



---

# Secure Access

## DMI Solution Guide

Release



Published: 2010-06-08  
Part Number: , Revision 1

Juniper Networks, Inc.  
1194 North Mathilda Avenue  
Sunnyvale, California 94089  
USA  
408-745-2000  
www.juniper.net

This product includes the Envoy SNMP Engine, developed by Epilogue Technology, an Integrated Systems Company. Copyright © 1986–1997, Epilogue Technology Corporation. All rights reserved. This program and its documentation were developed at private expense, and no part of them is in the public domain.

This product includes memory allocation software developed by Mark Moraes, copyright © 1988, 1989, 1993, University of Toronto.

This product includes FreeBSD software developed by the University of California, Berkeley, and its contributors. All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is copyrighted by the Regents of the University of California. Copyright © 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994. The Regents of the University of California. All rights reserved.

GateD software copyright © 1995, the Regents of the University. All rights reserved. Gate Daemon was originated and developed through release 3.0 by Cornell University and its collaborators. Gated is based on Kirton's EGP, UC Berkeley's routing daemon (routed), and DCN's HELLO routing protocol. Development of Gated has been supported in part by the National Science Foundation. Portions of the GateD software copyright © 1988, Regents of the University of California. All rights reserved. Portions of the GateD software copyright © 1991, D. L. S. Associates.

This product includes software developed by Maker Communications, Inc., copyright © 1996, 1997, Maker Communications, Inc.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

### *Secure Access DMI Solution Guide*

Revision History  
2010—Revised for SA release 7.0.

The information in this document is current as of the date listed in the revision history.

## END USER LICENSE AGREEMENT

**READ THIS END USER LICENSE AGREEMENT (“AGREEMENT”) BEFORE DOWNLOADING, INSTALLING, OR USING THE SOFTWARE.** BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE OR OTHERWISE EXPRESSING YOUR AGREEMENT TO THE TERMS CONTAINED HEREIN, YOU (AS CUSTOMER OR IF YOU ARE NOT THE CUSTOMER, AS A REPRESENTATIVE/AGENT AUTHORIZED TO BIND THE CUSTOMER) CONSENT TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT OR CANNOT AGREE TO THE TERMS CONTAINED HEREIN, THEN (A) DO NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND (B) YOU MAY CONTACT JUNIPER NETWORKS REGARDING LICENSE TERMS.

1. **The Parties.** The parties to this Agreement are (i) Juniper Networks, Inc. (if the Customer’s principal office is located in the Americas) or Juniper Networks (Cayman) Limited (if the Customer’s principal office is located outside the Americas) (such applicable entity being referred to herein as “Juniper”), and (ii) the person or organization that originally purchased from Juniper or an authorized Juniper reseller the applicable license(s) for use of the Software (“Customer”) (collectively, the “Parties”).

2. **The Software.** In this Agreement, “Software” means the program modules and features of the Juniper or Juniper-supplied software, for which Customer has paid the applicable license or support fees to Juniper or an authorized Juniper reseller, or which was embedded by Juniper in equipment which Customer purchased from Juniper or an authorized Juniper reseller. “Software” also includes updates, upgrades and new releases of such software. “Embedded Software” means Software which Juniper has embedded in or loaded onto the Juniper equipment and any updates, upgrades, additions or replacements which are subsequently embedded in or loaded onto the equipment.

3. **License Grant.** Subject to payment of the applicable fees and the limitations and restrictions set forth herein, Juniper grants to Customer a non-exclusive and non-transferable license, without right to sublicense, to use the Software, in executable form only, subject to the following use restrictions:

a. Customer shall use Embedded Software solely as embedded in, and for execution on, Juniper equipment originally purchased by Customer from Juniper or an authorized Juniper reseller.

b. Customer shall use the Software on a single hardware chassis having a single processing unit, or as many chassis or processing units for which Customer has paid the applicable license fees; provided, however, with respect to the Steel-Belted Radius or Odyssey Access Client software only, Customer shall use such Software on a single computer containing a single physical random access memory space and containing any number of processors. Use of the Steel-Belted Radius or IMS AAA software on multiple computers or virtual machines (e.g., Solaris zones) requires multiple licenses, regardless of whether such computers or virtualizations are physically contained on a single chassis.

c. Product purchase documents, paper or electronic user documentation, and/or the particular licenses purchased by Customer may specify limits to Customer’s use of the Software. Such limits may restrict use to a maximum number of seats, registered endpoints, concurrent users, sessions, calls, connections, subscribers, clusters, nodes, realms, devices, links, ports or transactions, or require the purchase of separate licenses to use particular features, functionalities, services, applications, operations, or capabilities, or provide throughput, performance, configuration, bandwidth, interface, processing, temporal, or geographical limits. In addition, such limits may restrict the use of the Software to managing certain kinds of networks or require the Software to be used only in conjunction with other specific Software. Customer’s use of the Software shall be subject to all such limitations and purchase of all applicable licenses.

d. For any trial copy of the Software, Customer’s right to use the Software expires 30 days after download, installation or use of the Software. Customer may operate the Software after the 30-day trial period only if Customer pays for a license to do so. Customer may not extend or create an additional trial period by re-installing the Software after the 30-day trial period.

e. The Global Enterprise Edition of the Steel-Belted Radius software may be used by Customer only to manage access to Customer’s enterprise network. Specifically, service provider customers are expressly prohibited from using the Global Enterprise Edition of the Steel-Belted Radius software to support any commercial network access services.

The foregoing license is not transferable or assignable by Customer. No license is granted herein to any user who did not originally purchase the applicable license(s) for the Software from Juniper or an authorized Juniper reseller.

4. **Use Prohibitions.** Notwithstanding the foregoing, the license provided herein does not permit the Customer to, and Customer agrees not to and shall not: (a) modify, unbundle, reverse engineer, or create derivative works based on the Software; (b) make unauthorized copies of the Software (except as necessary for backup purposes); (c) rent, sell, transfer, or grant any rights in and to any copy of the Software, in any form, to any third party; (d) remove any proprietary notices, labels, or marks on or in any copy of the Software or any product in which the Software is embedded; (e) distribute any copy of the Software to any third party, including as may be embedded in Juniper equipment sold in the secondhand market; (f) use any ‘locked’ or key-restricted feature, function, service, application, operation, or capability without first purchasing the applicable license(s) and obtaining a valid key from Juniper, even if such feature, function, service, application, operation, or capability is enabled without a key; (g) distribute any key for the Software provided by Juniper to any third party; (h) use the

Software in any manner that extends or is broader than the uses purchased by Customer from Juniper or an authorized Juniper reseller; (i) use Embedded Software on non-Juniper equipment; (j) use Embedded Software (or make it available for use) on Juniper equipment that the Customer did not originally purchase from Juniper or an authorized Juniper reseller; (k) disclose the results of testing or benchmarking of the Software to any third party without the prior written consent of Juniper; or (l) use the Software in any manner other than as expressly provided herein.

5. **Audit.** Customer shall maintain accurate records as necessary to verify compliance with this Agreement. Upon request by Juniper, Customer shall furnish such records to Juniper and certify its compliance with this Agreement.

6. **Confidentiality.** The Parties agree that aspects of the Software and associated documentation are the confidential property of Juniper. As such, Customer shall exercise all reasonable commercial efforts to maintain the Software and associated documentation in confidence, which at a minimum includes restricting access to the Software to Customer employees and contractors having a need to use the Software for Customer's internal business purposes.

7. **Ownership.** Juniper and Juniper's licensors, respectively, retain ownership of all right, title, and interest (including copyright) in and to the Software, associated documentation, and all copies of the Software. Nothing in this Agreement constitutes a transfer or conveyance of any right, title, or interest in the Software or associated documentation, or a sale of the Software, associated documentation, or copies of the Software.

8. **Warranty, Limitation of Liability, Disclaimer of Warranty.** The warranty applicable to the Software shall be as set forth in the warranty statement that accompanies the Software (the "Warranty Statement"). Nothing in this Agreement shall give rise to any obligation to support the Software. Support services may be purchased separately. Any such support shall be governed by a separate, written support services agreement. TO THE MAXIMUM EXTENT PERMITTED BY LAW, JUNIPER SHALL NOT BE LIABLE FOR ANY LOST PROFITS, LOSS OF DATA, OR COSTS OR PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THIS AGREEMENT, THE SOFTWARE, OR ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. IN NO EVENT SHALL JUNIPER BE LIABLE FOR DAMAGES ARISING FROM UNAUTHORIZED OR IMPROPER USE OF ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. EXCEPT AS EXPRESSLY PROVIDED IN THE WARRANTY STATEMENT TO THE EXTENT PERMITTED BY LAW, JUNIPER DISCLAIMS ANY AND ALL WARRANTIES IN AND TO THE SOFTWARE (WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE), INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT DOES JUNIPER WARRANT THAT THE SOFTWARE, OR ANY EQUIPMENT OR NETWORK RUNNING THE SOFTWARE, WILL OPERATE WITHOUT ERROR OR INTERRUPTION, OR WILL BE FREE OF VULNERABILITY TO INTRUSION OR ATTACK. In no event shall Juniper's or its suppliers' or licensors' liability to Customer, whether in contract, tort (including negligence), breach of warranty, or otherwise, exceed the price paid by Customer for the Software that gave rise to the claim, or if the Software is embedded in another Juniper product, the price paid by Customer for such other product. Customer acknowledges and agrees that Juniper has set its prices and entered into this Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the Parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the Parties.

9. **Termination.** Any breach of this Agreement or failure by Customer to pay any applicable fees due shall result in automatic termination of the license granted herein. Upon such termination, Customer shall destroy or return to Juniper all copies of the Software and related documentation in Customer's possession or control.

10. **Taxes.** All license fees payable under this agreement are exclusive of tax. Customer shall be responsible for paying Taxes arising from the purchase of the license, or importation or use of the Software. If applicable, valid exemption documentation for each taxing jurisdiction shall be provided to Juniper prior to invoicing, and Customer shall promptly notify Juniper if their exemption is revoked or modified. All payments made by Customer shall be net of any applicable withholding tax. Customer will provide reasonable assistance to Juniper in connection with such withholding taxes by promptly: providing Juniper with valid tax receipts and other required documentation showing Customer's payment of any withholding taxes; completing appropriate applications that would reduce the amount of withholding tax to be paid; and notifying and assisting Juniper in any audit or tax proceeding related to transactions hereunder. Customer shall comply with all applicable tax laws and regulations, and Customer will promptly pay or reimburse Juniper for all costs and damages related to any liability incurred by Juniper as a result of Customer's non-compliance or delay with its responsibilities herein. Customer's obligations under this Section shall survive termination or expiration of this Agreement.

11. **Export.** Customer agrees to comply with all applicable export laws and restrictions and regulations of any United States and any applicable foreign agency or authority, and not to export or re-export the Software or any direct product thereof in violation of any such restrictions, laws or regulations, or without all necessary approvals. Customer shall be liable for any such violations. The version of the Software supplied to Customer may contain encryption or other capabilities restricting Customer's ability to export the Software without an export license.

12. **Commercial Computer Software.** The Software is "commercial computer software" and is provided with restricted rights. Use, duplication, or disclosure by the United States government is subject to restrictions set forth in this Agreement and as provided in DFARS 227.7201 through 227.7202-4, FAR 12.212, FAR 27.405(b)(2), FAR 52.227-19, or FAR 52.227-14 (ALT III) as applicable.

13. **Interface Information.** To the extent required by applicable law, and at Customer's written request, Juniper shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Juniper makes such information available.

14. **Third Party Software.** Any licensor of Juniper whose software is embedded in the Software and any supplier of Juniper whose products or technology are embedded in (or services are accessed by) the Software shall be a third party beneficiary with respect to this Agreement, and such licensor or vendor shall have the right to enforce this Agreement in its own name as if it were Juniper. In addition, certain third party software may be provided with the Software and is subject to the accompanying license(s), if any, of its respective owner(s). To the extent portions of the Software are distributed under and subject to open source licenses obligating Juniper to make the source code for such portions publicly available (such as the GNU General Public License ("GPL") or the GNU Library General Public License ("LGPL")), Juniper will make such source code portions (including Juniper modifications, as appropriate) available upon request for a period of up to three years from the date of distribution. Such request can be made in writing to Juniper Networks, Inc., 1194 N. Mathilda Ave., Sunnyvale, CA 94089, ATTN: General Counsel. You may obtain a copy of the GPL at <http://www.gnu.org/licenses/gpl.html>, and a copy of the LGPL at <http://www.gnu.org/licenses/lgpl.html>.

15. **Miscellaneous.** This Agreement shall be governed by the laws of the State of California without reference to its conflicts of laws principles. The provisions of the U.N. Convention for the International Sale of Goods shall not apply to this Agreement. For any disputes arising under this Agreement, the Parties hereby consent to the personal and exclusive jurisdiction of, and venue in, the state and federal courts within Santa Clara County, California. This Agreement constitutes the entire and sole agreement between Juniper and the Customer with respect to the Software, and supersedes all prior and contemporaneous agreements relating to the Software, whether oral or written (including any inconsistent terms contained in a purchase order), except that the terms of a separate written agreement executed by an authorized Juniper representative and Customer shall govern to the extent such terms are inconsistent or conflict with terms contained herein. No modification to this Agreement nor any waiver of any rights hereunder shall be effective unless expressly assented to in writing by the party to be charged. If any portion of this Agreement is held invalid, the Parties agree that such invalidity shall not affect the validity of the remainder of this Agreement. This Agreement and associated documentation has been written in the English language, and the Parties agree that the English version will govern. (For Canada: Les parties aux présentes confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s'y rattache, soient rédigés en langue anglaise. (Translation: The parties confirm that this Agreement and all related documentation is and will be in the English language)).

# Front Part

- Related Documentation on page xiii
- Document Conventions on page xiii
- Requesting Technical Support on page xiv

## Related Documentation

---


- To download a PDF version of the Secure Access Administration Guide, go to the Secure Access/SSL VPN Product Documentation page of the Juniper Networks Customer Support Center.
- For information about the changes that Secure Access clients make to client computers, including installed files and registry changes, and for information about the rights required to install and run Secure Access clients, refer to the Client-side Changes Guide.
- For information on how to personalize the look-and-feel of the pre-authentication, password management, and Secure Meeting pages that Secure Access displays to end-users and administrators, refer to the Custom Sign-In Pages Solution Guide.

## Document Conventions

---

Table 1 on page xiii defines notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.

## Requesting Technical Support

---

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the JTAC User Guide located at <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf> .
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/> .
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

## Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://www.juniper.net/alerts/>
- Join and participate in the Juniper Networks Community Forum: <http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://tools.juniper.net/SerialNumberEntitlementSearch/>

## Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at <http://www.juniper.net/cm/> .
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <http://www.juniper.net/support/requesting-support.html> .



## Table of Contents

Table of Contents.....	2
Introduction .....	4
Related Information.....	4
Inbound DMI.....	5
Host System and Logical Systems .....	6
Device Specific RPCs.....	7
create-logical-system .....	8
delete-logical-system .....	18
get-user-stats .....	20
get-failed-login-count .....	23
get-role-count.....	25
get-resource-profile-count.....	27
get-vlan-throughput.....	29
get-ivs-throughput.....	32
get-rollback-partition-information .....	34
validate-custom-expression .....	36
get-active-users .....	39
disable-all-users.....	45
enable-all-users .....	46
delete-active-sessions .....	47
refresh-roles .....	52
add-certificate .....	52
get-certificate-info .....	57
get-staged-package-information.....	69
IVE Schema .....	72
Sample Code .....	73
Get DMI Agent Configuration .....	73
Configure DMI Agent .....	74
Get Client Types .....	75
Add Client Type .....	76
Get Network Configuration .....	77
Configure Network Settings.....	78
Create a Realm.....	79
Create a Realm in Logical System .....	82
Delete a Realm .....	84
Create a Role.....	85
Create a Role in Logical System .....	90
Delete a Role .....	96
Create a Resource Profile .....	97
Create a Resource Profile in Logical System.....	98
Delete a Resource Profile.....	98
Create a Resource Policy.....	99
Create a Resource Policy in Logical System .....	100
Delete a Resource Policy .....	101
Create a Web Bookmark for a Role .....	101
Create a Web Bookmark for a Role in Logical System.....	102
Delete a Web Bookmark for a Role.....	103

Get Syslog Events .....	104
Configure License Client Settings .....	105
Error conditions.....	107
References.....	108

## Introduction

---

The Device Management Interface (DMI) is an XML-RPC-based protocol used to manage Juniper devices. The protocol allows administrators and third-party applications to configure and manage Juniper devices bypassing their native interfaces. The Juniper Secure Access product, with IVE version 6.4, is compliant with DMI v1.3 specification. The readers of this document are urged to read the DMI specification before using this guide.

**IMPORTANT:** This feature is geared toward service providers. Juniper Networks Technical Support does not offer developer support for this feature. If you require assistance, contact your Juniper Networks account team.

DMI clients can be stand-alone applications, or can be embedded in larger applications, such as network management solutions and service provider OSS's. DMI clients can connect to the IVE in one of two ways: inbound and outbound. Inbound connection is initiated into the device by the client, while outbound connection is initiated by the device into an always-available application hosting a DMI client. Juniper's NSM product uses the outbound connection.

The DMI inbound and outbound connection features in the IVE enable the IVE administrator to connect to and manage the system without having to use the browser as the administrator's interface to the IVE. IVE version 6.3 supported the outbound connection type. 6.4 introduces support for the inbound connection type.

With the new inbound DMI feature, the administrator can now connect to the IVE using an SSH secure shell Command Line Interface (CLI) to manage the device. The IVE can also be managed by integrating any SSH-aware, netconf<sup>1</sup> supporting application by programming the application to comply with DMI version 1.3. More information about DMI is available in the DMI specification document<sup>2</sup>.

This document serves as a reference guide for achieving the following tasks in IVE:

- Configuring the inbound DMI agent
- Issuing RPC requests to retrieve the configuration of the device
- Issuing RPC requests to configure the device
- Issuing RPC requests to receive real time logs and alerts from the device
- Issuing IVE specific RPCs to get state parameter data from the device
- Issuing RPC requests for software image management
- Issuing RPC requests to backup/restore device configuration

## Related Information

---

In addition to this guide, the following should be referred to, while administering the IVE using inbound DMI connection.

- ◆ DMI specification document<sup>2</sup>
  - The specification document for the Juniper-wide Device Management Interface
- ◆ IVE Schema

- The XML configuration schema of the IVE. More information about the schema is available in the later part of this document
- ◆ Juniper Update repository
  - The repository contains the common schema of all DMI compliant devices and the main configuration schema of IVE. For each release of the product, the schema is updated in the repository. More information about the repository can be found in section 5.7.2 of DMI specification document.
- ◆ RFC 4741: NETCONF Configuration Protocol<sup>1</sup>
  - The protocol specification RFC document of NETCONF, the protocol that is used extensively by DMI.

## Inbound DMI

---

The inbound DMI connection is available to the administrator of the root IVS in the IVE. The base license for the IVE will enable DMI Agent configuration option available.

Once the base license is installed, the DMI agent in the IVE can be configured in the DMI Agent page under the Configuration menu. The page can be used to configure both inbound and outbound DMI agent.

