Cisco Prime IP Express BYOD

White Paper

September 2014

Contents

Introduction

This white paper discusses the functionality and configuration of the bring-your-own-device (BYOD) feature of Cisco Prime IP Express. The Cisco Prime IP Express BYOD portal is an easy to use self-service web portal for registering and managing devices. Employees can use their own mobile devices for business communications in a managed way - with the correct (authorized) IP addresses and network settings. It provides terms of use, branding and identity confirmation that all lead to an in-house provisioning experience that will lower operating expenses (OpEx) while satisfying administrators and end users.

BYOD is integrated with the Cisco Prime IP Express Dynamic Host Configuration Protocol (DHCP) and Caching Domain Name System (CDNS) servers. The methodology, architecture, and BYOD configuration required for this system are documented herein in detail. Using this white paper as a guide, you can easily configure BYOD for registering and managing the devices.

Problem Statement

All large IP networks face a common set of problems related to device configuration and network access, including:

- Provide hands-off, user-driven configuration of computers with correct IP addresses and network settings.
- Configure large numbers of devices in a short span of time.
- Acquire information about the devices being configured on the network.
- Control access to IP network resources.
- Collect information to assist troubleshooting of network and security events.

BYOD Feature - Functional Overview

You can use the BYOD feature of Cisco Prime IP Express to address each of the problems mentioned above, as it allows employees to use their own IP-enabled devices in a well-managed and secure way. It effectively eliminates the challenges of the IT administrators to manually onboard and track personal and corporate devices.

Cisco Prime IP Express DHCP automatically redirects the user to the BYOD registration portal when he or she tries to connect a BYOD device for the first time. Users must register his or her device using existing Active Directory credentials. During the registration, information about the user's device, such as its MAC address/ DHCP unique identifier (DUID) and other metadata, are captured through auto-detection or manual entry. This information is used to map the users to their devices and to track the IP activity for auditing and compliance. The BYOD registration portal is integrated with Cisco Prime IP Express DHCP.

User's Perspective

The BYOD feature provides a simple process to activate a device for the end user. The procedures are as follows:

1. Connect the device to the network.
2. Users will see a request for an HTTP URL from a browser.
3. Users are automatically redirected to the BYOD registration page.
4. Registration page populates with the device details and the system prompts you for user credentials.
5. Provide credentials, such as a username, password.
6. Accept terms of service.
7. Click the **Register** button.
8. Wait for few seconds, and the device will reboot.

This process normally takes about three minutes. When complete, the device is activated and the client is created in the Cisco Prime IP Express DHCP server.

Administrator's Perspective

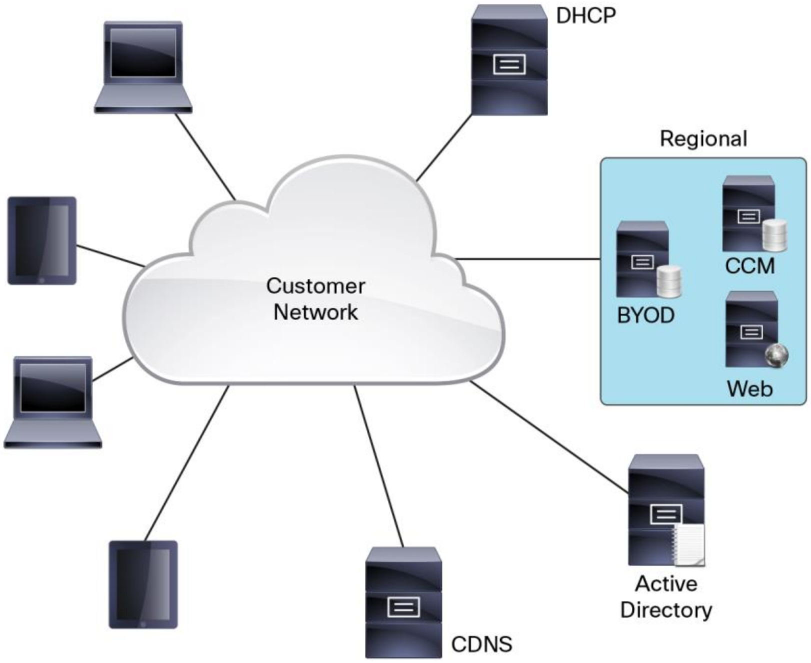
The BYOD feature is an easy to use self-service web portal and replaces many time−consuming and error-prone processes. Management of this self-service system is very simple:

1. Install Cisco Prime IP Express Web Server.
2. Configure a BYOD service (DHCP, CDNS servers).
3. Instruct users how to register their devices.
4. Instruct users how to use the user login page to manage devices.

