log is not rotated; use logrotate(8).
/ncs-config/logs/netconf-log/ enabled (boolean) [true]	If 'true', the log is enabled.
/ncs-config/logs/netconf-log/ file	—
/ncs-config/logs/netconf-log/ file/name (string)	*name* is the full path to the actual log file.
/ncs-config/logs/netconf-log/ file/enabled (boolean) [false]	If 'true', file logging is enabled.
/ncs-config/logs/netconf-log/syslog	—
/ncs-config/logs/netconf-log/ syslog/enabled (boolean) [false]	If 'true', syslog messages are sent.

Parameter	Description
/ncs-config/logs/netconf-log/ syslog/facility (daemon | authpriv | local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7 | uint32)	This optional value overrides the /ncs-config/logs/syslog-config/facility for the specified log.
/ncs-config/logs/snmp-log	—
/ncs-config/logs/snmp-log/ enabled (boolean) [true]	If 'true', the log is enabled.
/ncs-config/logs/snmp-log/file	—
/ncs-config/logs/snmp-log/ file/name (string)	*name* is the full path to the actual log file.
/ncs-config/logs/snmp-log/ file/enabled (boolean) [false]	If 'true', file logging is enabled.
/ncs-config/logs/snmp-log/ syslog	—
/ncs-config/logs/snmp-log/ syslog/enabled (boolean) [false]	If 'true', syslog messages are sent.
/ncs-config/logs/snmp-log/ syslog/facility (daemon | authpriv | local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7 | uint32)	This optional value overrides the /ncs-config/logs/syslog-config/facility for the specified log.
/ncs-config/logs/snmp-log-level (error | info) [info]	Controls which level of SNMP PDUs are printed in the SNMP log. The value 'error' means that only PDUs with error-status not equal to 'noError' are printed.
/ncs-config/logs/webui-browser-log	*webui-browser-log* makes it possible to log Java script errors/exceptions in a log file on the target device instead of just in the browser's error console. This log is not enabled by default and is not rotated; use logrotate(8).
/ncs-config/logs/webui-browser-log/ enabled (boolean) [false]	If 'true', the browser log is used.
/ncs-config/logs/webui-browser-log/filename (string)	This parameter is mandatory. The path to the filename where browser log entries are written.
/ncs-config/logs/webui-access-log	*webui-access-log* is an access log for the embedded WAE web server. This file adheres to the Common Log Format, as defined by Apache and others. This log is not enabled by default and is not rotated; use logrotate(8).
/ncs-config/logs/webui-access-log/ enabled (boolean) [false]	If 'true', the access log is used.

Parameter	Description
/ncs-config/logs/webui-access-log/ traffic-log (boolean) [false]	If 'true', all HTTP(S) traffic towards the embedded web server is logged in a log file named traffic.trace. This log is not enabled by default and is not rotated; use logrotate(8). **Caution** Do not use this log in a production setting.
/ncs-config/logs/webui-access-log/ dir (string)	This parameter is mandatory. The path to the directory where the access log is written.
/ncs-config/logs/netconf-trace-log	*netconf-trace-log* is a log for understanding and troubleshooting northbound NETCONF protocol interactions. When this log is enabled, all NETCONF traffic to and from WAE is stored to a file. By default, all XML is pretty-printed. This slows down the NETCONF server, so be careful when enabling this log. This log is not rotated; use logrotate(8).
/ncs-config/logs/netconf-trace-log/ enabled (boolean) [false]	If 'true', all NETCONF traffic is logged.
/ncs-config/logs/netconf-trace-log/ filename (string)	This parameter is mandatory. The name of the file where the NETCONF traffic trace log is written.
/ncs-config/logs/netconf-trace-log/ format (pretty | raw) [pretty]	The value 'pretty' means that the XML data is pretty-printed. The value 'raw' means that it is not pretty-printed.
/ncs-config/logs/xpath-trace-log	*xpath-trace-log* is a log for understanding and troubleshooting xpath evaluations. When this log is enabled, all xpath queries evaluated by WAE are logged to a file. This slows down WAE, so be careful when enabling this log. This log is not rotated; use logrotate(8).
/ncs-config/logs/xpath-trace-log/ enabled (boolean) [false]	If 'true', all xpath execution is logged.
/ncs-config/logs/xpath-trace-log/ filename (string)	This parameter is mandatory. The name of the file where the xpath trace log is written.
/ncs-config/logs/error-log	*error-log* is an error log used for internal logging from the WAE daemon. It is used for troubleshooting the WAE daemon itself, and should normally be disabled. This log is rotated by the WAE daemon.
/ncs-config/logs/error-log/ enabled (boolean) [false]	If 'true', error logging is performed.
/ncs-config/logs/error-log/ filename (string)	This parameter is mandatory. *filename* is the full path to the actual log file. This parameter must be set if the error log is enabled.
/ncs-config/logs/error-log/max-size (tailf:size) [S1M]	*max-size* is the maximum size of an individual log file before it is rotated. Log filenames are reused when five logs have been exhausted.
/ncs-config/logs/error-log/ debug	—
/ncs-config/logs/error-log/ debug/enabled (boolean) [false]	—

Parameter	Description
/ncs-config/logs/error-log/ debug/level (uint16) [2]	—
/ncs-config/logs/error-log/ debug/tag (string)	This parameter can be given multiple times.
/ncs-config/candidate	—
/ncs-config/candidate/ filename (string)	The candidate db-mode has been removed; this leaf no longer affects the WAE configuration. This leaf and the candidate container are retained for backward compatibility.
/ncs-config/sort-transactions (boolean) [true]	This parameter controls how WAE lists newly created, not yet committed list entries. If this value is set to 'false', WAE lists all new elements before listing existing data. If this value is set to 'true', WAE merges new and existing entries, and provides one sorted view of the data. This behavior works well when CDB is used to store configuration data, but if an external data provider is used, WAE does not know the sort order and cannot merge the new entries correctly. If an external data provider is used for configuration data, and if the sort order differs from CDB's sort order, this parameter should be set to 'false'.
/ncs-config/enable-attributes (boolean) [true]	This parameter controls whether WAE's attribute feature is enabled. There are two attributes: annotations and tags. These are available in northbound interfaces (the annotate command in the CLI, and the annotation XML attribute in NETCONF), but to be useful they need support from the underlying configuration data provider. CDB supports attributes, but if an external data provider is used for configuration data, and if it does not support the attribute callbacks, this parameter should be set to 'false'.
/ncs-config/enable-inactive (boolean) [true]	This parameter controls whether WAE's inactive feature is enabled. This feature also requires enableAttributes to be enabled. When WAE is used to control Juniper routers, this feature is required.
/ncs-config/session-limits	Limits concurrent access to WAE.
/ncs-config/session-limits/max-sessions (uint32 | unbounded) [unbounded]	Limits the total number of concurrent sessions to WAE.
/ncs-config/session-limits/session-limit	Limits concurrent access for a specific context to WAE. There can be multiple instances of this container element, each one specifying parameters for a specific context.
/ncs-config/session-limits/ session-limit/context (string)	The context is cli, netconf, webui, snmp, or any other context string defined through the use of MAAPI. For example, if you use MAAPI to implement a CORBA interface to WAE, the MAAPI program could send the string 'corba' as context.
/ncs-config/session-limits/ session-limit/max-sessions (uint32 | unbounded)	This parameter is mandatory. Limits the total number of concurrent sessions to WAE.

