# Cisco Prime IP Express 8.2 Release Notes

**March 20, 2014**

These release notes provide an overview of the new and changed features in Cisco Prime IP Express 8.2, and describe how to access information about the known problems in Cisco Prime IP Express 8.2.

**Note** You can access the most current Cisco Prime IP Express documentation, including these release notes, online at: http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-ip-express/tsd-products-support-series-home.html

## Contents

These release notes contain the following sections:




**Americas Headquarters:**
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

# Introduction

Cisco Prime IP Express is one of the Prime suite of network solution products. The Cisco Prime portfolio offerings empower IT organizations to more effectively manage their networks and the services they deliver. Built on a service-centric foundation, the Cisco Prime portfolio of products supports integrated lifecycle management through an intuitive workflow-oriented user experience and a set of common operational attributes.

Cisco Prime IP Express is comprised of these components:

- A Domain Name System (DNS) protocol service
- A Caching DNS service
- A Dynamic Host Configuration Protocol (DHCP) service.

Cisco offers these components as individually licensed applications or in a mix of suites.

# Before you Begin

Before you install Cisco Prime IP Express 8.2, review the system requirements and licensing information available in the *Cisco Prime IP Express 8.2 Installation Guide*.
Cisco Prime IP Express DHCP, Authoritative DNS, and Caching DNS components are licensed and managed from the regional server. All services in the local clusters are licensed through the regional cluster. Only a regional install requires a license file and only the regional server accepts new license files. Then the regional server can authorize individual local clusters based on available licenses.
For more details about Licensing, see the License Files section in the Overview chapter of the *Cisco Prime IP Express 8.2 Installation Guide*.

The Cisco Prime IP Express 8.2 kit contains the following files and directories:

- Linux5—Red Hat Linux ES 5.x or 6.x installation kit
- Windows—Windows Server 2008 R2 installation kit
- Docs—Product documentation in the PDF format

# New Features and Enhancements

This section describes the features added in Cisco Prime IP Express 8.2.


- External Authentication using Active Directory, page 2
- Bring Your Own Device Support, page 3
- Secured DDNS and Zone Transfer using GSS-TSIG, page 3


## External Authentication using Active Directory

Cisco Prime IP Express will supports authentication of users against Microsoft Active Directory.

Active Directory (AD) stores user, group, computer, and the other information about a network. AD enables clients to retrieve information from its data store in order to provide services such as authentication and authorization. AD makes use of the Lightweight Directory Access Protocol (LDAP) versions 2 and 3, Microsoft's version of Kerberos, and DNS.

Existing AD user accounts can be used to log into the Cisco Prime IP Express WebUI/CLI/SDK local and regional clusters by adding the user to the Cisco Prime IP Express access privileged group.

Cisco Prime IP Express CCM server will use Kerberos, LDAPv3 and DNS to provide secure, centralized authentication for the identified users in AD and to determine if an authenticated user is authorized to access Cisco Prime IP Express.

## Bring Your Own Device Support

Bring your own device (BYOD) support in Cisco Prime IP Express is to permit an employee to use their own mobile devices for the business communications in a secured way. The advantage of BYOD support is to provide hands-off, user-driven configuration of device with correct IP addresses and network settings.

The user is redirected to the BYOD self-registration web page to register the device, whenever a BYOD device is connected to the network for the first time. The web portal registration page populates the device details and prompts the user credentials to authenticate against the active directory server. Upon successful authentication, the device is registered with the DHCP server. The BYOD registration portal is tightly integrated with DHCP, CDNS of Cisco Prime IP Express.

To support BYOD feature in the Cisco Prime IP Express, the DHCP server and CDNS server (Changes also required in backup, if DHCP failover pairs are configured) needs to be configured with specific attributes.

## Secured DDNS and Zone Transfer using GSS-TSIG

The Cisco Prime IP Express will support the Dynamic DNS Update(s) and Zone Transfer through secured GSS-TSIG mechanism.

The RFC 3645 proposes to extend the TSIG to allow the Generic Security Service (GSS) method of secure key exchange, eliminating the need for manually distributing keys to all GSS clients. It defines an algorithm to use with TSIG, which is based on the Generic Security Service Application Program Interface, as specified in RFC2743.

In GSS-TSIG, a unique security context is required for each unique connection between GSS-TSIG enabled applications. So establishing a security context involves a negotiation between GSS-TSIG-client application and GSS-TSIG-server application. After the security context has been established, it has a finite lifetime during which it can be used to create and verify the transaction signature on messages between the two applications. The GSS-API implementation uses Kerberos V5 authentication protocol as its underlying security mechanism.

