Oracle® Communications Diameter Signaling Router

ENUM User Guide

Release 9.2.0.0.0
G44917-01
October 2025

Oracle Communications Diameter Signaling Router ENUM User Guide, Release 9.2.0.0.0

G44917-01

Contents

1 Introduction

1.1 Locate Product Release Software on the Oracle Software Delivery Cloud Site 1

2 Feature Description

2.1 Overview 1
2.2 ENUM MP 3
2.3 ENUM Application 3
2.4 BIND9 3
2.5 DNSDIST 4
2.5.1 Load Balancing 4
2.5.2 Congestion Control 5
2.5.3 Configuring Load Balancer 5

3 ENUM Queries Handling

3.1 ENUM Query Screening 1
3.2 ENUM Query Validation 2
3.3 vENUM Response for Enum Queries 2
3.3.1 UDR Lookup Flow 2
3.3.2 NAPTR ENUM Query Flow 3
3.3.3 NS ENUM Query Flow 4
3.3.4 CNAME ENUM Query Flow 5
3.3.5 Default ENUM Profile 5
3.4 UDR Connection with vENUM MP 6
3.5 Congestion Manager for Enum Queries 6
3.6 Flow Control for ENUM queries 6

4 Non-ENUM or DNS Query Handling

4.1 Zone Configuration 1
4.1.1 Master Zone Type 1
4.1.2 Slave Zone Type 2
4.1.3 Forward Zone Type 2

4.1.4 ENUM Zone Type 2
4.1.5 Static-Stub Zone Type 2
4.1.6 Default Zone 3
4.2 DNS Record Configuration 3
4.2.1 NAPTR Record 4
4.2.2 NS Record 5
4.2.3 A Record 5
4.2.4 AAAA Record 5
4.2.5 CNAME Record 6
4.2.6 SRV Record 6
4.2.7 PTR Record 6

5 Security Firewall

5.1 Firewall Configuration 1

6 Feature Configurations

6.1 Configurations 1
6.1.1 Configuring ENUM for UDR 2
6.1.2 UDR Redundancy 5
6.2 MMI Managed Objects for ENUM Support 6
6.3 GUI Configurations for ENUM Support 15
6.3.1 ENUM ACLs 15
6.3.2 ENUM Options 16
6.3.3 DNS Connection 17
6.3.4 DNS Zone Config 18
6.3.5 DNS Records 20
6.3.6 DNS Server Options 21
6.4 Bulk Import or Export 22
6.5 Alarms and Measurements 24

7 Troubleshooting

Preface

- Documentation Accessibility
- Diversity and Inclusion
- Conventions

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customer access to and use of Oracle support services will be pursuant to the terms and conditions specified in their Oracle order for the applicable services.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

My Oracle Support

My Oracle Support (https://support.oracle.com) is your initial point of contact for all product support and training needs. A representative at Customer Access Support can assist you with My Oracle Support registration.

Call the Customer Access Support main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. When calling, make the selections in the sequence shown below on the Support telephone menu:

1. Select **2** for New Service Request.
2. Select **3** for Hardware, Networking and Solaris Operating System Support.
3. Select one of the following options:
    - For Technical issues such as creating a new Service Request (SR), select **1**.
    - For Non-technical issues such as registration or assistance with My Oracle Support, select **2**.

You are connected to a live agent who can assist you with My Oracle Support registration and opening a support ticket.

My Oracle Support is available 24 hours a day, 7 days a week, 365 days a year.

What's New in This Guide

This section introduces the documentation updates for Release 9.2.0.0.0.

Release 9.2.0.0.0 - G44917-01, October 2025

There are no updates for the release.

1 Introduction

This document provides a brief description of the ENUM Support feature of the Oracle Communications Diameter Signaling Router. It contains the feature description, configurations, measurements, and troubleshooting details associated with the ENUM Support feature.

1.1 Locate Product Release Software on the Oracle Software Delivery Cloud Site

Oracle Communications software is available for electronic download at the Oracle Software Delivery Cloud site, https://edelivery.oracle.com. Only authorized customers with a valid password may download software from the site.

For directions on downloading the software and other information about using this site, click **FAQ** in the top right corner.

2
Feature Description

This chapter describes the ENUM Support feature.

2.1 Overview

The ENUM Support feature introduces ability in vSTP or DSR to handle DNS or ENUM queries using the UDR to store ENUM database. A new vENUM MP is introduced running ENUM application and using bind9 software to support DNS interface over UDP.

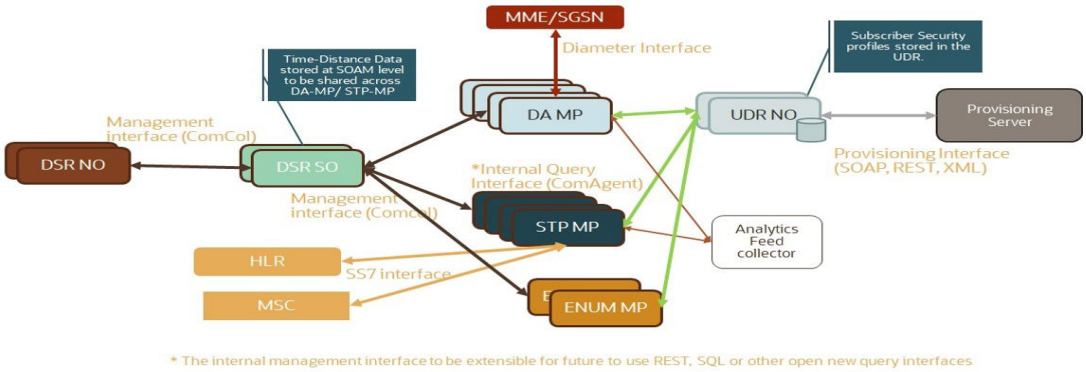
This feature introduces a new MP type (C-level server) as vENUM MP, that processes DNS or ENUM messages from external DNS clients. vENUM application running in the vENUM MP uses bind9 for interacting with the external Domain Name System (DNS) clients. vENUM MP makes UDP connections with external querying clients and receive DNS queries.

For ENUM queries, the ENUM application queries the UDR for DN received in the message. After receiving response from UDR, ENUM application generates the DNS response and sends it to the client through bind9 process.

ENUM Architecture with DSR

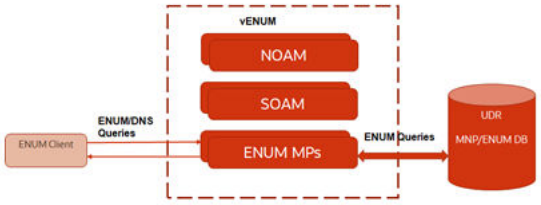
The following figure shows the overall system architecture for the ENUM feature with DSR:

Figure 2-1 ENUM Architecture with DSR



Architecture for vENUM

Figure 2-2 Architecture for vENUM

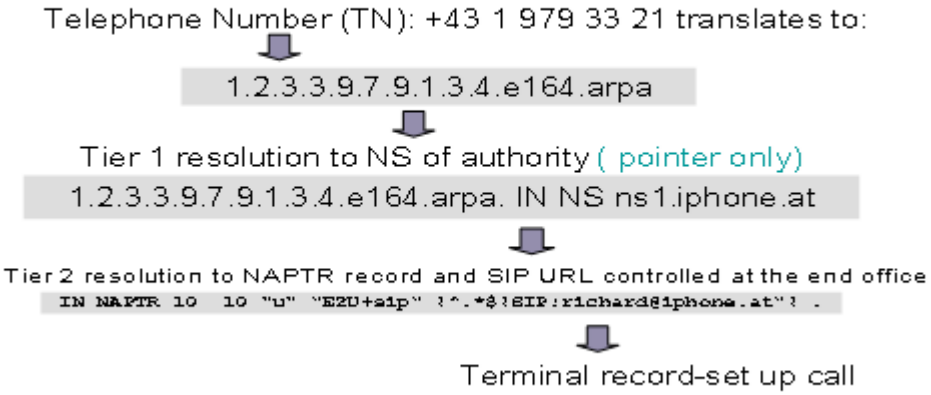


E.164 Number Mapping (ENUM)

E.164 Number Mapping (ENUM) is a Telephone Number Mapping standard defined for mapping traditional PSTN numbers in E.164 format to IP-based format such as URI. ENUM uses a special DNS record type to translate a telephone number into a URI that can be used in an IP network. ENUM allows Internet-based services, such as e-mail, VoIP, and Voice Mail, to be located based on the telephone number. ENUM accomplishes this by placing the telephone numbers into the global Domain Name System (**DNS**).

The following figure shows an example of the ENUM Tier resolution from a DNS perspective. The ENUM data format begins with a phone number, then reverses the digits, places a “.” between each number, and adds the .e164.arpa root domain that is common across both ENUM and this feature.

Figure 2-3 ENUM Tier Record Resolution



ENUM implementation is based on a tiered architecture. At Tier 0 is the **RIPE NCC** which maintains the e164.arpa zone. Entries in the RIPE NCC DNS server correspond to country codes or portions of country codes and point to the Tier 1 Registry, the authoritative DNS server for that country code or portion of country code. The Tier 1 Registry maintains records that indicate the authoritative DNS server for individual E.164 numbers in the country code or

portion thereof. The Tier 2 Provider for an E.164 number maintains the actual **NAPTR** records that contain information for specific communication services.

2.2 ENUM MP

A DSR site supports a maximum of 16 vENUM MPs. Each vENUM MP works as a standalone MP. There is no HA role for vENUM MP. By default, the ENUM process in the vENUM MP is switched OFF when a vENUM MP is deployed. User must enable the application from Graphical User Interface (GUI).

For more information, see GUI Configurations for ENUM Support. Each MP independently handles the queries received at its interface from external clients.

