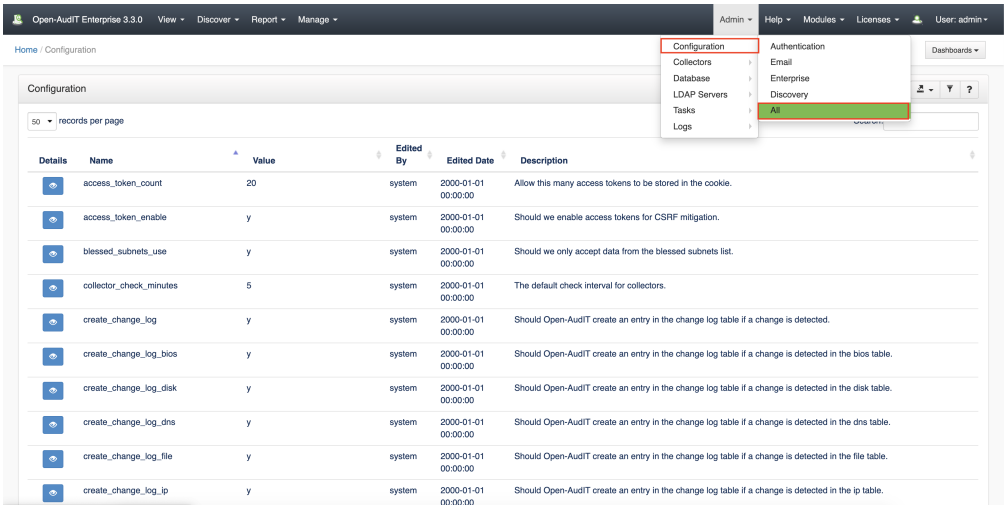
Open-AudIT Configuration

Open-AudIT Configuration

All settings apart from the database credentials should be accessible using the GUI. The GUI menu has entries for each major section and the Professional / Enterprise configuration options are separate from the Community options. The configuration options for Community are stored in the database. The configuration options for Professional / Enterprise are stored in a *text* file (Linux) /usr/local/omk/conf/opCommon.nmis and (Windows) c:\omk\conf\opCommon.nmis.



Common Settings to Consider Adjusting

The only attributes commonly set are those for email (see below). All other settings should likely be left as-is, unless a specific requirement is to be met.

Configuring Professional or Enterprise

In the config file is a section named authentication. You can verify users logging into Open-AudIT Enterprise using their Open-AudIT Community credentials if you set auth_method_1 to openaudit in this section. You can have up to three methods of authentication. openaudit then htaccess are the defaults.

To change these using the GUI in Open-AudIT navigate to menu -> Admin -> Configuration Enterprise

You may need to restart the omkd daemon / service after making changes to these items.

The file these settings are stored in is (Linux) /usr/local/omk/conf/opCommon.nmis and (Windows) c:\omk\conf\opCommon.nmis.

The settings are common to all Opmantek commercial applications.

Section	Name	Original Value		Possible Values	Description
openauditenterprise	oae_application_heading	undef			Unused.
openauditenterprise	oae_baseline_match_case	y		y, n	When we match software in the baselines endpoint, should we match regardless of case in software.name

openaudite nterprise	oae_cloud_server	https://cloud.open-audit.com		<url>	Unused in on-premise installations.
openaudite nterprise	oae_debug_level	0		0. 1. 2. 3	Log verbosity (larger is more verbosity).
openaudite nterprise	oae_gui_refresh_time	20		<integer>	Unused.
openaudite nterprise	oae_link	/open-audit/		<absolute url>	The standard link to Open-AudIT Community
openaudite nterprise	oae_password			<password>	Unused. The password for the Open-AudIT Enterprise user account.
openaudite nterprise	oae_rss_url	https://community.opmantek.com/rss/OAE.xml		<url>	The online address of the RSS feed.
openaudite nterprise	oae_rss_use	y		y, n	Should we use the RSS feed on the dashboard.
openaudite nterprise	oae_server	http://127.0.0.1/open-audit/		<url>	The link to Open-AudIT for internal connections. Should always be the original value unless explicitly directed by Opmantek to be changed.
openaudite nterprise	oae_type				Unused in on-premise installations.
openaudite nterprise	oae_username	open-audit_enterprise		<username>	The Open-AudIT Enterprise user (used internally).
openaudite nterprise	oae_collector_connect_timeout	10		<integer>	Seconds to timeout waiting for the server when in Collector mode.
openaudite nterprise	oae_collector_request_timeout	240		<integer>	Seconds to timeout waiting for the server when in Collector mode.
openaudite nterprise	oae_collector_inactivity_timeout	30		<integer>	Seconds to timeout waiting for the server when in Collector mode.