To enable the inbound DMI agent, the following needs to be configured:

- ◆ The network interface on which the inbound agent should be enabled
- ◆ The TCP port on which the inbound agent should accept connections
- ◆ The administrator realm to be used for authenticating the inbound DMI users

While the internal interface is available for all SA devices, the management interface is available for inbound in the SA6000 and SA6500 devices. The TCP port needs to be a valid value between 1 and 65535 and it is important that the port configured is not used by any other process in the IVE. It is recommended that either the default value or a value higher than 1024 be used for the TCP port. The default choice for the interface is the internal interface and the default value for the TCP port is 22.

DMI uses SSH protocol for communication<sup>1</sup>. To connect to the IVE using inbound connection, the standard SSH shell<sup>2</sup> can be used as the command line interface. For a better user experience, a simple client can be built around the standard SSH client. Since netconf protocol is used by DMI, while connecting to the IVE using inbound, netconf channel needs to be specified as a parameter in the `ssh` command.

The following command invokes ssh to connect to the IVE's inbound DMI agent

```
ssh -l <user> <ip address> -p <port> -s netconf
```

The `-s` parameter tells the ssh server to use the netconf channel for this connection. DMI relies on the Netconf protocol for managing device configurations.

After the user is authenticated, the IVE responds with “system:” capability string to the client. The SSH client displays this to the user. At this point, the user can execute RPC commands to configure, manage and get information from the IVE. The standard schema for the RPCs and the schema for the RPC-replies are elaborated in the DMI specification document.

To close the inbound session, close-session RPC can be used. More information about close-session RPC is available in section 7.8 of NETCONF Configuration Protocol RFC<sup>1</sup>

## Host System and Logical Systems

---

For DMI purposes, the root IVS system is called the “host system” and virtual systems are called “logical systems”. The connection is said to be either in the host system context or in the logical system context. Some RPCs are available in both contexts, while others are available only in host system context. The following table lists the standard (ie, non-product-specific) DMI RPCs and the contexts in which they are available.

DMI RPC	Host System	Logical System
get-system-information	✓	✗
get-cluster-information	✓	✗
get-hardware-inventory	✓	✗
get-software-inventory	✓	✗
get-license-inventory	✓	✗
edit-config	✓	✗
get-config	✓	✗
get-configuration-information	✓	✓
get-alarm-information	✓	✗
get-syslog-events	✓	✓
set-logical-system	✓	✓
clear-logical-system	✓	✓
get-logical-system-information	✓	✗
request-package-add	✓	✗
request-reboot	✓	✗
backup	✓	✗
restore	✓	✗

The DMI specification document describes the schema for the standard DMI RPCs and their replies. The *Sample Code* section contains examples of some of the RPCs listed in the table.

## Device Specific RPCs

---

DMI also allows products to define their own non-standard RPCs, called device-specific RPC's. IVE makes use of this option and supports a set of Remote Procedure Calls that are specific only to IVE. These are mainly used in getting runtime state information from the IVE.

The table below contains the list of device specific RPCs of IVE and the context in which the calls are available.

IVE specific RPC	Host System	Logical System
create-logical-system	✓	✗
delete-logical-system	✓	✗
get-user-stats	✓	✓
get-failed-login-count	✓	✓
get-role-count	✓	✓
get-resource-profile-count	✓	✓
get-vlan-throughput	✓	✓
get-ivs-throughput	✓	✓
get-rollback-partition-information	✓	✗
validate-custom-expression	✓	✗
get-active-users	✓	✗
disable-all-users	✓	✗
enable-all-users	✓	✗
refresh-roles	✓	✗
delete-active-sessions	✓	✗
add-certificate	✓	✗
get-certificate-info	✓	✗
get-staged-package-information	✓	✗

The following subsections elaborate these IVE-specific RPCs, outline the schema for the requests and the replies and also illustrate each of the calls with examples.

## ***create-logical-system***

---

The create-logical-system RPC is used to create a new IVS. This RPC can be issued only in the Root IVS context.

### **Schema for RPC**

```

<!-- create-logical-system -->
<xs:complexType name="create-logical-system">
  <xs:annotation>
    <xs:appinfo>
      <dmi:rpc-info>
        <name>Create Logical System</name>
        <avail>
          <matches>
            <match>
              <operational-mode>logical-
systems</operational-mode>
              <value>>false</value>
            </match>
            <match>
              <value>>true</value>
            </match>
          </matches>
        </avail>
        <description>
          This command creates a new logical system
        </description>
        <rpc-reply-tag>create-logical-system-reply</rpc-
reply-tag>
      </dmi:rpc-info>
    </xs:appinfo>
  </xs:annotation>
  <xs:sequence>
    <xs:element name="name" type="xs:string">
      <xs:annotation>
        <xs:appinfo>
          <dmi:param-info>
            <name>Logical System Name</name>
            <description>
              The name of the logical system to create
            </description>
          </dmi:param-info>
        </xs:appinfo>
      </xs:annotation>
    </xs:element>
  </xs:sequence>
</complexType>

```

```

    <xs:element name="description" type="xs:string"
minOccurs="0">
    <xs:annotation>
    <xs:appinfo>
    <dmi:param-info>
    <name>Logical System Description</name>
    <description>
    The detail description of the logical system
    </description>
    </dmi:param-info>
    </xs:appinfo>
    </xs:annotation>
</xs:element>
    <xs:element name="enabled" type="xs:boolean">
    <xs:annotation>
    <xs:appinfo>
    <dmi:param-info>
    <name>Enabled</name>
    <description>
    The enable/disable state of the logical
system.
    </description>
    </dmi:param-info>
    </xs:appinfo>
    </xs:annotation>
</xs:element>
    <xs:element name="initial-configuration"
type="xs:string">
    <xs:annotation>
    <xs:appinfo>
    <dmi:param-info>
    <name>Logical System Initial
configuration</name>
    <description>
    Initialize the IVS using the default
configuration or copy the configuration from an existing
IVS. Specify the name of an existing logical system, or "-
Default Config -"
    </description>
    </dmi:param-info>
    </xs:appinfo>
    </xs:annotation>
</xs:element>
    <xs:element name="admin-username" type="xs:string"
minOccurs="0">
    <xs:annotation>
    <xs:appinfo>
    <dmi:param-info>
    <name>Logical System Admin Username</name>
    <description>
    The default admin username for the logical

```

```

system
    </description>
    </dmi:param-info>
  </xs:appinfo>
</xs:annotation>
</xs:element>
<xs:element name="admin-password" type="xs:string"
minOccurs="0">
  <xs:annotation>
    <xs:appinfo>
      <dmi:param-info>
        <name>Logical System Admin Password</name>
        <description>
          The default admin password for the logical
system
          </description>
        </dmi:param-info>
      </xs:appinfo>
    </xs:annotation>
  </xs:element>
  <xs:element name="minimum-guaranteed-users"
type="xs:int">
    <xs:annotation>
      <xs:appinfo>
        <dmi:param-info>
          <name>Minimum Guaranteed Users</name>
          <description>
            The number of concurrent user logins
            </description>
          </dmi:param-info>
        </xs:appinfo>
      </xs:annotation>
    </xs:element>
    <xs:element name="burstable-maximum-users"
type="xs:int">
      <xs:annotation>
        <xs:appinfo>
          <dmi:param-info>
            <name>Burstable Maximum Users</name>
            <description>
              The maximum concurrent user logins during
peak time
              </description>
            </dmi:param-info>
          </xs:appinfo>
        </xs:annotation>
      </xs:element>
      <xs:element name="total-maximum-bandwidth"
type="xs:int" minOccurs="0">
        <xs:annotation>
          <xs:appinfo>

```

```

    <dmi:param-info>
      <name>Total Maximum Bandwidth</name>
      <description>
        The maximum bandwidth available to this
logical system
      </description>
    </dmi:param-info>
  </xs:appinfo>
</xs:annotation>
</xs:element>
<xs:element name="nc-maximum-bandwidth" type="xs:int"
minOccurs="0">
  <xs:annotation>
    <xs:appinfo>
      <dmi:param-info>
        <name>NC Maximum Bandwidth</name>
        <description>
          The maximum bandwidth available to Network
Connect in this logical system
        </description>
      </dmi:param-info>
    </xs:appinfo>
  </xs:annotation>
</xs:element>

<xs:element name="vlans">
  <xs:annotation>
    <xs:appinfo>
      <dmi:param-info>
        <name>VLANs</name>
        <description>
          VLANs available to this logical system
        </description>
      </dmi:param-info>
    </xs:appinfo>
  </xs:annotation>
  <xs:complexType>
    <xs:sequence>
      <xs:choice minOccurs="1" maxOccurs="unbounded">
        <xs:element name="vlan" minOccurs="1"
maxOccurs="unbounded">
          <xs:annotation>
            <xs:appinfo>
              <dmi:param-info>
                <name>VLAN</name>
                <description>
                  Selected VLAN
                </description>
              </dmi:param-info>
            </xs:appinfo>
          </xs:annotation>

```

```

        </xs:element>
    </xs:choice>
</xs:sequence>
</xs:complexType>
</xs:element>

<xs:element name="default-vlan" type="xs:string">
  <xs:annotation>
    <xs:appinfo>
      <dmi:param-info>
        <name>Default VLAN</name>
        <description>
          The default VLAN in this logical system
        </description>
      </dmi:param-info>
    </xs:appinfo>
  </xs:annotation>
</xs:element>

<xs:element name="sign-in-url-prefix" type="xs:string"
minOccurs="0">
  <xs:annotation>
    <xs:appinfo>
      <dmi:param-info>
        <name>Sign-in URL Prefix</name>
        <description>
          The sign-in URL prefix used for logical
system sign-in
        </description>
      </dmi:param-info>
    </xs:appinfo>
  </xs:annotation>
</xs:element>

<xs:element name="internal-interface-virtual-ports"
minOccurs="0">
  <xs:annotation>
    <xs:appinfo>
      <dmi:param-info>
        <name>Virtual Ports (Internal
Interface)</name>
        <description>
          The virtual port on internal interface used
for logical system sign-in
        </description>
      </dmi:param-info>
    </xs:appinfo>
  </xs:annotation>
  <xs:complexType>
    <xs:sequence>
      <xs:choice minOccurs="0" maxOccurs="unbounded">

```

```

        <xs:element name="internal-interface-virtual-
port" minOccurs="0" maxOccurs="unbounded">
        <xs:annotation>
        <xs:appinfo>
        <dmi:param-info>
        <name>Virtual Port</name>
        <description>
        Selected virtual port
        </description>
        </dmi:param-info>
        </xs:appinfo>
        </xsd:annotation>
        </xs:element>
    </xs:choice>
</xs:sequence>
</xs:complexType>
</xs:element>

    <xs:element name="external-interface-virtual-ports"
minOccurs="0">
    <xs:annotation>
    <xs:appinfo>
    <dmi:param-info>
    <name>Virtual Ports (External
Interface)</name>
    <description>
    The virtual port on external interface used
for logical system sign-in
    </description>
    </dmi:param-info>
    </xs:appinfo>
    </xs:annotation>
    <xs:complexType>
    <xs:sequence>
    <xs:choice minOccurs="0" maxOccurs="unbounded">
    <xs:element name="external-interface-virtual-
port" minOccurs="0" maxOccurs="unbounded">
    <xs:annotation>
    <xs:appinfo>
    <dmi:param-info>
    <name>Virtual Port</name>
    <description>
    Selected virtual port
    </description>
    </dmi:param-info>
    </xs:appinfo>
    </xsd:annotation>
    </xs:element>
    </xs:choice>
    </xs:sequence>
    </xs:complexType>

```

```

</xs:element>

<xs:element name="nc-ip-pools" minOccurs="0">
  <xs:annotation>
    <xs:appinfo>
      <dmi:param-info>
        <name>NC IP Ranges</name>
        <description>
          Network Connect Connection Profile IP
          address pools are restricted to the IP ranges listed here
        </description>
      </dmi:param-info>
    </xs:appinfo>
  </xs:annotation>
  <xs:complexType>
    <xs:sequence>
      <xs:choice minOccurs="0" maxOccurs="unbounded">
        <xs:element name="nc-ip-pool" minOccurs="0"
          maxOccurs="unbounded">
          <xs:annotation>
            <xs:appinfo>
              <dmi:param-info>
                <name>NC IP Range</name>
                <description>
                  Network Connect connection profile
                  IP address pool
                </description>
              </dmi:param-info>
            </xs:appinfo>
          </xsd:annotation>
        </xs:element>
      </xs:choice>
    </xs:sequence>
  </xs:complexType>
</xs:element>

```

### Schema for RPC-REPLY

```

<!-- logical-system-rpc-reply -->
<xs:complexType name="logical-system-rpc-reply">
  <xs:annotation>
    <xs:appinfo>
      <dmi:rpc-reply-info>
        <description>
          Reply to the create-logical-system and delete-
          logical-system RPCs
        </description>
      </dmi:rpc-reply-info>
    </xs:appinfo>
  </xs:annotation>
</xs:complexType>

```

```

        </description>
        <rpc-list>
            <rpc-tag>create-logical-system</rpc-tag>
            <rpc-tag>delete-logical-system</rpc-tag>
        </rpc-list>
    </dmi:rpc-reply-info>
</xs:appinfo>
</xs:annotation>

<xs:choice>
    <xs:element name="ok">
        <xs:annotation>
            <xs:appinfo>
                <dmi:field-info>
                    <name>OK</name>
                    <desc>Success return</desc>
                </dmi:field-info>
            </xs:appinfo>
        </xs:annotation>
        <xs:complexType/> <!-- empty element -->
    </xs:element>

    <xs:element name="rpc-error">
        <xs:annotation>
            <xs:appinfo>
                <dmi:field-info>
                    <name>RPC Error</name>
                    <desc>Error return</desc>
                </dmi:field-info>
            </xs:appinfo>
        </xs:annotation>
        <xs:complexType>
            <xs:sequence>
                <xs:element name="error-type">
                    <xs:annotation>
                        <xs:appinfo>
                            <dmi:field-info>
                                <name>Error Type</name>
                                <desc>Error Type</desc>
                            </dmi:field-info>
                        </xs:appinfo>
                    </xs:annotation>
                    <xs:simpleType>
                        <xs:restriction base="xs:string">
                            <xs:enumeration value="transport"/>
                            <xs:enumeration value="rpc"/>
                            <xs:enumeration value="protocol"/>
                            <xs:enumeration value="application"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>
            </xs:sequence>
        </xs:complexType>
    </xs:element>

```

```

<xs:element name="error-tag">
  <xs:annotation>
    <xs:appinfo>
      <dmi:field-info>
        <name>Error Tag</name>
        <desc>The reason for error</desc>
      </dmi:field-info>
    </xs:appinfo>
  </xs:annotation>
  <xs:simpleType>
    <xs:restriction base="xs:string">
      <xs:enumeration value="in-use"/>
      <xs:enumeration value="invalid-value"/>
      <xs:enumeration value="too-big"/>
      <xs:enumeration value="missing-attribute"/>
      <xs:enumeration value="bad-attribute"/>
      <xs:enumeration value="unknown-attribute"/>
      <xs:enumeration value="missing-element"/>
      <xs:enumeration value="bad-element"/>
      <xs:enumeration value="unknown-element"/>
      <xs:enumeration value="unknown-namespace"/>
      <xs:enumeration value="access-denied"/>
      <xs:enumeration value="lock-denied"/>
      <xs:enumeration value="resource-denied"/>
      <xs:enumeration value="rollback-failed"/>
      <xs:enumeration value="data-exists"/>
      <xs:enumeration value="data-missing"/>
      <xs:enumeration value="operation-not-
supported"/>
      <xs:enumeration value="operation-failed"/>
      <xs:enumeration value="partial-operation"/>
    </xs:restriction>
  </xs:simpleType>
</xs:element>
<xs:element name="error-severity">
  <xs:annotation>
    <xs:appinfo>
      <dmi:field-info>
        <name>Error Severity</name>
        <desc>Error Severity</desc>
      </dmi:field-info>
    </xs:appinfo>
  </xs:annotation>
  <xs:simpleType>
    <xs:restriction base="xs:string">
      <xs:enumeration value="error"/>
      <xs:enumeration value="warning"/>
    </xs:restriction>
  </xs:simpleType>
</xs:element>
</xs:sequence>

```

```

    </xs:complexType>
  </xs:element>
</xs:choice>
</xs:complexType>

```

The following is an example of creating a new logical system, passing only the mandatory parameters for the RPC. The XML code creates a logical system with default config, setting Internal Port as the default vlan port for the newly created IVS.

#### Example for RPC

```

<rpc message-id='101'
xmlns='urn:ietf:params:xml:ns:netconf:base:1.0'>
  <create-logical-system>
    <name>test</name>
    <initial-configuration>- Default Config -</initial-
configuration>
    <enabled>>true</enabled>
    <minimum-guaranteed-users>3</minimum-guaranteed-users>
    <burstable-maximum-users>4</burstable-maximum-users>
    <vlans>
      <vlan>Internal Port</vlan>
    </vlans>
    <default-vlan>Internal Port</default-vlan>
  </create-logical-system>
</rpc>

```

If the RPC is successful, the following is the response received. On error conditions, the error message explains the reason the command failed.

#### Example for RPC-REPLY

```

<rpc-reply message-id="101"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <ok/>
</rpc-reply>

```

An example of the same RPC with all the parameters passed is given below. This assumes that the virtual ports and the NC IP pools are already configured in the IVE, without which the command would fail. The RPC creates an IVS with configuration copied from the Root IVS.

#### Example for RPC

```

<rpc message-id='101'

```

```

xmlns='urn:ietf:params:xml:ns:netconf:base:1.0'>
  <create-logical-system>
    <name>test</name>
    <initial-configuration>Root</initial-
configuration>
    <enabled>true</enabled>
    <admin-username>admin</admin-username>
    <admin-password>dana123</admin-password>
    <minimum-guaranteed-users>3</minimum-
guaranteed-users>
    <burstable-maximum-users>4</burstable-maximum-
users>
    <vlans>
      <vlan>Internal Port</vlan>
    </vlans>
    <default-vlan>Internal Port</default-vlan>
    <internal-virtual-ports>
      <internal-virtual-port>int_vp1</internal-
virtual-port>
      <internal-virtual-port>int_vp2</internal-
virtual-port>
    </internal-virtual-ports>
    <nc-ip-pools>
      <nc-ip-pool>10.10.10.10-20</nc-ip-pool>
      <nc-ip-pool>10.10.10.50</nc-ip-pool>
    </nc-ip-pools>
  </create-logical-system>
</rpc>

```

## ***delete-logical-system***

---

The delete-logical-system RPC, as the name implies, deletes an IVS in the IVE. This command requires the name of the IVS to be specified as the parameter in the call.