# Limitations and Restrictions

This section describes limitations and restrictions you might encounter using Cisco Prime IP Express 8.2.

- The Regional Pull Replica Address Space fails when reservations are being pulled for new failover-pair objects. This problem occurs only if there is a new failover-pair and one or more reservations associated with that failover-pair.

  To work around this issue, repeat the operation twice—first checking Omit Reservations and then without checking Omit Reservations. After the failover-pairs have been pulled, subsequent pull replica address space operations will work correctly.

- In situations where a DHCPv6 server supports clients with multiple leases, the demand on server memory increases. DHCPv4 supports only one lease per client, while DHCPv6 supports multiple leases. Therefore, a server running DHCPv6 cannot support as many leases (clients) as the same

server running DHCPv4. For example, one DHCPv6 client might require 2,500 bytes of space compared to 1,000 bytes per DHCPv4 client. This means that a machine that would support one million DHCPv4 clients supports only 400,000 DHCPv6 clients. We recommend that you allow three times the memory for DHCPv6 clients as you would for DHCPv4.

You must:

- Be aware of how many prefixes per link are configured. If the configuration has two prefixes on a link, then with default configuration parameters, you have to cut in half the number of clients.
- Use care if you enable inhibit-all-renews. When enabled, each client would use at least two leases, and perhaps three, depending on the grace and affinity times per prefix.

# Cisco Prime IP Express Bugs

For more information on a specific bug or to search all bugs in a particular Cisco Prime IP Express release, see Using the Bug Search Tool, page 4.

This section contains the following information:



## Open Bugs

Table 1 lists the open issues in the Cisco Prime IP Express 8.2 release.

*Table 1 Open Bugs in Cisco Prime IP Express 8.2*

| Bug ID | Description |
|---|---|
| CSCun14677 | Linux ACL for GSS-TSIG clients not functioning |

## Using the Bug Search Tool

Use the Bug Search tool to search for a specific bug or to search for all bugs in a release.

**Step 1** Go to http://tools.cisco.com/bugsearch.

**Step 2** At the Log In screen, enter your registered Cisco.com username and password; then, click **Log In**. The Bug Search page opens.

**Note** If you do not have a Cisco.com username and password, you can register for them at http://tools.cisco.com/RPF/register/register.do.

**Step 3** To search for a specific bug, enter the bug ID in the Search For field and press **Return**.

**Step 4** To search for bugs in the current release:

a. In the Search For field, enter Prime IP Express 8.2 and press **Return**. (Leave the other fields empty.)

b. When the search results are displayed, use the filter tools to find the types of bugs you are looking for. You can search for bugs by status, severity, modified date, and so forth.

**Tip** To export the results to a spreadsheet, click the **Export All to Spreadsheet** link.

# Command Line Interface Enhancements

The following are the commands and attributes that were added in the CLI (see the *Cisco Prime IP Express 8.2 CLI Reference Guide*).

## New Commands

The following new commands were added to the CLI:

- **byod** command - Specifies the configure the BYOD web server in the Regional cluster.
  - **byod get** <*attribute*>
  - **byod set** <*attribute*>=<*value*> *[attribute*>=<*value ...]*
  - **byod unset** <*attribute*>
  - **byod show**
- **auth-ad-server** command - Configures the External Authentication Active Directory servers. If external authentication AD servers are configured, active directory server will be used to authorize subsequent log ins.
  - **auth-ad-server** <*name*> **create** <*addr*> <*domain*> <*base-dn*> <*ad-group-name*> <*ad-user-attr-map*> *[*<*attribute*>=<*value*> *...]*
  - **auth-ad-server** <*name*> **delete**
  - **auth-ad-server list**
  - **auth-ad-server listnames**
  - **auth-ad-server listbrief**
  - **auth-ad-server** <*name*> **show**
  - **auth-ad-server** <*name*> **get** <*attribute*>
  - **auth-ad-server** <*name*> *set* <*attribute*>=<*value*> *[*<*attribute*>=<*value*> *...]*
  - **auth-ad-server** <*name*> *unset* <*attribute*>
- **gss-tsig** command - configure a GSS-TSIG objects.
  - **gss-tsig list**
  - **gss-tsig listnames**
  - **gss-tsig listbrief**
  - **gss-tsig** <*name*> **show**
  - **gss-tsig** <*name*> **create** *[*<*attribute*>=<*value*>*...]*