Functional Architecture

The BYOD architecture (as shown in Figure 1) requires a minimum of four major components: a local DHCP server, a CDNS server, a regional server and an Active Directory server. In the regional server, a new Tomcat instance runs to support BYOD. The CDNS server is configured with the Domain Redirect rule with an access control list (ACL), which ensures that all the HTTP queries from specific range of addresses are resolved to the BYOD Web Server address. Figure 1 diagrams the functional architecture.

Figure 1. Cisco Prime IP Express BYOD Architecture

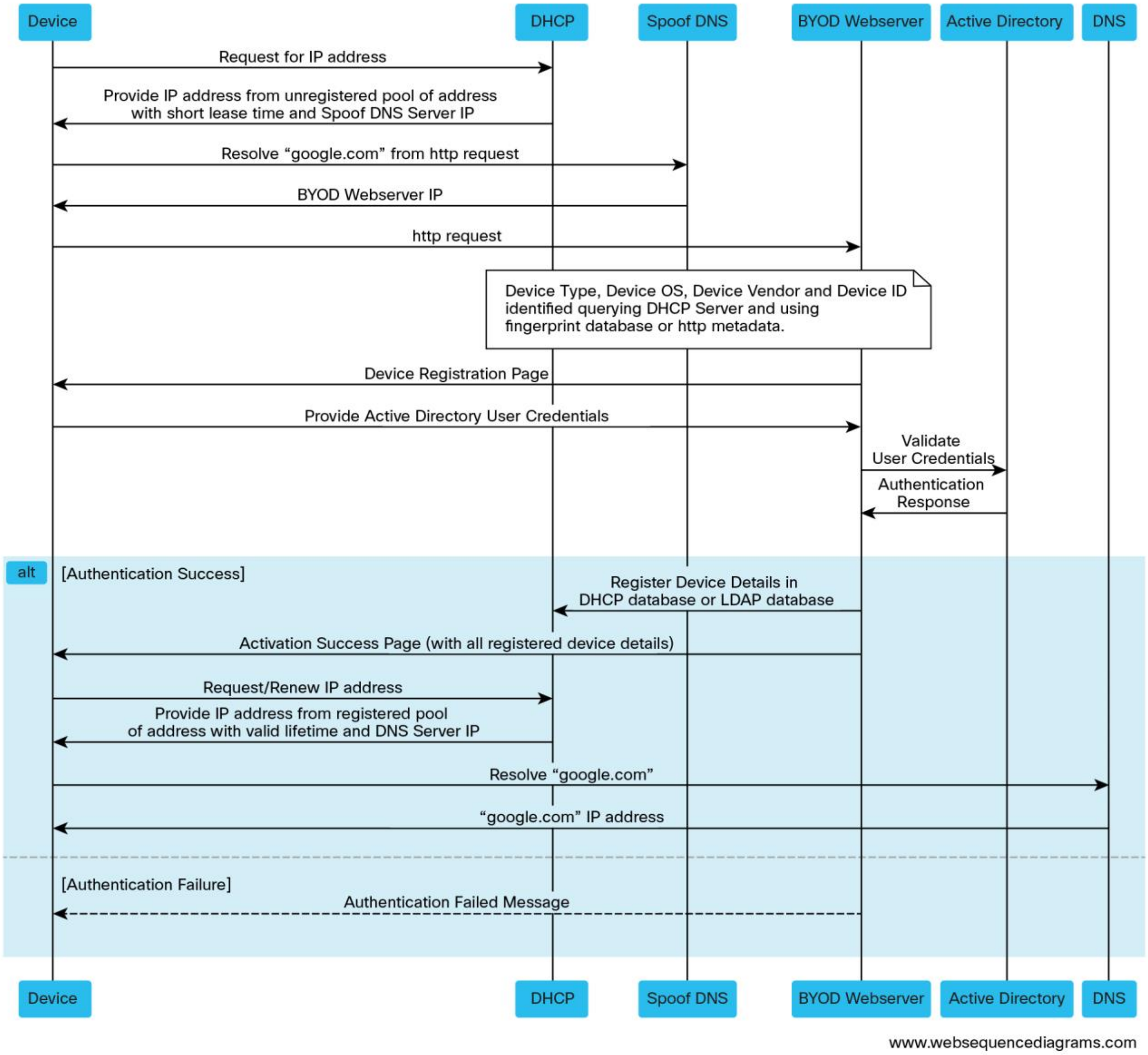


Process Flow

Figure 2 reflects the process flow of the web user interface when a user/client connects the BYOD to the network.

1. When a client connects a new device to the network, the DHCPDISCOVER/SOLICIT packet is sent to DHCP.
2. The DHCP server offers a temporary IP address and returns option 6 for DHCPv4 or option 23 for DHCPv6 with the CDNS server address.
3. The client sends a DNS resolver query to the CDNS server.
4. The CDNS domain redirect rule provides the BYOD web server with an IP address for the unregistered BYOD device and redirects to the device registration page.
5. The BYOD web server takes the client IP from the HTTP header data and checks the matching subnet/prefix to find the client DHCP server address.
6. If the matching subnet/prefix is not found, a System Configuration Protocol (SCP) request is sent to the regional Central Configuration Manager (CCM) to find the DHCP server which has served this client and updates the subnet/prefix information.
7. The BYOD web server sends a lease query with an address (as per RFC 4388 for DHCPv4 and as per RFC 5007 for DHCPv6) to the corresponding DHCP server to get the client identifier (Device ID) and populates the device registration page along with other details, such as device vendor, operating system, etc.
8. The client provides Active Directory credentials and submits the login form.
9. The BYOD web server authenticates the credentials against Active Directory.
