



Managing Resource Records

This chapter explains how to configure some of the more advanced DNS zone and server parameters by using the Cisco Prime IP Express web UI and CLI. Before you proceed with the concepts in this chapter, read [Managing Zones](#) which explains how to set up the basic properties of a primary and secondary DNS server and its zones.

- [Managing Resource Records for Zone, page 1](#)
- [Adding Resource Record to Zone, page 2](#)
- [Editing Resource Records, page 3](#)
- [Removing Resource Records from Zone, page 3](#)
- [Managing Resource Records for Host, page 4](#)
- [Protecting Resource Record Sets, page 4](#)
- [Searching Server-Wide for Records and Addresses, page 6](#)
- [Filtering Resource Records, page 7](#)
- [Advertising Services to Network Using Service Location \(SRV\) Records, page 8](#)
- [Name Resolution in a Namespace Using NAPTR Resource Records, page 8](#)

Managing Resource Records for Zone

Resource records (RRs) comprise the data within a DNS zone. Although there is no fixed limit to the number of RRs a zone may own, in general, a zone may own one or more RRs of a given type (the zone always has a Start of Authority, or SOA, record). There are some exceptions depending on the types involved. All RRs have the entries described in the following table.

Table 1: Resource Record Common Entries

RR Entry	Description
Name	Owner of the record, such as a zone or hostname.

RR Entry	Description
Class (not required for all formats)	Cisco Prime IP Express supports only the IN (Internet) class.
TTL (time to live)	Amount of time to store the record in a cache, in seconds. If you do not include a TTL, Cisco Prime IP Express uses the zone default TTL, defined as a zone attribute.
Type	Type of the record, such as A (AAAA for IPv6), NS, SOA, and MX. There are many types that various RFCs define, although fewer than ten are in common use.
Record data	Data types whose format and meaning varies with record type.

Related Topics

[Adding Resource Record to Zone, on page 2](#)

[Protecting Resource Record Sets, on page 4](#)

[Editing Resource Records, on page 3](#)

[Removing Resource Records from Zone, on page 3](#)

[Searching Server-Wide for Records and Addresses, on page 6](#)

[Filtering Resource Records, on page 7](#)

[Advertising Services to Network Using Service Location \(SRV\) Records, on page 8](#)

[Name Resolution in a Namespace Using NAPTR Resource Records, on page 8](#)

Adding Resource Record to Zone

Before adding or modifying RRs, keep in mind the two distinct dns edit modes that you can set and work in: staged and synchronous (see the *"Staged and Synchronous Modes"* section in *Cisco Prime IP Express 9.0 DHCP User Guide*).

Administrator roles required for RR management are the dns-admin role at the local cluster and the central-dns-admin role at the regional cluster. The host-admin role at the local cluster and the central-host-admin role at the regional cluster can view host records only.

Local Basic or Advanced and Regional Web UI

-
- Step 1** Choose **Forward Zones** from **Design > Auth DNS** to open the List/Add Forward Zones page.
- Step 2** In the Forward Zone pane, click the zone name to open the Edit Zone page. Note that resource record edits is managed jointly by CCM and DNS and a system lock is used to prevent DNS and CCM from accessing the resource record database at the same time.
- Tip** Records are listed in the formats that their respective RFCs specify, with only the first record in a set labeled with its name, and in DNSSEC order. To reduce or increase the items in the table, change the page size value at the bottom of the page, then click **Change Page Size**.
- Step 3** Click the **Resource Records** tab.
- Step 4** Add the RR name, TTL (if not using the default TTL), type, and data as appropriate.
- Step 5** By default, RRs are protected, which means that DNS Updates cannot overwrite them (see [Protecting Resource Record Sets, on page 4](#)). To unprotect the RRs, click the **Locked** icon to the left of the record name to change it to the Unlocked icon. Likewise, to protect the record, click the Unlocked icon to change it to the **Locked** icon.
- Step 6** Click **Add Resource Record**.
-

CLI Commands

Use **zone name addRR** to add a protected RR of a certain type. You can specify the name as a relative name, if the owner is in the same domain, an absolute name (by supplying the FQDN), or the same name as the zone name (by using the at [**@**] symbol).