Email

The email settings are used to email scheduled Queries and Reports. These should be changed to your required email server's settings.

To change these using the GUI in Open-AudIT navigate to menu -> Admin -> Configuration -> Email

You may need to restart the omkd daemon / service after making changes to these items.

The file these settings are stored in is (Linux) /usr/local/omk/conf/opCommon.nmis and (Windows) c:\omk\conf\opCommon.nmis.

The settings are common to all Opmantek commercial applications.

Section	Name	Original Value		Possible Values	Description
email	mail_domain	yourdomain.com		<domain>	
email	mail_from	yourmailname@yourdomain.com		<email>	
email	mail_password	your_password		<password>	
email	mail_server	smtp.yourdomain.com		<fqdn>	
email	mail_server_port	25		<integer>	
email	mail_subject_prefix	[automatic]			
email	mail_use_tls	true		true, false	
email	mail_user	your_user_account@your_domain.com		<username>	

Authentication

In the config file is a section named authentication. You can verify users logging into Open-AudIT Enterprise using their Open-AudIT Community credentials if you set auth_method_1 to openaudit in this section. You can have up to three methods of authentication. openaudit then htaccess are the defaults. These should mostly be left as their defaults unless a specific requirement is to be met. To enable MS Active Directory and/or OpenLDAP, see the bottom of this page.

To change these using the GUI in Open-AudIT navigate to menu -> Admin -> Configuration -> Authentication

You may need to restart the omkd daemon / service after making changes to these items.

The file these settings are stored in is (Linux) /usr/local/omk/conf/opCommon.nmis and (Windows) c:\omk\conf\opCommon.nmis.

The settings are common to all Opmantek commercial applications.

Section	Name	Original Value		Possible Values	Description
authentication	auth_crowd_password			<password>	
authentication	auth_crowd_server			<ip>	
authentication	auth_crowd_user			<username>	
authentication	auth_expire_seconds	3600		<integer>	
authentication	auth_htpasswd_encrypt	crypt		crypt, plaintext, apache-md5	
authentication	auth_htpasswd_file	<omk_conf>/users.dat		<relative filepath>	
authentication	auth_lockout_after	0		<integer>	seconds, 0 for none.
authentication	auth_login_motd	Authentication required: default credentials are nmis/nm1888			
authentication	auth_method_1	openaudit		htpasswd, openaudit, radias, tacacs, crowd, system, ldaps, ldap, ms-ldap, ms-ldaps, novell-ldap, connectwise, pam	
authentication	auth_method_2	htpasswd		htpasswd, openaudit, radias, tacacs, crowd, system, ldaps, ldap, ms-ldap, ms-ldaps, novell-ldap, connectwise, pam	
authentication	auth_method_3			htpasswd, openaudit, radias, tacacs, crowd, system, ldaps, ldap, ms-ldap, ms-ldaps, novell-ldap, connectwise, pam	
authentication	auth_ms_ldap_attr	sAMAccountName			
authentication	auth_ms_ldap_base	CN=Users,DC=your_domain,DC=com		<ldap>	
authentication	auth_ms_ldap_debug	true		true, false	
authentication	auth_ms_ldap_dn_acc	CN=Administrator,CN=Users, DC=your_domain,DC=com			
authentication	auth_ms_ldap_dn_psw	your_administrator_password		<password>	
authentication	auth_ms_ldap_group	CN=Users,DC=your_domain,DC=com		<ldap>	
authentication	auth_ms_ldap_server	your.ip.address.here		<ip>	
authentication	auth_ms_ldaps_capath	required			
authentication	auth_ms_ldaps_server	your.ip.address.here		<ip>	
authentication	auth_ms_ldaps_verify				
authentication	auth_sso_domain			<domain>	