10. Upon successful authentication, the BYOD web server sends an SCP request to the DHCP cluster or failover pair to create the client entry (client class name, authenticate until, device type, Vendor, OS, MAC/DUID, username) in the DHCP client database. If LDAP is configured, the client will be created only in the LDAP database.
11. Finally, the BYOD web server sends the successful registration message to the client with the details of all the devices that are registered by him/her.
12. If the authentication fails, the BYOD web server responds back to the client with a failure authentication message.

Figure 2. The Process Flow When a User/Client Connects the BYOD to the Network


Device
DHCP
Spoof DNS
BYOD Webserver
Active Directory
DNS
Request for IP address
Provide IP address from unregistered pool of address with short lease time and Spoof DNS Server IP
Resolve “google.com” from http request
BYOD Webserver IP
http request
Device Type, Device OS, Device Vendor and Device ID identified querying DHCP Server and using fingerprint database or http metadata.
Device Registration Page
Provide Active Directory User Credentials
Validate User Credentials
Authentication Response
alt
[Authentication Success]
Register Device Details in DHCP database or LDAP database
Activation Success Page (with all registered device details)
Request/Renew IP address
Provide IP address from registered pool of address with valid lifetime and DNS Server IP
Resolve “google.com”
“google.com” IP address
[Authentication Failure]
Authentication Failed Message
www.websequencediagrams.com

BYOD Configuration

To build the system for supporting the BYOD feature, you must modify the Cisco Prime IP Express configuration from its predefined settings to enable some of the server’s advanced features. You can easily accomplish this process (BYOD configuration setup) using the BYOD setup wizard in the Cisco Prime IP Express regional server.

For information on how to install Cisco Prime IP Express, refer to the Cisco Prime IP Express Install Guide.

