Troubleshooting

Health Report

On login, the system displays a health report indicating the status of the system before displaying the CLI user prompt. This health report shows the following:

```
host: AS01, role: webproxy,application,database, LOAD: 2.74
date: 2014-08-28 13:44:42 +00:00, up: 6 days, 5:23
network: 172.29.42.100, ntp: 196.26.5.10
HEALTH: NOT MONITORED
database: 20Gb
application: upCLUSTER: DOWN
   mail - local mail management          keys - ssh/sftp credentials
network - network management           backup - manage backups
   voss - voss management tools            log - manage system logs
  notify - notifications control     database - database management
    diag - system diagnostic tools   schedule - scheduling commands
    snmp - snmp configuration          system - system administration
cluster - cluster management             user - manage users
    web - web server management       drives - manage disk drives
security - security update tools          app - manage applications

platform@development:~$
```

The report explanation is shown below:

Name	Description
Last login	Last console login and IP address source.
load	The load average of the system.
USERS	The number of CLI users currently logged in.
up	The system uptime.
services	The status of the system services.
SECURITY	Whether security updates are available - refer to the Security Patches section in the Platform Guide. Security updates are installed using **security update**.
HEALTH	A Health notification, for example a scheduled mail message, is set up or not.
database	Current database size.
application	Status of the application.

- disk, CPU and memory warnings are shown if applicable
- warnings are displayed in upper-case to draw attention

A list of diagnostic tools is available in the topic on Diagnostic Tools.

Logs

The system maintains a comprehensive list of logs under `/var/log`:

- The `platform/` directory has logs pertaining the the general platform
  - `apps.log` contains application and process control logging
  - `backup.log` contains all logging pertaining to backups
  - `cluster.log` contains all control level management of the cluster
  - `config.log` contains information relating to the platform-level configuration
  - `execute.log` contains low-level information about command execution
  - `notifications.log` contains information relating to SNMP notifications
  - `reports.log` contains information relating to system reports. Refer to the Scheduling section on how reports can be created.
  - `security.log` contains low-level information relating to security updates
  - `ui.log` contains higher-level information relating to UI commands being executed.
  - `wsgi.log` contains information relating to API-level commands via the WSGI server

- The `provision/` directory contains logs relating to provisioning. Every module provision is logged to component log files.
- The `health/` directory contains health logs. These are stored automatically every half hour, or whenever health is run, and are of the format `health/summary_report-<date>-<time>`.
- The `process/` directory contains process logs instrumental in debugging particular processes. All of the output from each process is logged to an individual file `process/<application>.<process>.log`
- The `install/` directory contains logs detailing the install process.
- The `mongodb/` directory contains logs relating to the Database function.
- The `nginx/` directory contains logs relating to the WebProxy function.
- The `voss-deviceapi/` directory contains logs relating to the Application function.

log list [<prefix>] is used to display a list of logs, optionally within a particular section, e.g. **log list process** or **log list install**.

Once a filename is known, the particular log can be viewed with **log view <logfile>**, or watched (Unix terminology: **tail –f**) using **log follow <logfile>**, for example **log view process/mongodb.router.log**. When the log file is viewed, it can be searched for a particular regular expression using **/** as with the normal **less** command.

Note that the system will attempt to auto-complete the prefix if it uniquely identifies a file, e.g.

log view process/nginx

Single or multiple logfiles can be sent to a URI destination using **log send <logfile> <URI>** and **log send <prefix> <URI>** respectively. The URI must match the URI description detailed under the Networking section. An example of an email URI is `mailto:user@server.com`. Log files newer than a certain date can be sent using **log sendnewer <yyyy-mm-dd> <URI>**. If the remote URI destination requires a password, it will prompt for the password. A passwordless **scp** session can be enabled by generating keys locally with **key generate** and then sending the local keyset to the remote destination with **key send user@<hostname>**.

All email communication requires **notify emailrelay** to be configured with the IP address of your mail relay.