> **Note**
>
> ENUM requires a minimum of 150 GB disk space.
> The flavor for VM needs to have a minimum 150 GB disk space, any less space will raise issues.

2.3 ENUM Application

The ENUM application task on each vENUM MP provides the following functions:

- Receive ENUM Query messages
- Verify client IP addresses
- Validate incoming ENUM Queries
- Perform lookups in UDR
- Create and send ENUM Response messages

2.4 BIND9

vENUM MP uses BIND9 as a Domain Name Server for interacting with the Domain Name System (DNS) clients.

BIND is a suite of software for interacting with DNS. It acts as an authoritative name server for configured DNS zones and a recursive resolver in the network.

BIND9 facilitates the following functions:

Access Control

Access Control Lists (ACLs) are the address match lists that give users control over who can access the name server. These are configured in the following two categories:

- Allowed
- Blocked

The Blocked ACLs take precedence over allowed ACLs.

Forwarding ENUM queries to vENUM application

If the incoming DNS query is for an E164 number (that is ENUM query), then it if forwarded by Bind9 server to one of the available vENUM applications. The `e164.arpa` zone is the default zone configured in the Bind9 DNS server. More ENUM type zones can be added with Zone type as **ENUM** in **DNS Zone Config** MO. For further information, refer to the DNS Zone Config section.

Caching

BIND9 caches the responses through specified TTL. For ENUM queries, it uses the TTL configured in EnumOptions MO and for the non-ENUM DNS queries, it uses TTL defined in Zone and DNS Record. The advantages of caching responses are:

- Improvement in application performance
- Reduction in the load on the backend
- Reduction of database cost
- Elimination of database hotspots

> **Note**
>
> Due to caching, responses received from ENUM zones might be stale if the TTL is not set to 0 in **ENUM Options** table.

2.5 DNSDIST

vENUM MP uses DNSDIST for load balancing all incoming queries. DNSDIST is highly DNS-, DoS, and abuse aware loadbalancer, aiming to route traffic to the best server, delivering best performance to users while avoiding or blocking abusive traffic. vENUM employs DNDIST as a critical component to ensure efficient load balancing for DNS queries.

- High Availability: If a backend server is unavailable, DNDIST automatically skips it in the sequence, ensuring uninterrupted service.
- Efficiency: By evenly distributing queries, DNDIST minimizes the risk of overloading any single server, resulting in faster query responses and better user experience.
- Health Checks: DNDIST continuously monitors backend servers to identify and exclude any that are unresponsive.
- Scalability: DNDIST fluently handles increasing DNS query loads by adding more backend servers to the pool.

By leveraging DNDISTs aforementioned capabilities, vENUM ensures robust DNS load balancing, delivering optimal performance, and reliability to users. DNSDIST balances all DNS queries to all the vENUM servers in the same server group and also allows for congestion control. These are explained in the following sections.

2.5.1 Load Balancing

DNSDIST handles load balancing if the load balancer parameter is set to "Yes" in the ENUM Options MO. For more information, see ENUM Options.

DNSDIST load balances all queries over all vENUM servers in the same server group. Queries are load balanced in a round robin manner, which indiscriminately sends each query to the next server that is up.

2.5.2 Congestion Control

DNSDIST in addition includes Congestion Control functionality. The maximum query rate allowed is a total of 5k per ENUM MP that is, 5k*Number of ENUM MPs. When this threshold is crossed, the queries are silently discarded and not sent to vENUM process. This is done to ensure smooth functionality of the backend servers without overloading them.

2.5.3 Configuring Load Balancer

Following are the prerequisites to configure the load balancer:

- IMI IPs of all ENUM MPs (from same site), must be added in ENUM ACLs MO for Load Balancing.
- Load balancer must be set to "Yes" in Enum Options.
- Loadbalancer configuration can only be modified when no or low traffic is running.

3 ENUM Queries Handling

When ENUM application receives an E164 number ENUM query, it performs look-up at the UDR database on the ENUM data provisioned for the received DN in query message. Once the response is received from UDR, ENUM application generates the ENUM query response and sends it to the client through Bind9 service.

> **Note**
>
> ENUM MP supports ENUM DNS Query (NAPTR, NS, CNAME) processing.

3.1 ENUM Query Screening

The ENUM application allows ENUM Query messages to be received from only trusted ENUM clients. The ENUMACL table is used to provision the IP addresses of trusted ENUM clients. A Query message is discarded if the Query message is received from a client other than a trusted ENUM client stored in the ENUMACL table. The ENUMACL table has a maximum capacity of 100 IPADDR entries. For further information, refer to ENUM ACLs section.

Table 3-1 ENUMACL Table

Field Name	Constraints	Comments
IPADDR	• Four numbers in the range 0-255 separated by dots • Mandatory	The ENUM client IP address is allowed to query the ENUM server.

Wild Cards (*) in IP Addresses

An ACL IPADDR entry of *.*.*.* is invalid. ACL entries which overlap with other entries with wild cards are not allowed. DSR allows the use of wild cards to support IP address ranges covered by an ACL entry as follows:

- xxx.xxx.xxx.*
- xxx.xxx.*.*
- xxx.*.*.*

Table 3-2 ENUMACL Table Example Entries

IPADDR
10.250.80.41
10.250.60.*
10.252.*.*

3.2 ENUM Query Validation

The ENUM application validates the incoming ENUM Query message to verify whether the the message conforms to the Query format. At a minimum, ENUM supports validations for the error conditions shown in the following table to be handled during the validation of ENUM query:

Table 3-3 ENUM Query Validation Errors

Error Condition	Response
QR (Query/Response flag) Field in ENUM Query Header = 1	ENUM Error Response with RCODE=1 (Format Error)
OPCODE other than 0 (Not a standard DNS query)	ENUM Error Response with RCODE=4 (Not Implemented)
TC (Truncation Flag) in ENUM Query Header = 1	ENUM Error Response with RCODE=4 (Not Implemented)
TC (Truncation Flag) in ENUM query header = 0 and query packet size > 512 bytes	ENUM Error Response with RCODE=4 (Not Implemented)
Z (Reserved Field) in ENUM Query Header = 1	ENUM Error Response with RCODE=4 (Not Implemented)
RCODE(Response Code) in ENUM Query Header = 1	ENUM Error Response with RCODE=1 (Format Error)
QDCOUNT (Question Count) in ENUM Query Header > 1	ENUM Error Response with RCODE=4 (Not Implemented)
ENUM Query Question Section QNAME field root other than e164.arpa	ENUM Error Response with RCODE=3 (Non-Existent Domain Error)
ENUM Query Question Section QTYPE field other than NAPTR (35), NS (2) or CNAME (5)	ENUM Error Response with RCODE=4 (Not Implemented)
ENUM Query Question Section QCLASS field other than 1 (Internet)	ENUM Error Response with RCODE=4 (Not Implemented)

3.3 vENUM Response for Enum Queries

3.3.1 UDR Lookup Flow

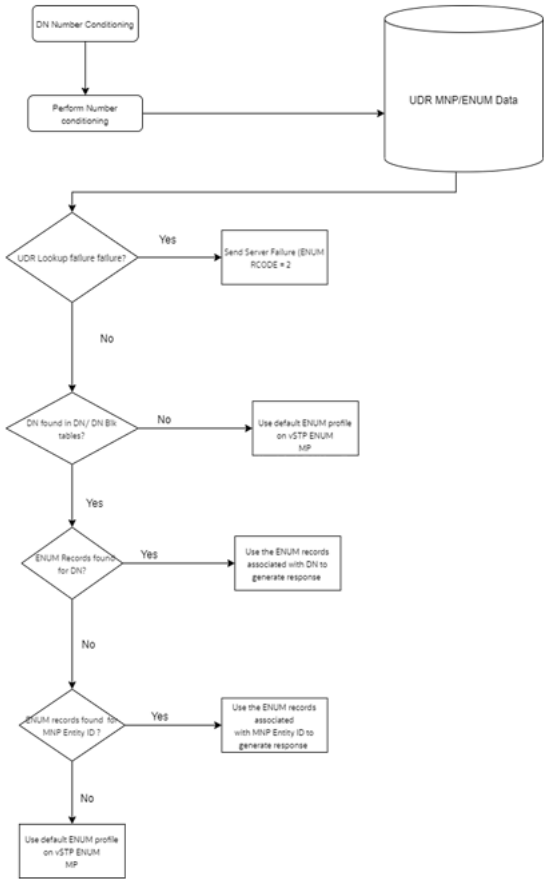
vENUM Response query flow is as follows:

1. When ENUM query is received on ENUM MP on vENUM, then retrieve the DN from the ENUM query and lookup UDR for required DN.
   If UDR is not connected to ENUM MP, then send RCODE=2 in ENUM response, otherwise proceed.
2. If DN is not found in UDR, then apply ENUM default action, otherwise proceed with the next step.
3. If ENUM Record is associated with MSISDN block in Subscriber profile, use this ENUM record while generating ENUM response, otherwise proceed with the next step.
4. If ENUM Record is associated with SPRN or GRN Entity profile, then use the preferred profile while generating ENUM response, otherwise proceed with the next step.

5. If ENUM record is not present in both subscriber and entity profile, then use default ENUM Profile from ENUMOPTION MO on ENUM MP.

The following is the flowchart for vENUM Response query.

Figure 3-1 vENUM Response



3.3.2 NAPTR ENUM Query Flow

ENUM application provides flexibility to operator to perform either of the following options:

- To provision the regex record on UDR with all required values such as RN-context, user=phone, and so on.
- To use MNP data, where ENUM application builds regex using MNP data, domain name and service configured on UDR.
  In this case, support for only below three services is provided.

  ```
  PSTNTEL ->"E2U+pstn:tel"
  PSTNSIP ->"E2U+pstn:sip"
  SIP ->"E2U+sip"
  ```

  Here, Regex is built using domain name and service is configured in UDR and RNContext (for PSTNTEL service only) and EXCLUDESP configured in EnumOptions MO. For Ported out numbers, MNP entity data is used.

