Contents

1.0 Introduction

For an enterprise that requires full PCI and or FIPS compliance, the KCCVoIP Asterisk Cluster Manager is available {HTTPS access, account logging, OSSEC integration, encryption, fallback and high-availability control etc..} designed to run as an customised enterprise free-standing system running on a pair of high-availability servers {Linux CentOS 6.9} within an Asterisk cluster. Sites that do not have the FIPS restrictions of single-function per server (or PCI 3.2 'separate server for different security levels') can implement the Asterisk Cluster Manager as the CMS to run on a high-availability pair of Asterisk servers provided it is sized correctly to ensure it does not overload any Asterisk functionality.

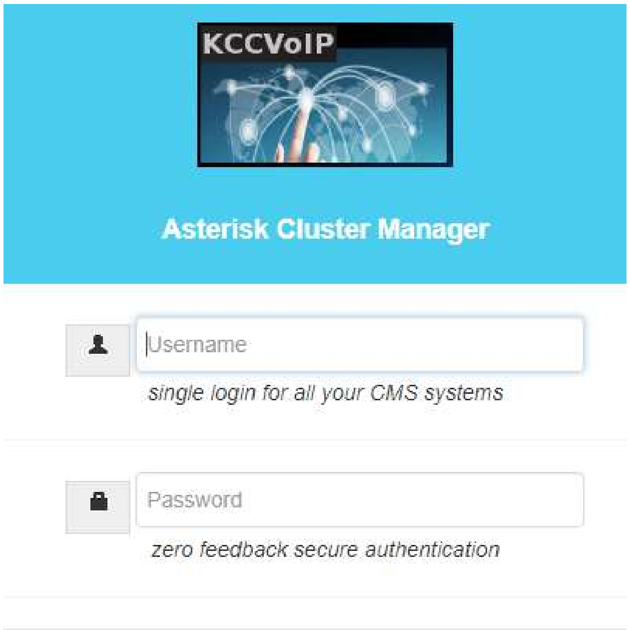
Full enterprise features for FIPS compliance ;

- Single function per server if required for FIPS compliance
- Cluster high availability with VIP failover
- High availability failover for TSP connectivity
- Load balancing on multi-server clusters
- Single central management of Asterisk configuration {central topology only}
- Single central reporting for Asterisk enterprise {central topology only}
- Full integration with OSSEC/SIEM
- Fallback configuration for isolated site operation
- Full redundancy of configurations, mysql databases, CDR reporting and monitoring
- Single login for different levels of users/helpdesk/NOC {central topology only}

The topology can be implemented **as an enterprise-wide system with central topology** allowing configuration, reporting and status for any element within the voice enterprise on a central CMS platform. Alternatively, the deployment can be **site/distributed** so that each site within the enterprise can manage the local clusters and all site voice elements from the main cluster within a site. Remote support can login to any distributed site cluster to manage each site cluster configuration and view the status. **IMPORTANT NOTE – THIS IS NOT AN OFF-THE-SHELF APPLICATION AND REQUIRES CUSTOMISATION TO MATCH THE REQUIREMENTS OF EACH SITE**

If implementing the distributed topology so that each site can be managed independently. Database replication will be confided to site level within the site cluster(s). This allows for a separate support team and policy for each site within the enterprise, but also allows central or remote support to access any of the site CMS platforms.

1.0.1 LOGIN AND GET STARTED

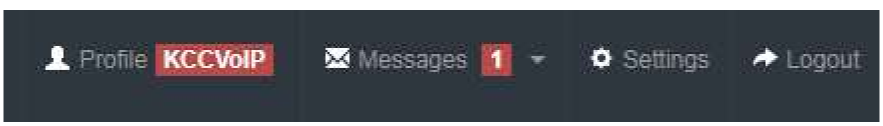


HTTPS SSL single login for all of the Asterisk Cluster Manager, reporting and CMS applications within the enterprise domain {central topology only}

When the password is entered correctly login begins - there is no feedback if the password is entered incorrectly or not recognised.

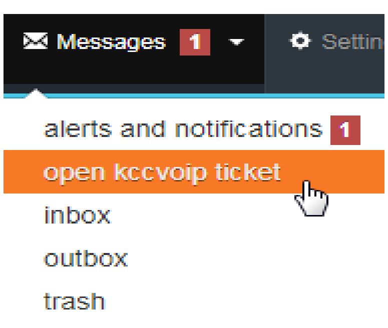
For example https://ast1.enterprise.net

NOTE – Sites that do not have a 'standard' corporate ip domain naming scheme - it is not possible to have SSL single sign-on when there are different domains assigned to each site and no overall corporate domain. Accedo do not have a standard single corporate domain naming scheme.



The profile will show your user group name - in this example KCCVoIP {mouse over will show login ID}

The messages tab allows you to access your open tickets, customization requests and other alerts for your login associated with the enterprise accounts and licenses.

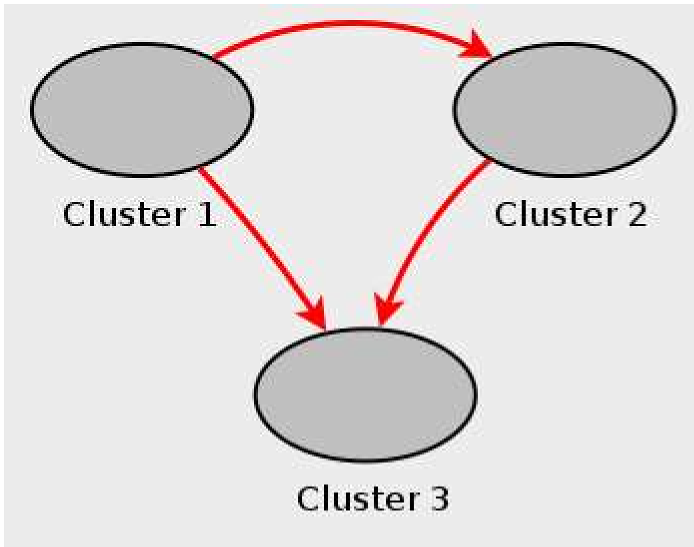


NOTE - Evaluation licenses have a 30 day lifetime. Full licenses can be 30 days or 12 months.

Software updates, customization, support and ticketing are available from the top line 'messages' tab on full licensed version of the software.

Depending upon your account profile, the settings tab allows change of the configuration for the cluster manager and database replication.

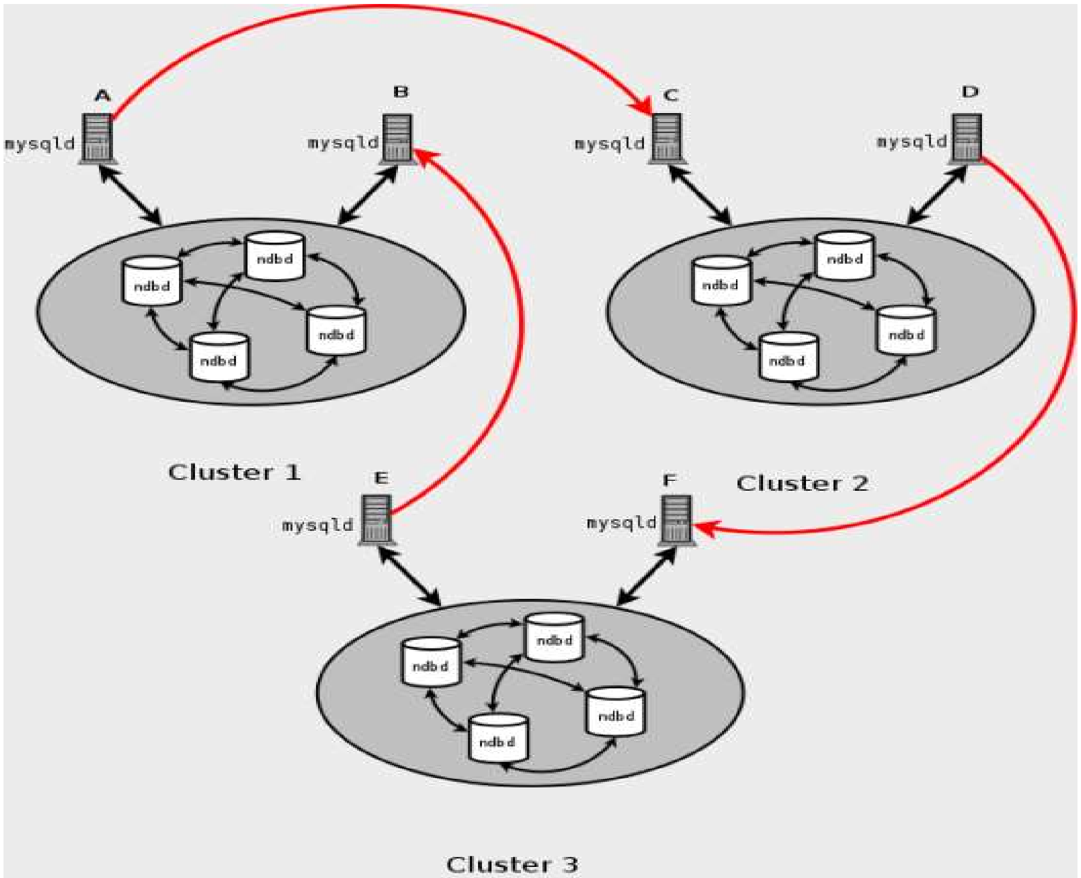
The central database is kept synchronised to all of the databases on the clusters through-out the enterprise and is configurable in master/master, master/slave and circular high resilience modes;



During any inter-site communications outages the clusters offer full application support within the isolated site. Each cluster can operate in isolation and still maintain the Asterisk services for the site.

For single site implementation, the servers within the site cluster(s) maintain the database within the that site and do not replicate through-out the enterprise. Management, configuration and reporting etc. are maintained at the site-level.

Central topology - In more detail – the MySQL database can be maintained in a circular configuration ;



Each Asterisk server runs the AMI-Poller to maintain a local database of the status and configuration of the local Asterisk servers within the local cluster. In turn the site cluster forwards the database changes to the next in line to maintain the enterprise database so all clusters are synchronized.

If communications should fail and a cluster becomes isolated, it uses the local configuration and database to maintain voice services for the local systems. When communications returns an update will be sent to synchronize the enterprise databases again.

Clusters in high availability topologies maintain local synchronized database and Asterisk configuration within the local cluster in addition to the enterprise connectivity.

Voice services VIPs provide Asterisk voice services for the local site and either load balance or failover based upon the polling within sip-ha for the cluster.

The MySQL topology for this enterprise - details in here

```
      KCCVoIP High Availability Routines for Asterisk
      ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

 -v verify information:

 This server is MASTER  in  active/standby HA pair
master server is : 192.168.0.216 service primary
slave server is  : 192.168.0.215 service secondary
local interface  : eth0  physical
timestamp        : 01/17/2018-10:09:32

VIP service address #1 : 192.168.0.218 controlled by kccvoip SIP-HA

 Source IP 192.168.0.216 reachable
 Replication IP 192.168.0.215 reachable
 Active services 192.168.0.218 reachable
 IPS/TALKTALK SIP Trunk interface 172.20.15.1  available
 BT SIP Trunk NOT configured - NOT available

Privilege escalation protection disabled!
See https://wiki.asterisk.org/wiki/x/1gKfAQ for more details.
 ACTIVE SERVICES ON THIS SERVER - This server is MASTER  in  active/standby HA pair
    - NOW IN NORMAL STATE -


 SIP-HA will replicate local files to 192.168.0.215
```

In the above example SIP-HA is maintaining the VIP for a pair of servers and controlling the voice service VIP on 192.168.0.218 for the local cluster. It is also maintaining the TSP SIP trunk using 172.20.15.1.

The configured files for replication will be sent from 192.168.0.216 to 192.168.0.215 to maintain synchronization.

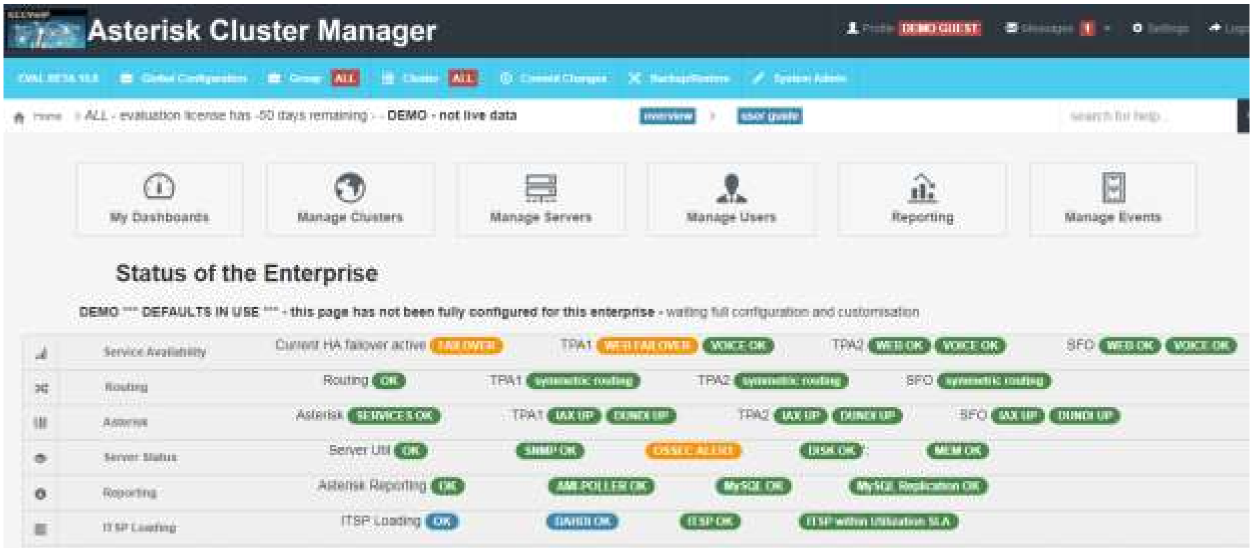
During a failure on the primary server of this pair, 192.168.0.215 secondary server would become the primary for all services and the VIP 192.168.0.218 would be taken over.