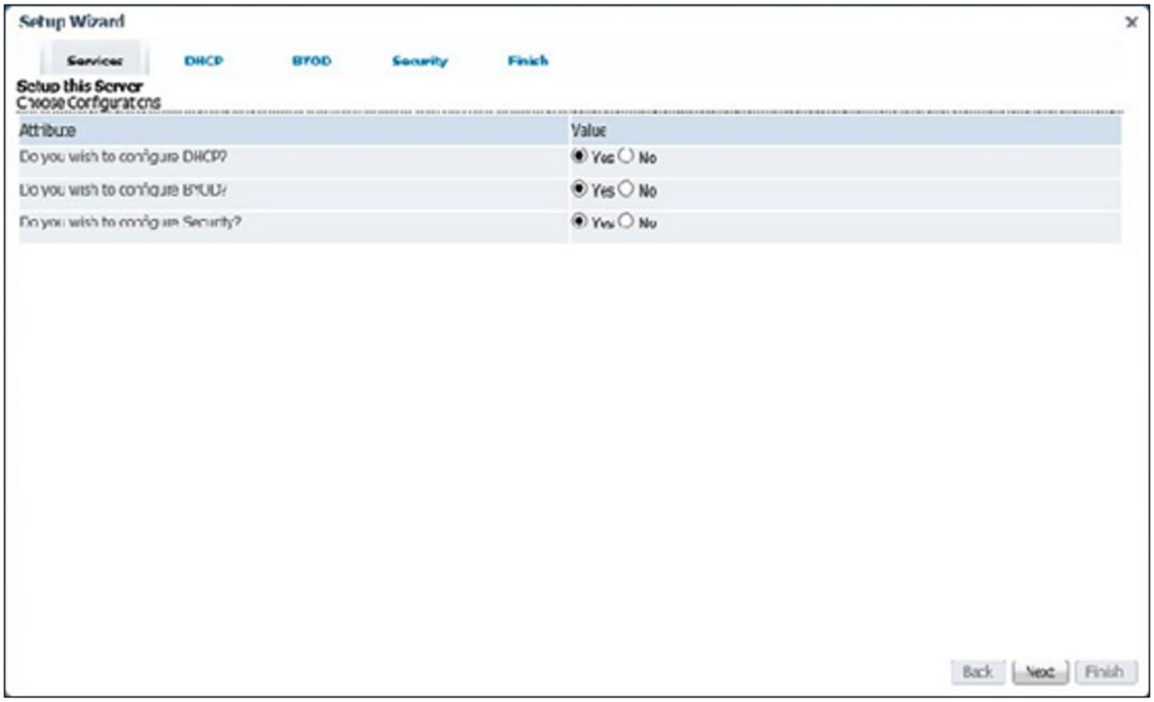
For more information on how to use the GUI, refer to the Quick Start Guide and User's Guide.

You can find all other Cisco Prime IP Express product documentation at: http://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/ip_express/8-2/doc_overview/guide/CPIPE_8_2_Doc_Guide.html.

BYOD Setup Wizard

The following sections explain the BYOD setup wizard workflow in the Cisco Prime IP Express regional server (see Figure 3). The overall process involves configuring both the DHCP and the CDNS servers. For simple setup, the default client is used for unregistered BYOD devices, while for complex setup, client-class-lookup-id and client-lookup-expression are used. Details are provided in user documentation, including the Deployment Guide.

Figure 3. BYOD Setup Wizard Sample Screen



Setup this Server
Choose Configurations

Attribute	Value
Do you wish to configure DHCP?	● Yes ○ No
Do you wish to configure BYOD?	● Yes ○ No
Do you wish to configure Security?	● Yes ○ No

DHCP Configuration

To configure the DHCP server, complete the following steps:

1. Select **No** for Failover.
2. Select **Yes** for DHCPv4.
3. Select **No** for DHCPv6 and then click **Next**.
4. The DHCPv4 Setup Wizard page opens.
5. Click **Add Scope Templates** to create scope.
6. Enter the scope template name in the Name box, and then click the **Add DHCP Scope Template** button.
7. Click **Save** to save the scope template, and then click **Next** to move to the next page.
8. Enter (**concat "byod-" subnet**) in the Scope Name Expression text box.
9. Enter (**create-range first-addr last-addr**) in the Range Expression text box and then click **Save** to save the page.
10. Click **Add Subnet** to create a subnet.
11. Enter the subnet IP in the Address text box, for example 10.76.206.0, and then click the **Add Subnet** button.
12. Click the **Push** icon to push the subnet to the local cluster.