Parameter	Description
/ncs-config/session-limits/ max-config-sessions (uint32 | unbounded) [unbounded]	Limits the total number of concurrent configuration sessions to WAE.
/ncs-config/session-limits/ config-session-limit	Limits concurrent read-write transactions for a specific context to WAE. There can be multiple instances of this container element, each one specifying parameters for a specific context.
/ncs-config/session-limits/ config-session-limit/context (string)	The context is cli, netconf, webui, snmp, or any other context string defined through the use of MAAPI. For example, if you use MAAPI to implement a CORBA interface to WAE, the MAAPI program could send the string 'corba' as context.
/ncs-config/session-limits/ config-session-limit/max-sessions (uint32 |unbounded)	This parameter is mandatory. Limits the total number of concurrent configuration sessions to WAE for the corresponding context.
/ncs-config/aaa	—
/ncs-config/aaa/ssh-login-grace-time (xs:duration) [PT10M]	WAE servers close SSH connections after this time if the client has not successfully authenticated itself. If the value is 0, there is no time limit for client authentication. This is a global value for all SSH servers in WAE. Changing this value affects only SSH connections that are established after the change is made.
/ncs-config/aaa/ssh-max-auth-tries (uint32 | unbounded) [unbounded]	WAE servers close SSH connections when the client has made this number of unsuccessful authentication attempts. This is a global value for all SSH servers in WAE. Changing this value affects only SSH connections that are established after the change is made.
/ncs-config/aaa/ssh-server-key-dir (string)	*ssh-server-key-dir* is the directory file path where the keys used by the WAE SSH daemon are found. This parameter must be set if SSH is enabled for NETCONF or the CLI. If SSH is enabled, the server keys used by WAE are on the same format as the server keys used by openssh (that is, the same format as generated by 'ssh-keygen'). Only DSA- and RSA-type keys can be used with the WAE SSH daemon, as generated by 'ssh-keygen' with the '-t dsa' and '-t rsa' switches, respectively. The key must be stored with an empty passphrase, and with the name 'ssh_host_dsa_key' if it is a DSA-type key, and with the name 'ssh_host_rsa_key' if it is an RSA-type key. The SSH server advertises support for those key types for which there is a key file available and for which the required algorithm is enabled. See the /ncs-config/ssh/algorithms/server-host-key leaf.

Parameter	Description
/ncs-config/aaa/ssh-pubkey-authentication (none | local | system) [system]	Controls how the WAE SSH daemon locates the user keys for public key authentication. If set to 'none', public key authentication is disabled. If set to 'local', and the user exists in /aaa/authentication/users, the keys in the user's 'ssh_keydir' directory are used. If set to 'system', the user is first looked up in /aaa/authentication/users, but only if /ncs-config/aaa/local-authentication/enabled is set to 'true'. If local-authentication is disabled, or if the user does not exist in /aaa/authentication/users but does exist in the OS password database, the keys in the user's $HOME/.ssh directory are used.
/ncs-config/aaa/default-group (string)	If the user group cannot be found in the AAA subsystem, a logged-in user ends up as a member of the default group (if specified). If a user logs in and the group membership cannot be established, the user has zero access rights.
/ncs-config/aaa/auth-order (string)	The default order for authentication is 'local-authentication pam external-authentication'. It is possible to change this order through this parameter.
/ncs-config/aaa/expiration-warning (ignore | display | prompt) [ignore]	When PAM or external authentication is used, the authentication mechanism might give a warning that the user's password is about to expire. This parameter controls how the WAE daemon processes that warning message. If set to 'ignore', the warning is ignored. If set to 'display', interactive user interfaces display the warning message at login. If set to 'prompt', interactive user interfaces display the warning message at login. The user must acknowledge the message before proceeding.
/ncs-config/aaa/audit-user-name (always | known | never) [known]	Controls the logging of the username when a failed authentication attempt is logged to the audit log. If set to "always", the username is always logged. If set to "known", the username is only logged when it is known to be valid (that is, when attempting local-authentication and the user exists in /aaa/authentication/users). Otherwise, it is logged as "[withheld]". If set to "never", the username is always logged as "[withheld]".
/ncs-config/aaa/pam	If PAM is used for login, the WAE daemon typically must run as root.
/ncs-config/aaa/pam/enabled (boolean) [false]	When set to 'true', WAE uses PAM for authentication.
/ncs-config/aaa/pam/service (string) [common-auth]	The PAM service to use for the login NETCONF/SSH CLI procedure. This can be any service installed in the /etc/pam.d directory. Different unices have different services installed under /etc/pam.d. Choose an existing service or create a new one.

Parameter	Description
/ncs-config/aaa/pam/timeout (xs:duration) [PT10S]	The maximum time that authentication waits for a reply from PAM. If the timeout is reached, the PAM authentication fails, but authentication attempts are made with other mechanisms as configured for /ncs-config/aaa/authOrder. The default is PT10S (10 seconds).
/ncs-config/aaa/external-authentication	—
/ncs-config/aaa/external-authentication/enabled (boolean) [false]	When set to 'true', external authentication is used.
/ncs-config/aaa/external-authentication/executable (string)	If external authentication is enabled, an executable on the local host can be launched to authenticate a user. The executable receives the username and the clear-text password on its standard input. The format is '[${USER};${PASS};]\n'. For example, if user is 'bob' and password is 'secret', the executable receives the line '[bob;secret;]' followed by a new line on its standard input. The program must parse this line. The task of the external program is to authenticate the user and also provide the user-to-groups mapping. If 'bob' is a member of the 'oper' and the 'lamers' groups, the program should echo 'accept oper lamers' on its standard output. If the user fails to authenticate, the program should echo 'reject ${reason}' on its standard output.
/ncs-config/aaa/external-authentication/use-base64 (boolean) [false]	When set to 'true', ${USER} and ${PASS} in the data passed to the executable are base64-encoded, allowing the password to contain ';' characters. For example, if user is 'bob' and password is 'secret', the executable receives the string '[Ym9i;c2VjcmV0;]' followed by a new line.
/ncs-config/aaa/external-authentication/include-extra (boolean) [false]	When set to 'true', additional information items are provided to the executable: source IP address and port, context, and protocol. The complete format is '[${USER};${PASS};${IP};$ {PORT};${CONTEXT};${PROTO};]\n'. Example: '[bob;secret;192.168.1.1;12345;cli;ssh;]\n'.
/ncs-config/aaa/local-authentication	—
/ncs-config/aaa/local-authentication/enabled (boolean) [true]	When set to 'true', WAE uses local authentication. The user data kept in the aaa namespace is used to authenticate users. When set to 'false', another authentication mechanism (such as PAM or external authentication) is used.
/ncs-config/aaa/authentication-callback	—
/ncs-config/aaa/authentication-callback/enabled (boolean) [false]	When set to 'true', WAE invokes an application callback when authentication succeeds or fails. The callback might reject an otherwise successful authentication. If the callback has not been registered, all authentication attempts fail.
/ncs-config/aaa/authorization	—