  - **gss-tsig** <*name*> **delete**
  - **gss-tsig** <*name*> **get** <*attribute*>
  - **gss-tsig** <*name*> **set** <*attribute*>=<*value*> *[<attribute>=<value>...]*
  - **gss-tsig** <*name*> **unset** <*attribute*>

# New Attributes

New attributes were added to, or definitions modified for, the following commands:

- **byod** command:
  - **name** -The name of this server.
  - **client-prefix**-Specifies the string to be prefixed during the client creation.
  - **client-active-period**-Sets client activation period.
  - **custom-theme**-Sets the custom theme to be used in BYOD Registration
  - **keystore-passwd**-Contains the secret representing the password used to authenticate the identity stored in the admin attribute
  - **security-algorithm**-Specifies the security mechanism to be used with kerberos server(kdc) in Active Directory.
  - **ldap**-Identifies the LDAP server object to be used.
- **BYOD Theme**:
  - **name**-An arbitrary name used to refer to an individual theme configuration.
  - **font-color**-Sets the title font color to be used in the BYOD Device Registration page.The value can be color code or color string.
  - **hdr-font-color**-Sets the header font color to be used in the BYOD Device Registration page. The value can be color code or color string.
  - **background-style-type**-Specifies background image or colur of BYOD login, and common page.
  - **bg-color**-Sets the background color to be used in the BYOD Device Registration page. The value can be color code or color string.
  - **background-image**-Sets the background image to be used in the BYOD Device Registration page. Dimension: (817 X 326) Supported image formats: png,jpg,jpeg,gif,bmp.
  - **common-header-image**-Sets the background image to be used in the Common page header. Dimension: (1724 X 133) Supported image formats: png,jpg,jpeg,gif,bmp.
  - **login**-logo-Sets the registration and login page logo image. Dimension: (62 X 62) Supported image formats: png,jpg,jpeg,gif,bmp.
  - **common-logo**-Sets the common page logo image. Dimension: (90 X 38) Supported image formats: png,jpg,jpeg,gif,bmp.
- **BYOD Content**:
  - **login-footnote**-To set message for footer in device registration and login pages of BYOD Web Server.
  - **about-content**-To set content for 'About' link in device registration and login pages of BYOD web Server.

  - **terms-of-services-content**-To set content for 'Terms of Service' link in device registration and login pages of BYOD web Server.
  - **contact-content**-To set content for 'Contact' link in device registration and login pages of BYOD web Server.
  - **help-content**-To set content for 'Help' link in device registration and login pages of BYOD web Server.

- **gss-tsig** command:
  - **name**-Identifies the name of the gss-tsig configuration object.
  - **tkey-table-max-size**-The server and client will maintain some required data in TKEY table when performing TKEY negotiation. This attribute bounds the TKEY table by defining the maximum number of key records. The new TKEY query negotiation will fail when TKEY table hit this maximum size. Default size is 250.
  - **tkey-table-purge-interval**-This attribute will define the interval to purge expired key records in TKEY table. Default value is 60 sec.
  - **tkey-max-exchanges**-The maximum number of times that a TKEY RRs will be exchanged between a client and the server during a particular key negotiation to prevent endless looping as per RFC 2930. Default value is 5.
  - **gss-tsig-processing**-Enables you to turn on and off gss-tsig security mode for DNS transactions. If both gss-tsig-processing and tsig-processing are enabled, gss-tsig security mode will be disabled. Default is disabled.
- **auth-ad-server** command:
  - **ad-group-name**- Specifies the Active Directory group name. Only users belonging to this group will be granted access to the IP Express application.
  - **ad-user-attr-map**- Specifies the User object attribute to be used to get one or more IP Express groups.
  - **addr**- Specifies the host name and Ports of the AD servers.
  - **base-dn**- Specifies the distinguished name at which to start the search. User object will be searched in the base-dn and all entries in the tree below the base.
  - **domain**- Specifies the domain name to be used.
  - **name**- Identifies this Active Directory remote authentication server.
  - **query-timeout**- Specifies the number of seconds the CCM server waits for a response to the search request. Default timeout is 3 seconds.
  - **auth-type**-Sets the external authentication type to be used: Local, RADIUS, Active Directory. Changes to this setting will take effect the next time the product is restarted.

# Related Documentation

See Cisco Prime IP Express Documentation Overview for a list of Cisco Prime IP Express 8.2 guides.

# Accessibility Features in Cisco Prime IP Express 8.2

All product documents are accessible except for images, graphics, and some charts. If you would like to receive the product documentation in audio format, braille, or large print, contact accessibility@cisco.com.

# Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as an RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.

---

This document is to be used in conjunction with the documents listed in the "Command Line Interface Enhancements" section.