Local softphones, tablets, smart phones and telephones configured for DNS SRV would continue to use the primary service. If the primary and secondary become unavailable, they would then change their connectivity to the next server/cluster handed out in the DNS SRV list.

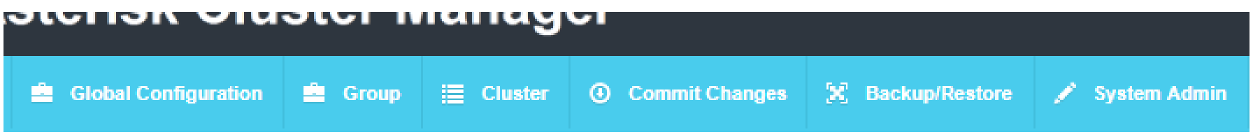
It is vital for the enterprise technical support and technical operations managers to understand the database synchronization, HA failover, SRV failover and traffic flow. The damage is obvious if the replication is incorrectly configured.

2.0 Home Menu Page

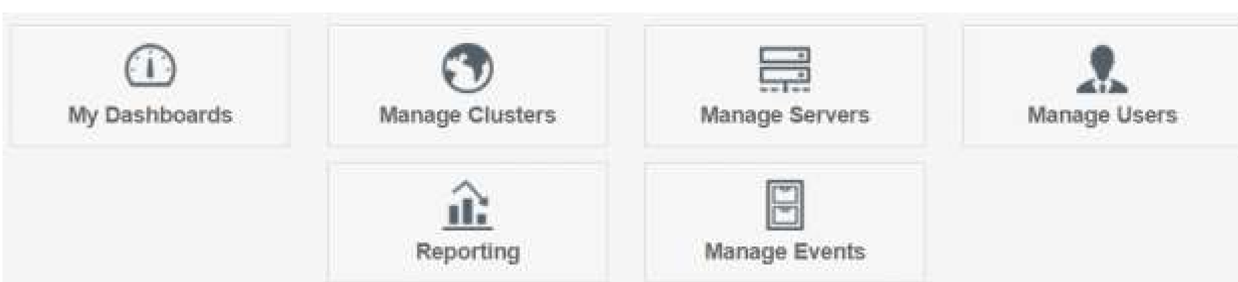
The HOME page is customised to the enterprise and shows the status at a glance. Each status item can be selected for more detailed information.



The main menu functions are found on the blue header tab selection bar which is available as the header from most of the cluster manager pages. These menu selections will change depending upon your profile account.



The HOME menu will also have large icons customised to your requirements to allow direct link to reporting, dashboards/wallboards, user and agent manager screens, voice recording manager etc..



All icons are customised to the individual account profile and enterprise site requirements.

The main menu page shows the enterprise status at a glace

The main index page is customized to show the status from all of the vital components

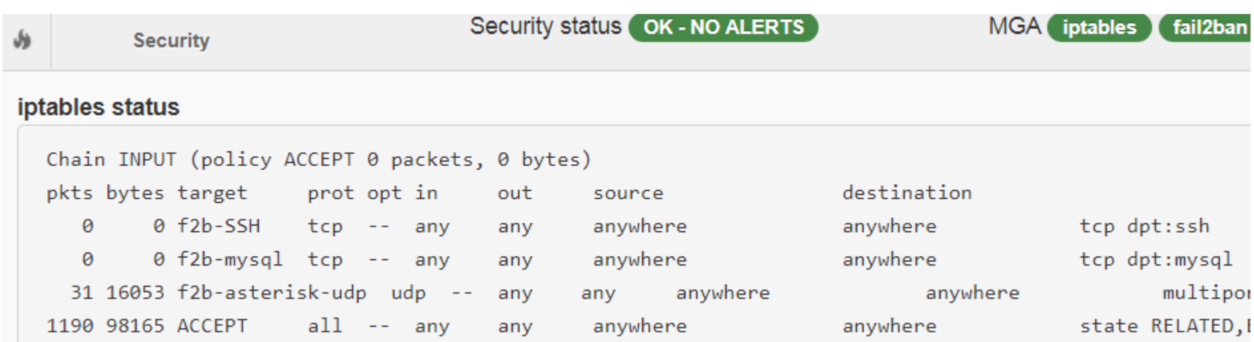
2.0.1 Service Availability

This example shows the current status from each of the clusters with their VIP, primary and secondary server interface address etc. at a glance you can see if the status is green there are no detected problems. If the icons are orange, there is a failover status detected

waiting - enterprise service addressing in here

2.0.2 Security

The quick glance icons show the current status of iptables, fail2ban, OSSEC, any SBC systems and blacklist blocking running on all of the clusters in the enterprise.



In this example - notice iptables and fail2ban icons are green and in the pulldown detail you can see fail2ban is running on three f2b targets {ssh, mysql and SIP}

```
Chain f2b-SSH (1 references)
 pkts bytes target     prot opt in
    0     0 RETURN     all  --  any

Chain f2b-asterisk-udp (1 references)
 pkts bytes target     prot opt in
   76 39543 RETURN     all  --  any

Chain f2b-mysql (1 references)
 pkts bytes target     prot opt in
    0     0 RETURN     all  --  any
```

You can also see that the f2b targets have no current banned addresses

In this example you can see f2b-asterisk has banned addressing as it has a history count of 76 packets

This tab can also show the details of access attempts and errors logged by security ;

```
Apr 18 11:10:17 ast16 sshd[4802]: Accepted password for root from 192.168.0.170 port 3458 ssh2

Apr 18 11:10:17 ast16 sshd[4802]: pam_unix(sshd:session): session opened for user root by (uid=0)
```

The original helpdesk scripts are still available if required for cli checks and routine maintenance if/when required - such as ' aststat ' to check the fail2ban ignore tables etc..

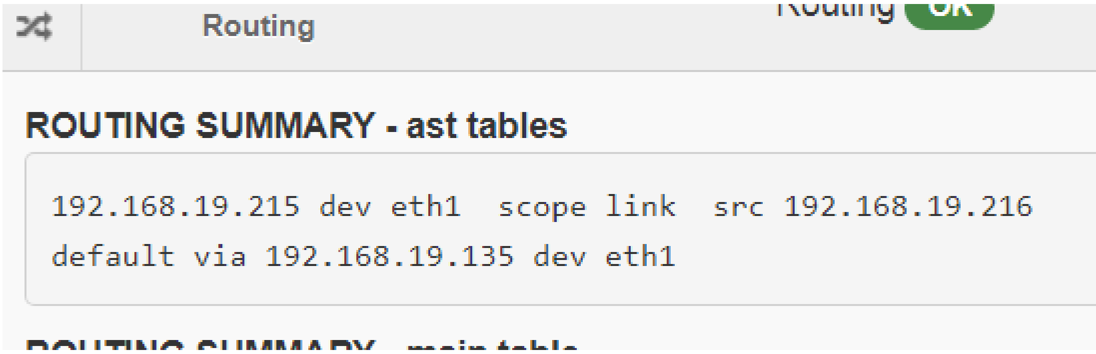
On the SBC clusters running Kamailio or Asterisk, ip blacklists are automatically kept up to date and can also be monitored ;

```
Chain BLACKLIST-INPUT (1 references)
 pkts bytes target     prot opt in     out     source               destination
   86 44326 DROP       all  --  *      *       0.0.0.0/8            0.0.0.0/0
    1    52 DROP       all  --  *      *       14.134.3.4           0.0.0.0/0
    1    52 DROP       all  --  *      *       205.209.159.19       0.0.0.0/0

Chain f2b-dropbear (1 references)
```

2.0.3 Routing

To maintain the symmetrical routing for multiple interfaces, Linux multiple ip routing tables are used. The status of these can be seen here.

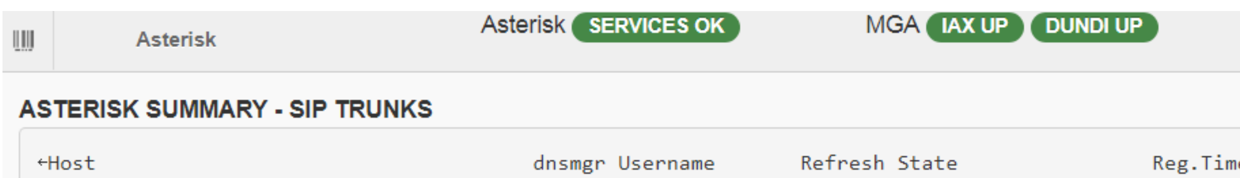


In this example we see that the eth1 interface is configured for symmetrical routing and has gateway on that VLAN addressed 192.168.19.135 and using the VIP 192.168.19.216 as the source address.

If the symmetrical routing should fail, it would no longer be possible for users to reach both voice and web services from a single VLAN. It is important that technical support teams understand why.

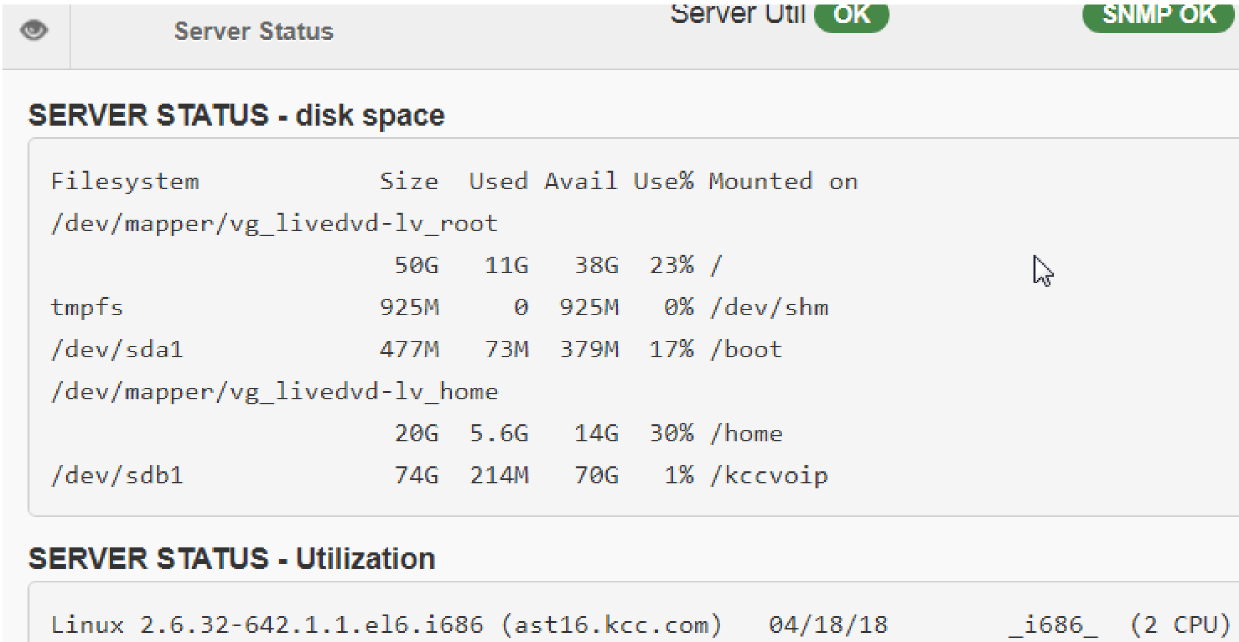
2.0.4 Asterisk

These icons show the high-level view of the current Asterisk processes



This display will show the current SIP trunks registration, IAX trunks and DUNDI peers, DHADI analogue channels and ITSPs at a glance and can be customised to show any important Asterisk status

2.0.5 Server Status



Shows the status from each server for a select set of parameters such as disk space, utilization and memory etc

2.0.6 Reporting

To see at a glance that the reporting is collecting stats, cron is running, AMI-poller is running and the MySQL replication is functioning

2.0.7 TSP & ITSP Status

Customised to each implementation

ITSP UTILIZATION - channels
26 active channels
13 of 160 max active calls (8.14% of capacity)
25348 calls processed

Shows the status for the main ITSP and Telco trunks, inter-site DUNDI status etc

Telnyx ITSP SIP Trunk Utilization

cluster	TNX	USSales	UKSales	EUSales	Development	Utilization	Date
lon	22	2	2	0	17	55 % of 40 channels	06/01/2018 20:24:40
tpa1	9	3	5	7	0	22 % of 40 channels	06/01/2018 20:08:43

there were **31** concurrent calls active on 06/01/2018 20:08:43
which equates to a Telnyx trunk utilization of **77 %**
and requires approx **2914 kbps** on the ISP networks