For example:

```
nrcmd> zone example.com addRR -sync host101 A 192.168.50.101
```

Use **zone name addDNSRR type data** to add an unprotected RR.

Editing Resource Records

You can edit RRs as an individual record or as an RR set:

- **Individual RRs**—Click the Edit icon next to the record name to open the Edit RR in Zone page.
- **RR sets**—Click the name of the record to open the Edit RR Set in Zone page.

For a description of the fields to enter data, see [Adding Resource Record to Zone, on page 2](#).

Removing Resource Records from Zone

You can remove RRs from a zone.

Local Basic or Advanced and Regional Web UI

On the local or regional the Resource Records tab for the Zone page:

- To remove an entire record name set, click the **Delete** icon next to the record set name in the list, then confirm the deletion.
- To remove individual records from the set, click the name of the record set to open the edit page, click the **Delete** icon next to the individual record in the list, then confirm the deletion.

CLI Commands

The CLI includes two removal commands, depending on the type of RR to remove:

- Use **zone name removeRR** to remove any RR. You must specify the owner. If you omit the data, Cisco Prime IP Express removes all records of the specified type for the specified owner. Similarly, if you omit the type, Cisco Prime IP Express removes all records for the specified owner.
- Use **zone name removeDNSRR** to remove unprotected RRs only.

Managing Resource Records for Host

You can manage the RRs for a host by configuring the host record rather than the individual RRs. When you define a host, the DNS server automatically creates an Address (A) RR for IPv4, or an AAAA RR for IPv6, for it. If the reverse zone for the host exists, the server can also create the associated Pointer (PTR) RR for it.

See [Managing Hosts](#) for details.

Protecting Resource Record Sets

When an RR is protected, DNS Updates cannot modify the record. Most administratively created RRs are protected. However, RRs created by DNS Updates must be unprotected to allow the server to modify them. You can set this protection status for each RR set on the List/Add DNS Server RRs for Zone page.

Note that only the primary DNS server can recognize this protection status; secondary servers do not recognize the protection status of their RRs.



Caution

Zone scavenging can remove RRs that are unprotected. See the *"Scavenging Dynamic Records"* section in *Cisco Prime IP Express 9.0 DHCP User Guide* for details.

Local Basic or Advanced and Regional Web UI

To protect an existing RR, do the following:

-
- Step 1** Choose **Forward Zones** from **Design > Auth DNS** to open the List/Add Forward Zones page.
 - Step 2** In the Forward Zone pane, click the zone name to open the List/Add Forward Zones page.
 - Step 3** Click the **Resource Records** tab.
 - Step 4** On the Resource Records tab, click the Resource Record name in the list of Resource Records to edit the resource record.
 - Step 5** Click **Protect Set** button to unprotect the selected RR set.
 - Step 6** Click **Save** to save the resource record attribute modification.
-

Unprotecting Resource Record Sets

You can also unprotect an RR. To unprotect an RR while adding, click the **Locked** icon next to the Resource Record name field. The icon changes to the **Unlocked** icon.

Local Basic or Advanced and Regional Web UI

To unprotect an existing RR, do the following:

-
- Step 1** Choose **Forward Zones** from **Design > Auth DNS** to open the List/Add Forward Zones page.
 - Step 2** In the Forward Zone pane, click the zone name to open the List/Add Forward Zones page.
 - Step 3** Click the **Resource Records** tab.
 - Step 4** On the Resource Records tab, click the Resource Record name in the list of Resource Records to edit the resource record.
 - Step 5** Click **Unprotect Set** button to unprotect the selected RR set.
 - Step 6** Click **Save** to save the resource record attribute modification.
- Note** The icon to the left of the RR set name indicates the status of the Resource Record, whether it is protected or unprotected.
-

CLI Commands

To protect the RR sets, use **zone name protect-name rrsset-name** ; to unprotect the zone, use the **unprotect-name rrsset-name** action instead. For example:

```
nrcmd> zone example.com protect-name boston
100 Ok
protected boston
nrcmd> zone example.com unprotect-name boston
```

```
100 Ok
unprotected boston
```

Searching Server-Wide for Records and Addresses

With Cisco Prime IP Express, you can search for RRs and IP addresses server-wide. The search is a filter mechanism whereby you can specify a combination of RR and address attributes to target one or more RRs or addresses configured for the network. The search function is available at the local cluster only.