Parameter	Description
/ncs-config/aaa/authorization/enabled (boolean) [true]	When set to 'false', all authorization checks are turned off, similar to the -noaaa flag in ncs_cli.
/ncs-config/aaa/authorization/ callback	—
/ncs-config/aaa/authorization/callback/enabled (boolean) [false]	When set to 'true', WAE invokes application callbacks for authorization. If the callbacks have not been registered, all authorization checks are rejected.
/ncs-config/aaa/namespace (string) [http://tail-f.com/ns/aaa/1.1]	To move the AAA data into another user-defined namespace, indicate that namespace here.
/ncs-config/aaa/prefix (string) [/]	To move the AAA data into another user-defined namespace, indicate the prefix path in that namespace where the WAE AAA namespace is mounted.
/ncs-config/rollback	Settings that control if and where rollback files are created. A rollback file contains a copy of the system configuration. The current running configuration is always stored in rollback0, the previous version in rollback1, and so on. The oldest saved configuration has the highest suffix.
/ncs-config/rollback/ enabled (boolean) [false]	When set to 'true', a rollback file is created whenever the running configuration is modified.
/ncs-config/rollback/ directory (string)	This parameter is mandatory. The location where rollback files are created.
/ncs-config/rollback/ history-size (uint32) [35]	The number of old configurations to save.
/ncs-config/rollback/ type (delta) [delta]	This parameter is deprecated. WAE supports only type 'delta'. It is not necessary to set a value for this parameter; it is retained only for backward compatibility. Type 'delta' means that only the changes are stored in the rollback file. Rollback file 0 contains the changes from the last configuration commit. This is space and time efficient for large configurations.
/ncs-config/rollback/ rollback-numbering (rolling | fixed) [fixed]	*rollback-numbering* is either 'fixed' or 'rolling'. If set to 'rolling', rollback file '0' always contains the last commit. If set to 'fixed', each rollback gets a unique increasing number.
/ncs-config/ssh	Controls the behavior of the SSH server built into WAE.
/ncs-config/ssh/idle-connection-timeout (xs:duration) [PT10M]	The maximum time that an authenticated connection to the SSH server is allowed to exist without open channels. If the timeout is reached, the SSH server closes the connection. The default is PT10M (10 minutes). A value of 0 means there is no timeout.
/ncs-config/ssh/algorithms	Defines custom lists of algorithms to be usable with the built-in SSH implementation. For each type of algorithm, an empty value means that all supported algorithms should be usable. A non-empty value (a comma-separated list of algorithm names) means that the intersection of the supported algorithms and the configured algorithms should be usable.

Parameter	Description
/ncs-config/ssh/algorithms/server-host-key (string) []	The supported serverHostKey algorithms (if implemented in libcrypto) are "ssh-dss" and "ssh-rsa", but for any SSH server, it is limited to those algorithms for which there is a host key installed in the directory given by /ncs-config/aaa/ssh-server-key-dir. To limit the usable serverHostKey algorithms to "ssh-dss", set this value to "ssh-dss" or avoid installing a key of any other type than ssh-dss in the sshServerKeyDir.
/ncs-config/ssh/algorithms/kex (string) []	The supported key exchange algorithms (as long as their hash functions are implemented in libcrypto) are "diffie-hellman-group-exchange-sha256", "diffie-hellman-group-exchange-sha1", "diffie-hellmangroup14-sha1", and "diffie-hellman-group1-sha1". To limit the usable key exchange algorithms to "diffie-hellman-group14-sha1" and "diffie-hellmangroup-exchange-sha256" (in that order), set this value to "diffie-hellman-group14-sha1, diffie-hellmangroup-exchange-sha256".
/ncs-config/ssh/algorithms/dh-group	The range of allowed group size the SSH server responds to the client during a "diffie-hellman-groupexchange". The range is the intersection of what the client requests. If there is none, the key exchange is terminated.
/ncs-config/ssh/algorithms/ dh-group/min-size (dh-group-size-type) [2048]	Minimum size of p, in bits.
/ncs-config/ssh/algorithms/dh-group/max-size (dh-group-size-type) [4096]	Maximum size of p, in bits.
/ncs-config/ssh/algorithms/mac (string) []	The supported mac algorithms (if implemented in libcrypto) are "hmac-md5", "hmac-sha1", "hmacsha2-256", "hmac-sha2-512", "hmac-sha1-96", and "hmac-md5-96".
/ncs-config/ssh/algorithms/encryption (string) []	The supported encryption algorithms (if implemented in libcrypto) are "aes128-ctr", "aes192-ctr", "aes256-ctr", "aes128-cbc", "aes256-cbc", and "3des-cbc".
/ncs-config/ssh/client-alive-interval (xs:duration | infinity) [infinity]	If no data has been received from a connected client for this long, a request that requires a response from the client is sent over the SSH transport.
/ncs-config/ssh/client-alive-count-max (uint32) [3]	If no data has been received from the client after this many consecutive client-alive-intervals have passed, the connection drops.
/ncs-config/cli	CLI parameters.
/ncs-config/cli/enabled (boolean) [true]	If 'true', the CLI server is started.
/ncs-config/cli/allow-implicit-wildcard (boolean) [true]	If 'true', users do not need to explicitly type * in the place of keys in lists, in order to see all list instances. If 'false', users must explicitly type * to see all list instances.
/ncs-config/cli/completion-show-max (cli-max) [100]	The maximum number of possible alternatives to present when doing completion.