3.0 CMS Reporting

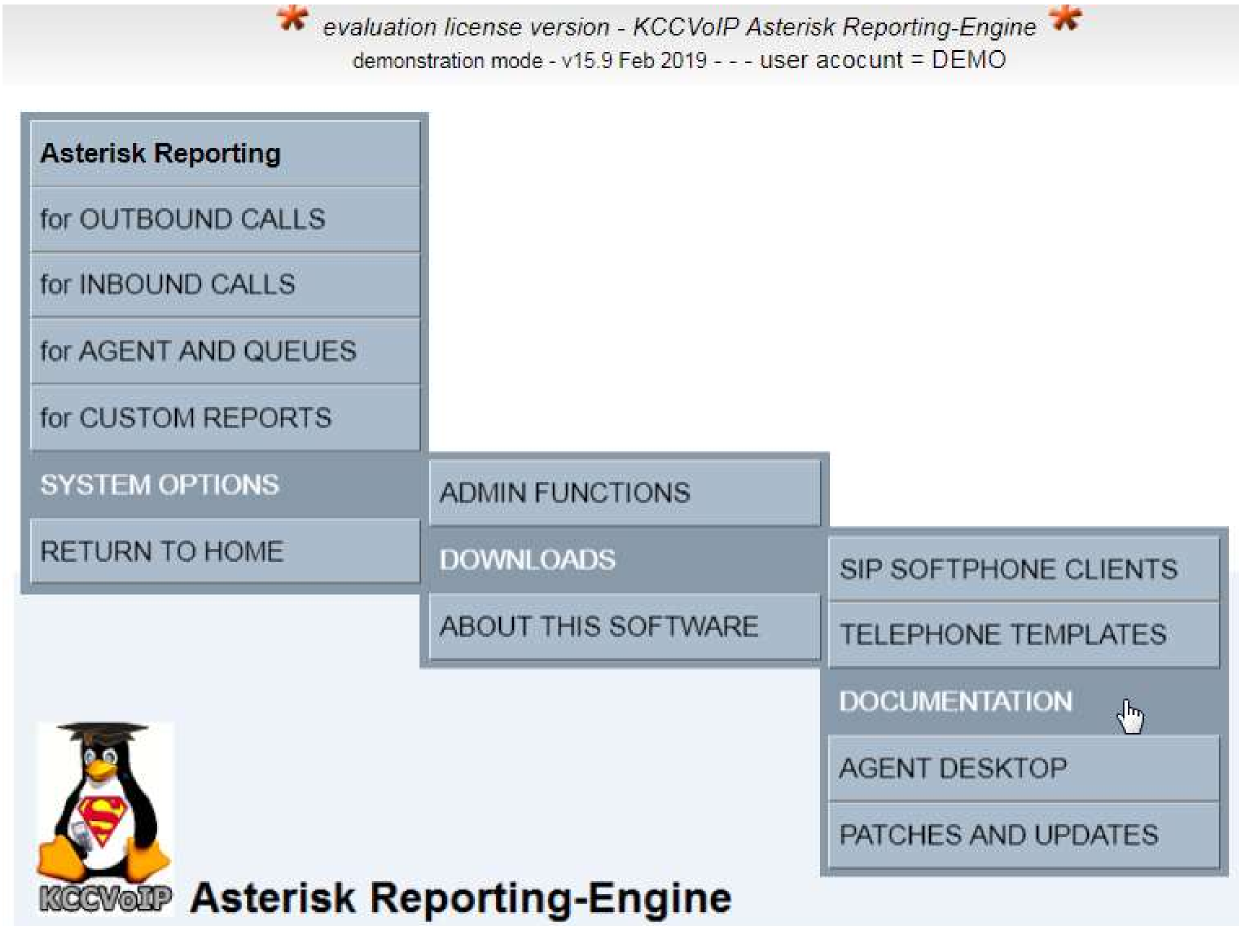
At default the reporting icon will link to the kccvoip CMS Reporting application menu {if installed} if allowed by the account profile ;

Asterisk Reporting
for OUTBOUND CALLS
for INBOUND CALLS
for AGENT AND QUEUES
for CUSTOM REPORTS
SYSTEM OPTIONS
RETURN TO HOME

Depending upon the account profile, this allows the user to reach

- CDR and agent reporting
- custom report generator
- voice recording manager
- original wallboard software
- download area which contains the softphone client software and documentation etc.
- MySQL manager and KCCVoIP MySQL

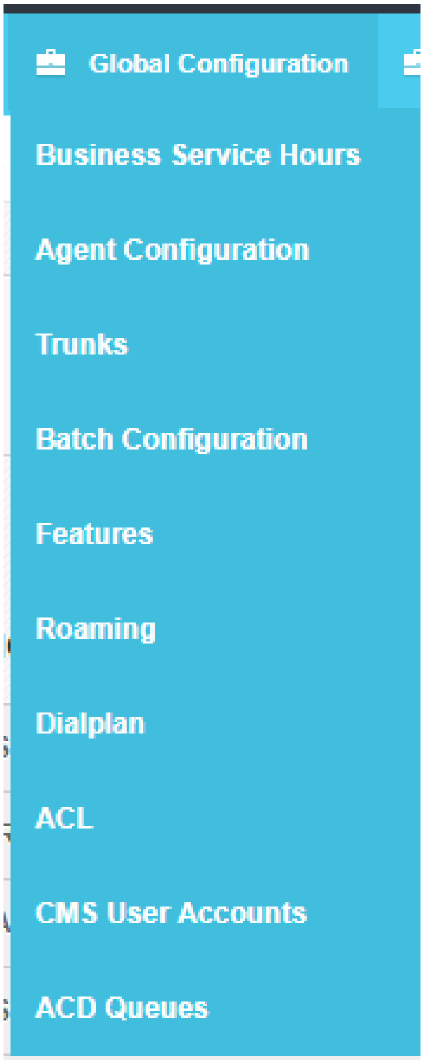
Users can have configured profiles that provide specific rights to their agent groups and/or applications such as wallboards/dashboards, CDR reports and voice recording etc.. From login the user can be sent to the application or link for their profile.



As always, the current documentation can always be found in the 'SYSTEM OPTIONS' – 'DOWNLOADS' – 'DOCUMENTATION' tabs from the reporting menu

custom site notes in here

3.0.1 CMS Global Configuration



Global Configuration tab ;

Business Service Hours (times when calls flow through different IVRs or get routed to group voicemail and/or announcements etc.)

Agent Configuration (CSQ/ACD) {PRIVILEDGED}

Trunks (Telco SIP/IAX trunks) {PRIVILEDGED}

Batch (add large range of extensions and/or users etc from templates, agents groups, copy from extension numbers or upload CSV

Features (call parking, intercom, paging, music on hold, conferencing, video, spy and call control etc.)

Roaming – check the current status and highlight any errors found in the roaming mapping

Dialplan – view and edit call flows {OPTION}

ACL (access lists for internal phones, trunks, users etc)

CMS access accounts and access rights {PRIVILEDGED}

ACD Queues and access rights {PRIVILEDGED}

Depending upon the group and server requirements, some of these functions may not be enabled for your profile account. All can be customised for each account profile.

3.0.2 Business Hours of Service

Each agent group can have allocated within the dialplan a business hours of service routine which sends the inbound callers to the appropriate number or voicemail etc. at certain times of the day, holidays, weekends etc..

Business Hours of Service

<< < Add View Change Copy Delete > >> Go to 1 Page: 1 of 1 Records: 8

v	Site	Cluster	Group	Function	Description	Active	start time	end time	start day	end day	start date	end date	announcement
◉	lon	lon	UKSALES	OPEN	UK hours	yes	08:00:00	18:30:00	mon	fri	*	*	
○	tpa	tpa1	USSales	OPEN	EST hours	yes	13:00:00	22:00:00	mon	fri	*	*	
○	ams	ams	EUSales	CLOSED	force closed	no	00:00:00	00:00:00	mon	sun	*	*	closed
○	tpa	tpa1	USSales	CLOSED	force closed	no	00:00:00	23:59:59	mon	sun	07/04	07/07	closed
○	tpa	tpa1	USSales	HOLIDAY3	Memorial Day	yes	00:00:00	23:59:59	mon		05/25	05/31	closed
○	tpa	tpa1	USSales	CHRISTMAS	2018 Christmas	yes	00:00:00	23:59:59	*		12/25	12/26	merry-christmas
○	tpa	tpa1	USSales	HOLIDAY4	Independance Day	yes	00:00:00	23:59:59	*		07/04		closed
○	tpa	tpa1	USSales	HOLIDAY5	Labour Day	yes	00:00:00	23:59:59	mon		09/01	09/07	closed

3.0.3 Agent Configuration

Allows for changes to each of the agent groups, CTI and CRM integration *{customise to site}*

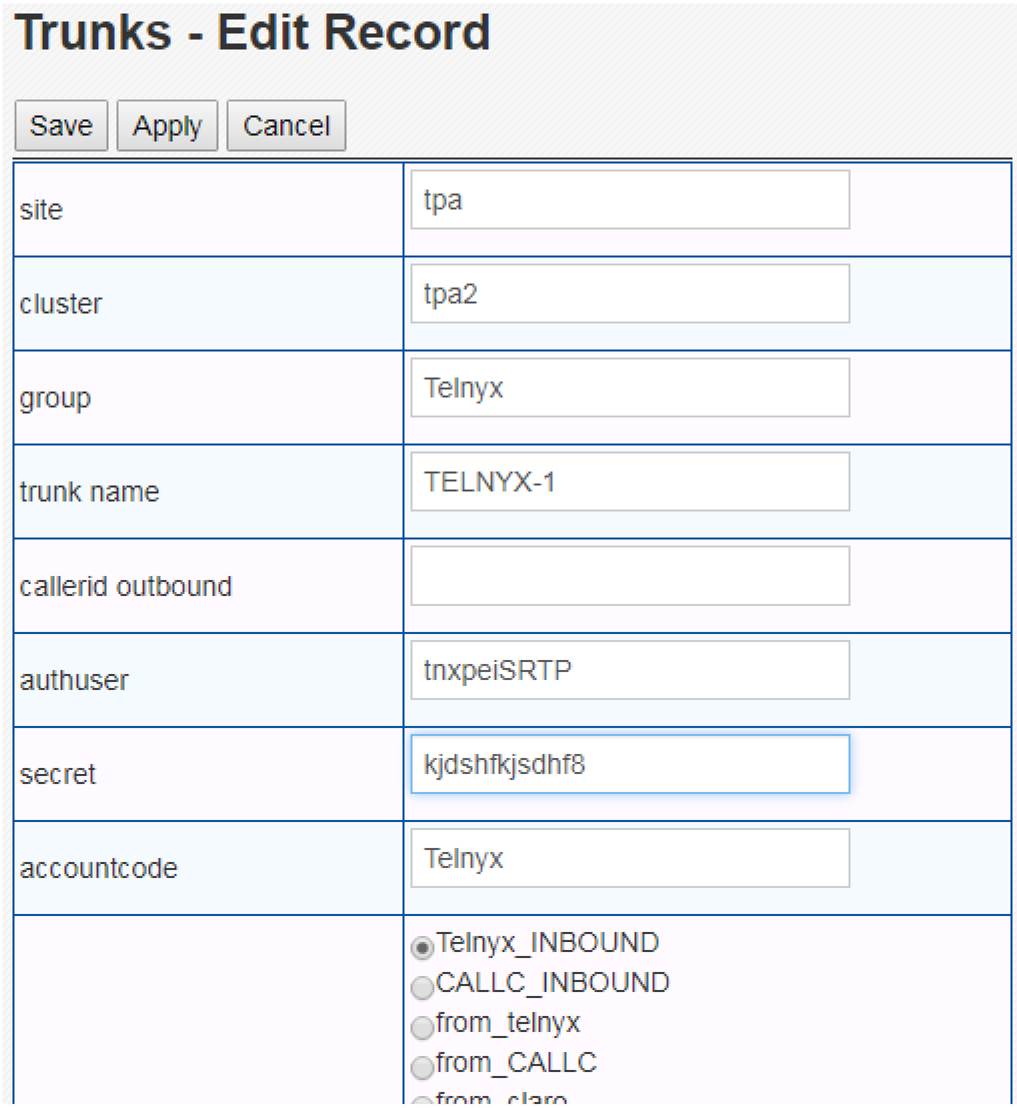
3.0.4 Trunk Configuration

Allows the configuration of new and existing trunks to ITSPs, Telcos and SBCs. Trunks that are associated with agents groups or specific clusters can also be configured from the cluster/group configuration menus.