### **Schema for the RPC**

```

<!-- delete-logical-system -->
<xs:complexType name="delete-logical-system">
  <xs:annotation>
    <xs:appinfo>
      <dmi:rpc-info>
        <name>Delete Logical System</name>
        <avail>
          <matches>
            <match>
              <operational-mode>logical-
systems</operational-mode>

```

```

        <value>>false</value>
    </match>
    <match>
        <value>>true</value>
    </match>
</matches>
</avail>
<description>
    This command deletes an existing logical system
</description>
<rpc-reply-tag>delete-logical-system-reply</rpc-
reply-tag>
</dmi:rpc-info>
</xs:appinfo>
</xs:annotation>
<xs:sequence>
    <xs:element name="name" type="xs:string">
        <xs:annotation>
            <xs:appinfo>
                <dmi:param-info>
                    <name>Logical System Name</name>
                    <description>
                        The name of the logical system to delete
                    </description>
                </dmi:param-info>
            </xs:appinfo>
        </xs:annotation>
    </xs:element>
</xs:sequence>
</xs:complexType>

```

Delete logical system RPC takes the name of the IVS as the parameter and if the IVS with the given name is present, deletes it from the IVE.

#### Example for RPC

```

<rpc message-id='101'
xmlns='urn:ietf:params:xml:ns:netconf:base:1.0'>
    <delete-logical-system>
        <name>test</name>
    </delete-logical-system>
</rpc>

```

If the RPC is successful the following reply is received.

#### Example for RPC-REPLY

```
<rpc-reply message-id="101"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <ok/>
</rpc-reply>
```

## ***get-user-stats***

---

The get-user-stats RPC retrieves the number of users existing presently and in the last 24 hour interval in the IVE. Optionally, the RPC takes a parameter if the data has to be reset after the retrieval. This call can be executed in both the host-system context and in the logical-system context and the data is pertinent to the appropriate IVS.

### **Schema for RPC**

```
<!-- get-user-stats -->
<xs:complexType name="get-user-stats">
  <xs:annotation>
    <xs:appinfo>
      <dmi:rpc-info>
        <name>Get user statistics</name>
        <description>
          This command returns AllocatedUserCount
          CurrentUserCount MaxUsersin24Hrs MinUsersin24Hrs
        </description>
        <rpc-reply-tag>user-stats</rpc-reply-tag>
      </dmi:rpc-info>
    </xs:appinfo>
  </xs:annotation>
  <xs:sequence>
    <xs:element name="reset" type="xs:boolean"
minOccurs="0">
      <xs:annotation>
        <xs:appinfo>
          <dmi:param-info>
            <name>Reset Stats</name>
            <description>
              This will govern the resetting of this
              statistics data. By default, the data is not reset.
            </description>
          </dmi:param-info>
        </xs:appinfo>
      </xs:annotation>
    </xs:element>
  </xs:sequence>
</xs:complexType>
```

As shown in the schema below, the following are the data sent back by the IVE:

- ◆ Total number of allocated users
- ◆ Total number of current users
- ◆ Maximum number of active users in the last 24 hour period
- ◆ Minimum number of active users in the last 24 hour period

### Schema for RPC-REPLY

```
<!-- user-stats -->
<xs:complexType name="user-stats">
  <xs:annotation>
    <xs:appinfo>
      <dmi:rpc-reply-info>
        <description>
          User Statistics
        </description>
        <rpc-list>
          <rpc-tag>get-user-stats</rpc-tag>
        </rpc-list>
      </dmi:rpc-reply-info>
    </xs:appinfo>
  </xs:annotation>
  <xs:sequence>
    <xs:element name="allocated-user-count"
type="xs:string">
      <xs:annotation>
        <xs:appinfo>
          <dmi:field-info>
            <name>Allocated User Count</name>
            <desc>The Allocated User Count for the logical
system</desc>
          </dmi:field-info>
        </xs:appinfo>
      </xs:annotation>
    </xs:element>

    <xs:element name="current-user-count"
type="xs:string">
      <xs:annotation>
        <xs:appinfo>
          <dmi:field-info>
            <name>Current user count</name>
            <desc>The number of users logged in
currently</desc>
          </dmi:field-info>
        </xs:appinfo>
      </xs:annotation>
    </xs:element>
  </xs:sequence>
</xs:complexType>
```

```

    <xs:element name="max-active-user-count-24hrs"
type="xs:string">
    <xs:annotation>
    <xs:appinfo>
    <dmi:field-info>
    <name>Max active user count in the last 24
Hrs</name>
    <desc>The Max active user count for a 24 Hrs
moving window</desc>
    </dmi:field-info>
    </xs:appinfo>
    </xs:annotation>
    </xs:element>

    <xs:element name="min-active-user-count-24hrs"
type="xs:string">
    <xs:annotation>
    <xs:appinfo>
    <dmi:field-info>
    <name>Min active user count in the last 24
Hrs</name>
    <desc>The Min active user count for a 24 Hrs
moving window</desc>
    </dmi:field-info>
    </xs:appinfo>
    </xs:annotation>
    </xs:element>
</xs:sequence>
</xs:complexType>

```

An example of the get-user-stats RPC call and the reply are rendered below.

#### Example for RPC

```

<rpc message-id="14">
<get-user-stats/>
</rpc>

```

#### Example for RPC-REPLY

```

<rpc-reply message-id="12"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <user-stats>
    <allocated-user-count>10</allocated-user-count>
    <current-user-count>3</current-user-count>
    <max-active-user-count-24hrs>2</max-active-user-
count-24hrs>

```

```

    <min-active-user-count-24hrs>0</min-active-user-
count-24hrs>
  </user-stats>
</rpc-reply>

```

## ***get-failed-login-count***

---

The get-failed-login-count RPC is used to retrieve the number of failures in the last 24 hour interval due to number of users exceeding the limit and due to authentication failure. Similar to get-user-stats RPC, this also takes the reset option as a parameter.

### **Schema for the RPC**

```

<!-- get-failed-login-count -->
<xs:complexType name="get-failed-login-count">
  <xs:annotation>
    <xs:appinfo>
      <dmi:rpc-info>
        <name>Get failed login count for Authentication
failure and Exceeded user</name>
        <description>
          This command returns the Number of Logins
refused due to exceeding allowed limits and Auth failure
(24 hour moving window)
        </description>
        <rpc-reply-tag>failed-login-count</rpc-reply-tag>
      </dmi:rpc-info>
    </xs:appinfo>
  </xs:annotation>
  <xs:sequence>
    <xs:element name="reset" type="xs:boolean"
minOccurs="0">
      <xs:annotation>
        <xs:appinfo>
          <dmi:param-info>
            <name>Reset Stats</name>
            <description>
              This will govern the resetting of this
statistics data. By default, the data is not reset.
            </description>
          </dmi:param-info>
        </xs:appinfo>
      </xs:annotation>
    </xs:element>
  </xs:sequence>
</xs:complexType>

```

**Schema for RPC-REPLY**

```

<!-- failed-login-count -->
<xs:complexType name="failed-login-count">
  <xs:annotation>
    <xs:appinfo>
      <dmi:rpc-reply-info>
        <description>
          Failed Login statistics Info
        </description>
        <rpc-list>
          <rpc-tag>get-failed-login-count</rpc-tag>
        </rpc-list>
      </dmi:rpc-reply-info>
    </xs:appinfo>
  </xs:annotation>

  <xs:sequence>

    <xs:element name="exceeded-user-count"
type="xs:string">
      <xs:annotation>
        <xs:appinfo>
          <dmi:field-info>
            <name>Number of login failures due to exceeded
login user limit</name>
            <desc>The Number of user logins refused due to
exceeded user count.</desc>
          </dmi:field-info>
        </xs:appinfo>
      </xs:annotation>
    </xs:element>

    <xs:element name="failed-auth-count" type="xs:string">
      <xs:annotation>
        <xs:appinfo>
          <dmi:field-info>
            <name>Number of login failures due to
authentication failure</name>
            <desc>The Number of user logins refused due to
authentication failure.</desc>
          </dmi:field-info>
        </xs:appinfo>
      </xs:annotation>
    </xs:element>
  </xs:sequence>
</xs:complexType>

```

An example of the get-failed-login-count RPC and its response are given below.

#### Example for RPC

```
<rpc message-id="12">
  <get-failed-login-count/>
</rpc>
```

#### Example for RPC-REPLY

```
<rpc-reply message-id="12"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <failed-login-count>
    <exceeded-user-count>2</exceeded-user-count>
    <failed-auth-count>4</failed-auth-count>
  </failed-login-count>
</rpc-reply>
```

## ***get-role-count***

---

To retrieve the number of administrative roles and the user roles available in the IVS, the get-role-count RPC can be used. The RPC can be executed in both the host-system and in the logical-system context and the RPC reply contains the statistics pertinent to the IVS currently set.

#### Schema for RPC

```
<!-- get-role-count -->
<xs:complexType name="get-role-count">
  <xs:annotation>
    <xs:appinfo>
      <dmi:rpc-info>
        <name>Get The roles count</name>
        <description>
          This command returns the admin and user role
          count.
        </description>
        <rpc-reply-tag>role-count</rpc-reply-tag>
      </dmi:rpc-info>
    </xs:appinfo>
  </xs:annotation>
</xs:complexType>
```

## Schema for RPC-REPLY

```

<!-- role-count -->
<xs:complexType name="role-count">
  <xs:annotation>
    <xs:appinfo>
      <dmi:rpc-reply-info>
        <description>
          Number for roles configured
        </description>
        <rpc-list>
          <rpc-tag>get-role-count</rpc-tag>
        </rpc-list>
      </dmi:rpc-reply-info>
    </xs:appinfo>
  </xs:annotation>
  <xs:sequence>
    <xs:element name="admin-role-count" type="xs:string">
      <xs:annotation>
        <xs:appinfo>
          <dmi:field-info>
            <name>Admin roles Count</name>
            <desc>The total number of admin roles
configured for the logical system</desc>
          </dmi:field-info>
        </xs:appinfo>
      </xs:annotation>
    </xs:element>

    <xs:element name="user-role-count" type="xs:string">
      <xs:annotation>
        <xs:appinfo>
          <dmi:field-info>
            <name>User roles Count</name>
            <desc>The total number of user roles
configured for the logical system</desc>
          </dmi:field-info>
        </xs:appinfo>
      </xs:annotation>
    </xs:element>

  </xs:sequence>
</xs:complexType>

```

An example of the RPC and its reply follow.

**Example for RPC**

```
<rpc message-id="12">
  <get-role-count/>
</rpc>
```

**Example for RPC-REPLY**

```
<rpc-reply message-id="12"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <role-count>
    <admin-role-count>2</admin-role-count>
    <user-role-count>1</user-role-count>
  </role-count>
</rpc-reply>
```

***get-resource-profile-count***

The number of resource profiles in the IVS can be retrieved with the get-resource-profile-count RPC. Here is the schema for the RPC and its reply.

**Schema for the RPC**

```
<!-- get-resource-profile-count -->
<xs:complexType name="get-resource-profile-count">
  <xs:annotation>
    <xs:appinfo>
      <dmi:rpc-info>
        <name>Get the resource profile count</name>
        <description>
          This command returns the number of resource
          profiles in the logical system.
        </description>
        <rpc-reply-tag>resource-profile-count</rpc-reply-
tag>
      </dmi:rpc-info>
    </xs:appinfo>
  </xs:annotation>
</xs:complexType>
```

**Schema for RPC-REPLY**

```

<!-- resource-profile-count -->
<xs:complexType name="resource-profile-count">
  <xs:annotation>
    <xs:appinfo>
      <dmi:rpc-reply-info>
        <description>
          Number for resource profiles configured.
        </description>
        <rpc-list>
          <rpc-tag>get-resource-profile-count</rpc-tag>
        </rpc-list>
      </dmi:rpc-reply-info>
    </xs:appinfo>
  </xs:annotation>
  <xs:sequence>
    <xs:element name="profile-count" type="xs:string">
      <xs:annotation>
        <xs:appinfo>
          <dmi:field-info>
            <name>Resource profile Count</name>
            <desc>The total number of resource profiles
configured for the logical system</desc>
          </dmi:field-info>
        </xs:appinfo>
      </xs:annotation>
    </xs:element>
  </xs:sequence>
</xs:complexType>

```

Example of the RPC request and its response are rendered below.

**Example for RPC**

```

<rpc message-id="12">
  <get-resource-profile-count/>
</rpc>

```

**Example for RPC-REPLY**

```

<rpc-reply message-id="12"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <resource-profile-count>
    <profile-count>20</profile-count>
  </resource-profile-count>
</rpc-reply>

```

## ***get-vlan-throughput***

---

The throughput of a specific VLAN can be retrieved using the get-vlan-throughput RPC. The RPC reply contains the throughput for the VLAN in bytes.

The schema for the RPC and its reply are given below.

### **Schema for the RPC**

```
<!-- get-vlan-throughput -->
<xs:complexType name="get-vlan-throughput">
  <xs:annotation>
    <xs:appinfo>
      <dmi:rpc-info>
        <name>Get VLAN Throughput</name>
        <description>
          This command returns the throughput for the VLAN
          id sent as parameter
        </description>
        <rpc-reply-tag>vlan-throughput</rpc-reply-tag>
      </dmi:rpc-info>
    </xs:appinfo>
  </xs:annotation>
  <xs:sequence>
    <xs:element name="vlanid" type="xs:string">
      <xs:annotation>
        <xs:appinfo>
          <dmi:param-info>
            <name>VLAN ID</name>
            <description>
              The ID of the VLAN whose throughput is
              required. The values should be in the range 0-4094. 0
              Indicated the internal interface.
            </decription>
          </dmi:param-info>
        </xs:appinfo>
      </xs:annotation>
    </xs:element>
    <xs:element name="reset" type="xs:boolean"
      minOccurs="0">
      <xs:annotation>
        <xs:appinfo>
          <dmi:param-info>
            <name>Reset Stats</name>
            <description>
              This will govern the resetting of the
              statistics data. By default, the data is not reset.
            </description>
          </dmi:param-info>
        </xs:appinfo>
      </xs:annotation>
    </xs:element>
  </xs:sequence>
</xs:complexType>
```

```

        </description>
      </dmi:param-info>
    </xs:appinfo>
  </xs:annotation>
</xs:element>
</xs:sequence>
</xs:complexType>

```

### Schema for RPC-REPLY

```

<!-- vlan-throughput -->
<xs:complexType name="vlan-throughput">
  <xs:annotation>
    <xs:appinfo>
      <dmi:rpc-reply-info>
        <description>
          VLAN throughput information
        </description>
        <rpc-list>
          <rpc-tag>get-vlan-throughput</rpc-tag>
        </rpc-list>
      </dmi:rpc-reply-info>
    </xs:appinfo>
  </xs:annotation>
  <xs:sequence>
    <xs:element name="max-throughput" type="xs:string">
      <xs:annotation>
        <xs:appinfo>
          <dmi:field-info>
            <name>Maximum throughput over the last 24
Hrs</name>
            <desc>Maximum throughput over the last 24
Hrs</desc>
          </dmi:field-info>
        </xs:appinfo>
      </xs:annotation>
    </xs:element>

    <xs:element name="min-throughput" type="xs:string">
      <xs:annotation>
        <xs:appinfo>
          <dmi:field-info>
            <name>Minimum throughput over the last 24
Hrs</name>
            <desc>Minimum throughput over the last 24
Hrs</desc>
          </dmi:field-info>
        </xs:appinfo>
      </xs:annotation>
    </xs:element>
  </xs:sequence>
</xs:complexType>

```

```

</xs:element>

<xs:element name="avg-throughput" type="xs:string">
  <xs:annotation>
    <xs:appinfo>
      <dmi:field-info>
        <name>Average throughput over the last 24
Hrs</name>
        <desc>Average throughput over the last 24
Hrs</desc>
      </dmi:field-info>
    </xs:appinfo>
  </xs:annotation>
</xs:element>

</xs:sequence>
</xs:complexType>

```

An example of the RPC and its response are given below.

#### Example for RPC

```

<rpc message-id="12">
  <get-vlan-throughput>
    <vlanid>0</vlanid>
  </get-vlan-throughput>
</rpc>

```

#### Example for RPC-REPLY

```

<rpc-reply message-id="12"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <vlan-throughput>
    <max-throughput>8591642</max-throughput>
    <min-throughput>0</min-throughput>
    <avg-throughput>4918466.471698</avg-throughput>
  </vlan-throughput>
</rpc-reply>

```

## ***get-ivs-throughput***

---

A variation to getting the throughput in IVE is to retrieve the value for a given IVS. If there are multiple VLANs assigned for an IVS, then the throughput will be a consolidated value of all the IVSes. The RPC also takes the reset parameter, which if set would reset the current throughput values.

The schema for the RPC and its reply follow.

### **Schema for the RPC**

```
<!-- get-throughput -->
<xs:complexType name="get-throughput">
  <xs:annotation>
    <xs:appinfo>
      <dmi:rpc-info>
        <name>Get throughput for the logical system</name>
        <description>
          This command returns the consolidated throughput
          for all the VLANS for a logical system
        </description>
        <rpc-reply-tag>ivs-throughput</rpc-reply-tag>
      </dmi:rpc-info>
    </xs:appinfo>
  </xs:annotation>
  <xs:sequence>
    <xs:element name="reset" type="xs:boolean"
      minOccurs="0">
      <xs:annotation>
        <xs:appinfo>
          <dmi:param-info>
            <name>Reset Stats</name>
            <description>
              This will govern the resetting of the
              statistics data. By default, the data is not reset.
            </description>
          </dmi:param-info>
        </xs:appinfo>
      </xs:annotation>
    </xs:element>
  </xs:sequence>
</xs:complexType>
```

### **Schema for RPC-REPLY**

```
<!-- ivs-throughput -->
<xs:complexType name="ivs-throughput">
```

```

<xs:annotation>
  <xs:appinfo>
    <dmi:rpc-reply-info>
      <description>
        IVS throughput information
      </description>
      <rpc-list>
        <rpc-tag>get-throughput</rpc-tag>
      </rpc-list>
    </dmi:rpc-reply-info>
  </xs:appinfo>
</xs:annotation>
<xs:sequence>
  <xs:element name="max-throughput" type="xs:string">
    <xs:annotation>
      <xs:appinfo>
        <dmi:field-info>
          <name>Maximum throughput over the last 24
Hrs</name>
          <desc>Maximum throughput over the last 24
Hrs</desc>
        </dmi:field-info>
      </xs:appinfo>
    </xs:annotation>
  </xs:element>

  <xs:element name="min-throughput" type="xs:string">
    <xs:annotation>
      <xs:appinfo>
        <dmi:field-info>
          <name>Minimum throughput over the last 24
Hrs</name>
          <desc>Minimum throughput over the last 24
Hrs</desc>
        </dmi:field-info>
      </xs:appinfo>
    </xs:annotation>
  </xs:element>

  <xs:element name="avg-throughput" type="xs:string">
    <xs:annotation>
      <xs:appinfo>
        <dmi:field-info>
          <name>Average throughput over the last 24
Hrs</name>
          <desc>Average throughput over the last 24
Hrs</desc>
        </dmi:field-info>
      </xs:appinfo>
    </xs:annotation>
  </xs:element>

```

```

</xs:sequence>
</xs:complexType>

```

An example of the RPC and its response are rendered below.

#### Example for RPC

```

<rpc message-id="12">
  <get-ivs-throughput>
    <name>test</name>
  </get-ivs-throughput>
</rpc>

```

#### Example for RPC-REPLY

```

<rpc-reply message
id="12" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <ivsthroughput>
    <maxthroughput>10972025</maxthroughput>
    <minthroughput>0</minthroughput>
    <avgthroughput>5527986.533333</avgthroughput>
  </ivsthroughput>
</rpc-reply>

```

### *get-rollback-partition-information*

The get-rollback-partition-information RPC retrieves the device rollback version information such as os-name, os-version and os build number.