Parameter	Description
/ncs-config/cli/style (j | c)	Style is either 'j' or 'c'. If set to 'j', the CLI is presented as a Juniper-style CLI. If 'c', the CLI appears as Cisco XR style.
/ncs-config/cli/ssh	—
/ncs-config/cli/ssh/enabled (boolean) [true]	*enabled* is either 'true' or 'false'. If 'true', the WAE CLI uses the built-in SSH server.
/ncs-config/cli/ssh/ip (ipv4-address | ipv6-address) [0.0.0.0]	*ip* is an IP address that the WAE CLI listens on for SSH connections. 0.0.0.0 means that it listens on the port (/ncs-config/cli/ssh/port) for all IPv4 addresses on the machine.
/ncs-config/cli/ssh/port (port-number) [2024]	The port number for CLI SSH.
/ncs-config/cli/ssh/banner (string) []	*banner* is a string that is presented to the client before authenticating when logging in to the CLI via the built-in SSH server.
/ncs-config/cli/ssh/banner-file (string) []	*banner-file* is the name of a file whose contents are presented (after any string given by the banner directive) to the client before authenticating when logging in to the CLI via the built-in SSH server.
/ncs-config/cli/ssh/extra-listen	A list of additional IP address and port pairs that the WAE CLI listens on for SSH connections.
/ncs-config/cli/ssh/extra-listen/ip (ipv4-address | ipv6-address)	—
/ncs-config/cli/ssh/extra-listen/port (port-number)	—
/ncs-config/cli/top-level-cmds-in-sub-mode (boolean) [false]	topLevelCmdsInSubMode is 'true' or 'false'. If 'true', all top-level commands in I and C style CLI are available in submodes.
/ncs-config/cli/completion-meta-info (false | alt1 | alt2) [false]	completionMetaInfo is 'false', 'alt1', or 'alt2'. If set to 'alt1', the alternatives shown for possible completions are prefixed as follows: containers with > lists with + leaf-lists + For example: Possible completions: ... > applications + apply-groups ... + dns-servers ... If set to 'alt2', possible completions are prefixed as follows: containers with > lists with children with +> lists without children + For example: Possible completions: ... > applications +>apply-groups ... + dns-servers ...
/ncs-config/cli/allow-abbrev-keys (boolean) [false]	allowAbbrevKeys is 'true' or 'false'. If 'false', key elements are not allowed to be abbreviated in the CLI. This is relevant in the J-style CLI when using the commands 'delete' and 'edit'. This is relevant in the C/I-style CLIs when using the commands 'no', 'show configuration', and for commands to enter submodes.

Parameter	Description
/ncs-config/cli/j-align-leaf-values (boolean) [true]	j-align-leaf-values is 'true' or 'false'. If 'true', the leaf values of all siblings in a container or list are aligned.
/ncs-config/cli/enter-submode-on-leaf (boolean) [true]	enterSubmodeOnLeaf is 'true' or 'false'. If 'true' (the default), setting a leaf in a submode from a parent mode results in entering the submode after the command has completed. If 'false', an explicit command for entering the submode is required—for example, if running the command **interface FastEthernet 1/1/1 mtu 1400** from the top level in config mode. If enterSubmodeOnLeaf is 'true', the CLI ends up in the 'interface FastEthernet 1/1/1' submode after the command execution. If 'false', the CLI remains at the top level. To enter the submode when set to 'false', the command **interface FastEthernet 1/1/1** is required. Applied to the C-style CLI.
/ncs-config/cli/table-look-ahead (int64) [50]	The tableLookAhead element tells confd how many rows to pre-fetch when displaying a table. The prefetched rows are used to calculate the required column widths for the table. If set to a small number, you should explicitly configure the column widths in the clispec file.
/ncs-config/cli/more-buffer-lines (uint32 | unbounded) [unbounded]	moreBufferLines is used to limit the buffering done by the more process. It can be 'unbounded' or a positive integer that describes the maximum number of lines to buffer.
/ncs-config/cli/show-all-ns (boolean) [false]	If showAllNs is 'true', all elem names are prefixed with the namespace prefix in the CLI. This is visible when setting values and when showing the configuration.
/ncs-config/cli/suppress-fast-show (boolean) [false]	suppressFastShow is 'true' or 'false'. If 'true', the fast show optimization is suppressed in the C-style CLI. The fast show optimization is somewhat experimental and might break certain operations.
/ncs-config/cli/use-expose-ns-prefix (boolean) [true]	If 'true', all nodes annotated with the tailf:cli-expose-ns-prefix result in the namespace prefix being shown/required. If 'false', the tailf:cli-expose-ns-prefix annotation is ignored. The container /devices/device/config has this annotation.
/ncs-config/cli/show-defaults (boolean) [false]	*show-defaults* is 'true' or 'false'. If 'true', default values are shown when displaying the configuration. The default value is shown inside a comment on the same line as the value. Showing default values can also be enabled in the CLI per session using the operational mode command **set show defaults true**.
/ncs-config/cli/default-prefix (string) []	*default-prefix* is a string that is placed in front of the default value when a configuration is shown with default values as comments.
/ncs-config/cli/commit-retry-timeout (xs:duration | infinity) [PT0S]	The commit timeout in the CLI. This timeout controls for how long the commit operation tries to complete the operation when some other entity is locking the database. A similar configuration parameter, /ncs-config/commit-retry-timeout, sets a timeout for WAE transactions in the JSON-RPC API.
/ncs-config/cli/timezone (utc | local) [local]	Time in the CLI can be local (as configured on the host) or UTC.

Parameter	Description
/ncs-config/cli/with-defaults (boolean) [false]	*with-defaults* is 'true' or 'false'. If 'false', leaf nodes that have their default values are not shown when the user displays the configuration, unless the user gives the 'details' option to the 'show' command. This is useful when there are many settings that are seldom used. If 'false', only the values actually modified by the user are shown.
/ncs-config/cli/banner (string) []	Banner shown to the user when the CLI is started. The default is empty.
/ncs-config/cli/banner-file (string) []	File whose contents are shown to the user (after any string set by the 'banner' directive) when the CLI is started. The default is empty.
/ncs-config/cli/prompt1 (string) [\u@\h\M>]	Prompt used in operational mode. The string might contain a number of backslash-escaped special characters that are decoded as follows: • \d—Date in 'YYYY-MM-DD' format (for example, '2006-01-18'). • \h—Hostname up to the first '.' (or delimiter as defined by promptHostnameDelimiter). • \H—Current time in 24-hour HH:MM:SS format. • \T—Current time in 12-hour HH:MM:SS format. • \@—Current time in 12-hour am/pm format. • \A—Current time in 24-hour HH:MM format. • \u—Username of the current user. • \m—Mode name (only used in XR style). • \M—Mode name inside parenthesis if in a mode.
/ncs-config/cli/prompt2 (string) [\u@\h\M%]	Prompt used in configuration mode. The string might contain a number of backslash-escaped special characters that are decoded as described for prompt1.
/ncs-config/cli/c-prompt1 (string) [\u@\h\M>]	Prompt used in operational mode in the Cisco XR-style CLI. The string might contain a number of backslash-escaped special characters that are decoded as described for prompt1.
/ncs-config/cli/c-prompt2 (string) [\u@\h\M%]	Prompt used in configuration mode in the Cisco XR-style CLI. The string might contain a number of backslash-escaped special characters that are decoded as described for prompt1.
/ncs-config/cli/prompt-hostname-delimiter (string) [.]	When the \h token is used in a prompt, the first part of the hostname up until the first occurrence of the promptHostnameDelimiter is used.
/ncs-config/cli/show-log-directory (string) [/var/log]	Location where the **show log** command looks for log files.
/ncs-config/cli/idle-timeout (xs:duration) [PT30M]	Maximum idle time before terminating a CLI session. The default is PT30M (30 minutes).