13. From the Cluster or Failover drop-down list select the local cluster host name to which you want to push the subnet.
14. Select the scope template from the Scope Template drop-down list.
15. Click the **Push Subnet** button.
16. Move to BYOD Setup page by clicking **Next**

BYOD Configuration

You can use the BYOD Setup page to capture the details for CDNS server configuration for creating domain redirect rule (spoof DNS) and lease times for the unregistered devices.

1. The policies and client classes mentioned below are created in the regional server and further used in the setup wizard pages:

   BYOD Policy name: BYOD_Unregistered.

   - Add DHCPv4 dhcp-lease-time option (51) and set DHCPv6 valid-lifetime and preferred-lifetime. Select domain name server option 6 for DHCPv4 and option 23 for DHCPv6.

   BYOD client class name: BYOD_Registered

   - Set selection criteria for excluded - BYOD_Unregistered.

   BYOD client class name: BYOD_Unregistered.

   - Set selection criteria -BYOD_Unregistered.
   - Set Policy -BYOD_Unregistered.
2. To configure BYOD, follow the steps below:
   - Select the CDNS server from the drop-down list.
   - Specify the time for the unregistered client and click.
   - Click **Next** to move to Policies page.
   - Click the **Push** icon, select the local cluster host name from the Available list and add it to the destination clusters by using back arrows, and then click **the Push Data to Clusters** button.
   - Close the View Push Data Report by clicking the **Close** button.
   - Click **Next** to move to the Client Classes page, click the **Push** icon, and then click the **Push Data to Clusters** button.
   - Close the View Push Data Report by clicking the **Close** button and click **Next** to move to the Scope Creation page.
   - Specify the percentage in the text box under Value to define the IP range for the unregistered client. By default the value is 10.
   - Click **Next** to move to the Report page. This page shows the IP range assigned to the particular client with other details such as scope, cluster, subnet, and IP range. Click **Next** to move to the HTTPS configuration page.

Regional Server-HTTPS Configuration

The setup wizard page can be used for HTTPS configuration; these details are required for the BYOD web server.

To configure the HTTPS, follow the step below:

- Upload the keystore file using the **Choose File** button and enter the keystore password in the Keystore Password text box. Click the **Upload** button, and then click **Next** to move to the Reload Server page.

Reloading the Servers

Once configuration is complete, the Reload Server page can be used to reload the DHCP server, CDNS server, and the BYOD web server.

To do so, follow the steps below:

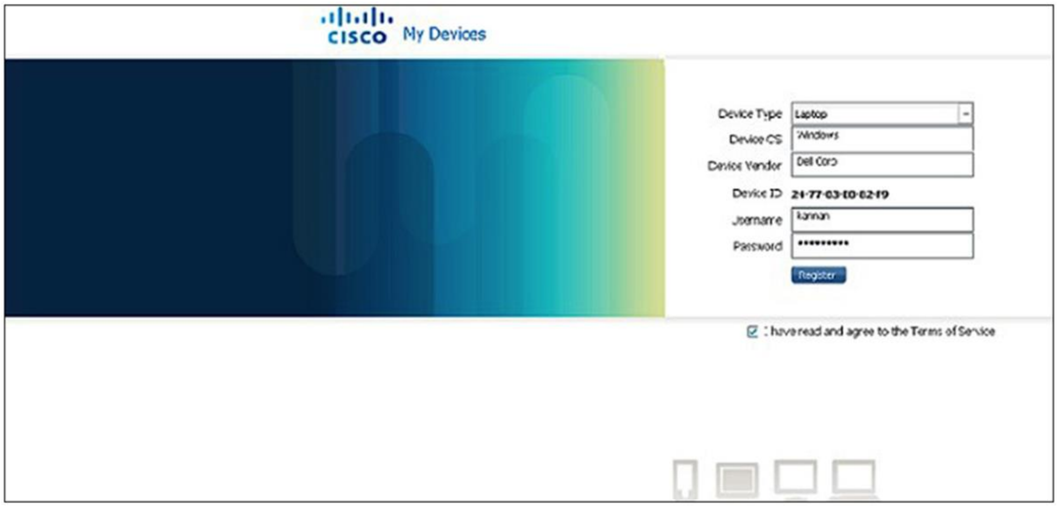
1. Specify value (Yes or No) to restart the BYOD web server, CDNS web server and DHCP servers/failover pair. Click the **Reload Servers** button, and then click **Next**. The Security page will open.
2. Choose the authentication type value **Active Directory** from the Value drop-down list.
3. Click **Save** and **Next**, move to the Active Directory page, and then click **Save**.
4. Enter the IP address, hostname and port (for example, IP=10.76.206.5, hostname = tmh2-chn-cnrent-AD1 and port= 389) in their respective text boxes, and then click **Add Address**.
5. Enter the domain name CPIPE.COM in the Domain text box.
6. Click **Next**, and the Successfully Configured page will open. Click **Finish** to complete the configuration setup process.