Trunks

<< < Add View Change Copy Delete > >> Go to 1 Page: 1 of 2 Records: 17

v	site	cluster	group	trunk name
◉	lon	lon	UKSales	SIP-32
○	lon	lon	inter-site	SFO
○	lon	lon	TechSupport	PRI-E1
○	lon	lon	inter-site	AMS
○	lon	lon	inter-site	TPA
○	sfo	sfo	inter-site	LON
○	sfo	sfo	inter-site	AMS
○	sfo	sfo	inter-site	TPA

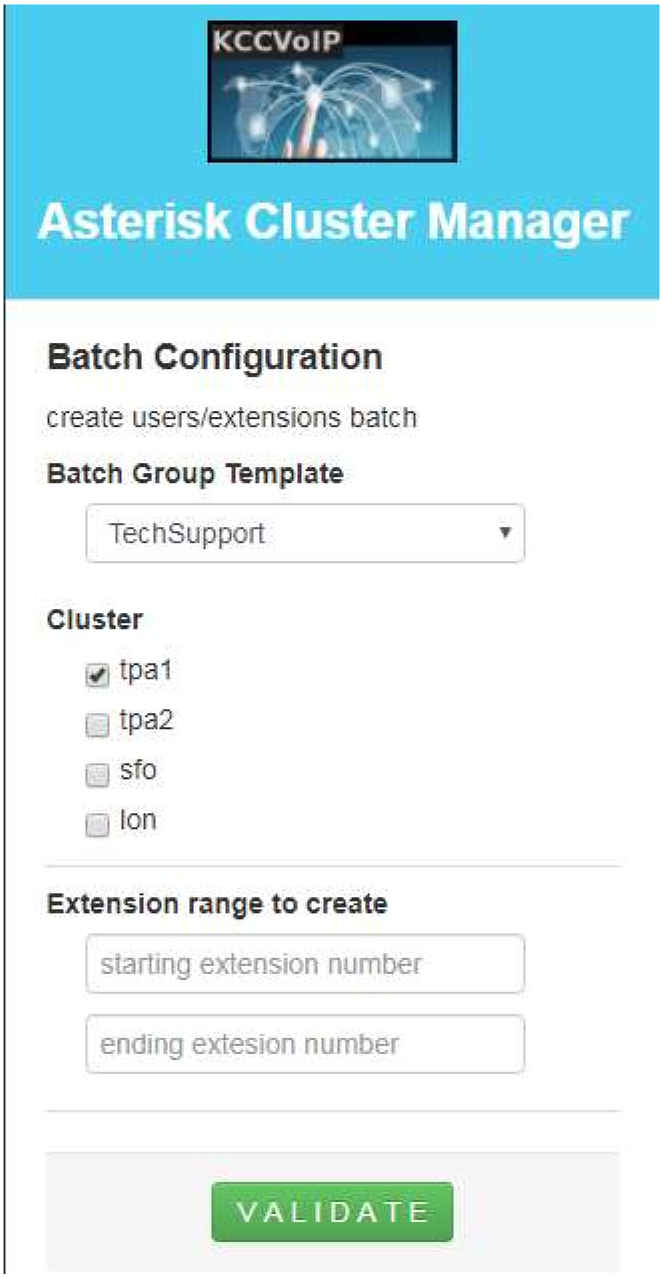

Trunks - Edit Record
Save
Apply
Cancel
site
tpa
cluster
tpa2
group
Telnyx
trunk name
TELNYX-1
callerid outbound
authuser
tnxpeiSRTP
secret
kjdshfkjsdhf8
accountcode
Telnyx
Telnyx_INBOUND
CALLC_INBOUND
from_telnyx
from_CALLC

	KCCVoIP
amaflags	
full contact or description	Telnyx
Telco host	sip.telnyx.com
insecure	
md5secret	
acl	providers
port	
qualify	
protocol	SIP
encryption	yes no
fallback	

Save Apply Cancel

3.0.5 Batch Configuration

One Extension, hotdesk phone or user can be configured from the cluster/group menus at a time. Sometimes it is beneficial to be able to configure a batch of extensions, hotdesks or users in one more efficient method ;



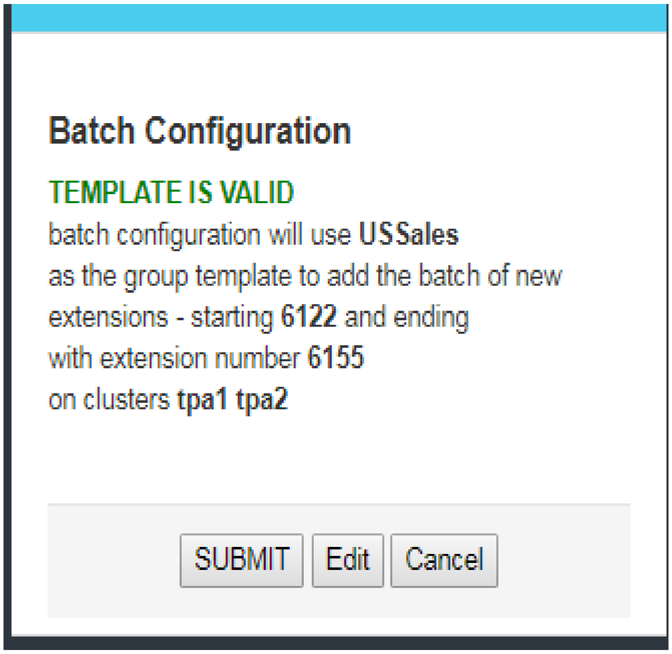
Use the batch configuration to add users, extensions or hotdeskphones to Asterisk.

Select from the pull down list of templates - enables easy addition of users to an existing agent group, extensions as hotdesk phones or use an existing extension as a template to create a batch of similar extensions.

Select the cluster where the new users/extensions are to be created.

Remember if you create the same extension number on different clusters you must consider the dialplan and how call roaming will be affected.

When you have input the range of extensions to be created and clicked the VALIDATE button, the system will check if the new numbers are compatible with the existing dialplan before adding to the database.



In this example we have validated a new range of extensions to be added into the USSales group.

The system will use the USSales group profile to create the new extensions

The validation was successful as the screen shows TEMPLATE IS VALID.

If the extension numbers were not valid for the chosen template, dialplan and cluster, the message INVALID would be seen and the initial form shown for re-entry.

Click SUBMIT to create the new extensions

3.0.6 Roaming

See at a glance which extension numbers are available on multiple clusters/sites and make configuration changes to the roaming dialplan mappings

group	cluster	extension	roam	voicemail	user name
HR	tpa2	5020	dundi	5020	Harold Fisher
HR	sfo	5020	5020 dundi		Harold Fisher Harold Fisher
Development	sfo	5200	dundi	5200	5200
TechSupport	tpa2	5200	5200 dundi	5200 duplicate	Eddie Chissem 5200 - name mismatch
Development	tpa1	5200	5200 dundi	5200 duplicate	5200 Eddie Chissem - name mismatch
IT	sfo	5601	dundi	5601	Robert Midson
IT	lon	5601	5601 dundi		Robert Midson Robert Midson
IT	sfo	5602	dundi	5602	Gordon Lock
IT	lon	5602	5602 dundi		Gordon Lock Gordon Lock
IT	sfo	5603	dundi		Reg Yates
IT	lon	5603	5603 dundi	5603	Reg Yates Reg Yates
IT	sfo	5604	dundi	5604	Jef Morris

In this example we see ;

5020 is configured for roaming and has extension 5020 defined on cluster tpa2 and sfo. The green name icon is showing that it has found no duplicate voicemail or name mismatches.

Extension number 5200 has been configured as a 'standard number' so that the technical support department can be reached locally from any cluster, but allowing the other sites to provide backup if the local number is offline.

USSales	tpa1	6102	dundi	6102	Mike Sydney
USSales	tpa1	6109	dundi	6109	George Lopez
Accounts	sfo	6179	dundi		Anne Stamp
Accounts	ams	6179	6179 dundi	6179	Anne Stamp Anne Stamp

6102 and 6109 are configured for roaming to permit DUNDI to make the extension numbers available directly dialled from any cluster within the enterprise.

6169 has been configured to allow the user to work from either the sfo or ams sites and have the extension number available for direct dialing from any location…. notice the voicemail has been configured only on the home cluster of ams.

Customised site details in here

3.0.6 Access Lists

The access lists used by various extensions, trunks, groups and functions in Asterisk can be edited here

ACL for ALL

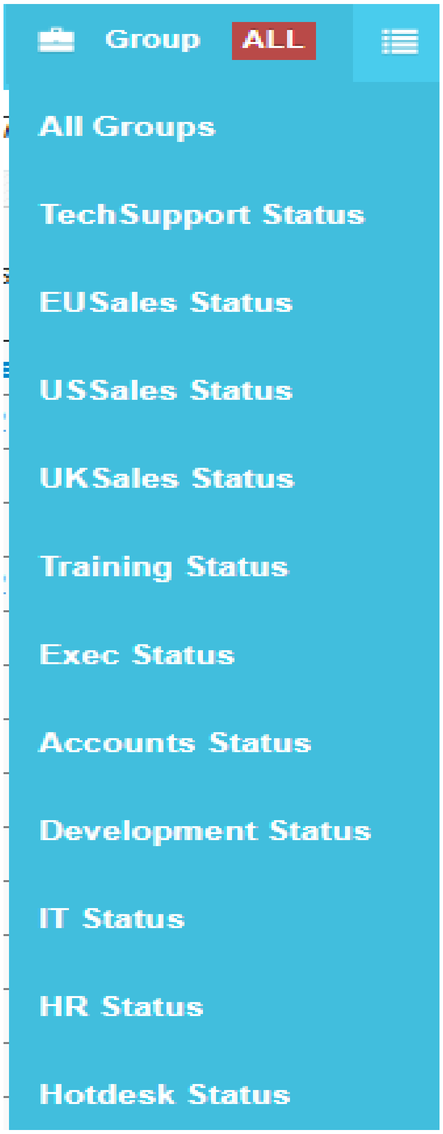
<< < Add View Change Copy Delete > >> Go to 1 Page: 1 of 1 Records: 5

v	ACL name	description	network 1	network 2	network 3
◉	ams_link	ams links	10.10.10.64/255.255.255.252	10.10.20.0/255.255.255.128	
○	internal_phones	ALL internal phone nets allowed	10.10.10.0/255.255.255.0	192.168.68.0/255.255.255.128	192.168.0.0/255.255.255.0
○	SERVICE_PROVIDER				
○	SIP_VPN	VPN SBC access 3	192.168.66.0/255.255.255.128		
○	tpa_link	internal TPA IAX and DUNDI	10.10.10.0/255.255.255.252		

The ACL_name is used by Asterisk to refer to the configured lists. In the first screen only the first three networks are shown, but when viewing or editing you will see many more ;


ACL - Edit Record
Save
Apply
Cancel
ACL name
ams_link
description
ams links
network 1
10.10.10.64/255.255.255.252
network 2
10.10.20.0/255.255.255.128
network 3
network 4
network 5
network 6
network 7

4.0 Group Tab



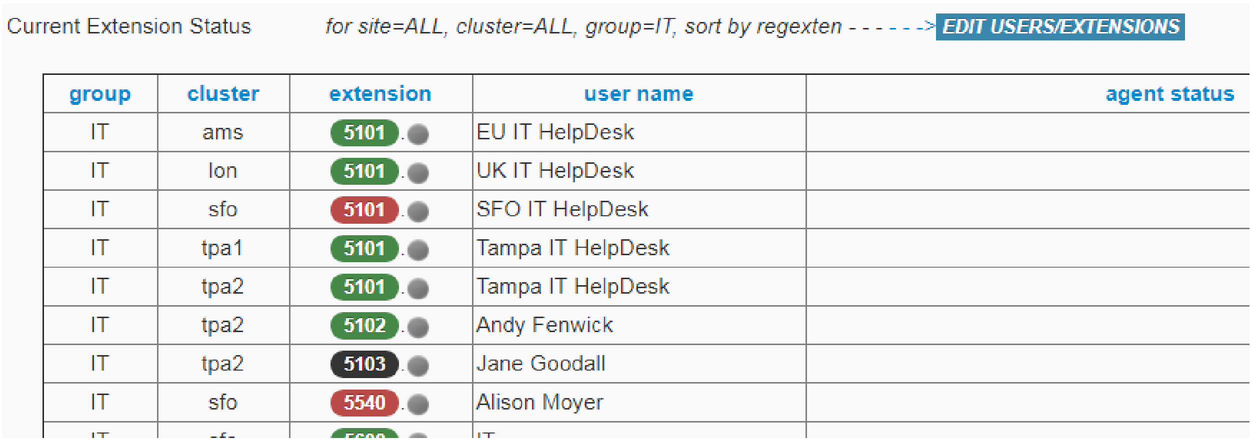
Allows you to select the agent or user group and view the status of that group anywhere in the enterprise

The listed user groups may change depending upon your account profile

These groups are customized for each enterprise to allow quick selection of agent groups, corporate departments or functional groups such as hotdesk, roaming, conference rooms etc…

4.0.1 Group Status and Extension Configuration

The group selected will show in red in the menu display - in the next example the group selected was ‘IT’ as shown in the red IT icon 



Current Extension Status *for site=ALL, cluster=ALL, group=IT, sort by regexten - - - - - ->* **EDIT USERS/EXTENSIONS**

group	cluster	extension	user name	agent status
IT	ams	5101	EU IT HelpDesk	
IT	lon	5101	UK IT HelpDesk	
IT	sfo	5101	SFO IT HelpDesk	
IT	tpa1	5101	Tampa IT HelpDesk	
IT	tpa2	5101	Tampa IT HelpDesk	
IT	tpa2	5102	Andy Fenwick	
IT	tpa2	5103	Jane Goodall	
IT	sfo	5540	Alison Moyer	

notice the selection header also shows **Cluster ALL** which is telling you that you are looking at the status of any member of the IT group on **ALL** clusters within the enterprise if using central topology {within the site only for site/distributed topology deployment} – so you can monitor and maintain user groups that are spread across multiple clusters and multiple sites.