Logs are rotated by the system whenever they exceed 100MB, and the system will attempt to keep 5 historic zipped files of each log. However, if the disk containing /var/log is exceeded, files will be purged to ensure that the system continues to function. All rotated log files and log files exceeding 1Gb can be manually be purged using **log purge**.

The Mail Command

The system monitors a number of events – these are described in more detail in the topic on Warnings and Notifications. The events can be signaled externally using email and snmp. However, a local copy of all events is maintained in the platform user's mailbox.

Command	Description
mail list	Display a list of events stored in the mailbox.
mail read all	Read all mail.

Command	Description
mail read <number>	Read a specific mail message.
mail del <number>	Delete a specific mail message.
mail del <from> <to>	Delete a range of mail messages.
mail del all	Delete all mail messages.

Mail events may accumulate over time. The system will purge old events automatically if the mailbox becomes too full (more than 500 messages).

Diagnostic Tools

There is an extensive list of diagnostic tools available under the **diag** menu.

```
platform@development:~$ diag
USAGE:
------
diag disk              - display diagnostics for disk usage
diag free              - display diagnostics relating to free memory
diag health            - display a health report
diag health report     - save a health report as a logfile
diag iostat            - IO subsystem statistics
diag iotop             - IO metrics
diag largefiles       - Find the largest files on your system no more than the top 10 items
 are display
diag mem               - display memory diagnostics
diag monitor           - update the system resource analysis. Use 'diag monitor list' to
view the results
diag monitor list      - display system resource analysis
diag nicstat           - Network Interface Statistics
diag perf <commands>   - Linux perf tools (try --help)
diag ping <host>       - ping a remote host to test network reachability
diag proc              - display a list of system processes
diag resolve <host>    - resolve a hostname to IP address
diag tasks             - display constant task listing
diag top               - Process resource statistics
diag traceroute <host> - Discover the network path to <host>
diag unmttests         - Run system unit tests
diag vmstat            - Virtual Memory subsystem statistics

    mail - local mail management          keys - manage ssh / sftp credenti
 network - network management           backup - manage backups
    voss - voss management tools           log - manage system logs
    cert - manage nginx certificates    notify - notifications control
     ssl                              schedule - scheduling commands
    diag - system diagnostic tools      system - system administration
    snmp - snmp configuration             user - manage users
  drives - manage disk drives              app - manage applications
security - security update tools
```

In particular, the following are mostly used:

Command	Description
diag ping <host>	Test network reachability to a network host.
diag resolve <hostname>	Test DNS resolution of a hostname.

Command	Description
diag free	Display the memory usage.
diag disk	Display the disk usage.
diag mem	Display a more detailed memory usage by process.
diag health	Display a comprehensive health summary.
diag top	Display a single Unix top summary.

Diagnostic Troubleshooting

The health displayed on login will normally include sufficient information to determine that the system is either working, or experiencing a fault. More detailed health reports can be be displayed with **diag health**.

A rich set of SNMP and SMTP traps are described in the Notifications section which can be used to automate fault discovery.

Determine if all processes are running using **app status**. If a process is not running, investigate its log file with:

log view process/<application>.<process>

For example, checking processes:

```
platform@development:~$ app status
development v0.8.0 (2013-08-12 12:41)
voss-deviceapi v0.6.0 (2013-11-19 07:37)
   |-voss-celerycam             running
   |-voss-queue_high_priority   running

   ...
core_services v0.8.0 (2013-08-27 10:46)
   |-wsgi                       running
   |-logsizemon                 running
   |-firewall                   running
   |-mountall                   running
   |-syslog                     running (completed)
   |-timesync                   stopped (failed with error 1)
nginx v0.8.0 (2013-08-27 10:53)
   |-nginx                      running
security v0.8.0 (2013-08-27 11:02)
```