Parameter	Description
/ncs-config/cli/prompt-sessions-cli (boolean) [false]	promptSessionsCLI is 'true' or 'false'. If 'true', only the current CLI sessions are displayed when the user tries to start a new CLI session and the maximum number of sessions has been reached. Note that MAAPI sessions with their context set to 'cli' are regarded as CLI sessions and are listed as such.
/ncs-config/cli/suppress-ned-errors (boolean) [false]	Suppress errors from NED devices. Make log-communication between WAE and its devices more silent. Be careful with this option, because it might suppress interesting errors as well.
/ncs-config/cli/disable-idle-timeout-on-cmd (boolean) [true]	*disable-idle-timeout-on-cmd* is 'true' or 'false'. If 'false', the idle timeout triggers even when a command is running in the CLI. If 'true', the idle timeout only triggers if the user is idling at the CLI prompt.
/ncs-config/cli/command-timeout (xs:duration | infinity) [infinity]	Global command timeout: terminate the command unless the command has completed within the timeout. We do not recommend using this feature because it might have undesirable effects in a loaded system where normal commands take longer to complete. This timeout can be overridden by a command-specific timeout specified in the ncs.cli file.
/ncs-config/cli/space-completion	—
/ncs-config/cli/space-completion/enabled (boolean)	—
/ncs-config/cli/ignore-leading-whitespace (boolean)	If 'false', the CLI shows completion help when you enter TAB or SPACE as the first characters on a row. If 'true', leading SPACE and TAB are ignored. Enter '?' for a list of possible alternatives. Setting the value to 'true' makes it easier to paste scripts into the CLI.
/ncs-config/cli/auto-wizard	The default value for autowizard in the CLI. Users can always enable or disable the autowizard in each session; this controls the initial session value.
/ncs-config/cli/auto-wizard/enabled (boolean) [true]	**enabled** is 'true' or 'false'. If 'true', the CLI prompts the user for required attributes when a new identifier is created.
/ncs-config/cli/restricted-file-access (boolean) [false]	*restricted-file-access* is 'true' or 'false'. If 'true', a CLI user cannot access files and directories outside the home directory tree.
/ncs-config/cli/restricted-file-regexp (string) []	*restricted-file-regexp* is either an empty string or a regular expression (AWK style). If not empty, all files and directories created or accessed must match the regular expression. This can be used to ensure that certain symbols do not occur in created files.
/ncs-config/cli/history-save (boolean) [true]	If 'true', the CLI history is saved between CLI sessions. The history is stored in the state directory.
/ncs-config/cli/history-remove-duplicates (boolean) [false]	If 'true', repeated commands in the CLI are only stored once in the history. Each invocation of the command only updates the date of the last entry. If 'false', duplicates are stored in the history.
/ncs-config/cli/history-max-size (int64) [1000]	Sets the maximum configurable history size.

Parameter	Description
/ncs-config/cli/message-max-size (int64) [10000]	Sets the maximum size of user messages.
/ncs-config/cli/show-commit-progress (boolean) [true]	*show-commit-progress* is 'true' or 'false'. If 'true', the commit operation in the CLI provides progress information.
/ncs-config/cli/commit-message (boolean) [true]	CLI prints a message when a commit is executed.
/ncs-config/cli/use-double-dot-ranges (boolean) [true]	*use-double-dot-ranges* is 'true' or 'false'. If 'true', range expressions are given as 1..3. If 'false', ranges are given as 1-3.
/ncs-config/cli/allow-range-expression-all-types (boolean) [true]	*allow-range-expression-all-types* is 'true' or 'false'. If 'true', range expressions are allowed for all key values regardless of type.
/ncs-config/cli/suppress-range-keyword (boolean) [false]	*suppress-range-keyword* is 'true' or 'false'. If 'true', the 'range' keyword is not allowed in C- and I-style for range expressions.
/ncs-config/cli/commit-message-format (string) [System message at $(time)... Commit performed by $(user) via $(proto) using $(ctx).]	The format of the CLI commit messages.
/ncs-config/cli/suppress-commit-message-context (string)	This parameter can be given multiple times. A list of contexts for which a commit message is not displayed. A good value is [system], which makes all system-generated commits go unnoticed in the CLI. A context is either the name of an agent (CLI, web UI, NETCONF, SNMP) or a free-form text string if the transaction is initiated from MAAPI.
/ncs-config/cli/show-subsystem-messages (boolean) [true]	*show-subsystem-messages* is 'true' or 'false'. If 'true', the CLI displays a system message whenever a connected daemon starts or stops.
/ncs-config/cli/show-editors (boolean) [true]	*show-editors* is 'true' or 'false'. If 'true', a list of current editors is displayed when a user enters configure mode.
/ncs-config/cli/rollback-aaa (boolean) [false]	If 'true', AAA rules are applied when a rollback file is loaded. Rollback might not be possible if other users made changes that the current user does not have access privileges to.
/ncs-config/cli/rollback-numbering (rolling | fixed) [fixed]	*rollback-numbering* is 'fixed' or 'rolling'. If 'rolling', rollback file '0' always contains the last commit. If 'fixed', each rollback gets a unique increasing number.
/ncs-config/cli/show-service-meta-data (boolean) [false]	If 'true', backpointers and refcounts are displayed by default when showing the configuration. The default can be overridden by the pipe flags 'display service-meta' and 'hide service-meta'.
/ncs-config/rest	Controls how the embedded WAE web server should behave with respect to TCP and SSL.

Parameter	Description
/ncs-config/rest/enabled (boolean) [false]	*enabled* is 'true' or 'false'. If 'true', the web server is started.
/ncs-config/rest/custom-headers	—
/ncs-config/rest/custom-headers/header	—
/ncs-config/rest/custom-headers/header/name (string)	—
/ncs-config/rest/custom-headers/header/value (string)	This parameter is mandatory.
/ncs-config/restconf	Controls settings for the RESTCONF API.
/ncs-config/restconf/enabled (boolean) [false]	*enabled* is 'true' or 'false'. If 'true', the RESTCONF API is enabled on the web server used by the web UI. Note that the web UI must also be enabled.
/ncs-config/restconf/root-resource (string) [restconf]	The RESTCONF root resource path.
/ncs-config/webui	Controls how the embedded WAE web server should behave with respect to TCP and SSL.
/ncs-config/webui/custom-headers	*custom-headers* contains any number of header elements, with a valid header-field as defined in RFC7230. The headers are part of HTTP responses on '/login.html', '/index.html', and '/jsonrpc'.
/ncs-config/webui/custom-headers/header	—
/ncs-config/webui/custom-headers/header/name (string)	—
/ncs-config/webui/custom-headers/header/value (string)	This parameter is mandatory.
/ncs-config/webui/enabled (boolean) [false]	*enabled* is 'true' or 'false'. If 'true', the web server is started.
/ncs-config/webui/server-name (string) [localhost]	The hostname that the web server serves.
/ncs-config/webui/match-host-name (boolean) [false]	Specifies whether the web server should only serve URLs that adhere to the server-name defined above. By default, the server-name is 'localhost' and match-host-name is 'false'; any server name can be given in the URL. If you want the server to only accept URLs that adhere to the server-name, enable this setting.
/ncs-config/webui/cache-refresh-secs (uint64) [0]	The WAE web server uses a RAM cache for static content. An entry sits in the cache for a number of seconds before it is reread from disk (on access). The default is 0.

