This PDF is generated from authoritative online content, and is provided for convenience only. This PDF cannot be used for legal purposes. For authoritative understanding of what is and is not supported, always use the online content. To copy code samples, always use the online content.

Configurations Options Reference Manual

[snmp] Section

5/9/2025

Contents

[snmp] Section

Options in this section define SNMP-related parameters, as for SNMPv1/v2 and for SNMPv3. Because of the differences in security implementation for different versions of SNMP, some options control access to Genesys MIB (management information base) objects via SNMPv1/v2 requests and others control access to Genesys MIB objects via SNMPv3 requests.

This section must be called **snmp**.

Use the following options to configure SNMPv1/v2 access:

- read_community
- write_community

These configuration options do not control access to MIB objects via SNMPv3 requests.

Use the following options to configure SNMPv3 access:

- v3_username
- v3auth_password
- v3priv_password
- v3auth_protocol
- v3priv_protocol
- password (in section **snmp-v3-auth**)
- password (in section **snmp-v3-priv**)

These configuration options do not control access to MIB objects via SNMPv1/v2 requests.

> Important
>
> If you do not configure the **snmp** section or any of its options, Genesys SNMP Master Agent provides access in SNMPv3 mode, with the default settings as described in this section. Access in SNMPv1/SNMPv2 mode is denied.

read_community

Default Value: No default value
Valid Values: Any valid community name
Changes Take Effect: After restart

Specifies the SNMP community name that Genesys SNMP Master Agent uses to authenticate SNMPv1/v2c GET and GET NEXT requests. That is, Read permissions for all Genesys MIB objects are granted to the specified community. If you do not configure the option or don't set its value, this **write_community** option controls SNMPv1/v2 Read access.

trap_target

Default Value: No default value
Valid Values: A list of any number of SNMP trap targets, separated by commas, in the following format:
`<host name>/<port number>:<community name>`
Changes Take Effect: After restart

Specifies where Genesys SNMP Master Agent sends trap notifications. You can specify a host IP address instead of a hostname. If you do not specify a community name, Genesys SNMP Master Agent sends trap notifications to the `public` community.

For example:
`host1/162:public_t1, 127.0.0.1/163:public_t2`

v3_username

Default Value: `default`
Valid Values:

`default`	
`<string>`	User name

Changes Take Effect: After restart

Specifies the user name used for issuing SNMPv3 requests. Genesys SNMP Master Agent does not accept SNMPv3 requests other users may send. A user with the specified user name receives:

- Read permissions for all Genesys MIB objects.
- Write permissions for all Genesys MIB objects except for the objects in the VACM and USM MIB files. Genesys SNMP Master Agent excludes VACM and USM MIB objects from the group of writable objects to prevent remote NMS users from changing security attributes.

The user should send SNMPv3 requests for the default (empty) context.

v3auth_password

Default Value: No default value
Valid Values: Any valid password
Changes Take Effect: After restart

Specifies the SNMPv3 user password used for authentication.

Warning

- The password specified by this option is visible in Genesys Administrator, and is not encrypted in the Configuration Database.
- To hide the password in the interface and encrypt it in the database, use the **password** option in the **[snmp-v3-auth]** section instead of this option.
- Do not use both of these options in the same SNMP Master Agent.

v3auth_protocol

Default Value: none
Valid Values:

`MD5`	HMAC-MD5-96 authentication protocol
`SHA`	HMAC-SHA5-96 authentication protocol
none	No authentication

Changes Take Effect: After restart

Specifies the authentication protocol, if any, to authenticate messages sent or received on behalf of this user. If you do not configure the option, do not set its value, or set it to an invalid value, Genesys SNMP Master Agent uses no authentication.

v3priv_password

Default Value: No default value
Valid Values: Any valid password
Changes Take Effect: After restart

Specifies the SNMPv3 user password used for the privacy of data.

Warning

- The password specified by this option is visible in Genesys Administrator, and is not encrypted in the Configuration Database.
- To hide the password in the interface and encrypt it in the database, use the **password** option in the **[snmp-v3-priv]** section instead of this option.
- Do not use both of these options in the same SNMP Master Agent.

v3priv_protocol

Default Value: none
Valid Values:

none	No encryption
DES	CBC-DES privacy protocol

Changes Take Effect: After restart

Specifies whether encryption is used for SNMPv3 messages sent or received on behalf of this user and, if so, using which privacy protocol. This option applies only if the **v3auth_protocol** option is set to a valid value other than none. If you do not configure the **v3auth_protocol** option, do not set its value, or set it to an invalid value, Genesys SNMP Master Agent uses no encryption.

write_community

Default Value: No default value
Valid Values: Any valid community name
Changes Take Effect: After restart

Specifies the SNMP community name that Genesys SNMP Master Agent uses to authenticate SNMPv1/v2c SET, GET, and GET NEXT requests. That is, the specified community receives:

- Read permissions for all Genesys MIB objects.
- Write permissions for all Genesys MIB objects except for the objects in the VACM and USM MIB files. Genesys SNMP Master Agent excludes VACM and USM MIB objects from the group of writable objects to prevent remote NMS users from changing security attributes.

If you do not configure the option or set its value, no SNMPv1/v2 Write access is allowed.