Followed by a log investigation for a stopped process:

```
platform@development:~$ log view process/core_services.timesync
2013-08-15 10:55:20.234932 is stopping from basic_stop
2013-08-15 10:55:20:    core_services:timesync killed
  successfully
2013-08-15 10:55:20: Apps.StatusGenerator core_services:timesync
  returned 1 after 1 loops
App core_services:timesync is not running with status stopped

...

+ /usr/sbin/ntpdate 172.29.1.15
2014-02-04 09:27:31: Apps.StatusGenerator core_services:timesync
  returned 0 after 1 loops
2014-02-04 09:27:31: WaitRunning core_services:timesync is reporting
  return code 0
```

```
core_services:timesync:/opt/platform/apps/core_services/timesync
  started
4 Feb 09:27:38 ntpdate[2766]: no server suitable for
  synchronization found
+ echo 'Failed to contact server: 172.29.1.15 - retrying'
Failed to contact server: 172.29.1.15 - retrying
+ COUNTER=2
+ sleep 1
+ test 2 -lt 3
+ /usr/sbin/ntpdate 172.29.1.15
4 Feb 09:27:48 ntpdate[3197]: no server suitable for
  synchronization found
+ echo 'Failed to contact server: 172.29.1.15 - retrying'
Failed to contact server: 172.29.1.15 - retrying
+ COUNTER=3
+ sleep 1
+ test 3 -lt 3
+ test 3 -eq 3
+ echo 'Timesync  - could not contact server 172.29.1.15 after
    three tries. Giving up'
Timesync  - could not contact server 172.29.1.15 after
   three tries. Giving up
+ exit 1
```

The error message and return code being displayed in the browser is also invaluable in determining the cause of the problem.

The system resources can be inspected as follows:

- **diag disk** will display the disk status
- **diag free** and **diag mem** will display the memory status
- **diag top** will display the CPU status

Warnings and Notifications

The system will monitor a number of conditions and generate events as necessary.

Events are grouped into 3 categories:

- info messages that are informational and do not require further attention
- warning notices that indicate that a recoverable event has occurred and further action is not required.
- error notices that indicate a failure and must be addressed.

The following conditions are monitored:

Condition	Message type	Detail and Action
Backups	Backup failed	Error. Corrective action: attempt a manual backup and monitor output; ensure that sufficient space on the disk is available; check the automated backup schedule with schedule list
Backups	Backup successful	info
Backups	Backup restored successfully	info

Condition	Message type	Detail and Action
Backups	Backup restore failed	Error. Corrective action: ensure that the requested backup exists using backup list; monitor output of the backup restore process; ensure that there is sufficient space on the database volume
Backups	Last successful backup more than 2 days ago	Error. Corrective action: perform a manual backup; schedule automated backups with schedule
Backups	Backups are running regularly	info

Condition	Message type	Detail and Action
Logs	Forcing log rotation as disk usage is high	info
Logs	Autopurging logs due to excessive disk usage	warn
Logs	Log files larger than 1GB found in `/var/log`	Error. Corrective action: diagnose large files with **diag largefiles**
Logs	Normal log rotation is running	info

Condition	Message type	Detail and Action
Disk usage	Disk full	Error. Corrective action: use diag disk to analyse disk usage, remove excess files in user home directories, purge logs with log purge, check that the disk is not mounted read-only due to disk problems
Disk usage	Disk usage greater than 80%	warn
Disk usage	Disk latency excessive (slow)	Error. Corrective action: monitor hardware performance using hardware specific tools such as Vsphere.
Disk usage	Disk latency returned to normal	info
Disk usage	Disk `/var/log` greater than 80%	Error. Corrective actions: purge logs with log purge

Condition	Message type	Detail and Action
Mailbox	Mailbox full, > 500 messages, autoarchiving	info
Mailbox	Messages reduced < 200	info

Condition	Message type	Detail and Action
Notifications	Email not configured for notifications	Warn. Corrective action: configure email address and mail relay
Notifications	Email is configured for notifications	info
Notifications	SNMP trap failed to be sent	Error. Corrective action: send test event with **notify test info**
Notifications	Test notification sent	info

Condition	Message type	Detail and Action
Health reports	Error sending health report via email	Error.
Health reports	Health reports successfully sent via email	info