#### Schema for RPC

```

<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">
<!-- get-rollback-partition-information -->
<xs:complexType name="get-rollback-partition-information">
  <xs:annotation>
    <xs:appinfo>
      <dmi:rpc-info>
        <name>Get Rollback Partition Information</name>
        <description>
          This command returns IVE's rollback partition

```

```

information
    </description>
    <rpc-reply-tag>rollback-partition-
information</rpc-reply-tag>
    </dmi:rpc-info>
  </xs:appinfo>
</xs:annotation>
</xs:complexType>

</xs:schema>

```

### Schema for RPC-REPLY

```

<xs:complexType name="rollback-partition-information">
  <xs:annotation>
    <xs:appinfo>
      <dmi:rpc-reply-info>
        <description>
          Rollback Software Image Information
        </description>
        <rpc-list>
          <rpc-tag>get-rollback-partition-
information</rpc-tag>
        </rpc-list>
      </dmi:rpc-reply-info>
    </xs:appinfo>
  </xs:annotation>
  <xs:sequence>
    <xs:element name="os-name" type="xs:string">
      <xs:annotation>
        <xs:appinfo>
          <dmi:field-info>
            <name>Software Image OS Name</name>
            <desc>Software Image OS Name</desc>
          </dmi:field-info>
        </xs:appinfo>
      </xs:annotation>
    </xs:element>
    <xs:element name="os-version" type="xs:string">
      <xs:annotation>
        <xs:appinfo>
          <dmi:field-info>
            <name>Software Image OS Version</name>
            <desc>Software Image OS Version</desc>
          </dmi:field-info>
        </xs:appinfo>
      </xs:annotation>
    </xs:element>
  </xs:sequence>
</xs:complexType>

```

```

    </xs:annotation>
  </xs:element>
  <xs:element name="build" type="xs:string">
    <xs:annotation>
      <xs:appinfo>
        <dmi:field-info>
          <name>Software Image Build Number</name>
          <desc>Software Image Build Number</desc>
        </dmi:field-info>
      </xs:appinfo>
    </xs:annotation>
  </xs:element>
</xs:sequence>
</xs:complexType>

```

The following is an example to retrieve rollback software image information.

#### Example for RPC

```

<rpc message-id='101'
xmlns='urn:ietf:params:xml:ns:netconf:base:1.0'>
  <get-rollback-partition-information/>
</rpc>

```

If the RPC is successful, the following is the response received. On error conditions, the error message explains the reason the command failed.

#### Example for RPC-REPLY

```

<rpc-reply message-id="101"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <rollback-partition-information>
    <os-name>ive-sa</os-name>
    <os-version>6.4R1</os-version>
    <build>14063</build>
  </rollback-partition-information>
</rpc-reply>

```

### *validate-custom-expression*

The validate-custom-expression RPC is used to validate custom expression. This RPC validates realm role mapping rule, policy detailed rule, log-filter-settings-query and sensor event expressions.

## Schema for RPC

```

<!--validate-custom-expression--!>
<xs:complexType name="validate-custom-expression">
  <xs:annotation>
    <xs:appinfo>
      <dm:rpc-info>
        <name>Validate Custom Expression</name>
        <description>This command will validate the
expression</description>
        <rpc-reply-tag>validate-custom-expression-
reply</rpc-reply-tag>
      </dm:rpc-info>
    </xs:appinfo>
  </xs:annotation>
  <xs:sequence>
    <xs:element name="expression" type="xs:string">
      <xs:annotation>
        <xs:appinfo>
          <dm:param-info>
            <name>Custom Expression</name>
            <description>Custom Expression to
validate</description>
          </dm:param-info>
        </xs:appinfo>
      </xs:annotation>
    </xs:element>
    <xs:element name="expression-usage">
      <xs:annotation>
        <xs:appinfo>
          <dm:field-info>
            <name>Custom Expression Usage</name>
            <desc>Identify the place in Admin UI where
the custom expression is being used.</desc>
          </dm:field-info>
        </xs:appinfo>
      </xs:annotation>
    </xs:element>
    <xs:simpleType>
      <xs:restriction base="xs:string">
        <xs:enumeration value="realm-role-mapping-rule"/>
        <xs:enumeration value="policy-detailed-rule"/>
        <xs:enumeration value="log-filter-settings-
query"/>
        <xs:enumeration value="sensor-event"/>
      </xs:restriction>
    </xs:simpleType>
  </xs:sequence>
</xs:complexType>

```

This RPC instructs device to validate expression provided in the <expression> parameter for realm role mapping.

#### Example for RPC

```
<rpc message-id='101'>
  xmlns='urn:ietf:params:xml:ns:netconf:base:1.0'>
  <validate-custom-expression>
    <expression>cacheCleanerStatus = 1</expression>
    <expression-usage>realm-role-mapping-rule</expression-usage>
  </validate-custom-expression>
</rpc>
```

This RPC instructs device to validate expression provided in the <expression> parameter for policy detailed rule.

#### Example for RPC

```
<rpc message-id='101'
xmlns='urn:ietf:params:xml:ns:netconf:base:1.0'>
  <validate-custom-expression>
    <expression>loginURL =
"partners.company.com/"</expression>
    <expression-usage>policy-detailed-rule</expression-usage>
  </validate-custom-expression>
</rpc>
```

This RPC instructs device to validate log filter setting expression provided in the <expression> parameter.

#### Example for RPC

```
<rpc message-id='101'
xmlns='urn:ietf:params:xml:ns:netconf:base:1.0'>
  <validate-custom-expression>
    <expression>result = 200 OR port = 210 OR method =
"GET"</expression>
    <expression-usage>log-filter-settings-
query</expression-usage>
  </validate-custom-expression>
</rpc>
```

This RPC instructs device to validate sensor event expression provided in the <expression> parameter.

**Example for RPC**

```
<rpc message-id='101'
xmlns='urn:ietf:params:xml:ns:netconf:base:1.0'>
  <validate-custom-expression><expression>idp.action =
'ignore' OR idp.action = 'none'</expression>
  <expression-usage>sensor-event</expression-usage>
</validate-custom-expression>
</rpc>
```

If the RPC is successful, the following is the response received. On error conditions, the error message explains the reason the command failed.

**Example for RPC-REPLY**

```
<rpc-reply message-id="101"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <ok/>
</rpc-reply>
```

***get-active-users***

The get-active-users RPC retrieves current active user sessions in host system and virtual system context.

**Schema for RPC**

```
<!--get-active-users -->
<xs:complexType name="get-active-users">
  <xs:annotation>
    <xs:appinfo>
      <dmi:rpc-info>
        <name>Search Active Users</name>
        <description>This RPC requests for a fixed number
of active users currently in the system based on a
specified name pattern. </description>
        <rpc-reply-tag>active-users</rpc-reply-tag>
      </dmi:rpc-info>
    </xs:appinfo>
  </xs:annotation>
  <xs:sequence>
    <xs:element name="name" type="xs:string">
      <xs:annotation>
        <xs:appinfo>
          <dmi:param-info>
            <name>User Name</name>
            <description>This is the user name to search for. A
```

```

regular expression may be used. </description>
  </dmi:param-info>
</xs:appinfo>
</xs:annotation>
</xs:element>
<xs:element name="number" type="xs:integer">
  <xs:annotation>
    <xs:appinfo>
      <dmi:param-info>
        <name>Maximum Number of Users to Display </name>
        <description>This is the maximum number of users to
return.</description>
      </dmi:param-info>
    </xs:appinfo>
  </xs:annotation>
</xs:element>
<xs:element name="sortby" type="xs:string">
  <xs:annotation>
    <xs:appinfo>
      <dmi:param-info>
        <name>Column to Sort By</name>
        <description>This is the column name the IVE will
use to sort. IVE will use name + number + sortby +
sortorder to return the correct result to
NSM.</description>
      </dmi:param-info>
    </xs:appinfo>
  </xs:annotation>
</xs:element>
<xs:element name="sortorder" type="xs:integer">
  <xs:annotation>
    <xs:appinfo>
      <dmi:param-info>
        <name>The Sort Order</name>
        <description> This is the requested sort order for the
reply. The meaning of the value: 1 for ascending, 2 for
descending and 0 for unsorted. <description>
      </dmi:param-info>
    </xs:appinfo>
  </xs:annotation>
</xs:element>
</xs:sequence>
</xs:complexType>
</xs:schema>

```

### Schema for RPC-REPLY

```

<!-- active-users -->
<xs:complexType name="active-users">

```

```

<xs:annotation>
  <xs:appinfo>
    <dmi:rpc-reply-info>
      <description>
        Active Users
      </description>
      <rpc-list>
        <rpc-tag>get-active-users</rpc-tag>
      </rpc-list>
    </dmi:rpc-reply-info>
  </xs:appinfo>
</xs:annotation>
<xs:sequence>

  <xs:element name="user-login-permission"
type="xs:boolean">
  <xs:annotation>
    <xs:appinfo>
      <dmi:field-info>
        <name>User Login Permission</name>
        <desc> The current system setting for allowing
or disallowing users to login: true for allowing and false
for disallowing. </desc>
      </dmi:field-info>
    </xs:appinfo>
  </xs:annotation>
</xs:element>

  <xs:element name="total-matched-record-number"
type="xs:integer">
  <xs:annotation>
    <xs:appinfo>
      <dmi:field-info>
        <name>Total Matched Record Number</name>
        <desc> Total number of active user records
that matched the search criterion </desc>
      </dmi:field-info>
    </xs:appinfo>
  </xs:annotation>
</xs:element>

  <xs:element name="total-returned-record-number"
type="xs:integer">
  <xs:annotation>
    <xs:appinfo>
      <dmi:field-info>
        <name> Total Returned Record Number </name>
        <desc> Number of active user records returned
in this reply </desc>
      </dmi:field-info>
    </xs:appinfo>

```

```

    </xs:annotation>
  </xs:element>

  <xs:element name="active-user-records">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="active-user-record" minOccurs="0"
maxOccurs="unbounded">
          <xs:complexType>
            <xs:sequence>
              <xs:element name="active-user-name" type="xs:string">
                <xs:annotation>
                  <xs:appinfo>
                    <dmi:field-info>
                      <name>Active User Name</name>
                      <desc>This is the name of an active
user</desc>
                    </dmi:field-info>
                  </xs:appinfo>
                </xs:annotation>
              </xs:element>

              <xs:element name="authentication-realm"
type="xs:string">
                <xs:annotation>
                  <xs:appinfo>
                    <dmi:field-info>
                      <name>Authentication Realm</name>
                      <desc>The authentication realm the user logged
in</desc>
                    </dmi:field-info>
                  </xs:appinfo>
                </xs:annotation>
              </xs:element>

              <xs:element name="user-roles" type="xs:string">
                <xs:annotation>
                  <xs:appinfo>
                    <dmi:field-info>
                      <name>User Roles </name>
                      <desc>The roles assigned to the user </desc>
                    </dmi:field-info>
                  </xs:appinfo>
                </xs:annotation>
              </xs:element>

              <xs:element name="user-sign-in-time"
type="xs:dateTime">
                <xs:annotation>
                  <xs:appinfo>
                    <dmi:field-info>

```

```

        <name>User Sign-in Time </name>
        <desc>The time the user signed in </desc>
    </dmi:field-info>
</xs:appinfo>
</xs:annotation>
</xs:element>

<xs:element name="events" type="xs:integer">
  <xs:annotation>
    <xs:appinfo>
      <dmi:field-info>
        <name>Events </name>
        <desc> Events for this session. Its value can
be 0, 1 or 2. If there are no IDP (intrusion detection)
events for the session, it.s set to 0. If there are IDP
events for the session, but the session has not been
quarantined, it.s set to 1. If the session has been
quarantined, it.s set to 2 </desc>
      </dmi:field-info>
    </xs:appinfo>
  </xs:annotation>
</xs:element>

<xs:element name="login-node" type="xs:string">
  <xs:annotation>
    <xs:appinfo>
      <dmi:field-info>
        <name>Login Node </name>
        <desc>The node from which the user signed in
</desc>
      </dmi:field-info>
    </xs:appinfo>
  </xs:annotation>
</xs:element>

<xs:element name="network-connect-ip"
type="xs:string">
  <xs:annotation>
    <xs:appinfo>
      <dmi:field-info>
        <name>Network Connect IP </name>
        <desc>The IP address assigned for the user's
network connect session </desc>
      </dmi:field-info>
    </xs:appinfo>
  </xs:annotation>
</xs:element>

<xs:element name="session-id" type="xs:string">
  <xs:annotation>
    <xs:appinfo>

```

```

        <dmi:field-info>
            <name><User Session ID/name>
            <desc>The unique user session ID</desc>
        </dmi:field-info>
    </xs:appinfo>
</xs:annotation>
</xs:element>

</xs:sequence>
</xs:complexType>
</xs:element>
</xs:sequence>
</xs:complexType>
</xs:element>
</xs:sequence>
</xs:complexType>

```

### Example for RPC

```

<rpc message-id='101'>
  xmlns='urn:ietf:params:xml:ns:netconf:base:1.0'>
  <get-active-users><name>*</name>
    <number>32</number>
  <orderby>userName</orderby>
  <sortorder>2</sortorder>
  </get-active-users>
</rpc>

```

An example of the RPC reply is shown below.

### Example for RPC-REPLY

```

<rpc-reply message-id="101"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<get-active-users>
  <user-login-permission>true</user-login-permission>
  <total-matched-record-number>3</total-matched-record-
number>
  <total-returned-record-number>3</total-returned-record-
number>
  <active-user-records>
    <active-user-record>
      <active-user-name>newadmin</active-user-name>
      <authentication-realm>Admin Users</authentication-
realm>
    <user-roles>.Administrators</user-roles>
  </active-user-records>
</get-active-users>
</rpc-reply>

```

```

    <user-sign-in-time>2009/05/28 13:37:31</user-sign-in-
time>
    <events>0</events>
    <login-node>localhost2</login-node>
    <network-connect-ip></network-connect-ip>
    <session-
id>userid25b50923ef52dcc2bc8d113a5e5d17a02a74fde8</session-
id>
    </active-user-record>
    <active-user-record>
    <active-user-name>admindb</active-user-name>
    <authentication-realm>Admin Users</authentication-
realm>
    <user-roles>.Administrators</user-roles>
    <user-sign-in-time>2009/05/29 15:22:33</user-sign-in-
time>
    <events>0</events>
    <login-node>localhost2</login-node>
    <network-connect-ip></network-connect-ip>
    <session-
id>userid9d896a45d2f2dd7e4e64a04ca57d070c5dc9228</session-
id>
    </active-user-record>
    <active-user-record>
    <active-user-name>admin</active-user-name>
    <authentication-realm>Admin Users</authentication-
realm>
    <user-roles>.Administrators</user-roles>
    <user-sign-in-time>2009/05/29 09:55:21</user-sign-in-
time>
    <events>0</events>
    <login-node>localhost2</login-node>
    <network-connect-ip></network-connect-ip>
    <session-
id>userid5c142fc2be8e15de7e4015257f1f14af386d6ale</session-
id>
    </active-user-record>
  </active-user-records>
</get-active-users>
</rpc-reply>

```

### *disable-all-users*

The disable-all-users RPC is used to disable all active user sessions in host system and virtual system context.

#### **Schema for RPC**

```
<!-- disable-all-users -->
```

```

<xs:complexType name="disable-all-users">
  <xs:annotation>
    <xs:appinfo>
      <dmi:rpc-info>
        <name>Disable All End User </name>
        <description>
          This RPC disables all the end users on the
system
          </description>
        <rpc-reply-tag>disable-all-users-reply</rpc-reply-
tag>
      </dmi:rpc-info>
    </xs:appinfo>
  </xs:annotation>
</xs:complexType>

```

#### Example for RPC

```

<rpc message-id='101'>
  xmlns='urn:ietf:params:xml:ns:netconf:base:1.0'>
    <disable-all-users/>
  </rpc>

```

If the RPC is successful, the following is the response received. On error conditions, the error message explains the reason the command failed.

#### Example for RPC-REPLY

```

<rpc-reply message-id="12"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <ok/>
</rpc-reply>

```

### *enable-all-users*

The enable-all-users RPC is used to enable all user sessions in host system and virtual system context.

#### Schema for RPC

```

<!--enable-all-users-->

```

```

<xs:complexType name="enable-all-users">
  <xs:annotation>
    <xs:appinfo>
      <dmi:rpc-info>
        <name>Enable All End User </name>
        <description>
          This RPC enables all the end users on the system
        </description>
        <rpc-reply-tag>enable-all-users-reply</rpc-reply-
tag>
      </dmi:rpc-info>
    </xs:appinfo>
  </xs:annotation>
</xs:complexType>

```

### Example for RPC

```

<rpc message-id='101'>
  xmlns='urn:ietf:params:xml:ns:netconf:base:1.0'>
    <enable-all-users/>
  </rpc>

```

If the RPC is successful an “ok” reply is sent. On error conditions, the error message explains the reason the command failed.

### *delete-active-sessions*

The delete-active-sessions RPC is used to delete selected user sessions in host system and virtual system context.