Parameter	Description
/ncs-config/webui/max-ref-entries (uint64) [100]	Leafref and keyref entries are represented as drop-down menus in the automatically generated web UI. By default, no more than 100 entries are fetched. This element makes this number configurable.
/ncs-config/webui/docroot (string)	The location of the document root on disk. If this configurable is omitted, the docroot points instead to the next generation docroot in the WAE distribution.
/ncs-config/webui/login-dir (string)	*login-dir* points out an alternative login directory that contains the HTML code used to log in to the web UI. This directory is mapped to https://<*ip-address*>/login. If this element is not specified, the default login/ directory in the docroot is used instead.
/ncs-config/webui/X-Frame-Options (DENY | SAMEORIGIN | ALLOW-FROM) [DENY]	By default the *X-Frame-Options* header is set to DENY for the /login.html and /index.html pages. With this header, you can set it to SAMEORIGIN or ALLOW-FROM instead.
/ncs-config/webui/disable-auth	—
/ncs-config/webui/disable-auth/dir (string)	This parameter can be given multiple times. The *disable-auth* element contains any number of *dir* elements. Each *dir* element points to a directory path in the docroot that should not be restricted by the AAA engine. If no *dir* elements are specified, the following directories and files are not restricted by the AAA engine: '/login' and '/login.html'.
/ncs-config/webui/allow-symlinks (boolean) [true]	Allows symlinks in the docroot directory.
/ncs-config/webui/transport	Controls which transport services (for example, TCP or SSL) the web server should listen on.
/ncs-config/webui/transport/tcp	Controls how the web server TCP transport service should behave.
/ncs-config/webui/transport/tcp/enabled (boolean) [true]	*enabled* is 'true' or 'false'. If 'true', the web server uses clear text TCP as a transport service.
/ncs-config/webui/transport/tcp/ redirect (string)	Redirects the user to the specified URL. Two macros can be specified: @HOST@ and @PORT@. For example: https://@HOST@:443 or https://192.12.4.3:@PORT@
/ncs-config/webui/transport/ tcp/ip (ipv4-address | ipv6-address) [0.0.0.0]	The IP address that the web server should listen on. 0.0.0.0 means that it listens on the port (/ncsconfig/webui/transport/tcp/port) for all IPv4 addresses on the machine.
/ncs-config/webui/transport/ tcp/port (port-number) [8008]	*port* is a valid port number to use in combination with the address in /ncs-config/webui/transport/tcp/ip.
/ncs-config/webui/transport/tcp/extra-listen	A list of additional IP address and port pairs that the web server should also listen on.

Parameter	Description
/ncs-config/webui/ transport/tcp/extra-listen/ip (ipv4-address | ipv6-address)	—
/ncs-config/webui/ transport/tcp/extra-listen/port (port-number)	—
/ncs-config/webui/ transport/ssl	Controls how the web server SSL transport service should behave. SSL is widely deployed on the Internet; virtually all online shopping and bank transactions are done with SSL encryption. There are many good sources that describe SSL in detail; for example, http://www.tldp.org/HOWTO/SSL-Certificates-HOWTO/ describes how to manage certificates and keys.
/ncs-config/webui/ transport/ssl/enabled (boolean) [false]	*enabled* is 'true' or 'false'. If 'true', the web server uses SSL as a transport service.
/ncs-config/webui/transport/ ssl/redirect (string)	Redirects the user to the specified URL. Two macros can be specified: @HOST@ and @PORT@. For example: http://@HOST@:80 or http://192.12.4.3:@PORT@
/ncs-config/webui/transport/ssl/ip (ipv4-address | ipv6-address) [0.0.0.0]	The IP address on which the web server listens for incoming SSL connections. 0.0.0.0 means that it listens on the port (/ncs-config/webui/transport/ssl/port) for all IPv4 addresses on the machine.
/ncs-config/webui/ transport/ssl/port (port-number) [8888]	*port* is a valid port number to use in combination with /ncs-config/webui/transport/ssl/ip.
/ncs-config/webui/transport/ssl/extra-listen	A list of additional IP address and port pairs on which the web server listens for incoming SSL connections.
/ncs-config/webui/ transport/ssl/extra-listen/ip (ipv4-address | ipv6-address)	—
/ncs-config/webui/ transport/ssl/extra-listen/port (port-number)	—
/ncs-config/webui/transport/ ssl/key-file (string)	Specifies the file that contains the private key for the certificate. Read more about certificates in /ncs-config/webui/ transport/ssl/cert-file. If this configurable is omitted, the keyFile points instead to a built-in, self-signed certificate/key in the WAE distribution. Note: Only use this certificate/key for test purposes.

Parameter	Description
/ncs-config/webui/transport/ ssl/cert-file (string)	Specifies the file that contains the server certificate. The certificate is either a self-signed test certificate or a genuine, validated certificate bought from a certificate authority (CA). If this configurable is omitted, the keyFile points instead to a built-in, self-signed certificate/key in the WAE distribution. Note: Only use this certificate/key for test purposes. The WAE distribution comes with a server certificate that can be used for testing (${NCS_DIR}/var/ncs/webui/ cert/host.{cert,key}). This server certificate has been generated using a local CA certificate: $ openssl OpenSSL> genrsa -out ca.key 4096 OpenSSL> req -new -x509 -days 3650 -key ca.key - out ca.cert OpenSSL> genrsa -out host.key 4096 OpenSSL> req -new -key host.key -out host.csr OpenSSL> x509 -req -days 365 -in host.csr -CA ca.cert \ -CAkey ca.key -set_serial 01 -out host.cert
/ncs-config/webui/transport/ ssl/ca-cert-file (string)	Specifies the file that contains the trusted certificates to use during client authentication and to use when attempting to build the server certificate chain. The list is also used in the list of acceptable CA certificates passed to the client when a certificate is requested. The WAE distribution comes with a CA certificate that can be used for testing (${NCS_DIR}/var/ncs/ webui/ca_cert/ca.cert). This CA certificate has been generated as shown above.

/ncs-config/webui/transport/ ssl/verify (1 | 2 | 3) [1]	Specifies the level of verification the server does on client certificates:
	• 1—No verification.
	• 2—The server asks the client for a certificate but does not fail if the client does not supply one.
	• 3—The server requires the client to supply a client certificate.
	