Condition	Message type	Detail and Action
Cluster	One or more nodes down in the cluster	Error. Corrective action: check cluster status and restart node as necessary
Cluster	No hosts defined in the cluster	Error. Corrective action: check cluster list and add nodes as necessary
Cluster	All nodes in the cluster running	info

Condition	Message type	Detail and Action
Network	Network failure	Error. Corrective actions: check network cables, firewalling, routing and hardware
Network	Network failure resolved	info
Network	NTP server is not configured	Error. Corrective action: ensure that the NTP server is set correctly with **network ntp**
Network	NTP server is configured	info
Network	NTP offset exceeds 1 second	Warn. Corrective action: check that the NTP server is correctly configured with **network ntp** and the NTP server is reachable and functioning correctly.
Network	NTP offset returns to normal	info

Condition	Message type	Detail and Action
Network	DNS server is not configured	warn
Network	DNS server is now configured	info
Network	No DNS domain configured	warn
Network	DNS domain is configured	info

Condition	Message type	Detail and Action
Applications	Failed to start service	Error. Corrective action: check the application status with **app status**; service log with **log view process/<application>.<process>**
Applications	Services started successfully	info
Aplications	Upgrade failed	Error. Corrective action: check the output from the upgrade; ensure that disk space is available with **diag disk**

Condition	Message type	Detail and Action
Security	Security updates available	Warn. Required action: run security update
Security	Security updates applied	info

Condition	Message type	Detail and Action
Resource usage	High memory usage	Error. Corrective action: check the memory usage with **diag free** and **diag mem**; ensure that sufficient memory resources are available to the host via Vsphere
Resource usage	Memory usage returned to normal	info
Resource usage	CPU has high utilisation	warn
Resource usage	Extremely high CPU utilisation	Error. Corrective action: check the CPU utilisation with **diag top**; ensure that sufficient CPU resources are available to server via Vsphere
Resource usage	CPU utilisation returned to normal	info

SNMP CPU load notifications are set using:

snmp load <1min load> <5min load> <15min load>

This results in notifications being sent should the threshold be exceeded. For a server with 2 CPUs, it is recommended that this setting be:

snmp load 8 4 2

This means that notifications are sent if the 2-CPU system load averages over the last 1, 5, and 15 minutes reach these values.

The system can be configured to forward warnings and notifications to a variety of destinations, including:

- local email
- remote email addresses
- remote SNMP destinations

The notification destinations can be displayed with **notify list**. The destinations for each event level can be set with **notify add info|warn|error <destination-URI>** Refer to the Network URI Specification topic for a detailed description of URIs. Note that email notifications require the mail relay to be set with **notify emailrelay <relayhost>**. A test event can be generated with **notify test info|warn|error** to test the notification delivery mechanism.

Examples:

- **notify add info mailto:sysadmin@mycompany.com**
- **notify add error snmp://public@mysnmpserver.com**

In addition to external email and SNMP alerts, the system also records various events to a local mailbox.

Error Messages

The tables below provide a reference to the error codes in the system.

To inspect application log messages from the command line, set the debug level on and view the app log.

```
voss set_debug 1
log view voss-deviceapi/app.log
```

The message strings are shown in template format: references to specific properties are shown as placeholders that are represented by {} .

The HTTP Code is 400 unless specified otherwise.

Default Error Code	Message	HTTP Code
0	Invalid Exception	

System Error Code	Message	HTTP Code
0000	Error, Mongo service not started	
0001	Error, Server too busy	
0002	Error, Celery service not started	

Python Internal Error Code	Message	HTTP Code
1000	Cannot import Python model name {}	404
1001	Python Type error	

Database Error Code	Message	HTTP Code
2000	Cannot setup Mongo DB collection {}	
2001	Find failed with spec={}, fields={}, skip={}, limit={}, sort_by={}, err={}	
2002	Find one failed with spec={}, fields={}, err={}	
2003	Get archive history failed with spec={}, fields={}, skip={}, limit={}, err={}	
2004	Remove failed with spec={}, err={}	
2005	Find and modify failed with spec={}, modify={}, err={}	
2006	Find and modify failed with spec={}, modify={}, err={}	
2007	Count failed for {}	
2008	Find failed with spec={}, fields={}, err={}	
2100	Error, Cannot connect to RESOURCE database collection	
2101	Error, Cannot connect to DATA database collection	
2102	Error, Cannot connect to ARCHIVE database collection	
2999	Unhandled Database Error	