Configuring Community

Below are the default values and a description for the configuration of Open-AudIT. These can all be changed to work as you desire.

To change these using the GUI in Open-AudIT navigate to menu -> Admin -> Configuration -> All

Name	Original Value		Possible Values	Description
access_token_count	20		<integer>	Allow this many access tokens to be stored in the cookie.
access_token_enable	y		y, n	Should we enable access tokens for CSRF mitigation.
blessed_subnets_use	n		y, n	Should we only accept data from the blessed subnets list.
collector_check_minutes	5		5, 10, 15, 20, 30, 60	The default check interval for collectors.
create_change_log	y		y, n	Should Open-AudIT create an entry in the change log table if a change is detected.
create_change_log_bios	y		y, n	Should Open-AudIT create an entry in the change log table if a change is detected in the bios table.
create_change_log_disk	y		y, n	Should Open-AudIT create an entry in the change log table if a change is detected in the disk table.
create_change_log_dns	y		y, n	Should Open-AudIT create an entry in the change log table if a change is detected in the dns table.
create_change_log_file	y		y, n	Should Open-AudIT create an entry in the change log table if a change is detected in the file table.
create_change_log_ip	y		y, n	Should Open-AudIT create an entry in the change log table if a change is detected in the ip table.
create_change_log_log	y		y, n	Should Open-AudIT create an entry in the change log table if a change is detected in the log table.
create_change_log_memory	y		y, n	Should Open-AudIT create an entry in the change log table if a change is detected in the memory table.
create_change_log_module	y		y, n	Should Open-AudIT create an entry in the change log table if a change is detected in the module table.
create_change_log_monitor	y		y, n	Should Open-AudIT create an entry in the change log table if a change is detected in the monitor table.
create_change_log_motherboad	y		y, n	Should Open-AudIT create an entry in the change log table if a change is detected in the motherboard table.
create_change_log_netstat	y		y, n	Should Open-AudIT create an entry in the change log table if a change is detected in the netstat table.
create_change_log_netstat_dynamic	n		y, n	Should Open-AudIT create an entry in the change log table if a change is detected in the netstat table and the port is 49152 or greater.
create_change_log_netstat_registered	n		y, n	Should Open-AudIT create an entry in the change log table if a change is detected in the netstat table and the port is in the range of 1024 to 49151.
create_change_log_netstat_well_known	y		y, n	Should Open-AudIT create an entry in the change log table if a change is detected in the netstat table and the port is 1023 or lower.
create_change_log_network	y		y, n	Should Open-AudIT create an entry in the change log table if a change is detected in the network table.
create_change_log_nmap	y		y, n	Should Open-AudIT create an entry in the change log table if a change is detected in the nmap table.
create_change_log_optical	y		y, n	Should Open-AudIT create an entry in the change log table if a change is detected in the optical table.
create_change_log_pagefile	y		y, n	Should Open-AudIT create an entry in the change log table if a change is detected in the pagefile table.
create_change_log_partition	y		y, n	Should Open-AudIT create an entry in the change log table if a change is detected in the partition table.
create_change_log_policy	y		y, n	Should Open-AudIT create an entry in the change log table if a change is detected in the policy table.
create_change_log_print_queue	y		y, n	Should Open-AudIT create an entry in the change log table if a change is detected in the print_queue table.
create_change_log_processor	y		y, n	Should Open-AudIT create an entry in the change log table if a change is detected in the processor table.
create_change_log_route	y		y, n	Should Open-AudIT create an entry in the change log table if a change is detected in the route table.
create_change_log_san	y		y, n	Should Open-AudIT create an entry in the change log table if a change is detected in the san table.
create_change_log_scsi	y		y, n	Should Open-AudIT create an entry in the change log table if a change is detected in the scsi table.