NAPTR Query Steps

1. Retrieve the DN from the ENUM query and lookup UDR for required DN.
   If DN is not found in UDR, then apply ENUM default action, otherwise proceed with next step.
2. If ENUM Record is found in UDR for retrieved DN, then check if NAPTR record is present in UDR response.
   If no NAPTR record is provisioned, then apply default action, otherwise proceed with next step.

> **Note**
>
> If service parameter is not provisioned on UDR for NAPTR then assume that NAPTR record as not found.

3. For NAPTR record, if regex is provisioned in UDR, use the service, regex, flag, order and preference value provisioned on UDR while generating the ENUM response, otherwise go to next step.
   No validation on NAPTR field's value is performed by ENUM MP. If flag, order or preference value is not present in NAPTR record then use value "u", 100 and 10 respectively while generating response.

> **Note**
>
> Operator should provision the regex record on UDR with all required values like RN-context, user-phone. ENUM MP on VENUM does not perform validation on NAPTR record values. The NAPTR record values is used in response as it is provisioned on UDR.

4. If regex value is not present, then use domain name, service, flag, order and preference value, RN provisioned on UDR and build regex values to generate ENUM response.

> **Note**
>
> - If NAPTR's regex is configured in UDR for ported out number, then provide 'RN' in the NAPTR Regex for that number in UDR.
> - For ENUM queries, if NAPTR record is not present in UDR, then the default NAPTR profile data is sent in response (if configured in EnumOption MO). NS domain information is not sent in response.

3.3.3 NS ENUM Query Flow

NS ENUM query flow is as follows

1. Retrieve the DN from the ENUM query and lookup UDR for required DN.
   If DN is not found in UDR, then apply ENUM default action or proceed with next step.
2. If ENUM Record is found in UDR for retrieved DN, then check if NS record is present in UDR response.
   If no NS record is provisioned, then apply default action or proceed with next step.

3. Build ENUM response with NS data in the authority section.

3.3.4 CNAME ENUM Query Flow

CNAME ENUM Query flow is as follows:

1. Retrieve the DN from the ENUM query and lookup UDR for required DN.
   If DN is not found in UDR then apply ENUM default action, otherwise proceed with next step.
2. If ENUM Record is found in UDR for retrieved DN, then check if CNAME record is present in UDR response.
   If no CNAME record is provisioned, then apply default action or proceed with next step.
3. Build ENUM response with CNAME data in the answer section.

3.3.5 Default ENUM Profile

The section provides the default values on ENUM MP for the optional ENUM Domain Name System (DNS) resource record fields on User Deposit Repository (UDR).

A default ENUM profile is allowed in the ENUMOPTS table on ENUM MP with the following default values:

- Default Congestion Notification = yes

> **Note**
>
> Traffic above 5k is not accepted when Congestion Notification is set to "No".

- Max Data Networking (DN) Digits = 15
- Default Regex, Default flag and Default Service parameters must be provided for Default Name Authority Pointer (NAPTR) profile.
- Default Profile Order (DPODR) = 100 (Hard coded)
- Default Profile Preference (DPPREF) = 10 (Hard coded)
- Default Network Server Domain parameter must be provisioned for Default NS profile.
- CNAME default profile cannot be provisioned. In case of CNAME query, NXDOMAIN error is sent in the ENUM response.

The default ENUM profile is used by ENUM MP to generate ENUM responses for following scenarios:

- If DN is not found in individual DN or DN range subscriber profile table.
- If an ENUM profile record appropriate for the DN in incoming ENUM query (NAPTR, NS, CNAME) is associated neither with individual DN or DN range subscriber profile nor with MNP entity data.

The following rules are followed to generate ENUM responses during above scenarios:

- In case of query type and default profile type mismatch, RCODE 3(Non-Existent Domain) is sent to the client.
- In case they are matched, correct response with RCODE 0 is sent to the client.

If QTYPE is CNAME, then send an ENUM error response message with RCODE=3 (Non-Existent Domain).

3.4 UDR Connection with vENUM MP

vENUM requires UDR connection for ENUM queries, due to which a connection is made with UDR through ComAgent. vENUM MP registers Routed Service with ComAgent, so that the configured ComAgent connection is present between UDR and ENUM MP.

3.5 Congestion Manager for Enum Queries

Congestion handling for ENUM queries done by vENUM. Non-ENUM (DNS) queries are managed by bind9.

Congestion control for ENUM queries has two threshold levels for outgoing messages. An alarm is raised if TPS for incoming messages exceeding Max vENUM TPS on ENUM MP.

ENUM options table has Congestion Notification flag for response. This indicates whether to generate a response with a Congestion Notification for discarded responses. The valid values are Yes or No.

3.6 Flow Control for ENUM queries

An ENUM application can process up to the set `Max vENUM TPS` limit, above which the MP performs the following actions:

- Discards the messages.
- Notifies the client with ENUM error response if the ENUMOPTS option CNGNTFY is TRUE.
- ENUM error response message due to congestion is paced at a rate of 1 error message per 100 discarded ENUM messages at the application level.
- Pegs the measurements for total discarded ENUM messages and messages discarded due to congestion at the application level.

4

Non-ENUM or DNS Query Handling

Non-ENUM DNS Query (NAPTR, SRV, A, AAA, PTR, SRV, CNAME) processing is added on ENUM MP. For DNS implementation, use bind9 ‘addzone’ functionality to add and remove zones at run-time dynamically, without editing `named.conf` and reload or reconfigure the name server.

4.1 Zone Configuration

Zone Configuration provides the option to configure the DNS Zone using “DNS Zone Config” MO on GUI. The supported Zone types are mentioned in the following table.

Table 4-1 Zone Configuration

Zone Type	Description
Forward	Forward this query to another nameserver for further resolution.
ENUM	Special type of forward zone, in which Query is forwarded to ENUM application.
Master	Your DNS server is the authoritative source of information.
Slave	Replica of a master zone. User must configure Master IP address for this slave zone.
static-stub	Zone data is statically configured through the server-address. Only the NS records are replicated.

4.1.1 Master Zone Type

User can configure the SOA (start of authority) record if the zone type is Master. The Start of Authority record announces important authoritative information about a namespace to the name server. In Zone file, there is one NS and A record created.

For SOA record, user has to configure the parameters in the following table.

Table 4-2 Master Zone Type

Parameter Name	Description
SOA Domain Name	Primary master name server for this zone.
SOA Mail Id	Email address of the administrator responsible for this zone.
SOA IP Address	IP address for the first A record.
SOA Refresh	Number of seconds after which secondary name servers should query the master for the SOA record, to detect zone changes.
SOA Retry	Number of seconds after which secondary name servers should retry to request the serial number from the master if the master does not respond.
SOA Expire	Number of seconds after which secondary name servers should stop answering request for this zone if the master does not respond.
SOA TTL	The default time-to-live field determines the TTL of records in the zone that do not have one set explicitly.

Once user configures the DNS zone then zone file is created. User can add new DNS records in this zone file using "DNS Record Configuration" MO.

Snapshot for ZoneFile

```
$ORIGIN demo.com.
$TTL 32767
@       SOA     hostname.      hostnamemail. (
                1
                32767
                32767
                32767
                32767 )


        NS      hostname
hostname        A       10.23.2.178
```

If ENUM MP restarts and there is no change in configuration for this zone, then this zone file is not deleted. The serial number of this zone file is stored in Internal table.

If there is no change in serial number in zone file already present, then on restart of ENUM MP, this file is not deleted. If there is change in serial number then this zone file is deleted on MP and a new zone file is created with updated DNS records.

4.1.2 Slave Zone Type

A slave zone is a replica of a master zone. The masters list specifies one or more IP addresses that the slave contacts to update its copy of the zone. User must configure the IP address of Master. It is recommended to make slave zone on different Site.

4.1.3 Forward Zone Type

Query is forwarded to another nameserver for resolution. User has to configure the IP address of the forward. This new zone is created in bind9 configuration file. The forward behavior is ‘forward only’.

4.1.4 ENUM Zone Type

ENUM is special kind of forward zone. If user configured Zone type as Enum, the query is forwarded to ENUM application on its default port.

The forward behavior is ‘forward only’.

By Default, “e164.arpa” entry is added on DNS Zone MO on startup of ENUM MP.

4.1.5 Static-Stub Zone Type

It allows to force queries for a particular zone to go to specified addresses instead of recursing for the name server records of that zone.

Zone data is statically configured through the server-address. Zone details is added in `named.conf` file.

Sample format:

```
zone "demo4.com" IN {
 type static-stub;
 server-addresses { ***.***.**.**; }; // ip on which query will be forwarded
for resolution
};
```

4.1.6 Default Zone

The default zone serves as a catch-all mechanism to ensure that all incoming DNS queries, regardless of the requested domain, are being processed appropriately. This means that even if a specific zone hasn't been defined in the DNS Zone Config MO, the vENUM application steps in to provide an NXDOMAIN response to the client.

4.2 DNS Record Configuration

This DNS record is associated with the zone specified by the user. The Record type in the following table are currently supported:

Table 4-3 Resource Record

Type	Description	Function	RDATA format
NAPTR	Naming Authority Pointer	Allows regular-expression-based rewriting of domain names which can then be used as URIs, further domain names to lookups.	Order, preference, flag, Regex and replacement domain.
NS	Name server record	Delegates a DNS zone to use the given authoritative name servers	Domain Name (A record must be present for this domain). If "." is not added to the end of RDATA, origin (zone name) is appended to it. If "." is added, nothing is appended to the RDATA. NS records cannot be looked up, these are only shared in the authority section.
A	Address record	Returns a 32-bit IPv4 address, most commonly used to map hostnames to an IP address of the host.	IP address
AAAA	IPv6 address record	Returns a 128-bit IPv6 address, most commonly used to map hostnames to an IP address of the host.	IPv6 address
CNAME	Canonical name record	Alias of one name to another. The DNS lookup continues by retrying the lookup with the new name.	Canonical Domain name If "." is not added to the end of RDATA, origin (zone name) is appended to it. If "." is added, nothing is appended to the RDATA.