API Error Code	Message	HTTP Code
3000	Hierarchy context may not be None, please select Hierarchy	
3001	Error, Incorrect request format	
3002	Error, Unhandled method for URL	
3003	Invalid import file specified. {}	

API Error Code	Message	HTTP Code
3004	Invalid export URL specified. {}	
3005	Error, Invalid list view sort key [{}]. Valid options are {}	
3006	Error, Invalid list direction [{}]. Valid options are {}	
3007	Error, No schema available during list view	
3008	Provisioning Workflow error [{}]	
3009	Nothing to export	
3010	List delete failed, error [{}]	
3011	List size not allowed, requested [{}], maximum [{}]	
3012	List sort by hierarchy path not allowed	
3013	Function not implemented	
3014	Attribute field name required	
3015	Hierarchy path [{}] not found.	
3016	Model type list [{}] not found.	
3017	Bulk update failed, error [{}].	
3018	Bulk operation {} failed, error [{}].	
3019	Schemas of data being imported have cyclic foreign keys {}.	
3999	Unhandled API Error	

Resource Error Code	Message	HTTP Code
4000	Error, Cannot delete Resource while children exist {}	
4001	Error, Duplicate Resource Found. {}	
4002	Resource Not Found {}	404
4003	Failed to save {}. {}	
4004	Failed to save {}. {}	

Resource Error Code	Message	HTTP Code
4005	Model Type cannot be None when adding a new Resource	
4006	Resource Parent {} not found	
4007	Resource Meta structure corrupt for {}	
4008	Cannot create a Resource without a Parent Hierarchy	
4009	Failed to save {}. {}	
4010	Cannot find Resource relation {}	
4011	Cannot find target device for model type {} in current hierarchy context	
4012	Cannot find summary attr [{}] in schema root	
4013	Cannot perform operation, model {} already has one or more instances	
4014	Cannot perform operation, resource is part of domain model {}	
4015	Resource Meta structure corrupt. {}	
4016	Badly-formed schema; properties missing for data type object	
4017	Cannot perform operation, model {} is already referenced by one or more resources: {}	
4018	Failed to execute {}. {}	
4019	One or more errors occurred during import	
4020	Transaction resource failed with errors {}	
4021	Resources are not of the same type	
4022	Model type for Resources not found	
4023	Cannot move Hierarchy Node {} to {}	
4024	Resource move failed with error {}	400
4025	Invalid business key {}, expected {}	
4026	Cascade delete failed with error {}	400
4999	Unhandled Resource Error	

Model Error Code	Message	HTTP Code
5000	[{}] Child model exists; ({})	
5001	[{}] Model already exists; ({})	
5002	[{}] One or more data sync errors occurred; ({})	
5003	[{}] The helper cannot instantiate a model it does not recognize; ({})	
5004	[{}] A model instance was expected and not found; ({})	404
5005	[{}] A single model instance was expected but more than one was found; ({})	404
5006	[{}] Attempt to modify a read-only model failed; ({})	
5007	[{}] Attempt to modify a read-only model field failed; ({})	
5008	[{}] Data does not conform to schema; {}	
5009	[{}] Badly-formed schema; ({})	
5010	[{}] Error manipulating schema; ({})	
5011	[{}] Error generating schema; ({})	
5008	[{}] Invalid foreign key to {} for business keys {}	
5017	[{}] Operation not supported; ({})	405
5018	Unable to determine workflow for operation {}	
5019	Workflow {} not found	
5020	Workflow operation {} clashes with an existing model attribute/method	
5021	Unable to execute provisioning workflow for {}, error {}	
5022	Unable to compile data for provisioning workflow for {}, error {}	
5022	[{}] Authentication error; ({})	401
5023	[{}] Connection timeout error after ({}) seconds	
5024	[{}] Connection error; ({})	
5998	{1}	
5999	[{}] Unexpected error; ({})	