create_change_log_server	y		y, n	Should Open-AudIT create an entry in the change log table if a change is detected in the server table.
create_change_log_server_item	y		y, n	Should Open-AudIT create an entry in the change log table if a change is detected in the server_item table.
create_change_log_service	y		y, n	Should Open-AudIT create an entry in the change log table if a change is detected in the service table.
create_change_log_share	y		y, n	Should Open-AudIT create an entry in the change log table if a change is detected in the share table.
create_change_log_software	y		y, n	Should Open-AudIT create an entry in the change log table if a change is detected in the software table.
create_change_log_software_key	y		y, n	Should Open-AudIT create an entry in the change log table if a change is detected in the software_key table.
create_change_log_sound	y		y, n	Should Open-AudIT create an entry in the change log table if a change is detected in the sound table.
create_change_log_task	y		y, n	Should Open-AudIT create an entry in the change log table if a change is detected in the task table.
create_change_log_usb	y		y, n	Should Open-AudIT create an entry in the change log table if a change is detected in the usb table.
create_change_log_user	y		y, n	Should Open-AudIT create an entry in the change log table if a change is detected in the user table.
create_change_log_user_group	y		y, n	Should Open-AudIT create an entry in the change log table if a change is detected in the user_group table.
create_change_log_variable	n		y, n	Should Open-AudIT create an entry in the change log table if a change is detected in the variable table.
create_change_log_video	y		y, n	Should Open-AudIT create an entry in the change log table if a change is detected in the video table.
create_change_log_vm	y		y, n	Should Open-AudIT create an entry in the change log table if a change is detected in the vm table.
create_change_log_windows	y		y, n	Should Open-AudIT create an entry in the change log table if a change is detected in the windows table.
database_show_row_limit	1000		<integer>	The limit of rows to show, rather than download when exporting a database table.
decrypt_credentials	y		y, n	When we display or export credentials, should we decrypt them.
default_network_address	http://localhost/open-audit/		<url>	The URL used by external devices to talk to Open-AudIT.
delete_noncurrent	n		y, n	Should we delete all non-current data.
delete_noncurrent_bios	n		y, n	Should we delete non-current bios data.
delete_noncurrent_disk	n		y, n	Should we delete non-current disk data.
delete_noncurrent_dns	n		y, n	Should we delete non-current dns data.
delete_noncurrent_file	n		y, n	Should we delete non-current file data.
delete_noncurrent_ip	n		y, n	Should we delete non-current ip data.
delete_noncurrent_log	n		y, n	Should we delete non-current log data.
delete_noncurrent_memory	n		y, n	Should we delete non-current memory data.
delete_noncurrent_module	n		y, n	Should we delete non-current module data.
delete_noncurrent_monitor	n		y, n	Should we delete non-current monitor data.
delete_noncurrent_motherboard	n		y, n	Should we delete non-current motherboard data.
delete_noncurrent_netstat	y		y, n	Should we delete non-current netstat data.
delete_noncurrent_network	n		y, n	Should we delete non-current network data.
delete_noncurrent_nmap	n		y, n	Should we delete non-current nmap data.

