



Model Based AAA

The NETCONF and RESTCONF interfaces implement the NETCONF Access Control Model (NACM). NACM is a form of role-based access control (RBAC) specified in RFC 6536.

- [Feature Overview, on page 1](#)
- [Prerequisites for Model Based AAA, on page 1](#)
- [Initial Operation, on page 1](#)
- [NACM Configuration Management and Persistence, on page 2](#)
- [Overview of Configuring NACM, on page 3](#)
- [Disabling NACM, on page 6](#)

Feature Overview

The NETCONF protocol does not provide any standard mechanisms to restrict the protocol operations and content that each user is authorized to access. NACM is defined in AAA subsystem to manage access-control for NETCONF/YANG RPC requests.

Prerequisites for Model Based AAA

Working with the model based AAA feature requires prior understanding of the following :

- NETCONF-YANG
- RFC 6536: Network Configuration Protocol (NETCONF) Access Control Model

Initial Operation

These are the NACM default values. By default a user is denied write permission, hence you'll not be able to edit the NACM configurations after enabling NACM authorization using AAA command.

```
<enable-nacm>true</enable-nacm>
<read-default>permit</read-default>
<write-default>deny</write-default>
<exec-default>permit</exec-default>
<enable-external-groups>true</enable-external-groups>
```

Therefore we recommend to enable NACM after configuring the required NACM configurations, or after changing the default NACM configurations. Here are few sample configurations:



Note If an user gets access-denied message while writing NACM configurations, then NACM authorization can be disabled to edit the NACM configurations.

```
<aaa xmlns="http://cisco.com/ns/yang/Cisco-IOS-XR-aaa-lib-cfg">
<usernames xmlns="http://cisco.com/ns/yang/Cisco-IOS-XR-aaa-locald-cfg">
<username>
<ordering-index>3</ordering-index>
<name>username</name>
<password>password</password>
  <usergroup-under-usernames>
    <usergroup-under-username>
      <name>root-lr</name>
    </usergroup-under-username>
    <usergroup-under-username>
      <name>cisco-support</name>
    </usergroup-under-username>
  </usergroup-under-usernames>
</username>
</usernames>
</aaa>

<nacm xmlns="http://cisco.com/ns/yang/Cisco-IOS-XR-aaa-nacm-cfg">
<read-default>permit</read-default>
<write-default>permit</write-default>
<exec-default>permit</exec-default>
<enable-external-groups>true</enable-external-groups>
<groups>
  <group>
    <name>nacm_group</name>
    <user-name>lab</user-name>
  </group>
</groups>
<rule-list>
<name>Rule-list-1</name>
<group>Group_nacm_0_test</group>
<rule>
  <name>Rule-1</name>
  <access-operations>read</access-operations>
  <action>permit</action>
  <module-name>ietf-netconf-acm</module-name>
  <rpc-name>edit-config</rpc-name>
    <access-operations>*</access-operations>
    <path>/</path>
    <action>permit</action>
  </rule>
</rule-list>
</nacm>
```

NACM Configuration Management and Persistence

The NACM configuration can be modified using NETCONF or RESTCONF. In order for a user to be able to access the NACM configuration, they must have explicit permission to do so, that is, through a NACM rule. Configuration under the /nacm subtree persists when the **copy running-config startup-config EXEC** command is issued, or the **cisco-ia:save-config** RPC is issued.

```
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<save-config xmlns="http://cisco.com/yang/cisco-ia"/>
</rpc>
```

Overview of Configuring NACM

Here are the steps involved in configuring NACM:

1. Configure all NACM rules
2. Enable NACM
3. Disconnect all active NETCONF sessions
4. Launch new NETCONF session



Note Enabling or disabling NACM doesn't affect any existing NETCONF sessions.

NACM Rules

As per the RFC 6536, NACM defines two categories of rules:

- Global Rules—It includes the following:
 - Enable/Disable NACM
 - Read-Default
 - Write-Default
 - Exec-Default
 - Enable external Groups
- Access Control Rules—It includes the following:
 - Module (used along with protocol rule / data node rule)
 - Protocol
 - Data Node

Configuring Global Rules

You must configure NACM groups and NACM rulelist before configuring NACM rules.