Macro Error Code	Message	HTTP Code
6000	Template must be a dictionary - got {}	
6001	No hierarchy supplied	
6002	Invalid macro specified: {}	
6003	Macro lookup of {} failed at hierarchy {}	
6004	Macro lookup of {} returned multiple values {} at hierarchy {}	
6005	Macro lookup of {} failed when fetching from {} at hierarchy {}	
6006	Macro lookup failed for field {} in context {}	
6007	Macro lookup failed for field {} in context {}, type str or int expected not type dict {}	
6008	Macro function {} not found	
6009	Macro function arguments error - {}	
6010	Macro function error - {}	
6011	Unexpected business key format - {}	
6999	Error,	

Workflow Error Code	Message	HTTP Code
7000	Workflow not found	
7001	Maximum workflow recursion depth exceeded	
7002	Invalid workflow script identifier {}	
7003	Specified workflow script name {} not found	
7004	Error looking up workflow script names against API	
7005	Invalid workflow action	
7006	Workflow {} at step {} failed. {}	

Workflow Error Code	Message	HTTP Code
7007	Advanced Find Options invalid - Resource not found with options {}	
7008	{}	
7999	Error,	

Script Error Code	Message	HTTP Code
8000	Script not found	
8002	Syntax error on line {}	
8003	Could not connect to {}	
8004	Authentication failed {}	
8999	Error,	

Schema Error Code	Message	HTTP Code
9000	Unhandled schema property error: [{}]	
9999	Error,	

Bulk Loader Error Code	Message	HTTP Code
10000	File Upload Error for File Name : ({})	
10001	General Error; ({})	
10002	Data does not conform to schema; ({})	

Data Import Error Code	Message	HTTP Code
11000	Multiple json files {} found in zip archive root; only 1 expected	
11999	Error,	

Test Connection Error Code	Message	HTTP Code
12000	Please specify the model type of the device connection parameters	
12999	Error,	

Cascade Delete Error Code	Message	HTTP Code
13000	Hierarchy path or pkid required	
13001	Could not delete {} out of {} resources.	
13999	Error,	

Cisco Unified Communications Domain Manager 10.6(1) Version Information

To find detailed information about your version of Cisco Unified Communications Domain Manager 10.6(1):

1. Login as hcsadmin administrator.
2. Select **About** > **Extended Version**.
3. Click the HcsBase version.

   The following information is displayed:

Field	Description
Name	Always HcsBase
Release	The Cisco Unified Communications Domain Manager release
Version	The version of the template file
Previous Version	The previous version of the template file, if the template has been upgraded or reinstalled
Build Number	Cisco's build number associated with this load
Branch	Development branch
View	Development view
Build Time	Build Time associated with this load
Author	Always Cisco HCS Base

Field	Description
Deployment Mode	HCM Standard
Platform Version	Matches the installed OVA file version or the version of the latest Cisco Unified Communications Domain Manager 10.6(1) upgrade ISO file. The platform version is not displayed if an HCM-F device has not been configured in Cisco Unified Communications Domain Manager 10.6(1).

4 To export the detailed version information, select **Action** > **Export**.

Single Sign On (SSO)

The following list provides troubleshooting solutions to common SSO problems:

- Browser error: This may occur when moving a user to a sub-directory.
- Logout error: This may occue when your Identity Provider asks the system to do a global logout, but your federated session is lost. Even if your local session in this system has been closed, you may have open sessions in other systems. In order to protect your personal information, close your browser window or remove cookies from your browser.
- An error may occur when attempting to log out while another browser window is still logged into OpenAM. The following error message appears:

```
{ message: "An internal system error occurred.",
code: -1,
http_code: 400,
traceback: "Traceback (most recent call last):
File "/opt/voss-deviceapi/eggs/Django-1
.4.5-py2.7.egg/django/core/handlers/base.py", line 111,
...
```

- Access Rights Violated - Permission Denied: When attempting an SSO log-in (if already logged into the IDP), you are re-directed to http://voss2product.visionoss.int/sso/acs/ with a "Permission denied" error. The heading in the browser tab shows **Access rights violated**.
- Incorrect URL for ACS in the IDP leads to HTTP 301 and HTTP 405

  If the assertion consumer service in the IDP's SP attributes is set incorrectly, the SAML trace is expected to provide a HTTP 301 and then a HTTP 405 error.