Table 4-3 (Cont.) Resource Record

Type	Description	Function	RDATA format
SRV	Service locator	Generalized service location record, used for newer protocols instead of creating protocol-specific records.	Priority weight port target
PTR	PTR Resource Record	Pointer to a canonical name. Unlike a CNAME, DNS processing stops and just the name is returned. The most common use is for implementing reverse DNS lookups.	Canonical Name If "." is not added to the end of RDATA, origin (zone name) is appended to it. If "." is added, nothing is appended to the RDATA.

Note

Before upgrade, it is recommended to delete all the invalid DNS Record entries from GUI for which the DNS alarm is `Active`. If these are not deleted, then all the DNS Config alarms for invalid DNS entries can be cleared after the upgrade, but GUI shall still hold the invalid entries.

4.2.1 NAPTR Record

NAPTR stands for Name Authority Pointer. NAPTR records are most commonly used for applications in Internet telephony.

A NAPTR record contains the following information:

- Type
- Order
- Preference
- Flags
- Service
- Regex
- Replacement

The following table lists example values for each field.

Table 4-4 NAPTR Record

Field	Example
domainName	9.0.0.9.9.8.4.7.3.3.e164.arpa.
TTL	86400
type	SRV
order	100
preference	10
flags	"p"

Table 4-4 (Cont.) NAPTR Record

Field	Example
service	"E2U+PSTN:SIP"
regex	"!^.*$!tel: +1-215-555-0123\;npdi\;rn=+1-215-555-0199!"
replacement	.

NAPTR records are formatted as follows:

```
domainName TTL type order preference flags service regex replacement
```

Formatting the sample record accordingly:

```
9.0.0.9.9.8.4.7.3.3.e164.arpa. 604800 NAPTR 100 10 "p" "E2U+PSTN:SIP" "!^.*$!
tel:+1-215-555-0123\;npdi\;rn=+1-215-555-0199!" .
```

4.2.2 NS Record

NS stands for nameserver, and the nameserver record indicates which DNS server is authoritative for that domain. It specified which server contains the actual DNS records.

The following table lists example values for each field.

Table 4-5 NS Record

Domain Name	TTL	Record Type	Value
example.com	14400	NS	ns1.exampleserver.com

4.2.3 A Record

The A stands for address and this is the most fundamental type of DNS record. It indicates the IP address of a given domain. The following table contains an example of an A record.

Table 4-6 A Record

Domain Name	TTL	Record Type	Value
example.com	14400	A	192.0.2.1

4.2.4 AAAA Record

DNS AAAA records match a domain name to an IPv6 address. The following table lists example values for each field.

Table 4-7 AAAA Record

Domain Name	TTL	Record Type	Value
example.com	14400	AAAA	2001:0db8:85a3:0000:0000:8a2e:0370:7334

4.2.5 CNAME Record

The DNS CNAME record works as an alias for domain names that share a single IP address. The following table lists example values for each field.

Table 4-8 CNAME Record

Domain Name	TTL	Record Type	Value
blog.example.com	14400	CNAME	www.example.com

4.2.6 SRV Record

The DNS "service" (SRV) record specifies a host and port for specific services.

An SRV record contains the information mentioned in the following table with example values for each field.

Table 4-9 SRV Record

Field	Example
service	XMPP
protocol	TCP
domainName	example.com
TTL	86400
recordType	SRV
priority	10
weight	5
port	5223
target	server.example.com.

SRV records are formatted as follows:

```
_service._protocol.domainName. TTL recordType priority weight port target
```

Formatting the sample record accordingly:

```
_xmpp._tcp.example.com. 86400 SRV 10 5 5223 server.example.com.
```

4.2.7 PTR Record

A DNS pointer record (PTR) provides the domain name associated with an IP address. DNS PTR records are used in reverse DNS lookups.

In IPv4: DNS PTR records are stored under the IP address (reversed), and with `.in-addr.arpa` added.

For example: The PTR record for the IP address 192.0.2.255 would be stored under `255.2.0.192.in-addr.arpa`.

Table 4-10 PTR Record - 192.0.2.255

Domain Name	TTL	Record Type	Value
1.2.0.192.in-addr.arpa	14400	PTR	example.com

In IPv6: IPv6 PTR records are stored under the IPv6 address (reversed) and converted into four-bit sections, along with `.ip6.arpa`.

Table 4-11 IPv6 PTR Records

Domain Name	TTL	Record Type	Value
7334.0370.8a2e.0000.0000.85a3.0db8.2001.ip6.arpa	14400	PTR	example.com

5 Security Firewall

vENUM achieves network security using the Linux firewall provided by the Oracle Linux distribution. This serves as the platform for vENUM software. vENUM configures firewall rules in the Linux firewall on each server to allow only essential network traffic. The VENUM software is composed of various components each providing unique services, each component is responsible to configure the firewall rules to allow the network traffic destined to and originated from the provided services.

This feature brings flexibility and capability in vENUM to dynamically determine and customize the Linux firewall on each vENUM-MP server in the vENUM node. This allows only the essential network traffic pertaining to the active configuration.

The in-bound signaling traffic is accepted by the vENUM application over the configured DNS Connections only. By monitoring the connections and allowed connections list, this feature determines the incoming packets to be processed. It then configures the Linux Firewall on the vENUM-MP servers to allow the network traffic for those connections only and completely denies the non-signaling network traffic. Thus, providing added security to the signaling networks.

> **Note**
>
> The non-signaling traffic is traffic from internal services, such as SSH, FTP, HTTP, HTTPS, and so on.

5.1 Firewall Configuration

To achieve the firewall security on VENUM server, follow the below recommendations:

- Add connection in DNS Connections MO on which external client communicates. Also, add Client's IP in ENUM ACLs MO to make its entry in the firewall trusted list.

  > **Note**
  >
  > – We can't provide drop packets protection on XMI interface since it is used for external communication and this IP is a publicly exposed IP.
  >
  > – IMI IPs of all ENUM MPs (from same site), must be added in ENUM ACLs MO for Load Balancing.

- In case of **Master Slave Zones and Zone Forwarding**, ensure the following configurations for firewall protection:
  - For forward zone, add connection in DNS Connections MO on which the source communicates. Also, IP of the source should be in destination's ACL MO.
  - If XMI interfaces is used, then check if there is any connection on the default DNS port at master server. If there is connection present on default DNS port, then have IP of the slave in master's ENUM ACL MO and Connection in the DNS Connection MO.

> **Note**
>
> Since Signaling Interfaces are blocked for SSH, do not use it for master slave replication.

6 Feature Configurations

This section provides procedures to perform the ENUM Support feature configurations.

The ENUM setup can be configured using ONE PUSH with the ENUM heat template.

Once the setup is complete, ENUM application can be configured using the ENUM managed objects and ENUM GUI. The MMI API contains details about the URI, an example, and the parameters available for each managed object.

6.1 Configurations

New Setup Configuration

Install and configure the ENUM application as mentioned in the following steps:

1. Configure the vENUM setup with ONE PUSH using the vENUM heat template. To refer a sample HEAT template, download *ENUM Heat Template.zip* file from OHC.

> **Note**
>
> Below is a sample heat template.
>
> **Table 6-1 vENUM MP VM profile**
>
> | Name | vCPUs | RAM (GB) | Disk Size (GB) |
> |---|---|---|---|
> | vENUM MP | 8 | 12 | 150 |

2. Create Server group with Function id `STPENUM` and add ENUM MPs (according to Requirement) under this Server Group for ENUM feature.
   ENUM tables needs to be configured further, the MO operations supported for this feature are:
   - ENUM ACLs
   - ENUM Options
   - DNS Connection
   - DNS Zone Config
   - DNS Record
   - DNS Server Options
3. Configure the ENUM application using MMI API or ENUM GUI.

Upgrading Existing setup

To upgrade an existing vSTP setup (without ENUM MPs), perform the following steps:

1. Create new ENUM MP(s) instance.

2. Create Server group with Function ID `STPENUM` at C level on Active NOAM.
3. Add the newly created MPs under the Server Group created in the above step.

Restricted IPs

The set of IPs that are restricted to be used or configured are listed in the below table.

Table 6-2 Restricted IPs

IP	Description
0.0.0.0/8	Broadcast messages to this network, RFC 1700
127.0.0.0/8	Used for loopback addresses to the local host
169.254.0.0/16	Link local, reserved by operating systems for APIPA
192.0.2.0/24	"TEST-NET" for documentation and example source code
192.88.99.0/24	Used by 6to4 anycast relays as specified by RFC 3068
198.18.0.0/15	Testing of inter-network communications, RFC 2544
198.51.100.0/24	"TEST-NET-2" for documentation and example source code
203.0.113.0/24	"TEST-NET-3" for documentation and example source code
224.0.0.0/4	Reserved for multicast assignments as specified in RFC 3171
240.0.0.0/4	255.255.255.255 is limited broadcast, others are reserved by the IANA

6.1.1 Configuring ENUM for UDR

Configuring ENUM feature for UDR involves adding vENUM MP(s) to UDR and then configuring UDR on the ComAgent server.

Assumptions:

- The user is aware of UDR and ComAgent functionality.
- UDR is already installed, and UDR topology is already configured.