	If ca-cert-file has been set to the ca.cert file generated above, you can verify that it works by using:
	
	$ openssl s_client -connect 127.0.0.1:8888 \ -cert client.cert -key client.key
	
	For this to work, client.cert must have been generated using the ca.cert from above:
	
	$ openssl OpenSSL> genrsa -out client.key 4096 OpenSSL> req -new -key client.key -out client.csr OpenSSL> x509 -req -days 3650 -in client.csr -CA ca.cert \ -CAkey ca.key -set_serial 01 -out client.cert

/ncs-config/webui/transport/ ssl/depth (uint64) [1]	Specifies the depth of certificate chains the server is prepared to follow when verifying client certificates.

Parameter	Description
/ncs-config/webui/transport/ ssl/ciphers (string) [DEFAULT]	Specifies the cipher suites for the server to use. The ciphers are a colon-separated list from the following set: ECDHEECDSA-AES256-SHA384, ECDHE-RSA-AES256-SHA384, ECDH-ECDSA-AES256-SHA384, ECDH-RSA-AES256-SHA384, DHE-RSA-AES256-SHA256, DHE-DSS-AES256-SHA256, AES256-SHA256, ECDHE-ECDSA-AES128-SHA256, ECDHE-RSA-AES128-SHA256, ECDHECDSA-AES128-SHA256, ECDH-RSA-AES128-SHA256, DHE-RSA-AES128-SHA256, DHEDSS-AES128-SHA256, AES128-SHA256, ECDHE-ECDSA-AES256-SHA, ECDHE-RSA-AES256-SHA, DHE-RSA-AES256-SHA, DHE-DSS-AES256-SHA, ECDH-ECDSA-AES256-SHA, ECDHRSA-AES256-SHA, AES256-SHA, ECDHE-ECDSA-DES-CBC3-SHA, ECDHE-RSA-DES-CBC3-SHA, EDH-RSA-DES-CBC3-SHA, EDH-DSS-DES-CBC3-SHA, ECDH-ECDSA-DES-CBC3-SHA, ECDH-RSA-DES-CBC3-SHA, DES-CBC3-SHA, ECDHE-ECDSA-AES128-SHA, ECDHE-RSAAES128-SHA, DHE-RSA-AES128-SHA, DHE-DSS-AES128-SHA, ECDH-ECDSA-AES128-SHA, ECDH-RSA-AES128-SHA, AES128-SHA, ECDHE-ECDSA-RC4-SHA, ECDHE-RSA-RC4-SHA, RC4-SHA, RC4-MD5, EDH-RSA-DES-CBC-SHA, ECDH-ECDSA-RC4-SHA, ECDH-RSA-RC4-SHA, and DES-CBC-SHA, or the word "DEFAULT" (use the listed set except the suites using DES, RC4, or MD5 algorithms) See the OpenSSL manual page ciphers(1) for the definition of the cipher suites. Note: The general cipher list syntax described in ciphers(1) is not supported.
/ncs-config/webui/transport/ ssl/protocols (string) [DEFAULT]	Specifies the SSL/TLS protocol versions for the server to use as a whitespace-separated list from the set sslv3 tlsv1 tlsv1.1 tlsv1.2, or the word "DEFAULT" (use all supported protocol versions except sslv3).
/ncs-config/webui/cgi	CGI-script support.
/ncs-config/webui/cgi/ enabled (boolean) [false]	*enabled* is 'true' or 'false'. If 'true', CGI-script support is enabled.
/ncs-config/webui/cgi/ dir (string) [cgi-bin]	The directory path to the location of the CGI-scripts.
/ncs-config/webui/cgi/ request-filter (string)	Specifies that characters not specified in the regexp should be filtered out silently.
/ncs-config/webui/cgi/ max-request-length (uint16)	Specifies the maximum number of characters in a request. All characters that exceed this limit are silently ignored.
/ncs-config/webui/cgi/php	PHP support.
/ncs-config/webui/cgi/php/ enabled (boolean) [false]	*enabled* is 'true' or 'false'. If 'true', PHP support is enabled.
/ncs-config/webui/ idle-timeout (xs:duration) [PT30M]	The maximum idle time before terminating a web UI session. PT0M means no timeout. The default is PT30M (30 minutes).

Parameter	Description
/ncs-config/webui/ absolute-timeout (xs:duration) [PT60M]	The maximum absolute time before terminating a web UI session. PT0M means no timeout. The default is PT60M (60 minutes).
/ncs-config/webui/ rate-limiting (uint64) [1000000]	The maximum number of JSON-RPC requests allowed every hour. 0 means infinity. The default is 1 million.
/ncs-config/webui/ audit (boolean) [true]	*audit* is 'true' or 'false'. If 'true', JSON-RPC/CGI requests are logged to the audit log.
/ncs-config/japi	Java-API parameters.
/ncs-config/japi/new-session-timeout (xs:duration) [PT30S]	The timeout for a data provider to respond to a control socket request; see DpTrans. If the Dp fails to respond within the given time, it is disconnected.
/ncs-config/japi/query-timeout (xs:duration) [PT120S]	The timeout for a data provider to respond to a worker socket query; see DpTrans. If the Dp fails to respond within the given time, it is disconnected.
/ncs-config/japi/connect-timeout (xs:duration) [PT60S]	The timeout for a data provider to send an initial message after connecting the socket to the WAE server. If the Dp fails to initiate the connection within the given time, it is disconnected.
/ncs-config/japi/object-cache-timeout (xs:duration) [PT2S]	The timeout for the cache used by the getObject() and iterator(),nextObject() callback requests. WAE caches the result of these calls and serves getElem() requests from northbound agents from the cache. Setting this timeout too low causes the callbacks to be non-functional. For example, getObject() can be invoked for each getElem() request from a northbound agent.
/ncs-config/japi/event-reply-timeout (xs:duration) [PT120S]	The timeout for the reply from an event notification subscriber for a notification that requires a reply; see the Notif class. If the subscriber fails to reply within the given time, the event notification socket is closed.
/ncs-config/netconf-north-bound	Controls how the NETCONF agent should behave with respect to NETCONF and SSH.
/ncs-config/netconf-north-bound/ enabled (boolean) [true]	*enabled* is 'true' or 'false'. If 'true', the NETCONF agent is started.
/ncs-config/netconf-north-bound/ transport	Controls which transport services (TCP or SSH) the NETCONF agent should listen on.
/ncs-config/netconf-north-bound/ transport/ssh	Controls how the NETCONF SSH transport service should behave.
/ncs-config/netconf-north-bound/ transport/ssh/enabled (boolean) [true]	*enabled* is 'true' or 'false'. If 'true', the NETCONF agent uses SSH as a transport service.
/ncs-config/netconf-north-bound/ transport/ssh/ip (ipv4-address | ipv6-address) [0.0.0.0]	*ip* is an IP address that the WAE NETCONF agent listens on. 0.0.0.0 means that it listens on the port (/ncs-config/netconf-north-bound/transport/ssh/port) for all IPv4 addresses on the machine.

