OMK Authentication Methods

Purpose

State the different authentication methods available for OMK applications.

Authentication Methods

OMK authentication methods are configured in /usr/local/omk/conf/opCommon.nmis inside the authentication hash. This entire file is a PERL hash, so be mindful of the syntax. After editing this file, a 'perl -c opCommon.nmis' will verify if the syntax is correct. For authentication method changes to take effect, the omkd service will need to be restarted.

The supported authentication methods for OMK applications are:

htpasswd

NMIS will use the users defined in the NMIS Users file, by default `/usr/local/nmis9/conf/users.dat`

The file is in the format created by the Apache htpasswd program.

htpasswd is the default authentication method for NMIS.

Key	Description	Example	Comment	
auth_htpasswd_file	Location of the password file		Default is `/usr/local/nmis9/conf/users.dat`	Not in GUI
auth_htpasswd_encrypt	Enable encrypted passwords	0/1	Default is 1. Plain text passwords are checked ONLY if value is 0 or 'plaintext'	Not in GUI

ldap and ldaps

You can choose to use ldap or ldaps (secure) you can not use both of these at the same time.

ldap

The Opmantek products will use the configured LDAP server to perform authentication.

Following are the configuration items:

Key	Description	Example	Comment

auth_ldap_server	LDAP Server Name	host[:port]	The LDAP Server Name. No defaults. Entry must be created.
auth_ldap_acc	Account Name		The LDAP account name to login to the Server. The entry must be created.
auth_ldap_psw	Account Password		The password associated with the above LDAP account. The entry must be created.
auth_ldap_context	Base Context	ou=people,dc=opmantek,dc=com	Base context to attempt to bind to.
auth_ldap_attr	Username LDAP Attributes		The LDAPs attribute(s) to match to username. Can be blank; if so, it defaults to ('uid', 'cn')
auth_ldap_privs	Use LDAP Privileges	0/1	Use LDAP for Privileges and Groups. See User Authorisation with Active Directory and LDAP. By default, set to 0 (disabled).

ldaps

The Opmantek products will use the configured LDAP (Secure) server to perform authentication.

Following are the configuration items:

Key	Description	Example	Comment
auth_ldaps_server	LDAPS Server Name	host[:port]	The LDAP Server Name. No defaults. Entry must be created.
auth_ldap_acc	Account Name		The LDAP account name to login to the Server. Entry must be created
auth_ldap_psw	Account Password		The password associated with the above LDAP account. The entry must be created.
auth_ldap_context	Base Context	ou=people,dc=opmantek,dc=com	Base context to attempt to bind to.
auth_ldap_attr	Username LDAP Attributes		The LDAPs attribute(s) to match to username. Can be blank; if so, it defaults to ('uid', 'cn')
auth_ldap_privs	Use LDAP Privileges	0/1	Use LDAP for Privileges and Groups. See User Authorisation with Active Directory and LDAP. By default, set to 0 (disabled).

ms-ldap and ms-ldaps

You can choose to use ms-ldap or ms-ldaps (secure) you can not use both of these at the same time.

ms-ldap

OMK will use the configured Microsoft Active Directory LDAP server to perform authentication.

Following are the configuration items:

Key	Description	Example	Comment
auth_ms_ldap_server	Microsoft LDAP Server Name	host[:port]	The LDAP Server Name. No defaults. Entry must be created.
auth_ms_ldap_acc	Account Name		The MS-LDAP Distinguished Name (DN)/account to login to the Server.
auth_ms_ldap_psw	Account Password		The password associated with the above MS-LDAP account. The entry must be created.
auth_ms_ldap_base	Base Context	dc=corp,dc=opmantek,dc=com	Base context to search from.
auth_ms_ldap_attr	Username LDAP Attributes	sAMAccountName	The MS-LDAP attribute(s) to match to username.
auth_ms_ldap_group	LDAP Group	Sales, SNMPSIM, GPON	Optional. The user is only allowed to log in if they are a member of the defined group. Must follow: CN=OMK Ops,CN=Users,DC=opmantek,DC=local
auth_ldap_privs	Use LDAP Privileges	0/1	Use LDAP for Privileges and Groups. See User Authorisation with Active Directory and LDAP. By default, set to 0 (disabled).
auth_ldap_group	Group LDAP Attribute	memberOf	Default is memberOf. The attribute to lookup the groups the user belongs to.

ms-ldaps

The Opmantek products will use the configured Microsoft Active Directory LDAP (Secure) server to perform authentication.