Perform the following steps to configure ENUM for UDR:

1. Add details about the vENUM MP on the ComAgent Remote Servers screen as a client. Navigate to **Communication Agent**, select **Configuration**, select **Remote Servers**, and click **Insert** on an active OCUDR NOAMP.
2. Select the OCUDR server group from the *Available Local Server Groups* that need to communicate with vENUM MP.
3. From the active OCUDR GUI, navigate to **Communication Agent**, select **Maintenance**, select **Connection Status** and verify if the connection is `InService`.
4. From the active OCUDR GUI, navigate to **Communication Agent**, select **Maintenance**, select **Routed Services Status** and verify if the *STPDbSvc* status is `Normal`.
5. From an active DSR NOAM, navigate to **Communication Agent**, select **Configuration**, select **Remote Servers**, and click **Insert**.
6. Add the UDR NO IP in the ComAgent Remote Server screen as a Server.
7. Select the STP MP server group from the *Local SG* that needs to communicate with UDR.
8. Also, add the Standby and DR NOs to the Local SG.
9. Navigate to **Communication Agent**, select **Configuration**, select **Connection Groups**, select *STPSvcGroup* and click `Edit`.
10. Add all available UDR NO servers.

11. Navigate to **Communication Agent**, select **Maintenance**, then **Connection Status**, then the server name, and check the connection status.

Output: UDR Configuration: SOAP Provisioning Request for MSISDN

> **Note**
>
> To enable all the following MNP, ENUM, SPLIT, SFAPP, and DSA features together, run the following command:
>
> `"enableMNPwithSplit_Enum_SFAPP"`

Steps to Enable ENUM Feature on UDR:

Enable ENUM feature on UDR by running the **enableEnumSec** loader on the Active NOAM Server console. Follow the below steps:

1. Go to the path: `/usr/TKLC/udr/prod/maint/loaders/upgrade`
2. On the path, run the **enableENUMSec** script.

For Subscriber data, user must configure Subscriber first and then add or attach **Entity Type** as `ENUM` with that Subscriber.

The following snippet provides an example of provisioning Subscriber data with the **Entity Type** as `ENUM`.

Subscriber Profile:

```
<subscriber>
    <field name="MSISDN">5555555555</field>
    <field name="CLDBL">1</field>
    <field name="CLNBL">1</field>
    <field name="PType">1</field>
    <field name="ASD">abcd</field>
    <field name="SPRNID"/>"685477777"</field>
    <field name="GRNID"/>12000"</field>
<![CDATA[<?xml version="1.0" encoding="UTF-8"?>
    <ENUM ID="ENUM">
        <ns_domain>ns.abc1.com</ns_domain>
        <cname_domain>abc1.com</cname_domain>
        <naptr1_order>100</naptr1_order>
        <naptr1_pref>50</naptr1_pref>
        <naptr1_flag>u</naptr1_flag>
        <naptr1_service>E2U+sip</naptr1_service>
        <naptr1_regex>!^.*$!sip:info@example.com!</naptr1_regex>
        <naptr1_domain> </naptr1_domain>
        <naptr2_order>10</naptr2_order>
        <naptr2_pref>50</naptr2_pref>
        <naptr2_service>E2U+pstn:sip</naptr2_service>
        <naptr2_regex> </naptr2_regex>
        <naptr2_domain>Gw3.nptrexample.com</naptr2_domain >
    </ENUM>]>
</subscriber>
```

The following snippet provides an example of provisioning Entity data with ENUM.

Entity data:

```
<MnpSPRN>
   <Type>RN</Type>
   <EDigit>685477777</EDigit>
   <RI>0</RI>
   <PC>111-222-444</PC>
   <PCDom>ansi</PCDom>
   <SSN>3</SSN>
   <SRFIMSI>111111111</SRFIMSI>
   <DigAct>INSERTENTITYID</DigAct>
   <ns_domain>ns.abc1.com</ns_domain>
   <cname_domain>abc1.com</cname_domain>
   <naptr1_order>100</naptr1_order>
   <naptr1_pref>50</naptr1_pref>
   <naptr1_flag>u</naptr1_flag>
   <naptr1_service>E2U+sip</naptr1_service>
   <naptr1_regex>!^.*$!sip:info@example.com!</naptr1_regex>
   <naptr1_domain> </naptr1_domain>
   <naptr2_order>10</naptr2_order>
   <naptr2_pref>50</naptr2_pref>
   <naptr2_service>E2U+pstn:sip</naptr2_service>
   <naptr2_regex> </naptr2_regex>
   <naptr2_domain>Gw3.nptrexample.com</naptr2_domain>
</MnpSPRN>
```

The following snippet provides an example of provisioning GRN data with ENUM.

GRN data:

```
<MnpGRN>
    <EDigit>10000</EDigit>
    <RI>0</RI>
    <PC>111-222-333</PC>
    <PCDom>ansi</PCDom>
    <SSN>3</SSN>
    <SRFIMSI>222222222</SRFIMSI>
    <DigAct>INSERTENTITYID</DigAct>
    <ns_domain>ns.abc2.com</ns_domain>
    <cname_domain>abc2.com</cname_domain>
    <naptr1_order>200</naptr1_order>
    <naptr1_pref>20</naptr1_pref>
    <naptr1_flag>u</naptr1_flag>
    <naptr1_service>E2U+sip</naptr1_service>
    <naptr1_regex>!^.*$!sip:info@example.com!</naptr1_regex>
    <naptr1_domain></naptr1_domain>
    <naptr2_order>201</naptr2_order>
    <naptr2_pref>21</naptr2_pref>
    <naptr2_service>E2U+pstn:sip</naptr2_service>
    <naptr2_regex></naptr2_regex>
    <naptr2_domain>Gw3.nptrexample.com</naptr2_domain>
</MnpGRN>
```

6.1.2 UDR Redundancy

In cases where there is one Connection Group on **vENUM NO** (with default priority set to 10) and no provision to configure one interface as the priority route and another interface as the secondary (when the primary interface fails).

The Connection Group feature provides redundancy between the local site and remote site for ENUM, where the following three priorities are provided for the Connection group for UDR lookup on vENUM NO GUI:

- STPSvcGroup=30 (default value) indicates highest priority.
- STPSvcBackGroup=20 indicates a lesser priority.
- STPSvcSpareGroup=10 indicates a much lesser priority.

Figure 6-1 Priorities for Connection Group

STPDbSvc	3 Connection Groups	-
	STPSvcGroup	30
	STPSvcBackupGroup	20
	STPSvcSpareGroup	10

ble Description: Connection Groups Table

Connection Group	Server
STPSvcBackupGroup	2 Servers
	Mul26Soam1-UDR00-xsi
	Mul26Soam1-UDR01-xsi
STPSvcGroup	2 Servers
	Mul26Soam1-UDR00-imi
	Mul26Soam1-UDR01-imi
STPSvcSpareGroup	2 Servers
	Palla1Soam1-UDR00-XSI2
	Palla1Soam1-UDR01-XSI2
UDRSvcGroup	0 Servers

Operator can add UDR connected with primary route in the highest priority Connection Group. For redundancy, the other UDR can be added to other connection groups.

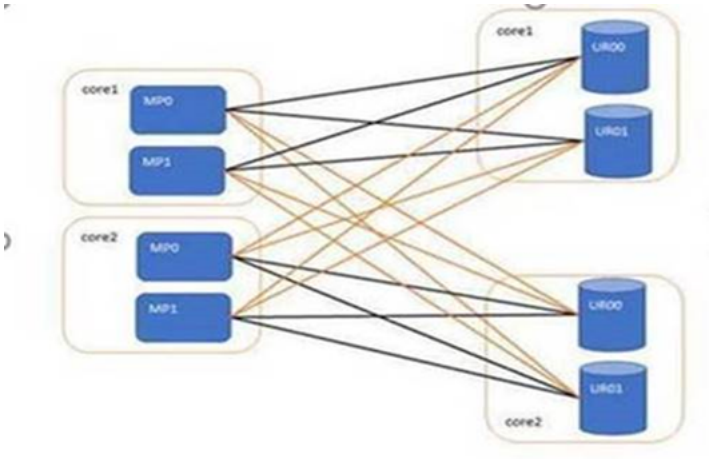
> **Note**
>
> These priority values are hardcoded through the loader and cannot be modified. If all UDRs are added to the same Connection Group, the load is distributed between these UDRs.

For example:

To configure the IMI as the priority route, the UDR connected with this Interface must be added to STPSvcGroup (highest priority) Connection Group.

The UDR connected with another Interface(XSI2) can be added to another Connection Group (STPSvcBackGroup) for redundancy.

Figure 6-2 IMI as the Priority Route



> **⚠ Caution**
>
> During connection group switch over, all UDRs in that connection group might go down, and this occurs when a message transfers from a UDR in one connection group to a UDR in another connection group. During such a switch over, message can be lost due to ComAgent limitation.

6.2 MMI Managed Objects for ENUM Support

MMI information associated with ENUM can be configured from a DSR NOAM or SOAM from **Main Menu**, and then **MMI API Guide**.

Once the *MMI API Guide* gets opened, use the application navigation to locate specific ENUM managed object information.

The following table lists the managed objects and operations supported for ENUM:

Managed Object Name	Supported Actions
ENUM ACLs	POST, DELETE
ENUM Options	PUT
DNS Connection	POST, DELETE
DNS Zone Config	POST, DELETE
DNS Records	POST, DELETE
DNS Server Options	PUT

ENUM ACLs

The `ENUM ACLs` MO supports the following parameters:

Table 6-3 ENUM ACLs Parameters

Parameter Name	Description
ipAddress	IPv4 or IPv6 addresses which are to be allowed or blocked for ENUM feature. Valid entries are valid IPv6 and IPv4 addresses.
prefix	Specifies number of bits in netmask. Allowed values are: • 1-32 for IPv4 • 32, 40, 48, 56, 64 or 96 for IPv6
filter	Specifies whether the configured IP is to be allowed or blocked. Blocked filter takes precedence over Allowed, if an IP falls in both ranges.