Parameter	Description
/ncs-config/netconf-north-bound/ transport/ssh/port (port-number) [2022]	*port* is a valid port number to use in combination with /ncs-config/netconf-north-bound/transport/ssh/ip. The standard port for NETCONF over SSH is 830.
/ncs-config/netconf-north-bound/ transport/ssh/extra-listen	A list of additional IP address and port pairs that the WAE NETCONF agent listens on.
/ncs-config/netconf-north-bound/ transport/ssh/extra-listen/ip (ipv4-address | ipv6-address)	—
/ncs-config/netconf-north-bound/ transport/ssh/extra-listen/port (port-number)	—
/ncs-config/netconf-north-bound/ transport/tcp	NETCONF over TCP is not standardized, but it can be useful during development (for example, to use netcat for scripting). It is also useful when using your own proprietary transport. You can set up the NETCONF agent to listen on localhost and then proxy it from your transport service module.
/ncs-config/netconf-north-bound/ transport/tcp/enabled (boolean) [false]	*enabled* is 'true' or 'false'. If 'true', the NETCONF agent uses clear text TCP as a transport service.
/ncs-config/netconf-north-bound/ transport/tcp/ip (ipv4-address | ipv6-address) [0.0.0.0]	*ip* is an IP address that the WAE NETCONF agent listens on. 0.0.0.0 means that it listens on the port (/ncs-config/netconf-north-bound/transport/tcp/port) for all IPv4 addresses on the machine.
/ncs-config/netconf-north-bound/ transport/tcp/port (port-number) [2023]	*port* is a valid port number to use in combination with /ncs-config/netconf-north-bound/transport/tcp/ip.
/ncs-config/netconf-north-bound/ transport/tcp/extra-listen	A list of additional IP address and port pairs that the WAE NETCONF agent listens on.
/ncs-config/netconf-north-bound/ transport/tcp/extra-listen/ip (ipv4-address | ipv6-address)	—
/ncs-config/netconf-north-bound/ transport/tcp/extra-listen/port (portnumber)	—
/ncs-config/netconf-north-bound/ extended-sessions (boolean) [false]	If extended-sessions are enabled, all WAE sessions can be terminated using <kill-session>. Not only can other NETCONF sessions be terminated, but also CLI sessions, web UI sessions, and so on. If a session holds a lock, its session ID is returned in the <lock-denied>, instead of '0'. This extension is not covered by the NETCONF specification; therefore, it is false by default.

Parameter	Description
/ncs-config/netconf-north-bound/ idle-timeout (xs:duration) [PT0S]	The maximum idle time before terminating a NETCONF session. If the session is waiting for notification or has a pending confirmed commit, the idle timeout is not used. The default value is 0, which means no timeout.
/ncs-config/netconf-north-bound/ rpc-errors (close | inline) [close]	If *rpc-errors* is 'inline' and an error occurs during the processing of a <get> or <get-config> request when WAE tries to fetch data from a data provider, WAE generates an rpc-error element in the faulty element, and continue to process the next element. If an error occurs and *rpc-errors* is 'close', WAE closes the NETCONF transport.
/ncs-config/netconf-north-bound/ max-batch-processes (uint32 | unbounded) [unbounded]	Controls the number of concurrent NETCONF batch processes. A batch process can be started by the agent if a new NETCONF operation is implemented as a batch operation.
/ncs-config/netconf-north-bound/ capabilities	Controls which NETCONF capabilities to enable.
/ncs-config/netconf-north-bound/ capabilities/url	Turns on the URL capability options to support.
/ncs-config/netconf-north-bound/ capabilities/url/enabled (boolean) [false]	*enabled* is 'true' or 'false'. If 'true', the URL NETCONF capability is enabled.
/ncs-config/netconf-north-bound/ capabilities/url/file	Controls how the URL file support should behave.
/ncs-config/netconf-north-bound/ capabilities/url/file/enabled (boolean) [true]	*enabled* is 'true' or 'false'. If 'true', the URL file scheme is enabled.
/ncs-config/netconf-north-bound/ capabilities/url/file/root-dir (string)	*root-dir* is a directory path on disk where ConfD stores the result from an NETCONF operation using the URL capability. This parameter must be set if the file URL scheme is enabled.
/ncs-config/netconf-north-bound/ capabilities/url/ftp	Controls how the URL FTP scheme should behave.
/ncs-config/netconf-north-bound/ capabilities/url/ftp/enabled (boolean) [true]	*enabled* is 'true' or 'false'. If 'true', the URL FTP scheme is enabled.
/ncs-config/netconf-north-bound/ capabilities/url/sftp	Controls how the URL SFTP scheme should behave.
/ncs-config/netconf-north-bound/ capabilities/url/sftp/enabled (boolean) [true]	*enabled* is 'true' or 'false'. If 'true', the URL SFTP scheme is enabled.
/ncs-config/netconf-north-bound/ capabilities/inactive	Controls the inactive capability option.

Parameter	Description
/ncs-config/netconf-north-bound/ capabilities/inactive/enabled (boolean) [true]	*enabled* is 'true' or 'false'. If 'true', the 'http://tail-f.com/ns/netconf/inactive/1.0' capability is enabled.
/ncs-config/southbound-source-address	Specifies the source address to use for southbound connections from WAE to devices. In most cases the source address assignment is best left to the TCP/IP stack in the OS, because an incorrect address might result in connection failures. However, if the stack could choose more than one address, and you need to restrict the choice to one address, these settings can be used.
/ncs-config/southbound-source-address/ ipv4 (ipv4-address)	The source address to use for southbound IPv4 connections. If not set, the source address is assigned by the OS.
/ncs-config/southbound-source-address/ ipv6 (ipv6-address)	The source address to use for southbound IPv6 connections. If not set, the source address is assigned by the OS.
/ncs-config/ha	—
/ncs-config/ha/enabled (boolean) [false]	If 'true', HA mode is enabled.
/ncs-config/ha/ip (ipv4-address | ipv6-address) [0.0.0.0]	The IP address that WAE listens to for incoming connections from other HA nodes.
/ncs-config/ha/port (port-number) [4570]	The port number that WAE listens to for incoming connections from other HA nodes.
/ncs-config/ha/tick-timeout (xs:duration) [PT20S]	Defines the timeout between keepalive ticks sent between HA nodes. The value 'PT0' means that no keepalive ticks are ever sent.
/ncs-config/scripts	It is possible to add scripts to control various things in WAE, such as post-commit callbacks. New CLI commands can also be added. The scripts must be stored under /ncs-config/scripts/dir, where there is a subdirectory for each script category. For some script categories it suffices to add a script in the correct subdirectory to enable the script. For others some configuration must be done.
/ncs-config/scripts/dir (string)	This parameter can be given multiple times. The directory path to the location of plug-and-play scripts. The scripts directory must have the following subdirectories: scripts/command/ post-commit/
/ncs-config/large-scale	—
/ncs-config/large-scale/lsa	—
/ncs-config/large-scale/lsa/enabled (boolean) [false]	Enables Layered Service Architecture (LSA), which requires a separate Cisco Smart License.

Additional WAE CLI Commands