Following are the configuration items:

Key	Description	Example	Comment
auth_ms_ldaps_server	Microsoft LDAPS Server Name	host[:port]	The LDAP Server Name. No defaults. Entry must be created.
auth_ms_ldap_acc	Account Name		The MS-LDAP Distinguished Name (DN)/account to to login to the Server.
auth_ms_ldap_psw	Account Password		The password associated with the above MS-LDAP account. The entry must be created.
auth_ms_ldap_base	Base Context	dc=corp, dc=opmantek, dc=com	Base context to search from.
auth_ms_ldap_attr	Username LDAP Attributes	sAMAccountName	The MS-LDAP attribute(s) to match to username.
auth_ldap_privs	Use LDAP Privileges	0/1	Use LDAP for Privileges and Groups. See User Authorisation with Active Directory and LDAP. By default, set to 0 (disabled).
auth_ms_ldap_group	LDAP Group	Sales, SNMPSIM, GPON	Optional. The user is only allowed to log in if they are a member of the defined group. Must follow: CN=OMK Ops,CN=Users,DC=opmantek,DC=local

novell-ldap

-- Deprecated --

apache

The Opmantek products will use Apache to perform authentication and provide an authenticated user to Opmantek products with all the authorisation policies applied.

connectwise

The Opmantek products will use the ConnectWise API configured for authentication. For this, you need to setup the ConnectWise API and then setup the system to use the same authentication method using `'auth_method_1' => 'connectwise'`.

Following are the configuration items for setting up the ConnectWise API in opCommon.json (Cannot be configured in GUI):

Key	Description	Example	Comment
auth_cw_server	IP address of the ConnectWise Server	1.2.3.4	No defaults. Entry must be created.
auth_cw_company_id	The company name in ConnectWise	COMPANY	
auth_cw_public_key	The ConnectWise Public Key	xxxxxxXXXXXxxxxx	
auth_cw_private_key	The Private Key associated with the above Public Key	yyyyyYYYYYyyyyy	

crowd

The Opmantek products will use Atlassian Crowd authentication. Use Crowd to assign additional groups to a user and define each service that requires authentication as an application in Crowd.

Following are the configuration items:

Key	Description	Example	Comment
auth_crowd_server	Crowd server		
auth_crowd_user	Crowd User name	username	
auth_crowd_password	Crowd Password	password	

openaudit

Other FirstWave products can use Open-AudIT to authenticate users. See reference. Open-AudIT can use Active Directory and/or OpenLDAP for user authentication and/or authorisation. Open-AudIT will query both types of LDAP servers to validate a user's username and password and retrieve the user details (roles and orgs the user has access to). The user will be automatically created when they are authenticated.

To configure the use of openaudit authentication the following items must be configured:

Key	Description	Example	Comment
oae_server	IP address of the Open-AudIT server	1.2.3.4	The link to Open-AudIT for internal connections. Should always be the original value unless explicitly directed by Opmantek to be changed.
oae_type			Unused in on-premise installations.
oae_cloud_server	cloud server URL		Unused in on-premise installations.
omk_ua_insecure	Validation for editing remote nodes	0 or 1	Allows insecure (self-signed) SSL certificates

openid_connect

Opmantek products use OKTA's OpenID Connect for authentication. In the authentication > auth_method_1 entry of opCommon.json, use the openid_connect. For more information, see OKTA OpenID authentication.

Following are the configuration items:

Key	Description	Example	Comment
type	Authentication type	okta	The authentication type shall be "okta".
YOUR_SUBDOMAIN	URL for your subdomain	https://YOUR_SUBDOMAIN.okta.com/oauth2/default/v1/token	Replace only the text in red with your subdomain name.
password	Password	password	The password shall remain "password", since the Opmantek's internal password field is mapped to the one returned by the OKTA service.
username	User name	username	The user name shall remain "username", since the Opmantek's internal username field is mapped to the one returned by the OKTA service.
YOUR_CLIENT_ID	The client ID		Enter the client ID.
YOUR_CLIENT_SECRET	The client secret		Enter the client secret.
grant_type		password	This grant type shall be "password".
scope		openid	The scope shall be "openid".