### Schema for RPC

```

<!-- delete-active-sessions -->
<xs:complexType name="delete-active-sessions">
  <xs:annotation>
    <xs:appinfo>
      <dmi:rpc-info>
        <name>Delete Specified Active User Sessions
</name>
        <description>
          This RPC deletes some active user sessions
currently on the system
        </description>
        <rpc-reply-tag>delete-sessions-reply</rpc-reply-
tag>
      </dmi:rpc-info>
    </xs:appinfo>
  </xs:annotation>
</xs:complexType>

```

```

    </dmi:rpc-info>
  </xs:appinfo>
</xs:annotation>
<xs:choice>
  <xs:element name="session-records">
    <xs:annotation>
      <xs:appinfo>
        <dmi:param-info>
          <name>Some Users</name>
          <description>
            This parameter tells the IVE to delete the
specified users on the system
          </description>
        </dmi:param-info>
      </xs:appinfo>
    </xs:annotation>
  <xs:complexType>
  <xs:sequence>
  <xs:element name="session-record" minOccurs="0"
maxOccurs="unbounded">
  <xs:complexType>
  <xs:sequence>
  <xs:element name="name" type="xs:string">
  <xs:annotation>
  <xs:appinfo>
    <dmi:param-info>
      <name>User Name</name>
      <description>
        This is the user name. No regular expression
may be used.
      </description>
    </dmi:param-info>
  </xs:appinfo>
  </xs:annotation>
</xs:element>
  <xs:element name="authentication-realm" type="xs:string">
  <xs:annotation>
  <xs:appinfo>
    <dmi:field-info>
      <name>Authentication Realm</name>
      <desc>The authentication realm the user logged
in</desc>
    </dmi:field-info>
  </xs:appinfo>
  </xs:annotation>
</xs:element>
  <xs:element name="session-id" type="xs:string">
  <xs:annotation>
  <xs:appinfo>
    <dmi:field-info>
      <name>User Session ID</name>

```

```

        <desc>The unique user session ID </desc>
    </dmi:field-info>
</xs:appinfo>
</xs:annotation>
</xs:element>
</xs:sequence>
</xs:complexType>
</xs:element>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="all">
    <xs:annotation>
        <xs:appinfo>
            <dmi:param-info>
                <name>All Users</name>
                <description>
                    This parameter tells the IVE to delete all
active users on the system
                </description>
            </dmi:param-info>
        </xs:appinfo>
    </xs:annotation>
</xs:complexType/>
</xs:element>
</xs:choice>
</xs:complexType>

```

### Schema for RPC-REPLY

```

<!-- delete-sessions -->
<xs:complexType name="delete-sessions-reply" >
    <xs:annotation>
        <xs:appinfo>
            <dmi:rpc-reply-info>
                <description>
                    Reply from the 'delete session' request
                </description>
                <rpc-list>
                    <rpc-tag>delete-active-sessions</rpc-tag>
                </rpc-list>
            </dmi:rpc-reply-info>
        </xs:appinfo>
    </xs:annotation>

    <xs:sequence>

        <xs:element name="failed-session-number"
type="xs:integer">

```

```

    <xs:annotation>
      <xs:appinfo>
        <dmi:field-info>
          <name> Number of Failed Sessions </name>
          <desc> Number of sessions the RPC failed to
delete</desc>
        </dmi:field-info>
      </xs:appinfo>
    </xs:annotation>
  </xs:element>

  <xs:element name="failed-session-records">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="failed-session-record" minOccurs="0"
maxOccurs="unbounded">
          <xs:complexType>
            <xs:sequence>

              <xs:element name="name" type="xs:string" >
                <xs:annotation>
                  <xs:appinfo>
                    <dmi:param-info>
                      <name>User Name</name>
                      <description>
                        This is the user name. No regular expression
may be used.
                      </description>
                    </dmi:param-info>
                  </xs:appinfo>
                </xs:annotation>
              </xs:element>

              <xs:element name="authentication-realm"
type="xs:string">
                <xs:annotation>
                  <xs:appinfo>
                    <dmi:field-info>
                      <name>Authentication Realm</name>
                      <desc>The authentication realm the user logged
in</desc>
                    </dmi:field-info>
                  </xs:appinfo>
                </xs:annotation>
              </xs:element>

              <xs:element name="session-id" type="xs:string">
                <xs:annotation>
                  <xs:appinfo>
                    <dmi:field-info>
                      <name><User Session ID/name>

```

```

        <desc>The unique user session ID</desc>
      </dmi:field-info>
    </xs:appinfo>
  </xs:annotation>
</xs:element>

</xs:sequence>
</xs:complexType>
</xs:element>
</xs:sequence>
</xs:complexType>
</xs:element>
</xs:sequence>

```

### Example 1 for RPC

```

<rpc message-id='101'>
  xmlns='urn:ietf:params:xml:ns:netconf:base:1.0'>\
  <delete-active-sessions>
    <session-records><session-record>
      <name>newadmin</name>
      <authentication-realm>Admin Users</authentication-realm>
      <session-
id>userid5c142fc2be8e15de7e4015257f1f14af386d6ale</session-
id>
      </session-record></session-records>
    </delete-active-sessions>
  </rpc>

```

### Example 2 for RPC

```

<rpc message-id='101'
  xmlns='urn:ietf:params:xml:ns:netconf:base:1.0'>
  <delete-active-sessions>
    <all/>
  </delete-active-sessions>
</rpc>

```

If the RPC is successful, the following is the response received. On error conditions, the error message explains the reason the command failed.

### Example for RPC-REPLY

```

<rpc-reply message-id="101"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <delete-active-sessions>
    <failed-session-number>0</failed-session-number>
  </delete-active-sessions>
</rpc-reply>

```

## *refresh-roles*

The refresh-roles RPC is used to refresh active user session roles in host system and virtual system context.

### Schema for RPC

```

<!-- refresh-roles -->
<xs:complexType name="refresh-roles">
  <xs:annotation>
    <xs:appinfo>
      <dmi:rpc-info>
        <name>Refresh User Roles</name>
        <description>
          The Refresh Roles request results in dynamic policy
          evaluation being triggered for the selected users.
        </description>
        <rpc-reply-tag>refresh-roles-reply</rpc-reply-tag>
      </dmi:rpc-info>
    </xs:appinfo>
  </xs:annotation>
</xs:complexType>

```

### Example for RPC

```

<rpc message-id='101'>
  xmlns='urn:ietf:params:xml:ns:netconf:base:1.0'>
  <refresh-roles/>
</rpc>

```

If the RPC is successful an “ok” reply is sent. On error conditions, the error message explains the reason the command failed.

## *add-certificate*

The add-certificate RPC is used to add a certificate to the IVE. The following types of certificates can be added using the RPC:

- Device certificate

- Sun Java code signing certificate
- Microsoft Authenticode certificate

The following are the parameters that need to be specified in the RPC:

- Certificate type, the value of which can be one of DEVICE\_CERT, CODESIGN\_MSFT or CODESIGN\_SUN
- The certificate to add, encoded in base-64 format. The certificate and the private key can be packed together and specified here.
- Private key, in base 64 format, if not present in the certificate
- Password for decrypting the certificate
- The interfaces to which the certificate needs to be applied to. This is applicable only for device certificates.

### Schema for RPC

```

<!-- add-certificate -->
<xs:complexType name="add-certificate">
  <xs:annotation>
    <xs:appinfo>
      <dmi:rpc-info>
        <name>Add Certificate to IVE</name>
        <avail>
          <matches>
            <match>
              <operational-mode>logical-
systems</operational-mode>
              <value>>false</value>
            </match>
            <match>
              <value>>true</value>
            </match>
          </matches>
        </avail>
        <description>
          This command adds a certificate
        </description>
        <rpc-reply-tag>add-certificate-reply</rpc-
reply-tag>
      </dmi:rpc-info>
    </xs:appinfo>
  </xs:annotation>
  <xs:sequence>
    <xs:element name="type" type="xs:string">
      <xs:annotation>
        <xs:appinfo>
          <dmi:param-info>
            <name>Certificate Type</name>
            <description>
              The type of certificate to add
            </description>
          </dmi:param-info>
        </xs:appinfo>
      </xs:annotation>
    </xs:element>
  </xs:sequence>
</xs:complexType>

```

```

        </dmi:param-info>
    </xs:appinfo>
</xs:annotation>
<xs:simpleType>
    <xs:restriction base="xs:string">
        <xs:enumeration value="DEVICE_CERT" />
        <xs:enumeration value="CODESIGN_MSFT" />
        <xs:enumeration value="CODESIGN_SUN" />
    </xs:restriction>
</xs:simpleType>
</xs:element>
<xs:element name="cert" type="xs:string"
minOccurs="0">
    <xs:annotation>
        <xs:appinfo>
            <dmi:param-info>
                <name>Certificate</name>
                <description>
                    The certificate to add
                </description>
            </dmi:param-info>
        </xs:appinfo>
    </xs:annotation>
</xs:element>
<xs:element name="password" type="xs:string">
    <xs:annotation>
        <xs:appinfo>
            <dmi:param-info>
                <name>Password</name>
                <description>
                    The password for certificate
                </description>
            </dmi:param-info>
        </xs:appinfo>
    </xs:annotation>
</xs:element>

    <xs:element name="internal-interfaces"
minOccurs="0">
    <xs:annotation>
        <xs:appinfo>
            <dmi:param-info>
                <name>Interface</name>
                <description>
                    List of internal interfaces to apply
the device certificate to
                </description>
            </dmi:param-info>
        </xs:appinfo>
    </xs:annotation>
</xs:complexType>

```

```

    <xs:sequence>
      <xs:choice minOccurs="0"
maxOccurs="unbounded">
        <xs:element name="internal-interface"
type="xs:string" minOccurs="0">
          <xs:annotation>
            <xs:appinfo>
              <dmi:param-info>
                <name>Interface</name>
                <description>
                  Name of internal interface to
apply the device certificate to
                </description>
              </dmi:param-info>
            </xs:appinfo>
          </xs:annotation>
        </xs:element>
      </xs:choice>
    </xs:sequence>
  </xs:complexType>
</xs:element>

  <xs:element name="external-interfaces"
minOccurs="0">
  <xs:annotation>
    <xs:appinfo>
      <dmi:param-info>
        <name>Interface</name>
        <description>
          List of external interfaces to apply
the device certificate to
        </description>
      </dmi:param-info>
    </xs:appinfo>
  </xs:annotation>
  <xs:complexType>
    <xs:sequence>
      <xs:choice minOccurs="0"
maxOccurs="unbounded">
        <xs:element name="external-interface"
type="xs:string" minOccurs="0">
          <xs:annotation>
            <xs:appinfo>
              <dmi:param-info>
                <name>Interface</name>
                <description>
                  List of external interfaces to
apply the device certificate to
                </description>
              </dmi:param-info>
            </xs:appinfo>
          </xs:annotation>
        </xs:element>
      </xs:choice>
    </xs:sequence>
  </xs:complexType>
</xs:element>

```

```

        </xs:annotation>
      </xs:element>
    </xs:choice>
  </xs:sequence>
</xs:complexType>
</xs:element>

  <xs:element name="management-interface"
type="xs:boolean" minOccurs="0">
  <xs:annotation>
    <xs:appinfo>
      <dmi:param-info>
        <name>Interface</name>
        <description>
          Option for setting the device
certificate to the management interface. Applicable
only for devices with management interface.
        </description>
      </dmi:param-info>
    </xs:appinfo>
  </xs:annotation>
</xs:element>
</xs:sequence>
</xs:complexType>

```

### Example for RPC

```

<rpc message-id="12">
  <add-certificate>
    <type>DEVICE_CERT</type>
    <cert>
      MIIIBgIBAzCCB8wGCSqGSIB3DQEHAaCCB70Egge5MIIHtTCCBIcGC
      SqGSIB3DQEHBqCCBHgwggR0AgEAMIIIEbQYJKoZIhvcNAQcBMBwGCi
      qGSIB3DQEEMAQYwDgQIAtiwIAYUYw0CAggAgIIEQIRnbl7WN3rhElt
      QCFsYgcaDuGYo/QVRnk/8oBEuIfBsiX3QX9ba3SS0T6em148QmA0j
      1KCJG7nzPnrAX+mqv4R/Az3WCw8GZVL3/j9RGYbEByXBKYB7++trb
      WOcbA6DZqwP0r0clFBzV1a2uG+Vm+uawcPbKti3x9nHel9AZnPMb/
      U/QRo/tCfdTAuti0Rgpmv1CdNe2vU19i/qGJB4etf17+GC4cSTOTm
      TxPlIrB889ST9KOPWPXpmRn2tY2AczWVM/9HqjDChyGTGT0eQICBq
      CdZ4a/zF7NcHe+ffWWvROcnvJx8UxcLwUylm2x1A+lCa8SMNz18Y
      nGxeWIHtrfiES5dSMUQ6ojLgJrKFoD/rE4MGAIqvbS/1kGbiQCvr7
      4y09qapCAqNEtRR/tow5JbXuuKSOUuhrpEzSRieOLAvnkmkEMcmR
      VNz75tH4i7+pU7dowFYJUT6vTEtn3ESNZCc jNAWNvPHz/cdiEsNGn
      31wmwR01WkgMzEhNKYhrZbIi039YbjoSq8FQDIrgoJpg7Nsdy8RUc
      YrJZiapSPBg6DIbc0QqvomubgYdIYWv0+D9V7ewe/ulddAzmvYCqD
      VGkdyDJyzlguNn84Y5J7Z8LJ39bGX1J5G5XX6z/Ju4WgOWO0S7wGp
      mNuY2O98XViS056gxewW8Yc8Z9DFzxxJcocB0oLsVXE0d0az3PJL0
      8zbJ4jU1haadjpuwF1dZKe+VGUN70cn7JbiP5YfI0GuCJFK/QJMbx
      2nD0N6s9/+9Gozo2tx01nx3pEOzHTmqNOUpXyZ10dRgQ/p3JHGpgk
    </cert>
  </add-certificate>
</rpc>

```

```

UGOFuI9/cVHha/jRI1QTruVpw8BzpyH5ESJ/eEFi6/YnQEzRaDU0v
KhH1PNOM95DrCscIm6JTfyA0eibL5UXBsfYWrfNtbAo9TruqXMFC3
okiHU+mQfNVF7eszeFQMZOVR3ZKFABLgltR/5zZxmvQbulvEJ0S+
x4lOWiARH4DXHS/Nase0I0S3zfx9ugZmXEZ7Qo5GBk4L0bOHcl1PZ
5N65eGyP9EIlFLEuCrOoDbrRFKo07JYpwgfsyecdgfoPKiW854WYO
04uTSvd7qwDl3cu5y2eHy2moepGfD5ihycVzut16bcdTBid+ZM+64
m10GCYUtXkhbbnlTj7SOR+zlkey3m8z29sajzT6H52ON8X569HrkH
rJZCwQwT+rqcZox23T1WKCl8oAeLJd95Ja0p5+N/3k3Nw+Zst/cbp
2j9Sy7kWeIXfOPSbc4R+6WpWevkV9BoV4+eQJjYk5Zagi/IV4hM70
X2GFQBaaWnQm/RlOMnAorhNipG909tvXwPNQRcp5CbtK7ajxo0hkG
QfCDBgOZY9lJ0gQTE+2EWHngkmJFJ+Kk jNkRDOior5hnXtqwxZurb
/jk6EgKgVp2coYC96IkhluFxFHIzuInEZ4OMzT1aTBhJr9luHtpZDn
S3KccJMIIDJgYJKoZIHvcNAQcBoIIDFwSCAxMwggMPMIIDCwYLKoZ
IhvcNAQwKAQKgggKmMIIcojAcBgoqhkiG9w0BDAEDMA4ECMCgXfB7
CuWXAgIIAASCAoA061b8b3oF+Kw5OGkmXxGMgqFWEgCGBUfAeX3UG
0QmQHnYJ0X+8iKkNZ2vqbtzbxo0/AL2QQTE3ckIOop31AvtmG9n8Y
S0MTLdauJQhYuAdNSvlfzMcEvjK/eS7pEl5WNAkJxFDBZsbZQI3yc
5whjbsyxZktx0UCuXeCxbDf8zUCbA/vNspjTjoe7Bk60oWZGceyZl
C7tgTt4s84TR8wTmlicc05wr1DZSmtyzocelH/oU59UOpZeT4GQWk
AL0Lgn0B27Xnw8/6CKJEUAA7+XNhYI1jBqMyyaK4wyGZe2e0ztarK
OifVRem0Z/6B5YLyFJMiTozlbJqB350cM5lo9ApYWJpwJNzOt9pKX
x7P9qf0tHDTtr9oLnJ0ymzJldRM37ct/OBOPLovEGbxMhIccQs9aQ
Xog4+I+EqCxdIbKT9hW03zCFBubQrxhfS2aPpyc7sDcFa7ehkBTGg
n0518HRWSK1M989c5fErmFuCgkYZZxmoXdzBwPMeVh0LtudeZvgqW
jDBH1zICWRE3cNr+5VjSbNA+RC9j+MKu+PI/KgkLEbOFPMQxADZWV
j9s++y+RzD2wiE3s4bae+A4X+JtHmqHfCJlwAsxxZKnu2mbGCvFmp
wKswPLuvkDADNki+74Xr2UaClz+q+jDihdbWjKaN2PfYsGuz+g/j8
soiHwDM0fIp1fKsKRY3ijPGZMXAI3WErvpy5dHx7oysBf0t+Ehmy3
Lh5ljtWaFmlN1fVDelWBHmfTnne0FbmVosp7kiawyRq8R8uN0tfVA
hbceKrzxA7fTnE7Fc3H1ZU/KxP9NpURG6XFFDLlv7XboO+WZyjGk
fhY7j2ZJUX6x+DY0toKGMVIwIwYJKoZIHvcNAQkVMRYEFGVBzyRqj
OEWZ6Fwz4G9v/uPgHgrMCsGCSqGSIB3DQEJFDEeHhwATQB5ACAAQw
BLAHIAdABpAGYAAQBJAGEAdABLMDEwITAJBgUrDgMCGGUABBRsavo
lCiL9JTZfoPt+4p2AWb7f+wQIDO65WtjEV/QCaggA</cert>
<password>juniper</password>
<external-interfaces>
  <external-interface>&#x3C;External
  Port&#x3E;</external-interface>
</external-interfaces>
</add-certificate>
</rpc>

```

If the request is successful an “ok” reply is sent. On error conditions, the error message explains the reason the command failed.

### get-certificate-info

The get-certificate-info RPC is used to get information about a certificate present in the IVE.

The following parameters need to be specified in the RPC to retrieve the information:

- Type of certificate, which can be one of DEVICE\_CERT, CODESIGN\_MSFT or CODESIGN\_SUN
- Subject common name, an optional parameter. If specified, information about the certificate with the specified common name will be retrieved and if not, information about all the certificates of the specified type will be retrieved.