delete_noncurrent_optical	n		y, n	Should we delete non-current optical data.
delete_noncurrent_pagefile	n		y, n	Should we delete non-current pagefile data.
delete_noncurrent_partition	n		y, n	Should we delete non-current partition data.
delete_noncurrent_policy	n		y, n	Should we delete non-current policy data.
delete_noncurrent_print_queue	n		y, n	Should we delete non-current print_queue data.
delete_noncurrent_processor	n		y, n	Should we delete non-current processor data.
delete_noncurrent_route	n		y, n	Should we delete non-current route data.
delete_noncurrent_san	n		y, n	Should we delete non-current san data.
delete_noncurrent_scsi	n		y, n	Should we delete non-current scsi data.
delete_noncurrent_server	n		y, n	Should we delete non-current server data.
delete_noncurrent_server_item	n		y, n	Should we delete non-current server_item data.
delete_noncurrent_service	n		y, n	Should we delete non-current service data.
delete_noncurrent_share	n		y, n	Should we delete non-current share data.
delete_noncurrent_software	n		y, n	Should we delete non-current software data.
delete_noncurrent_software_key	n		y, n	Should we delete non-current software_key data.
delete_noncurrent_sound	n		y, n	Should we delete non-current sound data.
delete_noncurrent_task	n		y, n	Should we delete non-current task data.
delete_noncurrent_usb	n		y, n	Should we delete non-current usb data.
delete_noncurrent_user	n		y, n	Should we delete non-current user data.
delete_noncurrent_user_group	n		y, n	Should we delete non-current user_group data.
delete_noncurrent_variable	y		y, n	Should we delete non-current variable data.
delete_noncurrent_video	n		y, n	Should we delete non-current video data.
delete_noncurrent_vm	n		y, n	Should we delete non-current vm data.
delete_noncurrent_windows	n		y, n	Should we delete non-current windows data.
devices_default_display_columns	system.id,system.icon,system.type, system.name,system.ip,system.dns_fqdn, system.identification,system.description, system.manufacturer,system.os_family, system.status			When requesting a list of devices, display these columns.
devices_default_group_columns	system.id,system.icon,system.type,system.name, system.ip,system.dns_fqdn,system.identification, system.description,system.manufacturer, system.os_family,system.status			When requesting a group of devices, retrieve and display these columns.

devices_default_retrieve_columns	system.id,system.uuid,system.name, system.ip,system.hostname, system.dns_hostname,system.domain, system.dns_domain, system.dbus_identifier,system.fqdn, system.dns_fqdn,system.description, system.type,system.icon,system. os_group,system.os_family, system.os_name,system.os_version, system.manufacturer,system.model, system.serial,system.form_factor,system. status,system.environment, system.class,system.function,system. org_id,system.location_id, system.snmp_oid,system.sysDescr, system.sysObjectID,system.sysUpTime, system.sysContact,system.sysName, system.sysLocation,system.first_seen, system.last_seen,system.last_seen_by, system.identification			When requesting a list of devices, provide these columns.
device_auto_delete	y		y, n	Should we delete the device data completely from the database when the device status is set to Deleted.
discovery_default_scan_option	1		<integer>	The default discovery options for Nmap.
discovery_ip_exclude			<ip>	Populate this list with ip addresses to be excluded from discovery. IPs should be separated by a space.
discovery_limit	20		<integer>	The maximum number of concurrent discoveries we should run.
discovery_linux_script_directory	/tmp/		<filepath>	The directory the script is copied into on the target device.
discovery_linux_script_permissions	700			The permissions set on the audit_linux.sh script when it is copied to the target device.
discovery_linux_use_sudo	y		y, n	When running discovery commands on a Linux target, should we use sudo.
discovery_override_nmap	n		y, n	Override the detction of Nmap to enable discoveries.
discovery_route_retrieve_limit	500		<integer>	When discovering a device using SNMP, do not retrieve the route table if it contains more than this number of entries.
discovery_ssh_timeout	300		<integer>	Timeout duration (in seconds) when discovering a device via SSH.
discovery_sudo_path			<filepath>	Optional hardcoded path to sudo executable. Comma seperated for multiple paths.
discovery_sunos_use_sudo	y		y, n	When running discovery commands on a SunOS target, should we use sudo.
discovery_use_dns	y		y, n	Should we use DNS for looking up the hostname and domain.
discovery_use_ipmi	y		y, n	Should we use ipmitool for discovering management ports if ipmitool is installed.
discovery_use_vintage_service	n		y, n	On Windows, use the old way of running discovery with the Apache service account.
download_reports	n		y, n	Tells Open-AudIT to advise the browser to download as a file or display the csv, xml, json reports.
graph_days	30		<integer>	The number of days to report on for the Enterprise graphs.
gui_trim_characters	25		<integer>	When showing a table of information in the web GUI, replace characters greater than this with "...".
homepage	groups			Any links to the default page should be directed to this endpoint.
log_level	5		1,2,3,4,5,6,7	Tells Open-AudIT which severity of event (at least) should be logged.
log_retain_level_0	180		<integer>	Tells Open-AudIT how many days to keep logs with severity 0.
log_retain_level_1	180		<integer>	Tells Open-AudIT how many days to keep logs with severity 1.
log_retain_level_2	180		<integer>	Tells Open-AudIT how many days to keep logs with severity 2.