The group selected will show in red in the menu display - in the next example the group selected was 'USSales' **Group USSales**

Current Extension Status *for site=ALL, cluster=ALL, group=USSales, sort by regexten - - - - - ->* **EDIT USERS/EXTENSIONS**

group	cluster	extension	user name	agent status	vm	calls
USSales	tpa2	5709	Daniela Vale	USSales2 static	3	0 / 0 / 0
USSales	tpa2	5710	Juliana Gutierrez	USSales2 static	0	0 / 0 / 0
USSales	tpa1	6101	Leon Johnstone	USSales1 busy on a call	3	13 / 23 /
USSales	tpa1	6102	Mike Sydney	USSales1 logged out	5	0 / 0 / 0
USSales	tpa1	6103	Sally Phillips	USSales1 ringing	1	7 / 3 / 1
USSales	tpa1	6104	Jessie Gonzalez	USSales1 busy TRAINING	0	0 / 0 / 0
USSales	tpa1	6105	Ken Thomas	USSales1 logged in available + 3 ACD calls, last call 2 mins ago	0	7 / 3 / 3
USSales	tpa1	6106	Jim Smith	USSales1 logged out	0	0 / 0 / 0

NOTICE - in this example display shows the extension status for 'USSales' group members on ALL sites, on ALL clusters with the display sorted by extension number;

for site=ALL, cluster=ALL, group=USSales, sort by regexten

The Agent status coulomb will show the current agent status {on a call, available, lunch, break, meeting, logged-out, admin etc..} it can also show ACD call counters if required.

4.0.2 Sort and Search

To change the sort order you can click on any of the blue headings - In this example we have re-sorted based upon user name ;

Current Extension Status for site=ALL, cluster=ALL, group=USSales, sort by name - - - - - > EDIT USERS/EXTENSIONS

group	cluster	extension	user name	agent status	
USSales	tpa2	5709	Daniela Vale	USSales2	static
USSales	tpa1	6109	George Lopez	USSales1	logged in ADMIN
USSales	tpa1	6108	Gerrit Rosbeek	USSales1	logged out
USSales	tpa1	6104	Jessie Gonzalez	USSales1	busy TRAINING
USSales	tpa1	6106	Jim Smith	USSales1	logged out
USSales	tpa1	6107	Jo Clayden	USSales1	logged out
USSales	tpa2	5710	Juliana Gutierrez	USSales2	static
USSales	tpa1	6105	Ken Thomas	USSales1	logged in available + 3 ACD calls, last call 2 mins ago

To edit, copy, delete, view in detail you can click the > **EDIT USERS/EXTENSIONS** at the top of the displayed table.

Users and Extensions

<< < Add View Change Copy Delete > >> Go to 1 Page: 1 of 1 Records: 12

v	site	cluster	group	name	extension	vm box
	tpa	tpa2	USSales	Daniela Vale	5709	5709
	tpa	tpa2	USSales	Juliana Gutierrez	5710	5710
	tpa	tpa1	USSales	Leon Johnstone	6101	6101
	tpa	tpa1	USSales	Mike Sydney	6102	6102
	tpa	tpa1	USSales	Sally Phillips	6103	6103
	tpa	tpa1	USSales	Jessie Gonzalez	6104	6104
	tpa	tpa1	USSales	Ken Thomas	6105	6105
	tpa	tpa1	USSales	Jim Smith	6106	6106
	tpa	tpa1	USSales	Jo Clayden	6107	6107

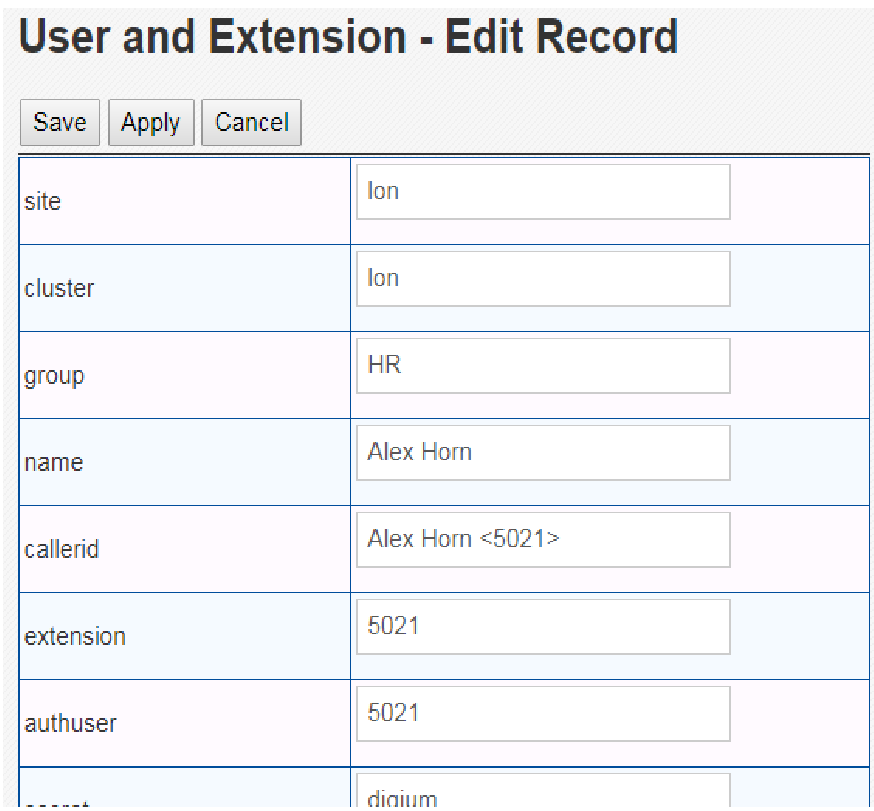
Again you can re-sort by clicking on a blue header name or you can use the search button if you need to find a particular user or extension etc…. **or select** v **to search** for an extension or user etc.

In this example we search for user name Keith Campbell ;

We can then choose to edit/change, copy or view this record in detail.

4.0.3 Edit/Configure Extension/User

In this next example we choose to edit a lon record by clicking on the Change button ;



Most fields are recognisable to anyone familiar with Asterisk

Some sites make use of all of the fields – other sites only use a few

Customised notes for this enterprise - in here

vm box	5605
voicemail password	1234
directory entry	yes no
accountcode	IT
context group rights	TechSupport IT HR USSales1 USSales2 TampaADMIN TampaReception SFOReception EUSales EUAdmin UKSales UKAdmin UKReception EUReception Training Exec

Remember to configure the voicemail box ONLY on the home cluster for any users that are going to be using the roaming features

VM password will be blank if the user has changed their password. If VM password entered here their password will be overwritten.

Directory entry places the name and number into the corporate directory - dial 411 to hear the default corp directory

These are the context or user rights groups which decide which numbers this extension is allowed to call and what features are allowed etc

Depending upon the CMS account rights, some of these fields may not be seen. Each user of the Asterisk Cluster Manager can have different levels of access

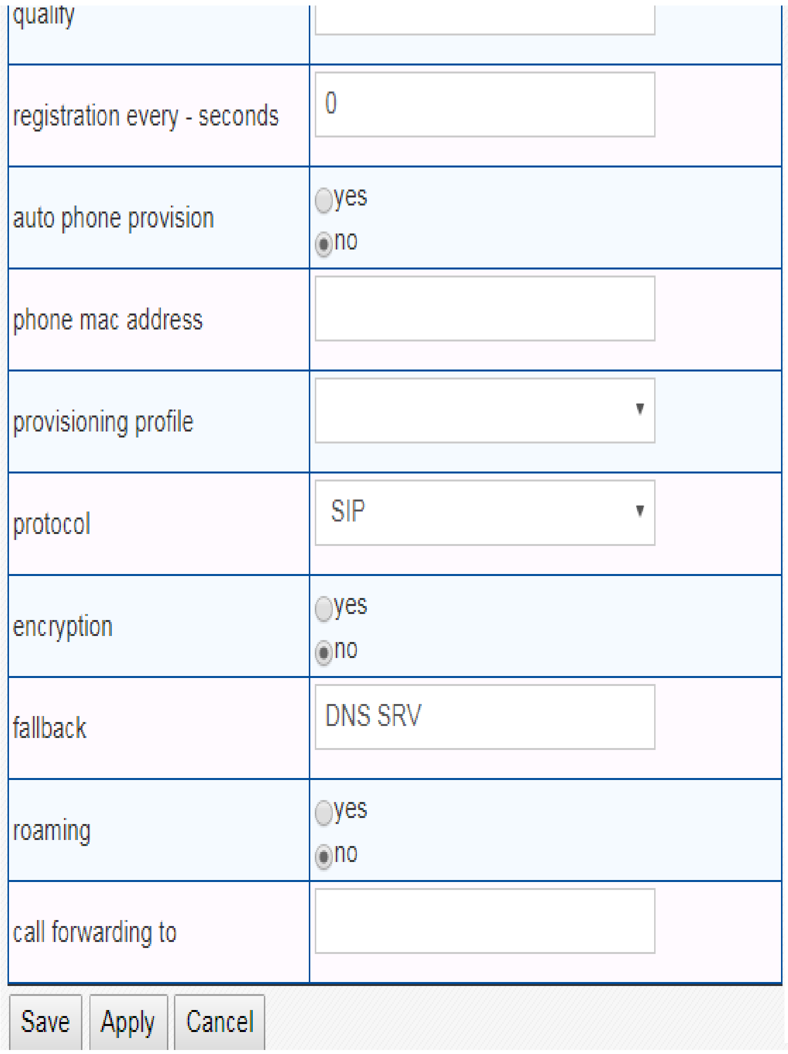
amaflags	
callgroup	5
pickup groups	5
fromuser	
full contact or description	Alex Horn
host	
insecure	
language	en
md5secret	
nat	no
acl	internal_phones

Usually an extension will be configured into a callgroup for their local operating group of users to allow other members of the same group to answer a ringing phone. The pickup group can be a list of callgroups that this extension is allowed to pickup and answer a ringing phone from.

The full contact is used by reporting, wallboards and detailed status screens to identifier this extensions/user

The access-list can be edited on the Asterisk Cluster Manager and will stop any telephones or softphones from registering that are not using the approved ip addresses

Customised enterprise notes in here



Auto phone provisioning allows the NOC/HelpDesk operators to make moves, adds and changes very quickly by entering the mac address of the telephone so that it will automatically pickup this configuration when it starts-up.

Select the profile to match the telephone {Mitel, Avaya, Cisco, Polycom, SNom, Digium etc..} , the telephone mac address and the protocol {SIP, SCCP, IAX etc..} to have the telephone automatically change to the configured extension details.

Select roaming to enable DUNDI to advertise this extension to all other clusters to allow users to connect at multiple sites and/or have standard numbers for departments (helpdesk, accounts etc…)

Customised enterprise details in here - - - - -

A blank entry for any fields will try to use the default for the field {roaming = no, fallback = none…}

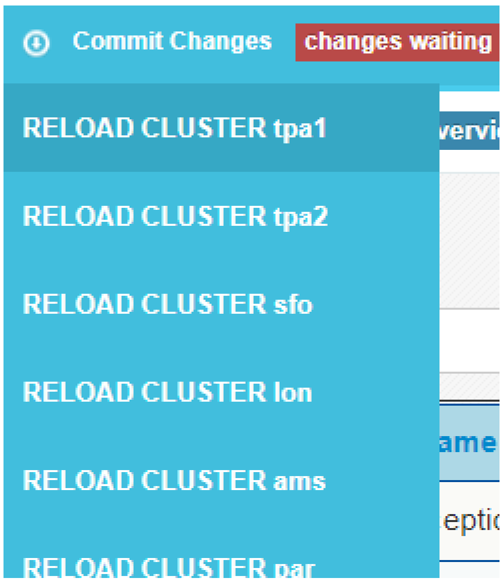
This allows you to edit the record for the user/extension. If you click 'Cancel' then the change will not be saved - so you can play with theses screens without making changes until you are familiar with the options and methods available for your account.

Depending upon your profile level, you will be able to change different elements of a user/extension. You should be able to set the extension number, username, secret/password for the phone, voicemail details, call and pickup groups, user groups, agent groups, enable encryption if required, auto provision, protocol etc….

To add a new user you can also use the COPY function which allows you to copy an existing user configuration so you can then modify the new copy with the new extension number, name, phone details etc. This is the quickest way to add a new user to an existing group. When finished editing you save the record by clicking Save or Apply.

Notice after you have made any changes or additions the icon will change to show 'changes waiting'

You can then reload the Asterisk cluster for the change to be committed. FYI changes are backed-up so that date/timed changes can be backed-out if necessary.



Reloading the cluster will commit the changes you have made to the Asterisk servers and make the changes active.

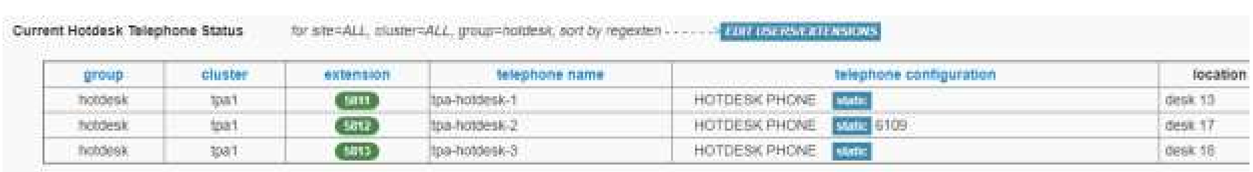
Changes are non-disruptive and safe to be done during business hours.

Automatic backups are created with each change so that changes can be backed-out or investigated at a later time.

4.0.3 Hot Desk Configuration

Hot desk configuration allows telephones to be setup with local dialing rights as hotdesk phones so that a user can login to a hotdesk phone and have their context/rights imposed onto the hotdesk phone. This is ideal for hotdesk working or share telephones that require control and account of the calls placed and received.