### Schema for RPC

```

<!-- get-certificate-info -->
<xs:complexType name="get-certificate-info">
  <xs:annotation>
    <xs:appinfo>
      <dmi:rpc-info>
        <name>Get Certificate from IVE</name>
        <avail>
          <matches>
            <match>
              <operational-mode>logical-
systems</operational-mode>
              <value>>false</value>
            </match>
            <match>
              <value>>true</value>
            </match>
          </matches>
        </avail>
        <description>
          This command gets information about a
certificate
        </description>
        <rpc-reply-tag>certificate-info</rpc-reply-tag>
      </dmi:rpc-info>
    </xs:appinfo>
  </xs:annotation>
  <xs:sequence>
    <xs:element name="type" type="xs:string">
      <xs:annotation>
        <xs:appinfo>
          <dmi:param-info>
            <name>Certificate Type</name>
            <description>
              The type of certificate to get
            </description>
          </dmi:param-info>
        </xs:appinfo>
      </xs:annotation>
    </xs:element>
    <xs:element name="subject-common-name"
type="xs:string" minOccurs="0">
      <xs:annotation>

```

```

    <xs:appinfo>
      <dmi:param-info>
        <name>Subject Common Name</name>
        <description>
          Subject common Name of certificate requested
        </description>
      </dmi:param-info>
    </xs:appinfo>
  </xs:annotation>
</xs:element>
</xs:sequence>
</xs:complexType>

```

### Schema for RPC-REPLY

```

<!-- get-certificate-info-reply -->
<xs:complexType name="certificate-info">
  <xs:annotation>
    <xs:appinfo>
      <dmi:rpc-reply-info>
        <description>
          Certificate information
        </description>
        <rpc-list>
          <rpc-tag>get-certificate-info</rpc-tag>
        </rpc-list>
      </dmi:rpc-reply-info>
    </xs:appinfo>
  </xs:annotation>

  <xs:sequence>

    <xs:element name="certificates">
      <xs:complexType>
        <xs:sequence>

          <xs:element name="certificate" minOccurs="0"
            maxOccurs="unbounded">
            <xs:complexType>
              <xs:sequence>

                <xs:element name="subject" minOccurs="0">
                  <xs:complexType>
                    <xs:sequence>

                      <xs:element name="common-name"
                        type="xs:string">
                        <xs:annotation>
                          <xs:appinfo>

```

```

        <dmi:field-info>
            <name>Subject Common Name</name>
            <desc>Subject Common Name</desc>
        </dmi:field-info>
    </xs:appinfo>
</xs:annotation>
</xs:element>

<xs:element name="email" type="xs:string">
    <xs:annotation>
        <xs:appinfo>
            <dmi:field-info>
                <name>Subject Email Address</name>
                <desc>Subject Email Address</desc>
            </dmi:field-info>
        </xs:appinfo>
    </xs:annotation>
</xs:element>

    <xs:element name="organization"
type="xs:string">
        <xs:annotation>
            <xs:appinfo>
                <dmi:field-info>
                    <name>Subject Organization</name>
                    <desc>Subject Organization</desc>
                </dmi:field-info>
            </xs:appinfo>
        </xs:annotation>
    </xs:element>

    <xs:element name="organization-unit"
type="xs:string">
        <xs:annotation>
            <xs:appinfo>
                <dmi:field-info>
                    <name>Subject Organization
Unit</name>
                    <desc>Subject Organization
Unit</desc>
                </dmi:field-info>
            </xs:appinfo>
        </xs:annotation>
    </xs:element>

    <xs:element name="locality" type="xs:string">
        <xs:annotation>
            <xs:appinfo>
                <dmi:field-info>
                    <name>Subject Locality</name>
                    <desc>Subject Locality</desc>
                </dmi:field-info>
            </xs:appinfo>
        </xs:annotation>
    </xs:element>

```

```

        </dmi:field-info>
    </xs:appinfo>
</xs:annotation>
</xs:element>

<xs:element name="state" type="xs:string">
    <xs:annotation>
        <xs:appinfo>
            <dmi:field-info>
                <name>Subject State</name>
                <desc>Subject State</desc>
            </dmi:field-info>
        </xs:appinfo>
    </xs:annotation>
</xs:element>

<xs:element name="country" type="xs:string">
    <xs:annotation>
        <xs:appinfo>
            <dmi:field-info>
                <name>Subject Country</name>
                <desc>Subject Country</desc>
            </dmi:field-info>
        </xs:appinfo>
    </xs:annotation>
</xs:element>

</xs:sequence>
</xs:complexType>
</xs:element>

<xs:element name="issued-by" minOccurs="0">
    <xs:complexType>
        <xs:sequence>

            <xs:element name="common-name"
type="xs:string">
                <xs:annotation>
                    <xs:appinfo>
                        <dmi:field-info>
                            <name>Issuer Common Name</name>
                            <desc>Issuer Common Name</desc>
                        </dmi:field-info>
                    </xs:appinfo>
                </xs:annotation>
            </xs:element>

            <xs:element name="email" type="xs:string">
                <xs:annotation>
                    <xs:appinfo>
                        <dmi:field-info>

```

```

        <name>Issuer Email Address</name>
        <desc>Issuer Email Address</desc>
    </dmi:field-info>
</xs:appinfo>
</xs:annotation>
</xs:element>

    <xs:element name="organization"
type="xs:string">
        <xs:annotation>
            <xs:appinfo>
                <dmi:field-info>
                    <name>Issuer Organization</name>
                    <desc>Issuer Organization</desc>
                </dmi:field-info>
            </xs:appinfo>
        </xs:annotation>
    </xs:element>

    <xs:element name="organization-unit"
type="xs:string">
        <xs:annotation>
            <xs:appinfo>
                <dmi:field-info>
                    <name>Issuer Organization
Unit</name>
                    <desc>Issuer Organization
Unit</desc>
                </dmi:field-info>
            </xs:appinfo>
        </xs:annotation>
    </xs:element>

    <xs:element name="locality" type="xs:string">
        <xs:annotation>
            <xs:appinfo>
                <dmi:field-info>
                    <name>Issuer Locality</name>
                    <desc>Issuer Locality</desc>
                </dmi:field-info>
            </xs:appinfo>
        </xs:annotation>
    </xs:element>

    <xs:element name="state" type="xs:string">
        <xs:annotation>
            <xs:appinfo>
                <dmi:field-info>
                    <name>Issuer State</name>
                    <desc>Issuer State</desc>
                </dmi:field-info>
            </xs:appinfo>
        </xs:annotation>
    </xs:element>

```

```

        </xs:appinfo>
    </xs:annotation>
</xs:element>

<xs:element name="country" type="xs:string">
    <xs:annotation>
        <xs:appinfo>
            <dmi:field-info>
                <name>Issuer Country</name>
                <desc>Issuer Country</desc>
            </dmi:field-info>
        </xs:appinfo>
    </xs:annotation>
</xs:element>

</xs:sequence>
</xs:complexType>
</xs:element>

<xs:element name="validity" minOccurs="0">
    <xs:complexType>
        <xs:sequence>

            <xs:element name="from" type="xs:string">
                <xs:annotation>
                    <xs:appinfo>
                        <dmi:field-info>
                            <name>from</name>
                            <desc>Date and time the certificate
is valid from</desc>
                        </dmi:field-info>
                    </xs:appinfo>
                </xs:annotation>
            </xs:element>

            <xs:element name="to" type="xs:string">
                <xs:annotation>
                    <xs:appinfo>
                        <dmi:field-info>
                            <name>to</name>
                            <desc>Date and time the certificate
is valid to</desc>
                        </dmi:field-info>
                    </xs:appinfo>
                </xs:annotation>
            </xs:element>

        </xs:sequence>
    </xs:complexType>
</xs:element>

```

```

<xs:element name="details" minOccurs="0">
  <xs:complexType>
    <xs:sequence>

      <xs:element name="version" type="xs:integer">
        <xs:annotation>
          <xs:appinfo>
            <dmi:field-info>
              <name>Version</name>
              <desc>version</desc>
            </dmi:field-info>
          </xs:appinfo>
        </xs:annotation>
      </xs:element>

      <xs:element name="serial-number"
type="xs:string">
        <xs:annotation>
          <xs:appinfo>
            <dmi:field-info>
              <name>Serial Number</name>
              <desc>Serial Number</desc>
            </dmi:field-info>
          </xs:appinfo>
        </xs:annotation>
      </xs:element>

      <xs:element name="signature-algorithm"
type="xs:string">
        <xs:annotation>
          <xs:appinfo>
            <dmi:field-info>
              <name>Signature Algorithm</name>
              <desc>Signature Algorithm</desc>
            </dmi:field-info>
          </xs:appinfo>
        </xs:annotation>
      </xs:element>

      <xs:element name="public-key-algorithm"
type="xs:string">
        <xs:annotation>
          <xs:appinfo>
            <dmi:field-info>
              <name>Public Key Algorithm</name>
              <desc>Public Key Algorithm</desc>
            </dmi:field-info>
          </xs:appinfo>
        </xs:annotation>
      </xs:element>

```

```

        <xs:element name="public-key-type"
type="xs:string">
            <xs:annotation>
                <xs:appinfo>
                    <dmi:field-info>
                        <name>Public Key Type</name>
                        <desc>Public Key Type</desc>
                    </dmi:field-info>
                </xs:appinfo>
            </xs:annotation>
        </xs:element>

        <xs:element name="public-key-bits"
type="xs:string">
            <xs:annotation>
                <xs:appinfo>
                    <dmi:field-info>
                        <name>Public Key Bits</name>
                        <desc>Public Key Bits</desc>
                    </dmi:field-info>
                </xs:appinfo>
            </xs:annotation>
        </xs:element>

        <xs:element name="public-key"
type="xs:string">
            <xs:annotation>
                <xs:appinfo>
                    <dmi:field-info>
                        <name>Public Key Modulus</name>
                        <desc>Public Key Modulus</desc>
                    </dmi:field-info>
                </xs:appinfo>
            </xs:annotation>
        </xs:element>

        <xs:element name="thumbprint-algorithm"
type="xs:string">
            <xs:annotation>
                <xs:appinfo>
                    <dmi:field-info>
                        <name>Thumbprint Algorithm</name>
                        <desc>Thumbprint Algorithm</desc>
                    </dmi:field-info>
                </xs:appinfo>
            </xs:annotation>
        </xs:element>

        <xs:element name="thumbprint"
type="xs:string">
            <xs:annotation>

```

```

        <xs:appinfo>
          <dmi:field-info>
            <name>Thumbprint</name>
            <desc>Thumbprint</desc>
          </dmi:field-info>
        </xs:appinfo>
      </xs:annotation>
    </xs:element>

    </xs:sequence>
  </xs:complexType>
</xs:element> <!-- details-->

</xs:sequence>
</xs:complexType>
</xs:element> <!-- certificate-->

</xs:sequence>
</xs:complexType>
</xs:element> <!-- certificates-->

</xs:sequence>
</xs:complexType> <!-- certificate-info -->

```

The following RPC gets information about all the device certificates present in the IVE.

#### Example for RPC

```

<rpc message-id="123">
  <get-certificate-info>
    <type>DEVICE_CERT</type>
  </get-certificate-info>
</rpc>

```

#### Example for RPC-REPLY

```

<rpc-reply message-id="123"
  xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <certificates>
    <certificate>
      <subject>
        <common-name>jn.net</common-name>
        <common-name>jn.net</common-name>
        <email>??</email>
        <organization>slt</organization>
        <organization-unit>??</organization-
unit>
        <locality>??</locality>
        <state>??</state>

```

```

        <country>??</country>
    </subject>
    <issued-by>
        <common-name>jn.net</common-name>
        <email>??</email>
        <organization>slt</organization>
        <organization-unit>??</organization-
unit>
        <locality>??</locality>
        <state>??</state>
        <country>??</country>
    </issued-by>
    <validity>
        <from>Feb 11 16:44:14 2010
GMT</from>
        <to>Aug  4 16:44:14 2015 GMT</to>
    </validity>
    <details>
        <version>1</version>
        <serial-
number>51:c9:6e:32:1d:96:36:20</serial-number>
        <signature-
algorithm>sha1WithRSAEncryption</signature-
algorithm>
        <public-key-algorithm>rsaEncryption
</public-key-algorithm>
        <public-key-type>RSA</public-key-
type>
        <public-key-bits>1024</public-key-
bits>
        <public-key>Modulus (1024 bit):
00:da:86:f8:59:27:51:88:59:61:69:7d:62:38:f2:
05:15:22:c0:50:05:30:fd:3f:65:9e:33:c9:70:fe:
73:aa:49:5f:c5:1e:6c:32:09:93:93:e9:21:f0:9d:
a5:f4:8c:f2:ee:3b:42:8f:33:88:62:0b:bf:87:ac:
e3:94:3b:c7:5a:3e:16:74:4f:d9:d7:cd:b7:c4:bd:
12:a4:bf:79:9e:2e:3f:f1:c1:9c:82:f8:70:88:29:
14:05:3f:94:9e:f3:62:cf:ac:d2:51:a4:7e:8f:56:
bd:78:09:ea:c3:d2:65:03:90:c8:40:12:83:0e:b5:
e5:7b:a5:65:a7:a4:83:7b:07
Exponent: 65537 (0x10001)
</public-key>
        <thumbprint-algorithm>SHA1</thumbprint-
algorithm>
        <thumbprint>94:A9:AB:84:4A:63:57:FC:82:40:
6D:CB:A2:95:BB:2C:C4:12:51:A1</thumbprint>
    </details>
</certificate>
<certificate>
    <subject>

```

```

name> <common-name>junipernet</common-
name>
name> <common-name>junipernet</common-
name>
<email>juniper@juniper.net</email>
<organization>Juniper
Networks</organization>
<organization-
unit>Security</organization-unit>
<locality>Sunnyvale</locality>
<state>California</state>
<country>US</country>
</subject>
<issued-by>
<common-name>junipernet</common-
name>
<email>juniper@juniper.net</email>
<organization>Juniper
Networks</organization>
<organization-
unit>Security</organization-unit>
<locality>Sunnyvale</locality>
<state>California</state>
<country>US</country>
</issued-by>
<validity>
<from>Feb 11 12:44:54 2010
GMT</from>
<to>Feb 11 12:44:54 2011 GMT</to>
</validity>
<details>
<version>3</version>
<serial-number>00</serial-number>
<signature-
algorithm>md5WithRSAEncryption</signature-algorithm>
<public-key-
algorithm>rsaEncryption</public-key-algorithm>
<public-key-type>RSA</public-key-
type>
<public-key-bits>1024</public-key-
bits>
<public-key>Modulus (1024 bit):
00:aa:d5:ba:03:cb:14:dd:29:d1:48:63:7c:db:12:
df:06:84:04:d1:e8:30:dd:4b:88:ee:b2:0f:f8:18:
18:f5:5c:14:11:15:5f:37:6f:36:44:c8:21:8c:56:
b5:6e:50:6d:ea:8f:44:79:c4:4c:eb:91:88:de:8d:
db:fd:58:72:db:2c:0f:ab:19:89:bc:43:ee:47:3a:
bd:9d:cb:3f:79:b9:c7:27:82:81:8e:44:fa:2d:63:
b5:57:18:20:39:98:0d:de:c0:1e:5b:71:f8:b7:7e:
e9:85:8f:98:fd:2d:3c:ca:7d:bf:21:f0:40:d1:4f:
de:fe:06:96:70:a8:ce:bd:0b

```

```

Exponent: 65537 (0x10001)
</public-key>
      <thumbprint-
algorithm>SHA1</thumbprint-algorithm>

<thumbprint>65:41:CF:24:6A:8C:E1:16:67:A1:70:CF:81:B
D:BF:FB:8F:80:78:2B</thumbprint>
      </details>
    </certificate>
  </certificates>
</rpc-reply>
]]>]]>

```

### *get-staged-package-information*

The get-staged-package-information RPC retrieves the device staged package information such as os-name, os-version and os build number.

#### Schema for RPC

```

<!-- get-staged-package-information -->
<xs:complexType name="get-staged-package-
information">
  <xs:annotation>
    <xs:appinfo>
      <dmi:rpc-info>
        <name>Get software package
Information</name>
        <description>
          This command returns IVE staged software
package information
        </description>
        <rpc-reply-tag>staged-package-
information</rpc-reply-tag>
      </dmi:rpc-info>
    </xs:appinfo>
  </xs:annotation>
</xs:complexType>

```

#### Schema for RPC-REPLY

```

<!-- staged-package-information -->
<xs:complexType name="staged-package-information">
  <xs:annotation>

```

```

<xs:appinfo>
  <dmi:rpc-reply-info>
    <description>
      Staged Software package Information
    </description>
    <rpc-list>
      <rpc-tag>get-staged-package-
information</rpc-tag>
    </rpc-list>
  </dmi:rpc-reply-info>
</xs:appinfo>
</xs:annotation>
<xs:sequence>
  <xs:element name="os-name" type="xs:string">
    <xs:annotation>
      <xs:appinfo>
        <dmi:field-info>
          <name>Software Image OS Name</name>
          <desc>Software Image OS Name</desc>
        </dmi:field-info>
      </xs:appinfo>
    </xs:annotation>
  </xs:element>
  <xs:element name="os-version" type="xs:string">
    <xs:annotation>
      <xs:appinfo>
        <dmi:field-info>
          <desc>Software Image OS Version</desc>
        </dmi:field-info>
      </xs:appinfo>
    </xs:annotation>
  </xs:element>
  <xs:element name="build" type="xs:string">
    <xs:annotation>
      <xs:appinfo>
        <dmi:field-info>
          <name>Software Image Build Number</name>
          <desc>Software Image Build Number</desc>
        </dmi:field-info>
      </xs:appinfo>
    </xs:annotation>
  </xs:element>

</xs:sequence>
</xs:complexType>

```

The following is an example to retrieve staged package information.

#### Example for RPC

```
<rpc message-id='124'  
  xmlns='urn:ietf:params:xml:ns:netconf:base:1.0'>  
  <get-staged-package-information/>  
</rpc>
```

If the RPC is successful, the following is the response received. On error conditions, the error message explains the reason the command failed.

#### Example for RPC-REPLY

```
<rpc-reply message-id="124"  
  xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">  
  <staged-package-information>  
    <os-name>ive-sa</os-name>  
    <os-version>7.0R1</os-version>  
    <build>15106</build>  
  </staged-package-information>  
</rpc-reply>
```

## IVE Schema

---

The IVE XML schema describes the configuration tree of the IVE and is useful in constructing the requests to configure and manage the IVE. The schema can be downloaded from the Admin UI in the Export XML page, in the Maintenance menu.

As described in the DMI specification, the standard NETCONF RPCs such as get-config, edit-config etc. can be used to retrieve and update the configuration. The standard NETCONF operations such as create, delete, merge and replace are supported by the IVE.

## Sample Code

---

In this section, we illustrate some of the operations that are typically executed by the IVE administrator, by issuing RPCs using the inbound DMI. These examples will not cover all possible cases and might need certain preconditions for the operation to be successful.

The examples given include operations that are possible only on the host system, or the Root IVS and operations that are possible in both host and logical systems.

Most of these examples use the standard NETCONF operations `get-config` and `edit-config`.

### ***Get DMI Agent Configuration***

---

The following snippet gets the configuration of the DMI agent settings from the IVE.

#### **Example for RPC**

```
<rpc message-id="12">
  <get-config>
    <source>
      <running/>
    </source>
    <filter>
      <configuration>
        <system>
          <configuration>
            <dmi-agent/>
          </configuration>
        </system>
      </configuration>
    </filter>
  </get-config>
</rpc>
```

The following is an example of the reply received for the RPC requesting information about DMI agent configuration.

#### Example for RPC-REPLY

```
<rpc-reply message-id="12"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <data>
    <configuration xmlns="http://xml.juniper.net/ive-
sa/6.4R1" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" iveData="1508" saData="1407">
      <system>
        <configuration>
          <dm-agent>
            <enabled>true</enabled>
            <primary-
server>10.209.117.19</primary-server>
            <device-id>C7B91C</device-id>
            <hmac-key>netscreen</hmac-key>
            <in-enabled>true</in-enabled>
            <in-int-port-enabled>true</in-int-
port-enabled>
            <inbound-port>22</inbound-port>
          </dm-agent>
        </configuration>
      </system>
    </configuration>
  </data>
</rpc-reply>
```

Note that the parameters are returned only if the values differ from the default values for the attributes.

## Configure DMI Agent

The following snippet configures some of the inbound and outbound settings for DMI agent in IVE.

#### Example for RPC

```
<rpc message-id="12">
<edit-config>
  <target>
    <running/>
  </target>
</edit-config>
```

```

<configuration>
  <system>
    <configuration>
      <dmi-agent>
        <enabled>>true</enabled>
        <primary-server>10.20.30.50</primary-server>
        <primary-port>7804</primary-port>
        <backup-server>10.20.30.60</backup-server>
        <backup-port>7805</backup-port>
        <device-id>TheDeviceId</device-id>
        <hmac-key>TheHMAC</hmac-key>
        <admin-realm>Admin Users</admin-realm>
        <in-enabled>>false</in-enabled>
        <in-mgt-port-enabled>>false</in-mgt-port-
enabled>
        <in-int-port-enabled>>true</in-int-port-enabled>
        <inbound-port>2222</inbound-port>
      </dmi-agent>
    </configuration>
  </system>
</configuration>
</config>
</edit-config>
</rpc>

```

Note that changing some of the DMI agent settings could make the server close the current DMI session.