Example- Insert

Create a file with the following content to set values of the parameters. File name could be anything, for example, option name can be used as filename:

```
{
"filter": "BLOCKED",
"ipAddress": "10.75.219.180",
"prefix": "24"
}
```

Run the following command on Active SOAM to insert the data:

```
/venum/enumacls/ -v POST –r <filename>.json
```

Run the following command to display the content:

```
/venum/enumacls
{
"filter": "BLOCKED",
"ipAddress": "10.75.219.180",
"prefix": "24"
}
```

ENUM Options

The `ENUM Options` MO supports the following parameters:

Table 6-4 ENUM Options Parameters

Parameter Name	Description
congestionNotification	Congestion Notification Flag for response. The valid values are Yes, No.
entityPref	Set Entity Priority to SPRN or GRN Default: SPRN

Table 6-4 (Cont.) ENUM Options Parameters

Parameter Name	Description
maxDnDigits	Max number of DN digits from an incoming ENUM query. Range [8,15] Default: 15
addRnContext	Flag for RNCONTEXT parameter in ENUM TEL URI. Valid values are Yes, No. The default value is No.
rnContextCC	Default country code for RN Context. Valid values are from 1 to 999.
excludeSP	Flag to indicate whether the SP entity Id shall be excluded in ENUN Tel and SIP URI. Valid values are Yes, No. The default value is No. **Note:** If the incoming DN is found in Individual/ range DN table with an associated SP entity Id and ENUM option EXCLUDESP set to NO, then use that Configured Entity Id on UDR for response. If EXCLUSESP is set to yes, that SP/RN entity info is ignored and response is generated with ENUM data without RN.
enumTtl	Time to live (in seconds) for ENUM response caching.
defaultNaptrSrvc	Service parameter. This parameter specifies the supported ENUM services. This parameter is only valid for NAPTR response type.
defaultNSDomain	This parameter specifies the domain name of the name server in the NS record. This parameter is only valid for the NS response type.
defaultNaptrFlag	A containing flags to control aspects of the rewriting and interpretation of the fields in the record. This parameter is only valid for NAPTR response type.
defaultNaptrRegex	NAPTR Regex Response. This parameter is only valid for NAPTR response type.
Loadbalancer	Load balancer flag. Valid values are Yes, No. Default value is Yes. **Note** Loadbalancer configuration can only be modified when no or low traffic is running.

Example- Update

Create a file with the following content to set values of the parameters. File name could be anything. For example, option name can be used as filename:

```
{
            "addRnContext": "Yes",
            "congestionNotification": "No",
            "entityPref": "SPRN",
            "defaultNSDomain": "abc2.com",
            "defaultNaptrFlag": "U",
            "defaultNaptrRegex": "!^.*$!sip:info@example.com!",
            "defaultNaptrSrvc": "SIP",
            "enumTtl": 3600,
            "excludeSP": "No",
            "maxDnDigits": 15,
            "rnContextCC": "91"
        }
```

Run the following command on Active SOAM to insert the data:

```
/venum/enumoptions -v PUT –r <filename>.json
```

Run the following command to display the content:

```
{
        "addRnContext": "No",
        "congestionNotification": "Yes",
        "defaultNSDomain": www.ns-oracle.com,
        "defaultNaptrFlag": "P",
        "defaultNaptrRegex": "!^.*$!sip:info@example.com!",
        "defaultNaptrSrvc": "sip",
        "entityPref": "SPRN",
        "enumTtl": 0,
        "excludeSP": "No",
        "loadbalancer": "Yes",
        "maxDnDigits": 15
            }
```

DNS Connection

The `DNS Connection` MO supports the following parameters:

> **Note**
>
> Only one connection per MP is allowed.

Table 6-5 DNS Connection

Parameter Name	Description
connName	Name of the DNS Connection. This is a mandatory value.

Table 6-5 (Cont.) DNS Connection

Parameter Name	Description
ipAddress	IPv4 or IPv6 of networks to run DNS. Valid entries are valid IPv6 and IPv4 addresses. This is a mandatory value.
udpPort	Port to listen on. The default value is 53.

Example - Insert

Create a file with the following content to set values of the parameters. The Connection name must be unique across all DNS Connections sat the SOAM.

For example:

```
{
            "connName": "Conn1",
            "ipAddress": "121.1.1.1",
            "udpPort": 54
}
```

Run the following command on Active SOAM to insert the data:

```
/venum/dnsconnections/ -v POST –r <filename>.json
```

Run the following command to display the content:

```
/venum/dnsconnections
{
            "connName": "Conn1",
            "ipAddress": "121.1.1.1",
            "udpPort": 54
}
```

DNS Zone Configs

The `DNS Zone Configs` MO supports the following parameters:

Table 6-6 DNS Zone Configs Parameters

Parameter Name	Description
zoneName	Name of the zone to be configured.

Table 6-6 (Cont.) DNS Zone Configs Parameters

Parameter Name	Description
zoneType	Specifies the zone type. It accepts the following options: ENUM - ENUM Zone a type of forward zone. Forward - Forwards all requests for information about this zone to other nameservers. Master - Designates the nameserver as authoritative for this zone. A zone should be set as the master if the zone's configuration files reside on the system. Slave - Designates the nameserver as a slave server for this zone. Master server is specified in masters directive. static-stub: Zone data is statically configured through the server-address. Only the NS records are replicated.
ipAddress	Specifies a valid IP address/addresses. If Zone Type is forward, this IP is treated as forwarder IP. IF zone Type is slave, this IP is the master IP. Multiple forward IPs can be configured seperated by semicolons.
port	Port for forwarder IP(Forward Zone Type), or for master IP (Slave Zone Type).
forward	Specifies the behavior of the forwarders directive. It accepts the following options: Only - When unable to query the nameservers listed in the forwarders directive, the server will not attempt to resolve the name on its own.
file	Specifies the name of the file in the named working directory that contains the zone's configuration data.
notify	Specifies whether to notify the secondary nameservers when a zone is updated. It accepts the following options: Yes - The server will notify all secondary nameservers. No - The server will not notify any secondary nameserver, Master - The server will notify primary server for the zone only.
soaDomainName	Domain Name for the SOA Record. Only applicable to Master type of zone.
soaMailId	Mail for the SOA Record. Only applicable to Master type of zone.
soaIpAddress	A or AAAA record IP Address.
soaRefresh	Time in seconds to refresh.
soaRetry	Time in seconds to retry.
soaExpire	Time in seconds to expire.
soaTtl	Time to live in seconds for SOA record.

Example - Insert

Create a new Dns Zone Config to the VENUM configuration by setting the values to the parameters.

For example:

```
{
            "file": "test.db",
            "soaDomainName": "dns1.test.com",
            "soaExpire": 111,
            "soaIpAddress": "10.75.219.13",
            "soaMailId": "abc.test.com",
            "soaRefresh": 111,
            "soaRetry": 111,
            "soaTtl": 111,
            "zoneName": "test.com",
            "zoneType": "master"
        },
{
        "forward": "only",
        "ipAddress": "1.2.3.4;1.2.3.5",
        "port": 34,
        "zoneName": "testmul",
        "zoneType": "forward"
    },
{
            "ipAddress": "1.5.4.2;1.6.6.1",
            "port": 53,
            "zoneName": "stst",
            "zoneType": "staticStub"
}
```

Run the following command on Active SOAM to insert the data:

```
/venum/dnszoneconfigs -v POST –r <filename>.json
```

Run the following command to display the content:

```
/venum/dnszoneconfigs{
            "file": "test.db",
            "soaDomainName": "dns1.test.com",
            "soaExpire": 111,
            "soaIpAddress": "10.75.219.13",
            "soaMailId": "abc.test.com",
            "soaRefresh": 111,
            "soaRetry": 111,
            "soaTtl": 111,
            "zoneName": "test.com",
            "zoneType": "master"
        },
{
        "forward": "only",
        "ipAddress": "1.2.3.4;1.2.3.5",
        "port": 34,
        "zoneName": "testmul",
        "zoneType": "forward"
    },
{
            "ipAddress": "1.5.4.2;1.6.6.1",
```

```
            "port": 53,
            "zoneName": "stst",
            "zoneType": "staticStub"
}
```

DNS Records

The DNS Records MO supports the following parameters:

Table 6-7 DNS Records Parameters

Parameter Name	Description
recordName	Name of the DNS Record.
zoneName	Name of the zone associated with the DNS Record.
recordType	Indicates type of DNS Record. Possible values are A, AAAA, NAPTR, NS, CNAME, SRV, PTR
domainNameAddress	Domain Name or address of the DNS Record.
ttl	Time to live in seconds for the DNS record.
rdata	Resolving Data like IP, Hostname or Regex.

Example - Insert

Create a new Dns Record to the VENUM configuration by setting the values to the parameters.

For example:

```
{
            "domainNameAddress": "spdomain",
            "rdata": "mailto:sip+9876543",
            "recordName": "test1",
            "recordType": "NAPTR",
            "ttl": 1,
            "zoneName": "sampleZone"
}
```

Run the following command on Active SOAM to insert the data:

```
/venum/dnsrecords -v POST –r <filename>.json
```

Run the following command to display the content:

```
/venum/dnsrecords{
            "domainNameAddress": "spdomain",
            "rdata": "mailto:sip+9876543",
            "recordName": "test1",
            "recordType": "NAPTR",
            "ttl": 1,
            "zoneName": "sampleZone"
}
```

DNS Server Options

The `DNS Server Options` MO supports the following parameters:

Table 6-8 DNS Server Options Parameters

Parameter Name	Description
enableEmptyZone	Controls whether or not empty zones are created. Default value is Yes.
maxCacheSize	Specifies the maximum amount of memory to be used for server caches in MB. When the limit is reached, the server causes records to expire prematurely so that the limit is not exceeded. In a server with multiple views, the limit applies separately to the cache of each view. The default option is 32M.
maxCacheTtl	Maximum time to live in seconds for cached responses.
recursion	Specifies whether to act as a recursive server. Default is Yes.