A hotdesk phone is defined as a telephone that has very basic dialing rights {local calls and emergency etc. – customised to the enterprise requirements} with the feature that allows a hotdesk user to login and use that hotdesk phone as if it were their own extension. The user profile is inherited by hotdesk phone when the user logs in.



Current Hotdesk Telephone Status for site=ALL, cluster=ALL, group=hotdesk, sort by regexten

group	cluster	extension	telephone name	telephone configuration	location
hotdesk	tpa1	5811	tpa-hotdesk-1	HOTDESK PHONE static	desk 13
hotdesk	tpa1	5812	tpa-hotdesk-2	HOTDESK PHONE static 6109	desk 17
hotdesk	tpa1	5813	tpa-hotdesk-3	HOTDESK PHONE static	desk 16

The status of the hotdesk phones can be seen and changes made as required. In the example above, you can see hotdesk phones 5811, 5812 and 5813 are all showing as available {telephone online and registered with Asterisk}, they are all in cluster tpa1 and located on desk 13, 17 and 18. The configuration shows they have been configured as hotdesk phones so they can be used locally without login to make local and emergency calls. Notice that 5812 is showing it is in use by hotdesk user 6109.

On the same screen we see that the hotdesk user 6109 is George Lopez and is a member of the USSales group, so George will be able to make calls using this hotdesk phone as if he were using his own extension and call records will show the calls he makes using his extension number and group details.

Current Hotdesk DB Status *for site=ALL, cluster=ALL, group=hotdesk, sort by extension*

user extension	hotdesk telephone	cid name	cid number	context - group	accountcode	cluster
1101	5841	KCampbell	1101	TechSupport	TechSupport	lon
1102	5101	Harry	1102	TechSupport	TechSupport	lon
5366	logged out	HDesk	5366	Training	Training	lon
6109	5812	George Lopez	6109	USSales	USSales	tpa1

4.0.4 Database

The full list of user-accessible MySQL fields for the status database are listed here ;

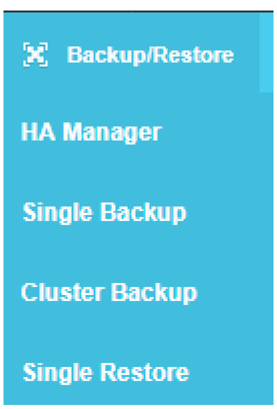
#	Name	Type	Notes
1	**id**	int(11)	index
2	**Site**	text	Site within the enterprise
3	**Astgroup**	text	Agent or extension group
4	**Cluster**	text	Cluster name
5	**name**	varchar(80)	User or extension name
6	**Callerid**	varchar(80)	Caller ID
7	**Defaultuser**	varchar(80)	Asterisk variable
8	**Regexten**	varchar(80)	Extension Number
9	**Authuser**	varchar(22)	Asterisk variable
10	**Secret**	varchar(80)	Extension password
11	**Mailbox**	varchar(50)	Voicemail box number
12	**Vmsecret**	varchar(22)	Voicemail password

#	Name	Type	Notes
13	**Accountcode**	varchar(20)	Reporting account reference
14	**Context**	varchar(80)	Asterisk privilege group
15	**Amaflags**	varchar(7)	Ama CDR flags
16	**Callgroup**	varchar(10)	Inbound call group #
17	**Canreinvite**	char(3)	Direct media flag
18	**Defaultip**	varchar(15)	Default ip address
19	**Dtmfmode**	varchar(7)	Defaults to RFC2833
20	**Fromuser**	varchar(80)	Asterisk variable
21	**Fromdomain**	varchar(80)	Asterisk variable
22	**Fullcontact**	varchar(80)	User Name for reports
23	**Host**	varchar(31)	Trunk host details
24	**Insecure**	varchar(4)	Asterisk variable
25	**Language**	char(2)	Asterisk variable
26	**md5secret**	varchar(80)	Asterisk variable
27	**NAT**	varchar(5)	Default = no
28	**ACL**	text	Access list
29	**Deny**	varchar(95)	Blocked ips
30	**Permit**	varchar(95)	Allowed ips
31	**Mask**	varchar(95)	Asterisk variable
32	**Pickupgroup**	varchar(10)	Call pick-up groups
33	**Port**	varchar(5)	Asterisk variable
34	**Qualify**	char(3)	Asterisk variable
35	**Restrictcid**	char(1)	Asterisk variable
36	**RTPtimeout**	char(3)	Asterisk variable
37	**RTPholdtimeout**	char(3)	Asterisk variable
38	**Type**	varchar(6)	Asterisk variable
39	**Disallow**	varchar(100)	Asterisk variable CODECS
40	**Allow**	varchar(100)	Asterisk variable CODECS
41	**Musiconhold**	varchar(100)	Asterisk variable
42	**Regseconds**	int(11)	Asterisk variable
43	**ipaddr**	varchar(45)	Asterisk variable
44	**Cancallforward**	char(3)	Default = yes
45	**call-limit**	int(2)	Default = 4
46	**Lastms**	int(11)	Asterisk variable
47	**Useragent**	char(255)	Asterisk variable
48	**Regserver**	varchar(100)	Asterisk variable
49	**Phoneprov**	text	Auto phone provision

#	Name	Type	Notes
50	**Phonemac**	text	Phone mac for provisioning
51	**Profile**	varchar(15)	Profile for provisioning
52	**Protocol**	text	Voice signal protocol
53	**Encryption**	varchar(3)	Default = no
54	**Fallback**	text	Fallback method
55	**Extstatus**	int(1)	Asterisk variable
56	**Agentstatus**	text	Asterisk variable
57	**Queue**	text	Asterisk variable
58	**callsDIN**	int(4)	Asterisk variable
59	**callsQIN**	int(4)	Asterisk variable
60	**callsOUT**	int(4)	Asterisk variable
61	**vmUNREAD**	int(3)	Asterisk variable
62	**vmOLD**	int(3)	Asterisk variable
63	**cfwdSET**	text	Asterisk variable
64	**cfwdTO**	text	Asterisk variable
65	**Callbackextension**	varchar(15)	Asterisk variable
66	**Directory**	text	Include in corp directory

5.0 System Admin

Most of the configuration menus make use of the same layout, so it is very easy to manage all configuration as soon as you are familiar with one ;

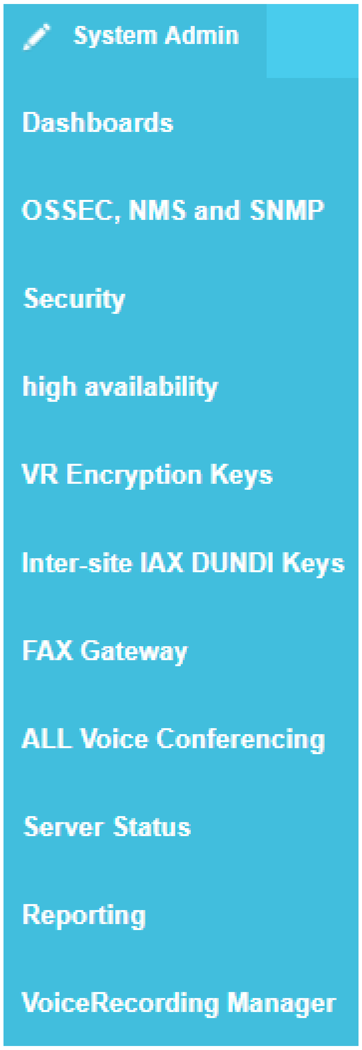


Backup/Restore menu tab {PRIVILEDGED}

Allows control of High Availability VIPs and cluster priority

Backups and restore options for individual servers or clusters

Backups are customized to save the Asterisk configuration + MySQL to any location. Due to the high availability, the backups/restore features are very rarely used.



System Admin menu tab

Link to the dashboard/wallboard menus

Allows control of OSSEC and NMS configuration

iptables firewalls, dynamic blacklists and fail2ban

customized options can be added for storage management, voice recording manager, dashboards, wallboards, CDR reporting, custom reporting, MySQL tuning and configuration etc…

Encryption Key Manager and storage management etc..

The FAX gateway and voice conference managers can be launched from this menu {OPTION}

Links are also found here to reach all of the reporting systems and voice recording manager

5.0.1 encryption keys

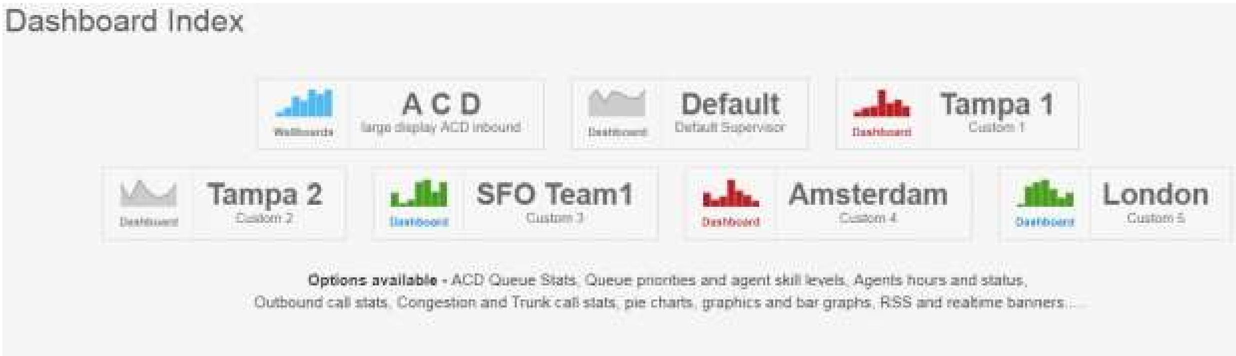
Example screen for encryption key management

Encryption keys for DUNDI and IAX links and voice recording encryption can be managed to suit the enterprise PCI or FIPS compliance policies

Customised notes for this enterprise - in here

5.0.2 Dashboards and Wallboards

Customized dashboards allow wallboard display and/or supervisor dashboards be configured to match the business requirements ;



Customized large screen wallboard example

Current Extension Status *for site=ALL, cluster=tpa1, group=USSales, sort by regexten* - - - - - -> EDIT USERS/EXTENSIONS

group	cluster	extension	user name	agent status	avail	lunch	break	meet	train	admin
USSales	tpa1	6101	Leon Johstone	USSales1 busy on a call	00:00:00	00:00:00	00:00:00	00:00:00	00:00:00	00:00:00
USSales	tpa1	6102	Mike Sydney	USSales1 logged out	logged off	00:00:00	00:00:00	00:00:00	00:00:00	00:00:00
USSales	tpa1	6103	Sally Phillips	USSales1 busy on a call	00:00:00	00:00:00	00:00:00	00:00:00	00:00:00	00:00:00
USSales	tpa1	6104	Jessie Gonzalez	USSales1 busy TRAINING	23:57:57	00:02:03	00:00:00	00:00:00	00:00:00	00:00:00
USSales	tpa1	6105	Ken Thomas	USSales1 logged in available 3 ACD calls, last call 9926757	00:00:00	00:00:00	00:00:00	00:00:00	00:00:00	00:00:00
USSales	tpa1	6106	Jim Smith	USSales1 logged out	logged off	00:00:00	00:00:00	00:00:00	00:00:00	00:00:00
USSales	tpa1	6107	Jo Clayden	USSales1 logged out	logged off	00:00:00	00:00:00	00:00:00	00:00:00	00:00:00
USSales	tpa1	6108	Gerrit Rosbeek	USSales1 logged out	logged off	00:00:00	00:00:00	00:00:00	00:00:00	00:00:00
USSales	tpa1	6109	George Lopez	USSales1 logged in ADMIN	23:56:06	00:03:54	00:00:00	00:00:00	00:00:00	00:00:00

examples of supervisor dashboards that are customized to show the required information

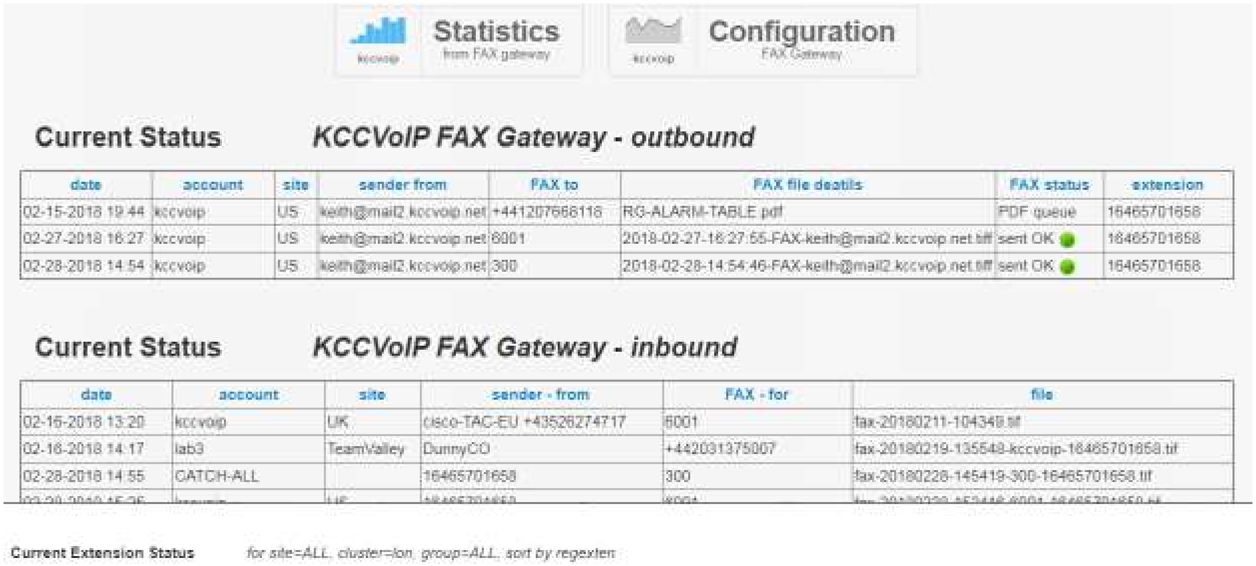
Current Trunk Status - - - -> EDIT TRUNKS

group	trunk status	trunk ID	provider	response	protocol	acl
UKSales	UP	SIP-32	BT	<150ms	SIP	providers
UKSales	UP	TELNYX-7	sip.telnyx.com	<150ms	SIP	providers
UKSales	UP	TELNYX-8	sip.telnyx.com	<150ms	SIP	providers