You can search RRs by:

- IP address
- Protection state
- Name prefix
- Type
- Zone

Local Advanced Web UI

To search resource records by IP address, do the following:

-
- Step 1** From the **Operate** menu, choose **DNS > RR By IP Address** from the **Reports** submenu to open the IP Address Search page.
- Step 2** To search by IP address, enter an IP address, then click **Search**.
- Note** In an IP address search, the DNS server does not search all forward zones for RRs that have the specified address in the data field. Instead, the server looks up the matching PTR record in the reverse zone and returns all the respective RRs in the forward zone.
-

Local Advanced Web UI

To search resource records, do the following:

-
- Step 1** From the **Operate** menu, choose **DNS > Resource Records** from **Reports** submenu to open the DNS Resource Record Search page.
- Step 2** Choose a filter attribute from the drop-down list.
- Step 3** Choose a filter type from the drop-down list depending on the filter attribute you chose:
- **RR Protection State**—RR Protection Status, either locked or unlocked.
 - **RR Name Prefix**—RR Name Prefix.
 - **RR Type**—RR Type.
 - **Zone**—Zone List, Regular expression, or Zone Flags

- Step 4** Enter or select a Value, based on the Type selected. To clear the filter, click **Clear Filter**.
- Step 5** Click **Add Element** to add the search element to the filter elements list. The Filter Elements heading changes to identify the filter attribute and value used for the filter. If you add more than one element, the heading identifies the ANDed values of the elements. For example, if you add an element for a name prefix search for user, then add another element for an RR type search for A records, the filter element heading will identify the search as ****RR Name Prefix = user AND RR Type = A**.
- Step 6** You can add as many elements as you like (remembering that the search results are an intersection of the filter elements). View the filter elements list by clicking the plus sign (+).
- Step 7** Click **Search**.
- Step 8** Check the table of resulting RRs from the search, which shows for each RR its zone, hostname, TTL, type, and associated data. If necessary, change the page size to see more entries at one time (you might still need to page forward and back). The RRs are sorted in DNSSEC order.
- Tip** If the search results are less than expected due to the ANDing of the filter elements, look at the filter list for any element that might be compromising the search, delete it by clicking the Delete icon next to it, then redo the search.

CLI Commands

Use **dns findRR** to find RRs across the zones. The command syntax is of two kinds:

```
nrcmd> dns findRR -name{fqdn | domainaddr}
nrcmd> dns findRR [-namePrefix nameprefix] [-rrTypes
RRtypelist] [-protected| -unprotected] [-zoneType
{forward| reverse| primary|secondary| ALL}]
```

You can search by domain or its address, or enter the beginning characters of the RR name (the name prefix). If you search by RR name prefix, you can narrow the search by a list of RR types, protection status, or zone type. The output clearly indicates the zone for each found entry. For example:

```
nrcmd> dns findRR -namePrefix user -rrTypes A

userhost101.example.com IN A 192.168.50.101
userhost102.example.com IN A 192.169.50.102
userhost103.boston.example.com IN A 192.168.50.103
```

Filtering Resource Records

You might want to filter records to display only one type of record, such as an A (or IPv6 AAAA) or PTR record. (See also [Searching Server-Wide for Records and Addresses](#), on page 6.)

Local Basic or Advanced and Regional Web UI

You can filter RRs right from the Edit Zone page. Look for the Name and Type fields just below the **Add Resource Record** button.

By default, RRs are sorted alphabetically by name, starting with the top-of-zone records (marked with the @ symbol), and secondarily sorted by type, then data. You can also sort them by:

- **Protected state**—You can click All, Unprotected, or Protected.

- **Name prefix**—Starting characters in the name. Note that the * character is not a wildcard. For example, entering **al** returns **alberta**, **allen.wrench**, and **allie**, whereas entering **al*** returns **al*** and **al*ert**.
- **RR type**—Click one of the RR types in the drop-down list, such as **A** (or **IPv6 AAAA**) or **TXT**.

When the selection is complete, click **Filter List**. This returns just the filtered entries in the table below the fields. To return to the full, unfiltered list, click **Clear Filter**.