  The example trace illustrates that the URL in the IDP was set to:

  http://nyasha.visionoss.int/sso/acs

  and it was set to:

  http://nyasha.visionoss.int/sso/acs/

  The difference between the two items is shown below:

```
Request URL:http://nyasha.visionoss.int/sso/acs
Request Method:POST
Status Code:301 MOVED PERMANENTLY
...
Response Headers view source
Connection:keep-alive
Content-Language:en-us
Content-Type:text/html; charset=utf-8
```

```
Date:Mon, 21 Oct 2013 14:35:00 GMT
Location:http://nyasha.visionoss.int/sso/acs/
Server:nginx/1.2.1
Transfer-Encoding:chunked
Vary:Accept-Language
Request URL:http://nyasha.visionoss.int/sso/acs/
Request Method:GET
Status Code:405 METHOD NOT ALLOWED
Request Headersview source
```

Troubleshooting Self-Provisioning

Getting Started

Always start by inspecting transactions and user management logs:

- Check Transactions: **Administration Tools** > **Transactions**
- Check User Management logs: **User Management** > **Log Messages**
- Check configurations

When Cisco Unified Communications Domain Manager is using LDAP for user management and new users synced with LDAP are not pushed to Cisco Unified Communications Manager confirm **Auto Push Users** is checked in **Site Management->Sites**.

When users are pushed to the call manager with an incorrect Primary Extension and Self Service ID check that the **Line Mask** is correct under **User Management->Self Provisioning->Line Mask**. Line Mask should exist for each site.

Troubleshooting Specific Failures

Line is not created

- Ensure that Directory Number Inventory exists and that the number is not in use already
- If the line mask is applicable, check the following
    - Ensure that the ULT has a site-specific partition
    - Ensure that the Line Mask is configured
    - Ensure that the User Profile is configured and set in the Site Defaults
    - Ensure that the user's attribute value is valid and that the mask is applicable
- For setting the Self-Service Id, check the following - Ensure Site Defaults default line partition is set - Check Quick Add Group configuration

Users are not in correct sites

Check that filters for each site exist in **Manage Filters** under **User Management**.

Users are not getting correct User Profile

Check that the correct User Profile is populated under Default User Profile in **Site Management -> Defaults**.

Quick Add subscriber not getting correct User Profile in Cisco Unified Communications Call Manager

Check that the correct Quick Add Group is selected for **Quick Add Subscriber**. If correct Quick Add Group is selected, open the **Quick Add Subscriber Group** and check that the correct template is selected for Default Cisco Unified Communications Manager User Template

Troubleshooting User Access

Credential Policies Rate Limiting

Cisco Unified Communications Domain Manager 10.6(1) makes use of two types of failed login attempt rate limiting. These make use of a token bucket algorithm.

- Per-user rate limiting
- Per-source rate limiting

Failed Login Attempt Per-user Rate Limiting

Per-user failed login attempt rate limiting works as follows:

- One token is added to the username-specific bucket at the interval specified in Reset failed Login Count per User (minutes).
- The bucket can hold at most the number of tokens as specified in Failed Login Count per User. If the token added when the bucket is full it is discarded.
- When a login attempt is made with an incorrect password, one token is removed form the bucket. When the last token is removed from the bucket, the rate limiting threshold is reached and the user account is locked for the number of minutes specified in Lock Duration (minutes).
- Rate limiting is done for both existing and non-existent system users.
- When an existing user account is locked, a transaction is triggered by the system user. Example detail: Password retry limit reached. Locking account with username "customer".
- When an account is locked, subsequent login requests (regardless of whether the password is correct or not) via the GUI will receive the following message: "Too many failed login attempts for this user account. Try again later."
- A locked account is automatically unlocked on the first login request after the number of minutes specified in Lock Duration (minutes) has lapsed. Account unlocking triggers a transaction as the "system" user. Example detail: Automatic account lockout duration lapsed. Unlocking account with username "customer".
- Per-user rate limiting can be disabled by checking the Disable Failed Login Limiting per User checkbox.