Example- Update

Update the DNS Server Options by setting the values supplied to the parameters.

> **Note**
>
> To update just one of the individual options, GET the set, modify the value for the option that needs to be changed, and then PUT the options.

For example:

```
{
            "enableEmptyZone": "Yes",
            "maxCacheSize": "32",
            "maxCacheTtl": 604800,
            "recursion": "Yes"
}
```

Run the following command on Active SOAM to insert the data:

```
/venum/dnsserveroptions -v PUT –r <filename>.json
```

Run the following command to display the content:

```
/venum/dnsserveroptions{
            "enableEmptyZone": "Yes",
            "maxCacheSize": "32",
            "maxCacheTtl": 604800,
            "recursion": "Yes"
}
```

6.3 GUI Configurations for ENUM Support

The ENUM Support feature can be configured from Active System OAM (SOAM). Select **VENUM** , and then **Configuration** page.

> **Note**
>
> It is recommended to configure DNS Zone and DNS Record when vENUM is ON. When a new entry is added while vENUM is OFF and then it is turned ON, the sequence of records might not be preserved. This might cause issues for records without a domain name.

6.3.1 ENUM ACLs

ENUM ACLs allow user to allow or block IPs from accessing the ENUM feature.

Select the **VENUM**, and then **Configuration**, and then **Enum ACLs** page. The page displays the elements on the **ENUM ACLs** View and Insert pages.

Table 6-9 Enum ACLs Elements

Element	Description	Data Input Notes
IP Address	IPv4 or IPv6 addresses which are to be allowed or blocked for ENUM feature. This is a mandatory field.	Valid IPv6 and IPv4 addresses
Prefix	Specifies number of bits in netmask.	Allowed values are • 1-32 for IPv4 • 32,40,48,56,64 or 96 for IPv6
Filter	Specifies whether the configured IP is to be allowed or blocked. Blocked filter takes precedence over Allowed, if an IP falls in both ranges. This is a mandatory field.	

You can perform add or delete tasks on **VENUMConfigurationEnum ACLs** page.

Adding Enum ACL

Perform the following steps to configure a new Enum ACL:

1. Click **Insert**.
2. Enter the applicable values.
3. Click **OK**, **Apply**, or **Cancel**

Deleting Enum ACL

Use the following procedure to delete a Enum ACL.

> **Note**
>
> A Enum ACL will only be deleted if all delete validation checks pass.

1. Select the **Enum ACL** to be deleted.
2. Click **Delete**.
3. Click **OK** or **Cancel**.

6.3.2 ENUM Options

The ENUM Options are the configuration values that govern the overall ENUM Application. There is a single instance of this resource, which contains each option that can be retrieved and set. A collection of instances is not there. The GET collection action is not supported. A New ENUM Options resource cannot be created, so the POST action is not supported. A single instance cannot be removed, so the DELETE action is not supported. GET action for a single instance is performed to retrieve the options, and PUT action is used to update one or more values within the set of options. A name for this single, non-deletable instance is neither required nor expected.

Select the **vENUM**, and then **Configuration**, and then **ENUM Options** page. The page displays the elements on the **ENUM Options** View and Edit pages.

Table 6-10 ENUM Options Elements

Element	Description	Data Input Notes
Congestion Notification	Congestion Notification Flag for response	Valid values are Yes, No Default value: Yes
Entity Preference	Set Entity Priority to SPRN or GRN.	Default: SPRN
Max DN Digits	Max number of DN digits from an incoming ENUM query.	Range [8,15] Default: 15
Add RN Context	Flag for RNCONTEXT parameter in ENUM TEL URI.	Valid values are Yes, No Default: No
RN Context CC	Default country code for RN Context.	Valid values are from 1 to 999
Exclude SP	Flag to indicate whether the SP entity Id shall be excluded in ENUM Tel and SIP URI.	Valid values are Yes, No Default: No
ENUM TTL	Time to live (in seconds) for ENUM response caching.	NA
Default NS Domain	This parameter specifies the domain name of the name server in the NS record. This parameter is only valid for the NS response type.	NA
Default Naptr Service	Service parameter. This parameter specifies the supported ENUM services. This parameter is only valid for NAPTR response type.	NA

Table 6-10 (Cont.) ENUM Options Elements

Element	Description	Data Input Notes
Default Naptr Flag	A character-string containing flags to control aspects of the rewriting and interpretation of the fields in the record. This parameter is only valid for NAPTR response type.	NA
Default Naptr Regex	NAPTR Regex Response. This parameter is only valid for NAPTR response type.	
Loadbalancer	Load balancer flag.	Valid values are Yes, No. Default value is Yes.

Note

Load balancer configuration can only be modified when no or low traffic is running.

You can perform edit task on **VENUMConfigurationEnum Options** page.

Editing ENUM Options

Use this procedure to change the field values for a selected ENUM Option. (The **ENUM Option Name** field cannot be changed:

1. Select the **Enum Option** row to be edited.
2. Click **Edit**.
3. Enter the updated values.
4. Click **OK**, **Apply**, or **Cancel**.

6.3.3 DNS Connection

DNS Connection allows user to establish connection to DNS through the ENUM feature.

Select the **VENUM**, and then **Configuration**, and then **DNS Connection** page. The page displays the elements on the DNS Connection View and Insert pages.

> **Note**
>
> Only one connection per MP is allowed.

Table 6-11 DNS Connection Elements

Element	Description	Data Input Notes
Connection Name	Name of the DNS Connection. This is mandatory.	
IP Address	IPv4 or IPv6 of networks to run DNS. Valid entries are valid IPv6 and IPv4 addresses. This is mandatory.	
UDP Port	Port to listen on.	Default value: 53 Range: 1 to 65534

You can add or delete connections on **DNS Connection** page.

Adding a Connection

Perform the following steps to add a new connection:

1. Click **Insert**.
2. Enter the applicable values for **Connection name**, **IP Address**, and **UDP PORT**.
3. Click **OK**.

Deleting a Connection

Perform the following steps to delete an existing connection:

1. Select the connection from **Connection name** row to be deleted.
2. Click **Delete**.
3. Click **OK**.

6.3.4 DNS Zone Config

DNS Zone Config allows user to configure DNS Zone through the ENUM feature.

Select the **VENUM**, navigate to **Configuration**, then click **DNS Zone Config**. The **DNS Zone Config** page displays the elements on the DNS Zone Config View and Insert pages.

Table 6-12 DNS Zone Config Elements

Element	Description	Data Input Notes
Zone Name	Name of the zone.	

Table 6-12 (Cont.) DNS Zone Config Elements

Element	Description	Data Input Notes
Zone Type	Specifies the zone type. • **ENUM**: ENUM Zone a type of Forward Zone. • **Forward**: Forwards all requests for information about this zone to other nameservers. • **Master**: Designates the nameserver as authoritative for this zone. A zone should be set as the master if the zone's configuration files reside on the system. • **Slave**: Designates the nameserver as a slave server for this zone. Master server is specified in masters directive. • **static-stub**: Zone data is statically configured through the server-address. Only the NS records are replicated. This is a mandatory field.	Valid values: • ENUM • Forward • Master • Slave • static-stub
IP Address	Specifies a valid IP address for nameservers to which the requests should be forwarded for resolution for Forward Zones or Master IP for Slave Zones. Also valid for static-stub zone IP Addresses.	
Port	Specifies port with the IP Address.	Range: 1 to 65534
Forward	Specifies the behavior of the forwarders directive. It accepts the following option: • **Only**: When unable to query the nameservers listed in the forwarders directive, the server does not attempt to resolve the name on its own. ENUM Zones can be configured to Forward Only.	Only
File	Specifies the name of the file in the named working directory that contains the zone's configuration data.	

Table 6-12 (Cont.) DNS Zone Config Elements

Element	Description	Data Input Notes
Notify	Specifies whether to notify the secondary nameservers when a zone is updated. It accepts the following options: • **Yes**: The server notifies all secondary nameservers. • **No**: The server does not notify any secondary nameserver. • **Master**: The server notifies primary server for the zone only.	Valid values: • Yes • No • Master
SOA Domain Name	Domain Name for SOA Record. Only for Master Zones.	
SOA Mail Id	Mail Id for SOA Record. Only for Master Zones.	
SOA IP Address	IP Address for A/AAAA record.	
SOA Refresh	Time in seconds to refresh for SOA Record. Only for Master Zones.	
SOA Retry	Time in seconds to retry for SOA Record. Only for Master Zones.	
SOA Expire	Time in seconds to expire for SOA Record. Only for Master Zones.	
SOA TTL	Time to Live in seconds for SOA Record. Only for Master Zones.	

You can perform add or delete tasks on **DNS Zone Config** page.

Adding a DNS Zone Config

Perform the following steps to add a new DNS Zone Config:

1. Click **Insert**.
2. Enter the applicable values.
3. Click **OK**.

Deleting a DNS Zone Config

Perform the following steps to delete an existing zone:

1. Select the Zone from **Zone name** row to be deleted.
2. Click **Delete**.
3. Click **OK**.

6.3.5 DNS Records

DNS Records allows user to view and configure DNS Records through the ENUM feature.

Select **VENUM**, navigate to **Configuration**, then click **DNS Records**. The **DNS Records** page displays the records on DNS to View and Insert pages.