CLI Commands

Use **zone zonename findRR** to search on RR name prefixes, RR types, or protection status:

```
nrcmd> zone zonename findRR [-namePrefix nameprefix]
[-rrTypes RRtypelist] [-protected| -unprotected]
```

Advertising Services to Network Using Service Location (SRV) Records

The service location (SRV) RR is used to advertise services to the network. This RR is defined in the RFC 2782, "A DNS RR for specifying the location of services (DNS SRV)." The SRV can have an associated A or AAAA record. Windows domain controller is one service that uses the SRV records.

The RFC defines the format of the SRV record (DNS type code 33) as:

```
_service._protocol.name ttl class SRV priority weight port target
```

There should always be an A record associated with the SRV record target so that the client can resolve the service back to a host. In the Microsoft Windows implementation of SRV records, the records might look like this:

```
myserver.example.com A 201.165.201.1
_ldap._tcp.example.com SRV 0 0 389 myserver.example.com
_kdc._tcp.example.com SRV 0 0 88 myserver.example.com
_ldap._tcp.dc._msdcs.example.com SRV 0 0 88 myserver.example.com
```

An underscore (`_`) always precedes the service and protocol names. In the example, `_kdc` is the Key Distribution Center. The priority and weight help a client choose between target servers providing the same service (the weight differentiating those with equal priorities). If the priority and weight are all set to zero, the client orders the servers randomly.



Note

For a description of how Windows clients interoperate with DNS and DHCP servers, including scavenging dynamic RRs, see the *"Configuring DNS Update for Windows Clients"* section in *Cisco Prime IP Express 9.0 DHCP User Guide*.

Name Resolution in a Namespace Using NAPTR Resource Records

Cisco Prime IP Express supports Naming Authority Pointer (NAPTR) RRs. These records help with name resolution in a particular namespace and are processed to get to a resolution service. Because NAPTR records

are a proposed standard, RFC 3403, Cisco Prime IP Express only validates their numeric record fields. However, the proposed standard requires a value for each field, even if it is null (""), and there are no preset values.

When using a NAPTR record to locate a Session Initiation Protocol (SIP) proxy, see the proposed standard, RFC 2916 or RFC 3263. In RFC 2916, the ENUM working group of the Internet Engineering Task Force specifies NAPTR records to map E.164 addresses to Universal Resource Identifiers (URIs). Using the NAPTR record resolves a name in the E.164 international public telecommunication namespace to a URI, instead of providing the name of a service to use as a resolver. The U flag was added to the NAPTR record for this purpose.

For example, to specify a SIP proxy for the phone number +4689761234, add a NAPTR record at the name 4.3.2.1.6.7.9.8.6.4.e164.arpa. with this content:

```
100 10 "u" "sip+E2U" "/^.*$/sip:info@example.com/" .
```

This sets these fields of the NAPTR record:

```
order = 100
preference = 10
flags = "u"
service = "sip+E2U"
regexp = "/^.*$/sip:info@example.com/"
replacement = .
```

After you configure these fields, the DNS client dealing with phone number +4689761234 can now find an SIP service URI by replacing the number with sip:info@tele2.se. The E.164 zone mostly uses the NAPTR record for wholesale replacement of the input telephone number. Section 3.2.3 of RFC 2916 includes an example of one transformation to a Lightweight Directory Access Protocol (LDAP) query that preserves some of the digits. The E.164 zone does not map to service location (SRV) records because it wants to obtain a SIP URL that is more humanly readable to the left of the at (@) symbol.

Local Basic or Advanced and Regional Web UI

-
- Step 1** On the Edit Zone page, click the **Resource Records** tab.
 - Step 2** Enter the owner of the record in the Name field.
 - Step 3** Enter the TTL (if necessary).
 - Step 4** Click **NAPTR** in the Type drop-down list.
 - Step 5** Enter the data as a string embedded in quotes and separated by spaces:
 - a) Order
 - b) Preference
 - c) Flags
 - d) Service
 - e) Regular expression
 - f) Replacement string
 For example:

Example:

```
"100 10 u sip+E2U /^.*$/sip:info@tele2.se/ ."
```

Step 6 Click **Add Resource Record**.

CLI Commands

Use **zone name addRR** to add a protected resource record to a zone.