## ***Get Client Types***

---

To get the list of client types available in the IVE, the following get-config RPC can be issued.

### **Example for RPC**

```

<rpc message-id="12">
  <get-config>
    <source>
      <running/>
    </source>
    <filter>
      <configuration>
        <system>
          <configuration>
            <client-types/>
          </configuration>
        </system>
      </configuration>
    </filter>
  </get-config>
</rpc>

```

```

        </system>
      </configuration>
    </filter>
  </get-config>
</rpc>

```

## Add Client Type

---

The following snippet adds a client type to the client types list. By default, the client type is added to the top of the list.

### Example for RPC

```

<rpc message-id="12">
  <edit-config>
    <target><running/></target>
  <config>
    <configuration
xmlns:xsi="http://www.w3.org/2000/10/XMLSchema-instance">
      <system>
        <configuration>
          <client-types>
            <client-type-data operation="create">
              <user-agent-string-pattern>*new client
type*</user-agent-string-pattern>
              <client-type>smart-phone-html-basic</client-
type>
            </client-type-data>
          </client-types>
        </configuration>
      </system>
    </configuration>
  </config>
</edit-config>
</rpc>

```

On success, the following reply is received.

### Example for RPC-REPLY

```

<rpc-reply message-id="12"
  xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <ok/>

```

```
</rpc-reply>
```

## Get Network Configuration

---

To get only the network configuration of the device, the network sub tree can be specified in the filter in the get-config call. The following snippet shows the method to retrieve network configuration in IVE.

### Example for RPC

```
<rpc message-id="12">  
<get-config>  
  <source>  
    <running/>  
  </source>  
  <filter>  
    <configuration>  
      <system>  
        <network/>  
      </system>  
    </configuration>  
  </filter>  
</get-config>  
</rpc>
```

## Configure Network Settings

---

The network configuration can be updated using the edit-config RPC and specifying the additions or modifications in the network sub tree. For example, the following snippet creates a new VLAN.

### Example for RPC

```
<rpc message-id="12">
<edit-config>
  <target>
    <running/>
  </target>
  <config>
    <configuration>
      <system>
        <network>
          <vlans>
            <node>localhost2</node>
            <vlan operation="create">
              <name>vlan200</name>
              <settings>
                <vlan-id>200</vlan-id>
                <ip-address>10.20.30.40</ip-address>
                <netmask>255.255.0.0</netmask>
                <default-gateway>10.20.31.1</default-
gateway>
              </settings>
            </vlan>
          </vlans>
        </network>
      </system>
    </configuration>
  </config>
</edit-config>
</rpc>
```

The VLAN created with the previous RPC can be deleted with the following snippet. Only the name of the VLAN is needed for deleting it.

### Example for RPC

```
<rpc message-id="12">
<edit-config>
  <target>
```

```

    <running/>
</target>
<config>
  <configuration>
    <system>
      <network>
        <vlans>
          <node>localhost2</node>
          <vlan operation="delete">
            <name>vlan200</name>
          </vlan>
        </vlans>
      </network>
    </system>
  </configuration>
</config>
</edit-config>
</rpc>

```

## Create a Realm

---

The following samples are configurations that are available to both the host system and the logical systems. To retrieve and edit configuration for IVSes, the configuration subtree needs to be embedded inside the <logical-systems> tag and the name of the IVS needs to be specified.

The example below creates a realm with name *Admin Users*. If a realm with the name already exists, the RPC will fail.

### Example for RPC

```

<rpc message-id='101'
xmlns='urn:ietf:params:xml:ns:netconf:base:1.0'>
<edit-config>
  <target><running/></target>
  <config><configuration>
    <administrators>
      <admin-realms>
        <realm operation="create">
          <name>Admin Users</name>
          <authentication-policy>
            <source-ip>
              <customized>any-ip</customized>
            </source-ip>
            <allow-admin-signin-external-port>false
            </allow-admin-signin-external-port>
            <allow-admin-signin-internal-port>true
          </authentication-policy>
        </realm>
      </admin-realms>
    </administrators>
  </config>
</edit-config>
</rpc>

```

```

    </allow-admin-signin-internal-port>
</source-ip>
<browser>
  <customized>any-user-agent</customized>
  <user-agent-patterns>
  </user-agent-patterns>
</browser>
<certificate>
  <customized>allow-all-users</customized>
  <cert-key-value-pairs>
  </cert-key-value-pairs>
</certificate>
<password>
  <primary-password-restricted>
    allow-passwords-of-minimum-length
  </primary-password-restricted>
  <primary-password-management>false
  </primary-password-management>
  <primary-password-minimum-length>4
  </primary-password-minimum-length>
  <primary-password-expiration-warning-
days>14</primary-password-expiration-warning-days>
</password>
<host-checker>
  <evaluate-all-policies>false
  </evaluate-all-policies>
  <enforce-all-policies>false
  </enforce-all-policies>
  <evaluate-policy-list>
  </evaluate-policy-list>
  <enforce-policy-list>
  </enforce-policy-list>
  <evaluate-logic>all-policies-must-succeed
  </evaluate-logic>
</host-checker>
<limits>
  <limit-concurrent-users>false
  </limit-concurrent-users>
  <guaranteed-minimum xsi:nil="true"/>
  <maximum>-1</maximum>
</limits>
</authentication-policy>
<role-mapping-rules>
<rule>
  <name>rule 0</name>
  <user-name>
    <test>is</test>
    <user-names>*</user-names>
  </user-name>
  <roles>.Administrators</roles>
  <stop-rules-processing>>false

```

```

        </stop-rules-processing>
    </rule>
    <user-selects-role>>false
</user-selects-role>
    <user-selects-roleset>>false
</user-selects-roleset>
</role-mapping-rules>
    <description>Default authentication
realm for administrators
    </description>
    <editing-description>>false
</editing-description>
    <authentication-server>Administrators
</authentication-server>
    <directory-server>None
</directory-server>
    <accounting-server>None
</accounting-server>
    <secondary-authentication-settings>
        <name>-</name>
        <authentication-must-succeed>>true
        </authentication-must-succeed>
        <user-name-input>user
        </user-name-input>
        <predefined-user-name>
        </predefined-user-name>
        <predefined-password>
        </predefined-password>
    </secondary-authentication-settings>
    <dynamic-policy>
        <dynamic-policy-evaluation>>false
        </dynamic-policy-evaluation>
        <refresh-roles>>false</refresh-roles>
        <refresh-policies>>false
        </refresh-policies>
        <refresh-interval>60
        </refresh-interval>
    </dynamic-policy>
</realm>
</admin-realms>
</administrators>
</configuration>
</config>
</edit-config>
</rpc>

```

## Create a Realm in Logical System

---

The snippet below creates a realm with name *Admin Users*, in the IVS named *IVS1*.

### Example for RPC

```
<rpc message-id='101'
xmlns='urn:ietf:params:xml:ns:netconf:base:1.0'>
<edit-config>
  <target><running/></target>
  <config><configuration>
    <logical-systems>
      <logical-system>
        <name>IVS1</name>
        <administrators>
          <admin-realms>
            <realm operation="create">
              <name>Admin Users</name>
              <authentication-policy>
                <source-ip>
                  <customized>any-ip</customized>
                  <ips></ips>
                  <allow-admin-signin-external-port>>false
                  </allow-admin-signin-external-port>
                  <allow-admin-signin-internal-port>>true
                  </allow-admin-signin-internal-port>
                </source-ip>
                <browser>
                  <customized>any-user-agent</customized>
                  <user-agent-patterns>
                    </user-agent-patterns>
                  </browser>
                <certificate>
                  <customized>allow-all-users</customized>
                  <cert-key-value-pairs>
                    </cert-key-value-pairs>
                  </certificate>
                <password>
                  <primary-password-restricted>
                    allow-passwords-of-minimum-length
                  </primary-password-restricted>
                  <primary-password-management>>false
                  </primary-password-management>
                  <primary-password-minimum-length>4
                  </primary-password-minimum-length>
                  <primary-password-expiration-warning-
days>14</primary-password-expiration-warning-days>
                </password>
              </authentication-policy>
            </realm>
          </admin-realms>
        </administrators>
      </logical-system>
    </logical-systems>
  </config>
</edit-config>
</rpc>
```

```

<evaluate-all-policies>>false
</evaluate-all-policies>
<enforce-all-policies>>false
</enforce-all-policies>
<evaluate-policy-list>
</evaluate-policy-list>
<enforce-policy-list>
</enforce-policy-list>
<evaluate-logic>all-policies-must-succeed
</evaluate-logic>
</host-checker>
<limits>
<limit-concurrent-users>>false
</limit-concurrent-users>
<guaranteed-minimum xsi:nil="true"/>
<maximum>-1</maximum>
</limits>
</authentication-policy>
<role-mapping-rules>
<rule>
<name>rule 0</name>
<user-name>
<test>is</test>
<user-names>*</user-names>
</user-name>
<roles>.Administrators</roles>
<stop-rules-processing>>false
</stop-rules-processing>
</rule>
<user-selects-role>>false
</user-selects-role>
<user-selects-roleset>>false
</user-selects-roleset>
</role-mapping-rules>
<description>Default authentication
realm for administrators
</description>
<editing-description>>false
</editing-description>
<authentication-server>Administrators
</authentication-server>
<directory-server>None
</directory-server>
<accounting-server>None
</accounting-server>
<secondary-authentication-settings>
<name>-</name>
<authentication-must-succeed>>true
</authentication-must-succeed>
<user-name-input>user
</user-name-input>

```

```

        <predefined-user-name>
        </predefined-user-name>
        <predefined-password>
        </predefined-password>
    </secondary-authentication-settings>
    <dynamic-policy>
        <dynamic-policy-evaluation>>false
        </dynamic-policy-evaluation>
        <refresh-roles>>false</refresh-roles>
        <refresh-policies>>false
        </refresh-policies>
        <refresh-interval>60
        </refresh-interval>
    </dynamic-policy>
    </realm>
    </admin-realms>
    </administrators>
    </logical-system>
    </logical-systems>
    </configuration>
    </config>
</edit-config>
</rpc>

```

## Delete a Realm

---

This XML snippet deletes an administrator realm with name *Admin Users3*.

### Example for RPC

```

<rpc message-id='101'
xmlns='urn:ietf:params:xml:ns:netconf:base:1.0'>
<edit-config>
  <target><running/></target>
  <config><configuration>
    <administrators>
      <admin-realms>
        <realm operation="delete">
          <name>Admin Users3</name>
        </realm>
      </admin-realms>
    </administrators>
  </configuration>
</config>
</edit-config>
</rpc>

```

## Create a Role

---

This XML snippet creates an administrator role with name *role1*.

### Example for RPC

```
<rpc message-id='101'
xmlns='urn:ietf:params:xml:ns:netconf:base:1.0'>
<edit-config>
  <target><running/></target>
  <config>
    <configuration>
      <administrators>
        <admin-roles>
          <admin-role operation="create">
            <name>role1</name>
            <general>
              <overview>
                <description></description>
                <options>
                  <session-options>false</session-options>
                  <ui-options>false</ui-options>
                </options>
              </overview>
              <restrictions>
                <source-ip>
                  <customized>any-ip</customized>
                  <ips>
                    </ips>
                </source-ip>
                <browser>
                  <customized>any-user-agent</customized>
                  <user-agent-patterns>
                    </user-agent-patterns>
                </browser>
                <certificate>
                  <customized>allow-all-users</customized>
                  <cert-key-value-pairs>
                    </cert-key-value-pairs>
                </certificate>
                <host-checker>
                  <host-check-enforce>disable</host-check-
enforce>
                  <host-check-policies></host-check-
policies>
                  <host-check-match>all</host-check-match>
                </host-checker>
              </restrictions>
            <session-options>
              <idle-timeout>9</idle-timeout>
            </session-options>
          </admin-role>
        </admin-roles>
      </administrators>
    </configuration>
  </config>
</edit-config>
</rpc>
```

```

        <max-timeout>59</max-timeout>
        <roaming>disabled</roaming>
        <netmask></netmask>
    </session-options>
    <ui-options>
        <header-background-color>#336699</header-
background-color>
        <navigation-menus>auto-enabled</navigation-
menus>
        <show-copyright-notice>true</show-copyright-
notice>
    </ui-options>
</general>
<administrators>
    <manage-admin-roles>
        <enable>false</enable>
        <allow-add-remove-admin-
roles>false</allow-add-remove-admin-roles>
        <access>deny-all</access>
        <role-pages-custom-settings>
            <general>deny</general>
            <system>deny</system>
            <users>deny</users>
            <administrators>deny</administrators>
            <resource-policies>deny</resource-
policies>
            <resource-profiles>deny</resource-
profiles>
        </role-pages-custom-settings>
    </manage-admin-roles>
    <manage-admin-realms>
        <enable>false</enable>
        <allow-add-remove-admin-
realms>false</allow-add-remove-admin-realms>
        <access>deny-all</access>
        <realm-pages-custom-settings>
            <general>deny</general>
            <authentication-
policy>deny</authentication-policy>
            <role-mapping>deny</role-mapping>
        </realm-pages-custom-settings>
    </manage-admin-realms>
</administrators>
<users>
    <roles>
        <delegate-user-roles>
            <apply-to-all-roles>false</apply-to-
all-roles>
            <selected-roles>Users</selected-roles>
            <access>custom-settings</access>
            <role-pages-custom-settings>

```

```

        <general>write</general>
        <web>read</web>
        <files>write</files>
        <sam>deny</sam>
        <telnet-ssh>write</telnet-ssh>
        <terminal-services>write</terminal-
services>
        <network-connect>read</network-
connect>
        <meetings>deny</meetings>
        <email-client>deny</email-client>
        </role-pages-custom-settings>
    </delegate-user-roles>
    <delegate-read-only-roles>
        <apply-to-all-roles>false</apply-to-
all-roles>
        <selected-roles></selected-roles>
    </delegate-read-only-roles>
</roles>
<realms>
    <delegate-user-realms>
        <apply-to-all-realms>false</apply-
to-all-realms>
        <selected-realms>Users</selected-
realms>
        <access>custom-settings</access>
        <realm-pages-custom-settings>
            <general>read</general>
            <role-mapping>deny</role-mapping>
            <authentication-
policy>write</authentication-policy>
            </realm-pages-custom-settings>
        </delegate-user-realms>
        <delegate-read-only-realms>
            <apply-to-all-realms>false</apply-
to-all-realms>
            <selected-realms></selected-realms>
        </delegate-read-only-realms>
    </realms>
</users>
<system>
    <system-tasks>
        <access>deny-all</access>
        <custom-settings>
            <status>deny</status>
            <configuration>deny</configuration>
            <network>deny</network>
            <clustering>deny</clustering>
        </custom-settings>
    </system-tasks>
    <log-monitoring>

```

```

        <access>deny-all</access>
        <custom-settings>
            <events>deny</events>
            <user-access>deny</user-access>
            <admin-access>deny</admin-access>
            <sensors>deny</sensors>
            <client-logs>deny</client-logs>
            <snmp>deny</snmp>
            <statistics>deny</statistics>
        </custom-settings>
    </log-monitoring>
    <authentication>
        <access>deny-all</access>
        <custom-settings>
            <sign-in-policies>deny</sign-in-
policies>
                <sign-in-pages>deny</sign-in-pages>
                <endpoint-security>deny</endpoint-
security>
                    <servers>deny</servers>
            </custom-settings>
        </authentication>
        <maintenance-tasks>
            <access>deny-all</access>
            <custom-settings>
                <system>deny</system>
                <archiving>deny</archiving>
        </maintenance-tasks>
    </system>
    <resource-policies>
        <access>custom-settings</access>
        <web>
            <access>read</access>
            <additional-access-policies>
                <policies></policies>
                <access>read</access>
            </additional-access-policies>
        </web>
        <file>
            <access>write</access>
            <additional-access-policies>
                <policies></policies>
                <access>read</access>
            </additional-access-policies>
        </file>
        <sam>
            <access>deny</access>
            <additional-access-policies>

```

```

        <policies></policies>
        <access>read</access>
    </additional-access-policies>
</sam>
<telnet-ssh>
    <access>write</access>
    <additional-access-policies>
        <policies></policies>
        <access>read</access>
    </additional-access-policies>
</telnet-ssh>
<terminal-services>
    <access>read</access>
    <additional-access-policies>
        <policies></policies>
        <access>read</access>
    </additional-access-policies>
</terminal-services>
<network-connect>
    <access>deny</access>
    <additional-access-policies>
        <policies></policies>
        <access>read</access>
    </additional-access-policies>
</network-connect>
<email-client>
    <access>deny</access>
</email-client>
</resource-policies>
<resource-profiles>
    <access>deny-all</access>
    <web>
        <access>deny</access>
        <additional-access-profiles>
            <profiles></profiles>
            <access>read</access>
        </additional-access-profiles>
    </web>
    <file>
        <access>deny</access>
        <additional-access-profiles>
            <profiles></profiles>
            <access>read</access>
        </additional-access-profiles>
    </file>
</sam>
    <access>deny</access>
    <additional-access-profiles>
        <profiles></profiles>
        <access>read</access>
    </additional-access-profiles>

```

```

    </sam>
    <telnet_ssh>
      <access>deny</access>
      <additional-access-profiles>
        <profiles></profiles>
        <access>read</access>
      </additional-access-profiles>
    </telnet_ssh>
    <terminal-services>
      <access>deny</access>
      <additional-access-profiles>
        <profiles></profiles>
        <access>read</access>
      </additional-access-profiles>
    </terminal-services>
  </resource-profiles>
</admin-role>
<admin-role-default-options>
  <session-options>
    <idle-timeout>10</idle-timeout>
    <max-timeout>60</max-timeout>
    <roaming>enabled</roaming>
    <netmask></netmask>
  </session-options>
  <ui-options>
    <header-background-color>#336699</header-
background-color>
    <navigation-menus>auto-enabled</navigation-
menus>
    <show-copyright-notice>true</show-copyright-
notice>
  </ui-options>
</admin-role-default-options>
</admin-roles>
</administrators>
</configuration>
</config>
</edit-config>
</rpc>

```

## Create a Role in Logical System

---

The snippet below creates an admin role *role1*, in IVS named *IVS1*.