Failed Login Attempt Per-source Rate Limiting

Per-source rate limiting process is similar to the per-user variant and works as follows:

- One token is added to the source-specific bucket at the interval specified in Reset Failed Login Count per User (minutes).

- The bucket can hold at most the number of tokens as specified in Failed Login Count per Source. If a token is added when the bucket is full, it is discarded.
- When a login attempt is made with an incorrect password, one token is removed from the bucket. When the last token is removed from the bucket, the rate limiting threshold is reached and subsequent login requests from the source IP address are locked out for the number of minutes specified in Lock Duration (minutes).
- No transactions are triggered when per-source rate limits triggered, since there is no associated resource.
- When a source IP address is locked out, subsequent login requests (regardless of whether the password is correct or not) from the given IP address via the GUI will receive the following message: "Too many failed login attempts from the computer. Try again later."
- A locked out source IP address is automatically unlocked on the first login request after the number of minutes specified in Lock Duration (minutes) has lapsed.
- Per-source rate limiting can be disabled by checking Disable Failed Login Limiting per Source checkbox.

Manage Your Own Account Password

Logged in users or administrators can manage their own account passwords.

Note Users who are configured for Single Sign On or through LDAP do not manage their account passwords in Cisco Unified Communications Domain Manager 10.6(1).

Change Password

To change your own password when you are logged in to Cisco Unified Communications Domain Manager 10.6(1).

Reset My Password

To reset your password from the Login page when you have forgotten your password.

Password Reset Questions

To configure your own password reset questions.

Change Your Own Password

Follow this procedure to change your own password if required:

1. Log in to Cisco Unified Communications Domain Manager 10.6(1) .
2. Click the arrow next to the logged in user at the top right-hand side of the screen.
3. Choose the Change Password option from the drop-down menu. The Change Password screen is displayed.
4. Enter your existing password in the Old Password field.
5. Enter your new password in the New Password field.
6. Confirm your new password by re-entering it in the Repeat New Password field.

7 Click **Change Password** in the button bar. Your password is changed.

Reset Your Own Password

You can reset your password only if you have already provided answers to the security questions created by your administrator.

If you forget your password while attempting to log in to Cisco Unified Communications Domain Manager 10.6(1):

1 Enter your username in the Username field on the Log in screen.

2 Click the **Forgot Password?** hyperlink located below the Log in button.

3 Enter your username again.

4 Click **Reset my password**.

5 Click in each security question field and type the correct answer.

6 Click in the **New Password** field and type your new password.

7 Click in the **Repeat Password** field and re-type your new password.

8 Click **Reset my Password**. Your password is changed.

9 Click the **Login** hyperlink if you want to attempt to log in again.

Configure Your Own Password Reset Questions

Note Configuring your own password reset questions is available only if the credential policy applied to your user account has **Number of Questions Asked During Password Reset** set to > 0.

1 Log in to Cisco Unified Communications Domain Manager 10.6(1).

2 Click the arrow next to the logged in user at the top right-hand side of the screen.

3 Choose the **Password Reset Questions** option from the drop-down menu. The Password Reset Questions screen is displayed.

4 Type your password in the **Current Password*** field.

5 Choose the required security question from the **Question*** drop-down list.

6 Enter your answer to the above question in the **Answer*** field.

7 Repeat steps 5 and 6 until you have configured the required amount of security questions (as determined by your administrator).

8 Click the **Update Security Questions** button in the button bar when complete. Your security questions and answers are updated.