Customised enterprise details in here

5.0.3 FAX Manager

{OPTIONAL MODULE}



date	account	site	sender from	FAX to	FAX file deatils	FAX status	extension
02-15-2018 19:44	kccvoip	US	keith@mail2.kccvoip.net	+441207668118	RG-ALARM-TABLE.pdf	PDF queue	16465701658
02-27-2018 16:27	kccvoip	US	keith@mail2.kccvoip.net	6001	2018-02-27-16:27:55-FAX-keith@mail2.kccvoip.net.tiff	sent OK	16465701658
02-28-2018 14:54	kccvoip	US	keith@mail2.kccvoip.net	300	2018-02-28-14:54:46-FAX-keith@mail2.kccvoip.net.tiff	sent OK	16465701658

date	account	site	sender - from	FAX - for	file
02-16-2018 13:20	kccvoip	UK	cisco-TAC-EU +43526274717	6001	fax-20180211-104349.tif
02-16-2018 14:17	lab3	TeamValley	DunnyCO	+442031375007	fax-20180219-135548-kccvoip-16465701658.tif
02-28-2018 14:55	CATCH-ALL		16465701658	300	fax-20180228-145419-300-16465701658.tif

example from the FAX Manager

The FAX Manager is an optional addition to the Cluster Manager which provides a FAX gateway on one or more HA pair of servers. The MySQL database holds the user configuration which maps username, email and any associated FAX numbers to allow the sending and receiving of FAXs using email and PDF files. The FAX manager shows the status of FAXs sent and received and allows resending and detailed logging.

5.0.4 Conference Manager

{OPTIONAL MODULE}

The Voice Conference Manager is an optional addition to the Cluster Manager which provides a management of voice conferencing for the Asterisk enterprise. Conferences can be scheduled, monitored and logged.

Current Status *Conference Manager*

Current Conferencing Status ----> EDIT OR CREATE CONFERENCE

start	end	reoccur	conf num	external num	owner	acount	description	max users	status	record	video
2018-05-30 00:00:00	0000-00-00 00:00:00	weekly	8602	16465701658 8602	keith	UKSales	weekly chat on UKSales	10	OK	no	no
2018-05-30 00:00:00	0000-00-00 00:00:00	weekly	8608	16465701658 8608		USSales	weekly chat on USSales	16		no	no
2018-06-22 14:00:00	2018-06-23 00:00:00	no	8603			USSales	TPA site move	10		yes	follow_talker

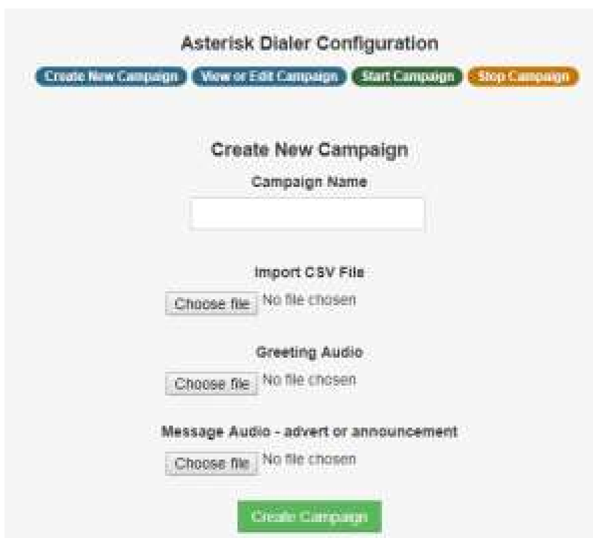
Conference Manager - booking

<< < Add View Change Copy Delete > >> Go to 1 Page: 1 of 1 Records: 3

v	conf number	start	end	reoccur	account	cluster	external number	description	maxuseers	user pin	record conf	video mode
◉	8602	2018-05-30 00:00:00	0000-00-00 00:00:00	weekly	UKSales	lon	16465701658 8602	weekly chat on UKSales	10	1234	no	no
○	8608	2018-05-30 00:00:00	0000-00-00 00:00:00	weekly	USSales	tpa2	16465701658 8608	weekly chat on USSales	16	1234	no	no
○	8603	2018-06-22 14:00:00	2018-06-23 00:00:00	no	USSales	tpa1		TPA site move	10	1234	yes	follow_talker

6.0 Outbound Dialer

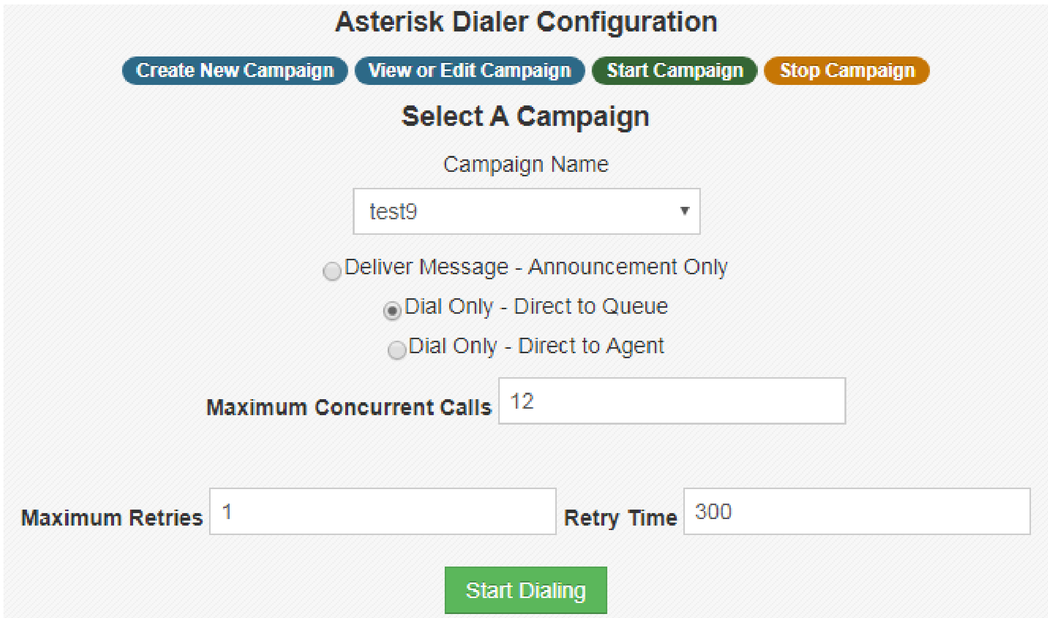
{OPTIONAL MODULE}



Customised to the agent group to match the requirements for campaign {concurrent calls, ACD inbound queue, direct agent routing, announce only outbound calling, CRM integration and/or csv file import for outbound contacts etc…

{see the ACD-OUTBOUND DIALER training presentations for more details}

Blended queues combines inbound and outbound calling allows agents to be utilized for several campaigns and inbound ACDs. SMS, Chat, eMail also can be integrated.



Example screens from the Asterisk Dialer within the Cluster Manager

7.0 Essentials for Implementation

NOTE - By 2021 we will move to Centos 7 and Asterisk 16.x

Prior to Nov 2020 ;

CentOS 6.9 64 bit minimum of 2 servers in HA cluster

MySQL version required = > 5.5

PHP version required = > 5.6

Asterisk version > 13.18 cert 2

OSSEC > 2.9

iptables/fail2ban modified for MySQL, SSH, HTTPS, SIP, SCCP, DUNDI, IAX etc..

SNMP NMS require Asterisk MIBs installed on any NMS/SIEM systems used by the enterprise

Local site DNS requires configuration for DNS SRV and local server identification

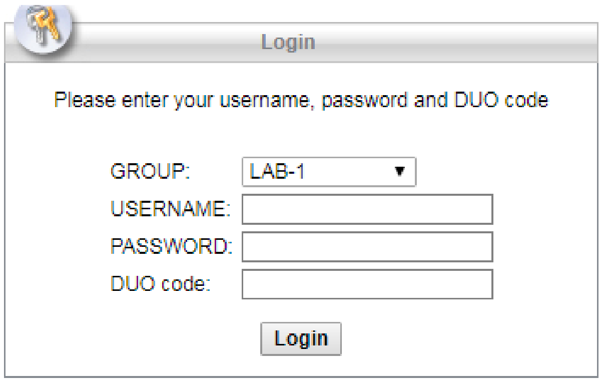
Local site support training is a prerequisite to the implementation to ensure the systems are customised to match the enterprise requirements and that the local support and/or technical operations team can maintain and modify the system configuration.

6.0.1 OSSEC INTEGRATION NOTES

All Asterisk servers within a cluster send encrypted UDP notifications to the master OSSEC servers in the UK {a free on-demand service or a subscription service for 24/7 PCI compliance}. These servers analyse and filter the streams to prioritize and forward the required notification to the enterprise NMS/SIEM systems, notification to department managers via email and urgent emails and SMS to engineers/helpdesks as required for the enterprise.

OSSEC continuously monitors the servers within all clusters for FIM/HIDS etc. in compliance with FIPS/PCI recommendations.

OSSEC analyser login is available for technical and security engineers via the VPN AnyConnect gateway ;

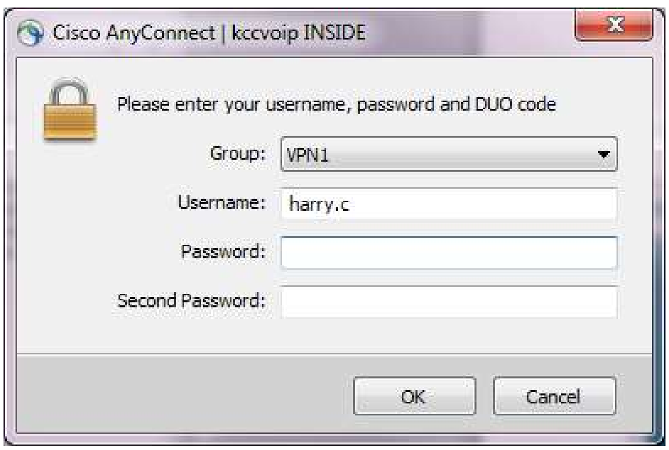


Example of a web SSL login to the client portal

{ https://kcc1.webhop.net:8088 }

Cisco ASA AnyConnect gateway uses DUO multi-factor authentication for full FIPS compliance

Login is also possible using Cisco AnyConnect client and DUO ;

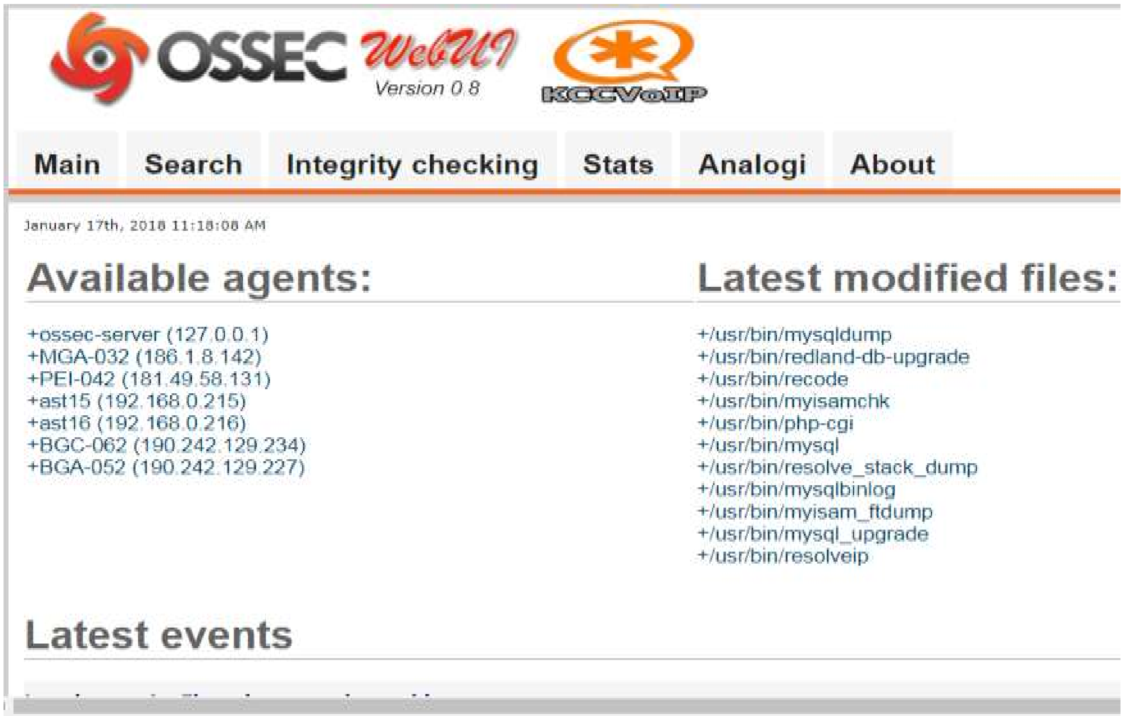


Example of a AnyConnect login to the client portal

{ kcc1.webhop.net }

Cisco ASA AnyConnect gateway uses DUO multi-factor authentication for full FIPS compliance