log_retain_level_3	180		<integer>	Tells Open-AudIT how many days to keep logs with severity 3.
log_retain_level_4	180		<integer>	Tells Open-AudIT how many days to keep logs with severity 4.
log_retain_level_5	90		<integer>	Tells Open-AudIT how many days to keep logs with severity 5.
log_retain_level_6	30		<integer>	Tells Open-AudIT how many days to keep logs with severity 6.
log_retain_level_7	7		<integer>	Tells Open-AudIT how many days to keep logs with severity 7.
maps_api_key				The API key for Google Maps.
maps_url	/omk/open-audit/map		<absolute url>	The web server address of opMaps.
match_dbus	n		y, n	Should we match a device based on its dbus id.
match_dns_fqdn	n		y, n	Should we match a device based on its DNS fqdn.
match_dns_hostname	n		y, n	Should we match a device based on its DNS hostname.
match_fqdn	y		y, n	Should we match a device based on its fqdn.
match_hostname	y		y, n	Should we match a device based only on its hostname.
match_hostname_dbus	y		y, n	Should we match a device based on its hostname and dbus id.
match_hostname_serial	y		y, n	Should we match a device based on its hostname and serial.
match_hostname_uuid	y		y, n	Should we match a device based on its hostname and UUID.
match_ip	y		y, n	Should we match a device based on its ip.
match_ip_no_data	y		y, n	Should we match a device based on its ip if we have an existing device with no data.
match_mac	y		y, n	Should we match a device based on its mac address.
match_mac_vmware	n		y, n	Should we match a device based mac address even if its a known likely duplicate from VMware.
match_serial	y		y, n	Should we match a device based on its serial number.
match_serial_type	y		y, n	Should we match a device based on its serial and type.
match_sysname	y		y, n	Should we match a device based only on its SNMP sysName.
match_sysname_serial	y		y, n	Should we match a device based only on its SNMP sysName and serial.
match_uuid	y		y, n	Should we match a device based on its UUID.
nmis	n		y, n	Enable import / export to NMIS functions.
nmis_url			<absolute url>	The web server address of NMIS.
oae_location			<filepath>	The directory into which Open-AudIT Enterprise is installed, if not the default. Unused, do not change.
oae_url	/omk/open-audit		<absolute url>	The web server address of Open-AudIT Enterprise.
output_escape_csv	y		y, n	Escape CSV output so Excel will not attempt to run contents.
page_size	1000		<integer>	The default limit of rows to retrieve.
process_netstat_windows_dns	n		y, n	Should we keep track of Windows netstat ports used by DNS above port 1000.
queue_limit	20		<integer>	The maximum number of concurrent device scans we should run.
rss_enable	y		y, n	Enable the RSS feed.
rss_url	https://community.opmantek.com/rss/OA.xml		<url>	The RSS feed URL.

MS Active Directory & OpenLDAP settings

Open-AudIT can be configured to use LDAP servers (Microsoft Active Directory and/or OpenLDAP) to authenticate and authorize a user and in addition, to create a user account in Open-AudIT using assigned roles and orgs based on LDAP group membership.

See our page on LDAP Servers for more details - LDAP_Servers