### Example for RPC

```

<rpc message-id='101'
xmlns='urn:ietf:params:xml:ns:netconf:base:1.0'>
<edit-config>

```

```

<target><running/></target>
<config>
  <configuration>
    <logical-systems>
      <logical-system>
        <name>IVS1</name>
        <administrators>
          <admin-roles>
            <admin-role operation="create">
              <name>role1</name>
              <general>
                <overview>
                  <description></description>
                  <options>
                    <session-options>false</session-options>
                    <ui-options>false</ui-options>
                  </options>
                </overview>
                <restrictions>
                  <source-ip>
                    <customized>any-ip</customized>
                    <ips>
                      </ips>
                    </source-ip>
                  <browser>
                    <customized>any-user-agent</customized>
                    <user-agent-patterns>
                      </user-agent-patterns>
                    </browser>
                  <certificate>
                    <customized>allow-all-users</customized>
                    <cert-key-value-pairs>
                      </cert-key-value-pairs>
                    </certificate>
                  <host-checker>
                    <host-check-enforce>disable</host-check-
enforce>
                    <host-check-policies></host-check-
policies>
                    <host-check-match>all</host-check-match>
                  </host-checker>
                </restrictions>
                <session-options>
                  <idle-timeout>9</idle-timeout>
                  <max-timeout>59</max-timeout>
                  <roaming>disabled</roaming>
                  <netmask></netmask>
                </session-options>
                <ui-options>
                  <header-background-color>#336699</header-
background-color>

```

```

        <navigation-menus>auto-enabled</navigation-
menus>
        <show-copyright-notice>>true</show-copyright-
notice>
        </ui-options>
    </general>
    <administrators>
        <manage-admin-roles>
            <enable>>false</enable>
            <allow-add-remove-admin-
roles>>false</allow-add-remove-admin-roles>
            <access>deny-all</access>
            <role-pages-custom-settings>
                <general>deny</general>
                <system>deny</system>
                <users>deny</users>
                <administrators>deny</administrators>
                <resource-policies>deny</resource-
policies>
                <resource-profiles>deny</resource-
profiles>
            </role-pages-custom-settings>
        </manage-admin-roles>
        <manage-admin-realms>
            <enable>>false</enable>
            <allow-add-remove-admin-
realms>>false</allow-add-remove-admin-realms>
            <access>deny-all</access>
            <realm-pages-custom-settings>
                <general>deny</general>
                <authentication-
policy>deny</authentication-policy>
                <role-mapping>deny</role-mapping>
            </realm-pages-custom-settings>
        </manage-admin-realms>
    </administrators>
    <users>
        <roles>
            <delegate-user-roles>
                <apply-to-all-roles>>false</apply-to-
all-roles>
                <selected-roles>Users</selected-roles>
            <access>custom-settings</access>
            <role-pages-custom-settings>
                <general>write</general>
                <web>read</web>
                <files>write</files>
                <sam>deny</sam>
                <telnet-ssh>write</telnet-ssh>
                <terminal-services>write</terminal-
services>

```

```

connect>
    <network-connect>read</network-
connect>
    <meetings>deny</meetings>
    <email-client>deny</email-client>
    </role-pages-custom-settings>
</delegate-user-roles>
<delegate-read-only-roles>
    <apply-to-all-roles>>false</apply-to-
all-roles>
    <selected-roles></selected-roles>
</delegate-read-only-roles>
</roles>
<realms>
    <delegate-user-realms>
to-all-realms>
    <apply-to-all-realms>>false</apply-
realms>
    <selected-realms>Users</selected-
realms>
    <access>custom-settings</access>
    <realm-pages-custom-settings>
    <general>read</general>
    <role-mapping>deny</role-mapping>
    <authentication-
policy>write</authentication-policy>
    </realm-pages-custom-settings>
</delegate-user-realms>
<delegate-read-only-realms>
to-all-realms>
    <apply-to-all-realms>>false</apply-
realms>
    <selected-realms></selected-realms>
</delegate-read-only-realms>
</realms>
</users>
<system>
    <system-tasks>
    <access>deny-all</access>
    <custom-settings>
    <status>deny</status>
    <configuration>deny</configuration>
    <network>deny</network>
    <clustering>deny</clustering>
    </custom-settings>
</system-tasks>
<log-monitoring>
    <access>deny-all</access>
    <custom-settings>
    <events>deny</events>
    <user-access>deny</user-access>
    <admin-access>deny</admin-access>
    <sensors>deny</sensors>
    <client-logs>deny</client-logs>

```

```

        <snmp>deny</snmp>
        <statistics>deny</statistics>
    </custom-settings>
</log-monitoring>
<authentication>
    <access>deny-all</access>
    <custom-settings>
        <sign-in-policies>deny</sign-in-
policies>
        <sign-in-pages>deny</sign-in-pages>
        <endpoint-security>deny</endpoint-
security>
        <servers>deny</servers>
    </custom-settings>
</authentication>
<maintenance-tasks>
    <access>deny-all</access>
    <custom-settings>
        <system>deny</system>
        <archiving>deny</archiving>
</maintenance-tasks>
<troubleshooting>deny</troubleshooting>
    </custom-settings>
</troubleshooting>
</system>
<resource-policies>
    <access>custom-settings</access>
    <web>
        <access>read</access>
        <additional-access-policies>
            <policies></policies>
            <access>read</access>
        </additional-access-policies>
    </web>
    <file>
        <access>write</access>
        <additional-access-policies>
            <policies></policies>
            <access>read</access>
        </additional-access-policies>
    </file>
    <sam>
        <access>deny</access>
        <additional-access-policies>
            <policies></policies>
            <access>read</access>
        </additional-access-policies>
    </sam>
    <telnet-ssh>
        <access>write</access>
        <additional-access-policies>

```

```

        <policies></policies>
        <access>read</access>
    </additional-access-policies>
</telnet-ssh>
<terminal-services>
    <access>read</access>
    <additional-access-policies>
        <policies></policies>
        <access>read</access>
    </additional-access-policies>
</terminal-services>
<network-connect>
    <access>deny</access>
    <additional-access-policies>
        <policies></policies>
        <access>read</access>
    </additional-access-policies>
</network-connect>
<email-client>
    <access>deny</access>
</email-client>
</resource-policies>
<resource-profiles>
    <access>deny-all</access>
    <web>
        <access>deny</access>
        <additional-access-profiles>
            <profiles></profiles>
            <access>read</access>
        </additional-access-profiles>
    </web>
    <file>
        <access>deny</access>
        <additional-access-profiles>
            <profiles></profiles>
            <access>read</access>
        </additional-access-profiles>
    </file>
    <sam>
        <access>deny</access>
        <additional-access-profiles>
            <profiles></profiles>
            <access>read</access>
        </additional-access-profiles>
    </sam>
    <telnet_ssh>
        <access>deny</access>
        <additional-access-profiles>
            <profiles></profiles>
            <access>read</access>
        </additional-access-profiles>

```

```

        </telnet_ssh>
        <terminal-services>
            <access>deny</access>
            <additional-access-profiles>
                <profiles></profiles>
                <access>read</access>
            </additional-access-profiles>
        </terminal-services>
    </resource-profiles>
</admin-role>
<admin-role-default-options>
    <session-options>
        <idle-timeout>10</idle-timeout>
        <max-timeout>60</max-timeout>
        <roaming>enabled</roaming>
        <netmask></netmask>
    </session-options>
    <ui-options>
        <header-background-color>#336699</header-
background-color>
        <navigation-menus>auto-enabled</navigation-
menus>
        <show-copyright-notice>true</show-copyright-
notice>
    </ui-options>
</admin-role-default-options>
</admin-roles>
</administrators>
</logical-system></logical-systems>
</configuration>
</config>
</edit-config>
</rpc>

```

## Delete a Role

---

The following snippet deletes an administrator role with name *role1*.

### Example for RPC

```

<rpc message-id='101'
xmlns='urn:ietf:params:xml:ns:netconf:base:1.0'>
<edit-config>
    <target><running/></target>
    <config>
        <configuration>
            <administrators>
                <admin-roles>

```

```

        <admin-role operation="delete">
            <name>role1</name>
        </admin-role>
    </admin-roles>
</administrators>
</configuration>
</config>
</edit-config>
</rpc>

```

## Create a Resource Profile

---

The snippet below creates a telnet resource profile for the role named *Users*.

### Example for RPC

```

<rpc message-id='101'
xmlns='urn:ietf:params:xml:ns:netconf:base:1.0'>
<edit-config>
    <target><running/></target>
    <config>
        <configuration>
            <users>
                <resource-profiles>
                    <telnet-ssh-profiles>
                        <telnet-ssh-profile operation="create">
                            <name>New Telnet Profile</name>
                            <description>Created through
Inbound</description>
                            <host>10.20.30.40</host>
                            <port>2345</port>
                            <roles>Users</roles>
                        </telnet-ssh-profile>
                    </telnet-ssh-profiles>
                </resource-profiles>
            </users>
        </configuration>
    </config>
</edit-config>
</rpc>

```

## Create a Resource Profile in Logical System

---

The snippet below creates a telnet resource profile for the role named *Users*, in IVS named *IVS1*.

### Example for RPC

```
<rpc message-id='101'
xmlns='urn:ietf:params:xml:ns:netconf:base:1.0'>
<edit-config>
  <target><running/></target>
  <config>
    <configuration>
      <logical-systems>
        <logical-system>
          <name>IVS1</name>
          <users>
            <resource-profiles>
              <telnet-ssh-profiles>
                <telnet-ssh-profile operation="create">
                  <name>New Telnet Profile</name>
                  <description>Created through
Inbound</description>
                  <host>10.20.30.40</host>
                  <port>2345</port>
                  <roles>Users</roles>
                </telnet-ssh-profile>
              </telnet-ssh-profiles>
            </resource-profiles>
          </users>
        </logical-system>
      </logical-systems>
    </configuration>
  </config>
</edit-config>
</rpc>
```

## Delete a Resource Profile

---

The snippet below deletes a telnet resource profile named *New Telnet Profile* for the role named *Users*.

### Example for RPC

```
<rpc message-id='101'
```

```

xmlns='urn:ietf:params:xml:ns:netconf:base:1.0'>
<edit-config>
  <target><running/></target>
  <config>
    <configuration>
      <users>
        <resource-profiles>
          <telnet-ssh-profiles>
            <telnet-ssh-profile operation="delete">
              <name>New Telnet Profile</name>
            </telnet-ssh-profile>
          </telnet-ssh-profiles>
        </resource-profiles>
      </users>
    </configuration>
  </config>
</edit-config>
</rpc>

```

## Create a Resource Policy

---

The example below creates a Windows resource access control list and assigns it to the *Users* role.

### Example for RPC

```

<rpc message-id='101'
xmlns='urn:ietf:params:xml:ns:netconf:base:1.0'>
  <edit-config>
    <target><running/></target>
    <config>
      <configuration>
        <users>
          <resource-policies>
            <file-policies>
              <file-win-acls>
                <file-win-acl operation="create">
                  <name>My Domain Windows Policy</name>
                  <description>Created through Inbound
DMI</description>
                  <resources>https://*.mydomain.com/*</resources>

                  <parent-type>none</parent-type>
                  <apply>selected</apply>
                  <role>Users</role>
                  <read-only>>false</read-only>
                </file-win-acl>
              </file-win-acls>
            </file-policies>
          </resource-policies>
        </users>
      </configuration>
    </config>
  </edit-config>
</rpc>

```

```

        </file-win-acls>
    </file-policies>
</resource-policies>
</users>
</configuration>
</config>
</edit-config>
</rpc>

```

## Create a Resource Policy in Logical System

---

The example below creates a Windows resource access control list in *IVS1* and assigns it to the *Users* role.

### Example for RPC

```

<rpc message-id='101'
xmlns='urn:iETF:params:xml:ns:netconf:base:1.0'>
  <edit-config>
    <target><running/></target>
    <config>
      <configuration>
        <logical-systems>
          <logical-system>
            <name>IVS1</name>
            <users>
              <resource-policies>
                <file-policies>
                  <file-win-acls>
                    <file-win-acl operation="create">
                      <name>My Domain Windows Policy</name>
                      <description>Created through Inbound
DMI</description>
                      <resources>https://*.mydomain.com/*</resources>

                      <parent-type>none</parent-type>
                      <apply>selected</apply>
                      <role>Users</role>
                      <read-only>>false</read-only>
                    </file-win-acl>
                  </file-win-acls>
                </file-policies>
              </resource-policies>
            </users>
          </logical-system>
        </logical-systems>
      </configuration>

```

```

</config>
</edit-config>
</rpc>

```

## Delete a Resource Policy

---

The following snippet deletes a Windows resource access control list resource policy with name *My Domain Windows Policy*.

### Example for RPC

```

<rpc message-id='101'
xmlns='urn:ietf:params:xml:ns:netconf:base:1.0'>
  <edit-config>
    <target><running/></target>
    <config>
      <configuration>
        <users>
          <resource-policies>
            <file-policies>
              <file-win-acls>
                <file-win-acl operation="create">
                  <name>My Domain Windows Policy</name>
                  <description>Created through Inbound
DMI</description>
                  <resources>https://*.mydomain.com/*</resources>

                  <parent-type>none</parent-type>
                  <apply>selected</apply>
                  <role>Users</role>
                  <read-only>>false</read-only>
                </file-win-acl>
              </file-win-acls>
            </file-policies>
          </resource-policies>
        </users>
      </configuration>
    </config>
  </edit-config>
</rpc>

```

## Create a Web Bookmark for a Role

---

The following example creates a web bookmark for the user role *Users*.

**Example for RPC**

```

<rpc message-id='101'
xmlns='urn:ietf:params:xml:ns:netconf:base:1.0'>
<edit-config>
  <target><running/></target>
  <config>
    <configuration>
      <users>
        <user-roles>
          <user-role>
            <name>Users</name>
            <web>
              <web-bookmarks>
                <bookmark operation='create'>
                  <name>Google</name>
                  <parent>--none--</parent>
                  <description>Google web site
</description>
                  <standard>
                    <url>http://www.google.com</url>
                  </standard>
                </bookmark>
              </web-bookmarks>
            </web>
          </user-role>
        </user-roles>
      </users>
    </configuration>
  </config>
</edit-config>
</rpc>

```

***Create a Web Bookmark for a Role in Logical System***

The following example creates a web bookmark for the user role *Users* in IVS named *IVS1*.

**Example for RPC**

```

<rpc message-id='101'
xmlns='urn:ietf:params:xml:ns:netconf:base:1.0'>
<edit-config>
  <target><running/></target>
  <config>
    <configuration>
      <logical-systems>

```

```

<logical-system>
  <name>IVS1</name>
  <users>
    <user-roles>
      <user-role>
        <name>Users</name>
        <web>
          <web-bookmarks>
            <bookmark operation='create'>
              <name>Gmail</name>
              <parent>--none--</parent>
              <description>Google mail</description>
              <standard>
                <url>http://mail.google.com</url>
              </standard>
            </bookmark>
          </web-bookmarks>
        </web>
      </user-role>
    </user-roles>
  </users>
</logical-system>
</logical-systems>
</configuration>
</config>
</edit-config>
</rpc>

```

### *Delete a Web Bookmark for a Role*

---

The following snippet deletes a web bookmark named *Google* which is created for the user role *Users*. Note that multiple identifiers are specified in the RPC. Both the role name and the bookmark name need to be specified.

#### **Example for RPC**

```

<rpc message-id='101'
xmlns='urn:ietf:params:xml:ns:netconf:base:1.0'>
<edit-config>
  <target><running/></target>
  <config>
    <configuration>
      <users>
        <user-roles>
          <user-role>
            <name>Users</name>
            <web>

```

```

        <web-bookmarks>
            <bookmark operation="delete">
                <name>Google</name>
            </bookmark>
        </web-bookmarks>
    </web>
</user-role>
</user-roles>
</users>
</configuration>
</config>
</edit-config>
</rpc>

```

## Get Syslog Events

---

The `get-syslog-events` RPC can be used to receive the syslog events. The administrator is advised to use a separate dedicated channel for receiving the events, as sending other RPCs in the same channel could potentially create confusion in interpreting the RPC replies received. **default-log-messages** is the only log stream supported by an IVE device.

The following example illustrates getting syslog events from the IVE.

### Example for RPC

```

<rpc message-id='101'>
  <get-syslog-events>
    <stream>default-log-messages</stream>
  </get-syslog-events>
</rpc>

```

All the syslog events that occur after the RPC is issued are notified as they occur in the inbound session. Filters can be applied to be notified of specific syslog events. For example, the following snippet notifies only the configuration change events.

### Example for RPC

```

<rpc message-id='101'>
  <get-syslog-events>
    <stream>default-log-messages</stream>
    <event>configuration-change</event>
  </get-syslog-events>
</rpc>

```

Syslog events can be filtered for logical systems. The following snippet sets the IVE to notify those syslog events that are pertinent only to *IVS1*.

#### Example for RPC

```
<rpc message-id='101'>
  <get-syslog-events>
    <stream>default-log-messages</stream>
    <parameter>ivs='IVS1'</parameter>
  </get-syslog-events>
</rpc>
```

#### Limitations in get-syslog-events

DMI recommends following the draft “draft-shafer-netconf-syslog-00.txt” for implementing the get-syslog-events RPC. Some limitations in the implementation of the RPC from the specifications in the draft are mentioned below:

1. **recorded** argument is not supported in the rpc request. This argument is ignored if specified in the request.
2. **text-pattern** argument is not supported in the rpc request. This argument is ignored if specified in the request.
3. **process** argument is not supported in the rpc request. This argument is ignored if specified in the request.
4. **priority** argument is not supported in the rpc request. This argument is ignored if specified in the request.
5. The time format specified in **start-time** and **stop-time** parameters have to be in UTC time format. Local time formats with a clock difference from UTC time is not supported.
6. If **event** parameter has **configuration-change** as the value in the RPC request, all the other filters are ignored. This is used to capture asynchronous configuration notifications from the IVE.
7. **parameter** argument can be used to filter IVE logs. The filter implementation supports custom expressions that can be used as a query for log filters. The implementation does not support generic regular expressions.

### *Configure License Client Settings*

---

The following snippet configures the IVE license client settings to enable the IVE to lease licenses from the license server. This is currently applicable only for IVE Virtual Appliances.

The client device ID specified uniquely identifies the license client in the server. For the server to lease licenses to the IVE, this client needs to be added to the license server.

**Example for RPC**

```
<rpc message-id="12"
xmlns='urn:ietf:params:xml:ns:netconf:base:1.0'>
<edit-config>
<target><running/></target>
<config>
<configuration>
<system>
<configuration>
<license-client>
<grantors>
<grantor>
<server-hostname>10.10.10.10
</server-hostname>
<preferred-network>internal
</preferred-network>
<ssl-verify>false</ssl-verify>
<node-config>
<node>localhost2</node>
<client-device-id>10.204.54.212
</client-device-id>
<password-encrypted>
3u+UR6n8AgABAAAAe9Px2XELrbvvAZACco
OJXBM1051lgG8QQLNR4hcLNrE=
</password-encrypted>
</node-config>
</grantor>
</grantors>
</license-client>
</configuration>
</system>
</configuration>
</config>
</edit-config>
</rpc>
```

## Error conditions

---

This section documents some of the probable error conditions and the reasons they could occur.

<b>Error</b>	<b>Possible reason</b>
In the DMI page in UI, the Inbound status reports "Error", when the Inbound is enabled.	The port configured for inbound might already be in use by another process.
"Connection Refused" error when trying to connect to inbound	The inbound might not have been enabled or the port might be used by some other process other than DMI.
Login unsuccessful when an inbound connection attempt is made.	If a DMI session already exists for a user, another session can not be established. Check in the Admin Access log for information.
When an RPC is issued to get or edit IVS related configuration, there is no error, but no data is returned in the rpc-reply	It is possible that the data requested is pertinent only for the host system or the root IVS.

## References

---

1. RFC 4741: NETCONF Configuration Protocol  
<http://www.ietf.org/rfc/rfc4741.txt>
2. DMI Specification version 1.2
3. Secure Shell connectivity tool:  
<http://www.openssh.com/>