The following sample configuration shows a NACM group configuration:

```
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" >
<edit-config>
  <target><candidate/></target>
<config xmlns:xc="urn:ietf:params:xml:ns:netconf:base:1.0">
  <nacm xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-acm">
    <groups>
```

```

    <group>
      <name>group1</name>
      <user-name>user1</user-name>
      <user-name>user2</user-name>
      <user-name>user3</user-name>
    </group>
  </groups>
</nacm>
</config>
</edit-config>
</rpc>

```

The following sample configuration shows a NACM rulelist configuration:

```

<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" >
<edit-config>
<target><candidate/></target>
<config xmlns:xc="urn:ietf:params:xml:ns:netconf:base:1.0">
  <nacm xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-acm">
    <rule-list>
      <name>rulelist-1</name>
      <group>root-lr</group>
      <group>group1</group>
      <group>group2</group>
    </rule-list>
  </nacm>
</config>
</edit-config>
</rpc>

```

This is the sample for configuring the NACM global rules:

```

<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" >
<edit-config>
  <target><candidate/></target>
<config xmlns:xc="urn:ietf:params:xml:ns:netconf:base:1.0">
  <nacm xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-acm">
    <read-default>permit</read-default>
    <write-default>permit</write-default>
    <exec-default>permit</exec-default>
    <enable-external-groups>>false</enable-external-groups>
  </nacm>
</config>
</edit-config>
</rpc>

```

Configuring Access Control Rules

This is the sample configuration for the NACM protocol rules:

```

<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" >
<edit-config>
<target><candidate/></target>
<config xmlns:xc="urn:ietf:params:xml:ns:netconf:base:1.0">
  <nacm xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-acm">
    <rule-list>
      <name>rulelist-1</name>
      <rule>
        <name>rule1</name>
        <module-name>ietf-netconf-acm</module-name>
        <rpc-name>edit-config</rpc-name>
        <access-operations>*</access-operations>
        <action>permit</action>
      </rule>
    </rule-list>
  </nacm>
</config>
</edit-config>
</rpc>

```

```

    </rule>
  <rule>
    <name>rule2</name>
    <module-name>ietf-netconf-acm</module-name>
    <rpc-name>get-config</rpc-name>
    <access-operations>create read update exec</access-operations>
    <action>permit</action>
  </rule>
</rule-list>
</nacm>
</config>
</edit-config>
</rpc>

```



Note '*' refers to all operations.

This is the sample configuration for the NACM data node rules:

```

<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" >
<edit-config>
<target><candidate/></target>
<config xmlns:xc="urn:ietf:params:xml:ns:netconf:base:1.0">
  <nacm xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-acm">
    <rule-list>
      <name>rulelist-2</name>
      <rule>
        <name>rule4</name>
        <module-name>*</module-name>
        <path>/nacm/groups/group</path>
        <access-operations>*</access-operations>
        <action>permit</action>
      </rule>
      <rule>
        <name>rule5</name>
        <module-name>ietf-netconf-acm</module-name>
        <path>/nacm/rule-list</path>
        <access-operations>read</access-operations>
        <action>deny</action>
      </rule>
    </rule-list>
  </nacm>
</config>
</edit-config>
</rpc>

```



Note '*' refers to all modules, and all operations.

Enabling NACM

To enable NACM, use the **aaa authorization nacm default local** command in configuration mode:

```
Router(config)#aaa authorization nacm default local
```

Verification

Use the **show nacm summary** command to verify the default values after enabling NACM:

```
Router# show nacm summary
Mon Jan 15 16:47:43.549 UTC
NACM SUMMARY
-----
Enable Nacm : True
Enable External Groups : True
Number of Groups : 0
Number of Users : 0
Number of Rules : 0
Number of Rulelist : 0
Default Read : permit
Default Write : deny
Default Exec : permit
Denied Operations : 0
Denied Data Writes : 0
Denied Notifications : 0
```

Verify the NACM Configurations

Use the **show nacm summary** command to verify the NACM configurations:

```
Router# show nacm summary
Mon Jan 15 17:02:46.696 UTC
NACM SUMMARY
-----
Enable Nacm : True
Enable External Groups : True
Number of Groups : 3
Number of Users : 3
Number of Rules : 4
Number of Rulelist : 2
Default Read : permit
Default Write : permit
Default Exec : permit
Denied Operations : 1
Denied Data Writes : 0
Denied Notifications : 0
-----
```

Disabling NACM

There are two ways you can disable NACM:

1. Configuring NACM authorization as none:

```
Router(config)# aaa authorization nacm default none
```

2. Using no form of AAA authorization command:

```
(config)# no aaa authorization nacm default
```

Verification

Use the **show nacm summary** command to verify the default values after disabling NACM:

```
Router# show nacm summary
```

```
Mon Jan 15 17:02:46.696 UTC
```

```
NACM SUMMARY
```

```
-----  
Enable Nacm : False
```

```
Enable External Groups : True
```

```
Number of Groups : 0
```

```
Number of Users : 0
```

```
Number of Rules : 0
```

```
Number of Rulelist : 0
```

```
Default Read : permit
```

```
Default Write : deny
```

```
Default Exec : permit
```

```
Denied Operations : 0
```

```
Denied Data Writes : 0
```

```
Denied Notifications : 0
```