The account will then connect you to the software ticketing, account console and OSSEC gateways depending upon your account ;


OSSEC WebUI
Version 0.8
KCCVoIP
Main
Search
Integrity checking
Stats
Analogi
About
January 17th, 2018 11:18:08 AM
Available agents:
+ossec-server (127.0.0.1)
+MGA-032 (186.1.8.142)
+PEI-042 (181.49.58.131)
+ast15 (192.168.0.215)
+ast16 (192.168.0.216)
+BGC-062 (190.242.129.234)
+BGA-052 (190.242.129.227)
Latest modified files:
+/usr/bin/mysqldump
+/usr/bin/redland-db-upgrade
+/usr/bin/recode
+/usr/bin/myisamchk
+/usr/bin/php-cgi
+/usr/bin/mysql
+/usr/bin/resolve_stack_dump
+/usr/bin/mysqlbinlog
+/usr/bin/myisam_ftdump
+/usr/bin/mysql_upgrade
+/usr/bin/resolveip
Latest events

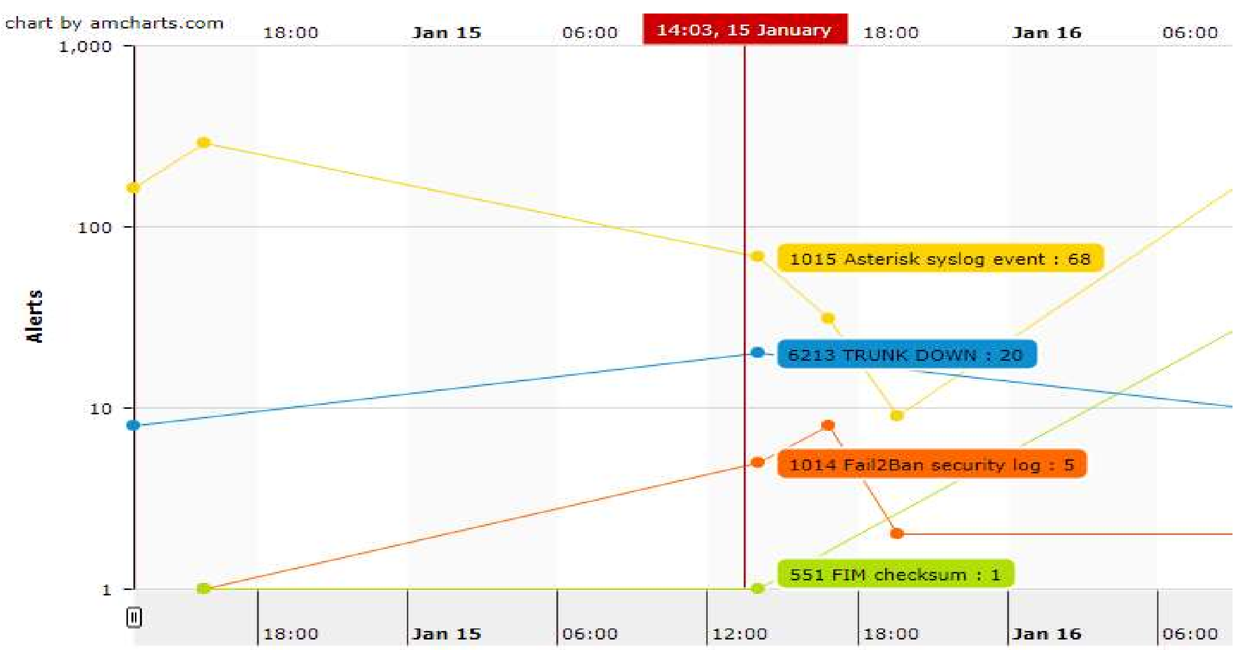
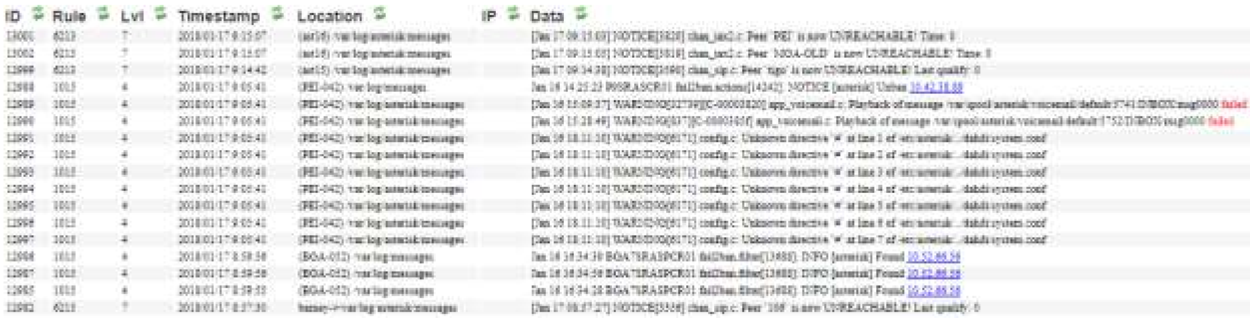
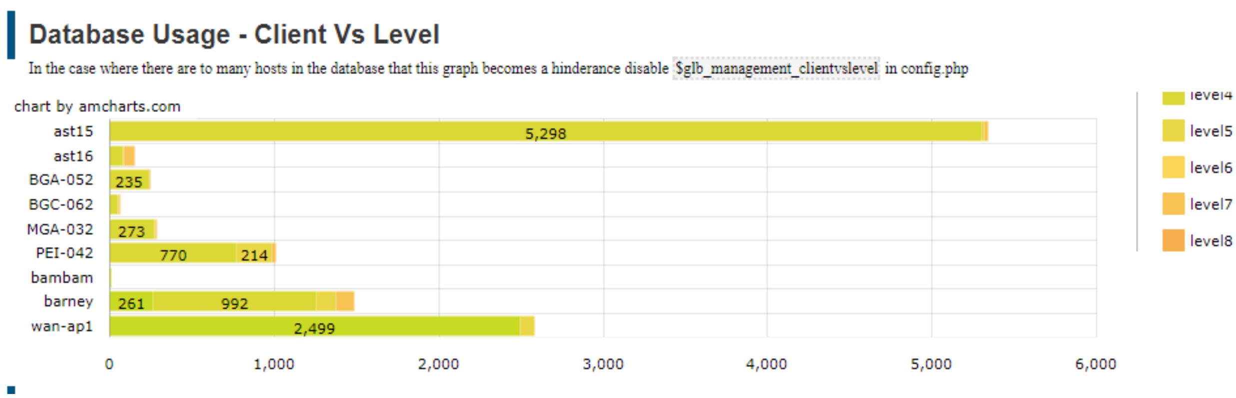


chart by amcharts.com
14:03, 15 January
Alerts
1,000
100
10
1
18:00
Jan 15
06:00
12:00
18:00
Jan 16
06:00
1015 Asterisk syslog event : 68
6213 TRUNK DOWN : 20
1014 Fail2Ban security log : 5
551 FIM checksum : 1



ID	Rule	Lvl	Timestamp	Location	IP	Data
13001	6213	7	2018/01/17 9:15:07	(ast16) /var/log/asterisk/messages		[Jan 17 09:15:03] NOTICE[3820] chan_iax2.c: Peer 'PEI' is now UNREACHABLE! Time: 0
13002	6213	7	2018/01/17 9:15:07	(ast16) /var/log/asterisk/messages		[Jan 17 09:15:03] NOTICE[3819] chan_iax2.c: Peer 'MGA-OLD' is now UNREACHABLE! Time: 0
12999	6213	7	2018/01/17 9:14:42	(ast15) /var/log/asterisk/messages		[Jan 17 09:14:38] NOTICE[[illegible]] chan_sip.c: Peer '[illegible]' is now UNREACHABLE! Last qualify: 0
12988	1015	4	2018/01/17 9:05:41	(PEI-042) /var/log/messages		Jan 16 14:25:22 [illegible] fail2ban.actions[14242]: NOTICE [asterisk] Unban [illegible]
12989	1015	4	2018/01/17 9:05:41	(PEI-042) /var/log/asterisk/messages		[Jan 16 15:09:37] WARNING[[illegible]] app_voicemail.c: Playback of message /var/spool/asterisk/voicemail/default/[illegible]/INBOX/msg0000 failed
12990	1015	4	2018/01/17 9:05:41	(PEI-042) /var/log/asterisk/messages		[Jan 16 15:28:49] WARNING[[illegible]] app_voicemail.c: Playback of message /var/spool/asterisk/voicemail/default/[illegible]/INBOX/msg0000 failed
12991	1015	4	2018/01/17 9:05:41	(PEI-042) /var/log/asterisk/messages		[Jan 16 18:11:10] WARNING[6171] config.c: Unknown directive '#' at line 1 of /etc/asterisk/.../dahdi/system.conf
12992	1015	4	2018/01/17 9:05:41	(PEI-042) /var/log/asterisk/messages		[Jan 16 18:11:10] WARNING[6171] config.c: Unknown directive '#' at line 2 of /etc/asterisk/.../dahdi/system.conf
12993	1015	4	2018/01/17 9:05:41	(PEI-042) /var/log/asterisk/messages		[Jan 16 18:11:10] WARNING[6171] config.c: Unknown directive '#' at line 3 of /etc/asterisk/.../dahdi/system.conf
12994	1015	4	2018/01/17 9:05:41	(PEI-042) /var/log/asterisk/messages		[Jan 16 18:11:10] WARNING[6171] config.c: Unknown directive '#' at line 4 of /etc/asterisk/.../dahdi/system.conf
12995	1015	4	2018/01/17 9:05:41	(PEI-042) /var/log/asterisk/messages		[Jan 16 18:11:10] WARNING[6171] config.c: Unknown directive '#' at line 5 of /etc/asterisk/.../dahdi/system.conf
12996	1015	4	2018/01/17 9:05:41	(PEI-042) /var/log/asterisk/messages		[Jan 16 18:11:10] WARNING[6171] config.c: Unknown directive '#' at line 6 of /etc/asterisk/.../dahdi/system.conf
12997	1015	4	2018/01/17 9:05:41	(PEI-042) /var/log/asterisk/messages		[Jan 16 18:11:10] WARNING[6171] config.c: Unknown directive '#' at line 7 of /etc/asterisk/.../dahdi/system.conf
12986	1015	4	2018/01/17 8:58:58	(BGA-052) /var/log/messages		Jan 16 16:34:30 BGA[illegible] fail2ban.filter[13688]: INFO [asterisk] Found [illegible]
12987	1015	4	2018/01/17 8:58:58	(BGA-052) /var/log/messages		Jan 16 16:34:59 BGA[illegible] fail2ban.filter[13688]: INFO [asterisk] Found [illegible]
12985	1015	4	2018/01/17 8:58:58	(BGA-052) /var/log/messages		Jan 16 16:34:28 BGA[illegible] fail2ban.filter[13688]: INFO [asterisk] Found [illegible]
12982	6213	7	2018/01/17 8:37:30	barney->/var/log/asterisk/messages		[Jan 17 08:37:27] NOTICE[3558] chan_sip.c: Peer '108' is now UNREACHABLE! Last qualify: 0

Example screens from the analogi from OSSEC



Log extract examples

- Jan 17 09:14:36 ast16 kernel: wct4xxp 0000:03:02.0: RCLK source set to span 1
- Jan 17 09:14:36 ast16 kernel: wct4xxp 0000:03:02.0: Recovered timing mode, RCLK set to span 1
- Jan 17 09:14:41 ast16 ntpd[2735]: Listen normally on 6 eth0:2 172.20.15.1 UDP 123
- Jan 17 09:14:41 ast16 ntpd[2735]: Listen normally on 7 eth0:1 192.168.0.218 UDP 123
- Jan 17 09:22:39 ast16 kernel: wct4xxp 0000:03:02.0: Need to increase latency. Estimated latency should be 3
- Jan 17 09:22:39 ast16 kernel: wct4xxp 0000:03:02.0: Increased latency to 3

Level 5 and above are usually forwarded to the enterprise HelpDesk/NOC

Level 7 and above usually trigger email and SMS notification for department heads and support engineers

Rules can be customised to send alerts for defined sites to the appropriate email, NMS and/or syslog within the enterprise. At default there are >500 rules and alerts configured into the various alert levels. The configuration and tuning of OSSEC is a complex and lengthy process and is usually done in stages to match the enterprise requirements.

Enterprise OSSEC details in here

```
Level:     3 - Asterisk warning message.                                   2018 Apr 18 13:31:02
Rule Id:   6202
Location:  bambam->/var/log/messages
Apr 18 14:31:02 bambam asterisk[1910]: WARNING[18979]: chan_sip.c:4073 in retrans_pkt: Retransmission timeout reached on transmission 535156364-922389285-380306499 for seqno 1 (Critical Response) -- See https://wiki.asterisk.org/wiki/display/AST/SIP+Retransmissions#012Packet timed out after 31999ms with no response
```

Asterisk timeout and retransmission example