Table 6-13 DNS Records Table Elements

Element	Description	Data Input Notes
Record Name	Record Name of the DNS Record. This is a mandatory field.	
Zone Name	Name of the zone associated with the DNS Record. This is a mandatory field.	**Note:** Valid zone names are the Master Zones added in the `DNS Zone Config` managed object.
Record Type	Indicates type of DNS Record. This is a mandatory field.	Valid values: • A • AAAA • NAPTR • NS • CNAME • SRV • PTR
Domain Name or Address	Domain Name or address of the DNS Record. This is a mandatory field for A/ AAAA Records.	
TTL	Time to live in seconds for DNS record.	
RDATA	Resolving Data like IP, Hostname or Regex. This is a mandatory field.	

You can perform add or delete tasks on **DNS Records** page.

Adding a DNS Record

Perform the following steps to add a new DNS record:

1. Click **Insert**.
2. Enter the applicable values.
3. Click **OK**.

Deleting a DNS Record

Perform the following steps to delete an existing DNS record:

1. Select the Record from **Record Name** row to be deleted.
2. Click **Delete**.
3. Click **OK**.

6.3.6 DNS Server Options

The DNS Server Options provide those configuration values that allows to modify the DNS Server and Records.

Select the **VENUM**, navigate to **Configuration**, then click **DNS Server Options** page. The page displays the elements on the **DNS Server Options** View and Edit pages.

Table 6-14 DNS Server Options Elements

Element	Description	Data Input Values
Enable Empty Zone	Controls whether or not empty zones are created.	Valid values are Yes, No Default: Yes
Max Cache Size	Specifies the maximum amount of memory to be used for server caches in MB. When the limit is reached, the server causes records to expire prematurely so that the limit is not exceeded. In a server with multiple views, the limit applies separately to the cache of each view.	Default: 32MB
Max Cache TTL	Maximum time to live in seconds for cached responses.	
Recursion	Specifies whether to act as a recursive server.	Valid values are Yes, No Default: Yes

You can perform edit task on **DNS Server Options** page.

Editing DNS Server Option

Perform the following steps to change the field values for a selected DNS Server option:

1. Select the **DNS Server Option** row to be edited.
2. Click **Edit**.
3. Enter the updated values.
4. Click **Apply**.

6.4 Bulk Import or Export

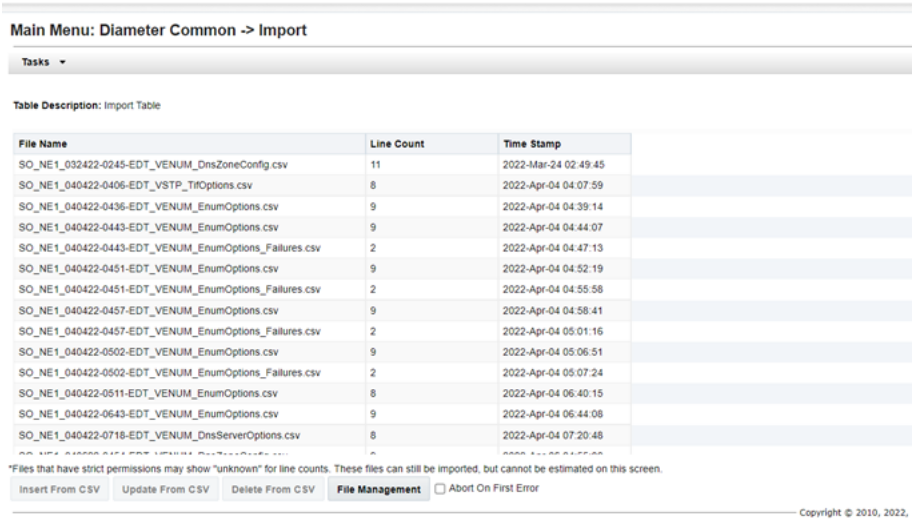
All the MOs and their actions can also be executed using Bulk Import Export mechanism. This mechanism allows for tasks such as updating, provisioning and deleting entries using CSV files (according to the supported MO actions).

> **Note**
>
> Bulk import or export takes time for large number of DNS records. Average time for adding a new DNS record is around "0.19" seconds.

Import

Bulk Import can be executed from **Diameter Common**, and then **Import** in GUI.

Figure 6-3 Import Page



Export

Bulk Import can be executed from **Diameter Common**, and then **Export** in GUI.

Figure 6-4 Export Page 1

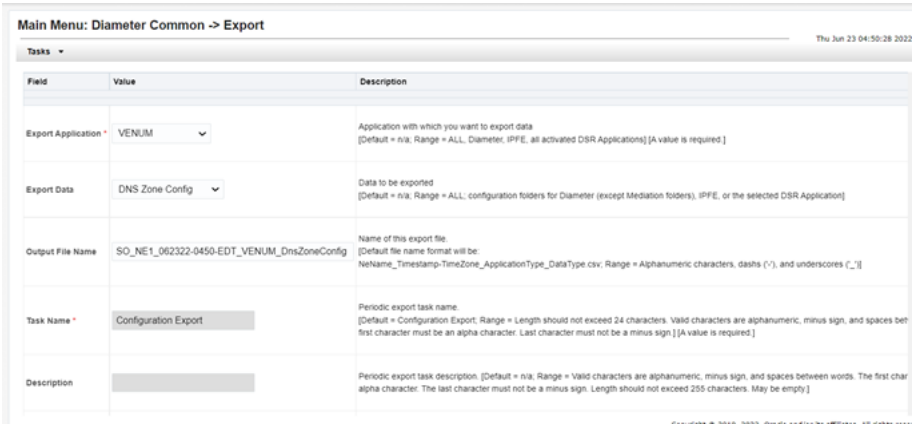
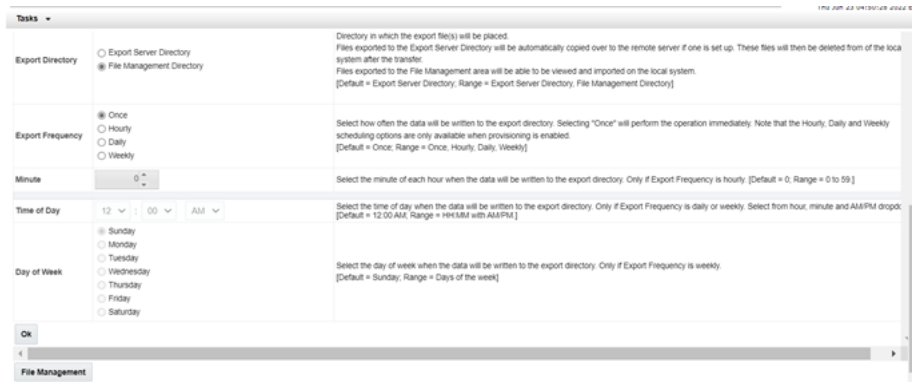


Figure 6-5 Export Page 2



6.5 Alarms and Measurements

Alarms and Events

The following table lists the alarms or events for vENUM:

Alarm/Event ID	Alarm/Event Name
70461	ENUM Threshold exceeded
70464	ENUM MP capacity exceeded
70467	UDR ENUM DB unavailable
70468	ENUM message decode failed
70469	ENUM received invalid message
70470	ENUM MP TPS exceeded
70472	ENUM Profile not found
70474	ENUM Event Queue Utilization
70475	ENUM UDP Event Queue Utilization
70900	DNS Record Configuration Error **Note** To remove this alarm, delete the corresponding entry.
70901	DNSDIST Configuration Error
70902	ENUM MP CPU Overload
70903	ENUM MP HDD full

For more details related to measurements, refer to *Diameter Signaling Router Alarms and KPIs Reference*.

Measurements

The following table lists the measurements specific to the ENUM Support functionality for vSTP:

Measurement ID	Measurement Name
22256	EnumQueryRx
22257	NaptrQueryRx
22258	NsQueryRx
22259	CnameQueryRx
22260	EnumQueryReject
22261	EnumQueryCongestionDiscard
22262	SuccessfulEnumTx
22263	EnumTxRC1
22264	EnumTxRC2
22265	EnumTxRC3
22266	EnumTxRC4

Measurement ID	Measurement Name
22267	EnumTxRC5
22268	EnumTxDefltProfile
22277	EnumUdrLookupFailure
22278	VstpEnumEventQueuePeak
22279	VstpEnumEventQueueAvg
22280	VstpEnumUdpEventQueuePeak
22281	VstpEnumUdpEventQueueAvg
22282	VstpEnumStackQueueFull
22283	VstpENUMUDPStackQueueFull
22284	VstpEnumMpCpuPeak
22285	VenumMpCpuAvg
22289	EnumQueryRxPeak
22290	EnumQueryRxAvg

For more details related to measurements, refer to *Diameter Signaling Router Measurement Reference*.

7 Troubleshooting

Following are the fixes for the common issues:

- To check status of named process, run the following command:

  ```
  sudo service named status
  ```

- In case the named process is down, it can be started manually by performing the following command:

  ```
  sudo service named start
  ```

- To check status of DNDIST process, run the following command:

  ```
  sudo service dnsdist status
  ```

- If `loadbalancer` is set to "Yes", but `dnsdist` process is down, it can be started manually by performing the following command:

  ```
  sudo service dnsdist start
  ```

- Alarm 70902 (ENUM MP CPU Overload) and Alarm 70903 (ENUM MP HDD full) are raised on basis of the measurement values from SysMetric. These can be referred by running the following command:

  ```
  sysmetric -W
  ```

- In the event of restart, alerts are generated for the NS records. To clear alarms, these records must be deleted and then re-added.
- If loadbalancer is set to "Yes" and the IMI IP is down, the query response time increases and queries will get timed out.
- To recover from congestion, traffic must be reduced to below 5k TPS.
- In case of any issues with replication of DNS records or zones, restart the vENUM MP so that replication can resume.
- In case of the error scenarios, the ENUM measurements are pegged. For information related to ENUM measurements, see *Oracle Communications Measurements* guide.