After making the required changes, restart the omkd service.

radius

The Opmantek products will use the configured radius server (for example, Cisco ACS or Steel Belted Radius).

Following are the configuration items:

Key	Description	Example	Comment
auth_radius_server	The Radius Server Name	host:port	No defaults. Entry must be created.
auth_radius_secret	Also known as the Key	secret	

tacacs

The Opmantek products will use the configured TACACS+ server (for example, Cisco ACS).

Key	Description	Example	Comment
auth_tacacs_server	The TACACS Server Name	host:port	
auth_tacacs_secret	The Key	secret	

token

The Opmantek products support a new authentication method called `token,` which offers delegated authentication. This enables an external party to pre-authenticate a user, who can access the Opmantek products without having to log in with username and password.

Key	Description	Example	Comment
`auth_token_key`	One or more shared keys	extusr-1Kf! yVXt8TrP9zi	
`auth_token_maxage`	The maximum length of time a token will remain valid. Must be a positive number, and defines how long a token remains valid after creation (in seconds).	60	If not present, the default of 300 seconds is used.

For more information on how to generate and log in with a token, see Delegated Authentication.

Multiple Authentication Methods

You can use up to 3 authentication methods for fail back. If authentication with method 1 fails, then if they are defined, the remaining methods are tried in order. Authentication fails if they all fail. For example, if you set auth_method_1 to be LDAP and auth_method_2 to be htpasswd and login with the default NMIS credentials (and you have not changed the password), the authentication for LDAP will fail, and then htpasswd authentication with the users.dat will succeed and the NMIS user will be logged in.

Here is an example of the authentication hash inside opCommon.nmis. Remember that statements preceded by the '#' sign are 'commented out' and will not be evaluated. In this example, if ms-ldap fails, it will fail back to htpasswd.

/usr/local/omk/conf/opCommon.nmis

```
  'authentication' => {
    'auth_htpasswd_file' => '<omk_conf>/users.dat',
    'auth_htpasswd_encrypt' => 'crypt',
    'auth_method_1' => 'htpasswd',
    'auth_method_2' => '',
    'auth_method_3' => '',
    'auth_login_motd' => 'Authentication required: default credentials are nmis/nm1888',
    'auth_crowd_server' => '',
    'auth_crowd_user' => '',
    'auth_crowd_password' => '',
    'auth_sso_domain' => '',
    'auth_expire_seconds' => '3600',
    'auth_lockout_after' => 0,
    #'auth_ms_ldap_attr' => 'sAMAccountName',
    #'auth_ms_ldap_base' => 'CN=Users,DC=your_domain,DC=com',
    #'auth_ms_ldap_group' => 'CN=Users,DC=your_domain,DC=com',
    #'auth_ms_ldap_debug' => 'false',
    #'auth_ms_ldap_dn_acc' => 'CN=Administrator,CN=Users,DC=your_domain,DC=com',
    #'auth_ms_ldap_dn_psw' => 'your_administrator_password',
    #'auth_ms_ldap_server' => 'your.ip.address.here'
  },
```

Configuration of the External Authentications

In the OMK configuration, you can configure multiple methods, which are used for auth failure. Therefore, for example, if ms-ldap fails, it will fail back to htpasswd. This means, if you set auth_method_1 to be ldap and auth_method_2 to be htpasswd, and login with the default NMIS credentials (and you have not changed the password), the authentication for LDAP will fail, and then authentication with the users.dat will succeed and the user will be logged in.

It is important to change your default passwords if you expect any level of security.

Authentication methods are evaluated in sequence. The first method that returns successful authentication, terminates the authentication process. If a method returns an unsuccessful authentication, the process does not terminate, the next authentication method will be evaluated. Consider the following scenario when provisioning authentication for OMK applications.

- OMK First authentication method: LDAP
- OMK Second authentication method: htpasswd
  - User Bob has an LDAP account and has a user in the htpasswd users file.
  - User Bob leaves the company
    - The IT department removes Bob's LDAP account assuming he will no longer be able to access corporate systems.
    - Bob will still be able to access OMK applications because there is a user Bob in the htpasswd user file.

NMIS9 Notes

From NMIS9, changes will instead need to be made to the opCommon.json configuration file (located in /usr/local/omk/conf/). As we are using .json format files instead of .nmis, the format of the attributes to use is slightly different. See the examples below:

LDAP:

/usr/local/omk/conf/opCommon.json

```
"authentication" : {
   "auth_ldap_server" : "the_fqdn_of_your_ad_server:389", # you could also use an IP address here, but you need
to ensure that the LDAP/LDAPS port is added in the value, eg. 192.168.1.22:389
   "auth_ldap_acc" : "svc_omk_admin@contoso.local",
   "auth_ldap_psw" : "password_of_the_auth_ldap_acc_above",
   "auth_ldap_context" : "dc=contoso,dc=local",



},
```

LDAPS (Secure)

/usr/local/omk/conf/opCommon.json

```
"authentication" : {
   "auth_ldaps_server" : "the_fqdn_of_your_ad_server:389", # you could also use an IP address here, but you
need to ensure that the LDAP/LDAPS port is added in the value, eg. 192.168.1.22:389
   "auth_ldap_acc" : "svc_omk_admin@contoso.local",
   "auth_ldap_dn_psw" : "password_of_the_auth_ldap_acc_above",
   "auth_ldap_context" : "dc=contoso,dc=local",



},
```

TACACS:

```
"auth_tacacs_server" : "host:port",
"auth_tacacs_secret" : "secret",
```

MS-LDAP
An example of integrating your ms-ldap setup with modules such as opConfig, opEvents, opCharts etc. is below. Ensure you have also included ms-ldap as in one of the auth_methods:

/usr/local/omk/conf/opCommon.json

```
"authentication" : {
...
   "auth_ms_ldap_server" : "IP_ADDRESS_OF_YOUR_MS_LDAP_SERVER", #eg. 192.168.1.22
   "auth_ms_ldap_dn_acc" : "svc_omk_admin", #you should only need to use the username of the user here, but if
this is not successful, you can use username@domain as well.
   "auth_ms_ldap_dn_psw" : "password_of_the_dn_acc_above",
   "auth_ms_ldap_attr" : "sAMAccountName",
   "auth_ms_ldap_base" : "OU=Network Admins,DC=contoso,DC=local",
...


},
```

MS-LDAPS (Secure)

/usr/local/omk/conf/opCommon.json

```
"authentication" : {
...
   "auth_ms_ldaps_server" : "IP_ADDRESS_OF_YOUR_MS_LDAPS_SERVER", #eg. 192.168.1.23
   "auth_ms_ldap_dn_acc" : "svc_omk_admin", #you should only need to use the username of the user here, but if
this is not successful, you can use username@domain as well.
   "auth_ms_ldap_dn_psw" : "password_of_the_dn_acc_above",
   "auth_ms_ldap_attr" : "sAMAccountName",
   "auth_ms_ldap_base" : "OU=Network Admins,DC=contoso,DC=local",
...


},
```

RADIUS

```
"auth_radius_server" : "host:port",
"auth_radius_secret" : "secret",
```

Once you have saved the updated opCommon.json configuration, you will then need to restart the omkd daemon.

Troubleshooting

If you are experiencing issues with configuring your external authentication method, extra debug can be enabled to assist.

Depending on the authentication method you are using, the following two attributes can be added to your opCommon.json. This should cover most, if not all of our authentication methods to debug.

/usr/local/omk/conf/opCommon.json

```
"authentication" : {
...
        "auth_debug" : 1,
        "auth_ldap_debug" : "true"
...

},
```

Save the file once you have added these two extra lines and restart omkd. Repeat the authentication process again, then review auth.log (located in the /usr/local/omk/log directory) and troubleshoot.

Related Topics

- User Management in NMIS8
- User Authorisation with Active Directory and LDAP
- OKTA OpenID authentication