Device Registration Page

The Device Registration page allows users to register their devices. In this page, some fields such as Device Type, Device OS, Device Vendor and Device/MAC ID are pre-populated and also allow the user to edit the details. However, the users need to enter credentials such as:

- Username
- Password
- Terms of service

Figure 4. Sample Device Registration Page



My Devices

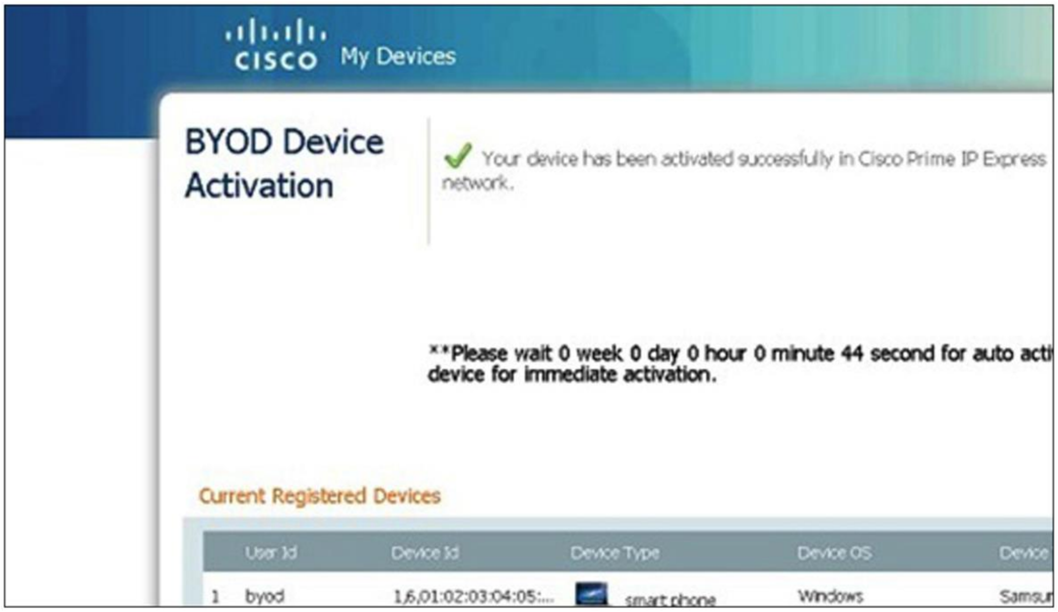
Device Type: Laptop
Device OS: Windows
Device Vendor: Dell Corp
Device ID: 24-77-03-E0-82-F9
Username: kannan
Password: •••••••••

☑ I have read and agree to the Terms of Service

Activation Success Page

Upon successful registration, the Activation Success page displays the message with lease time for automatic activation as shown below in Figure 5. The Activation Success page also displays the list of currently and previously registered devices for the same user. Users can delete a device by clicking the Delete icon.

Figure 5. Sample Activation Success Page



My Devices

BYOD Device Activation

✓ Your device has been activated successfully in Cisco Prime IP Express network.

**Please wait 0 week 0 day 0 hour 0 minute 44 second for auto acti
device for immediate activation.

Current Registered Devices

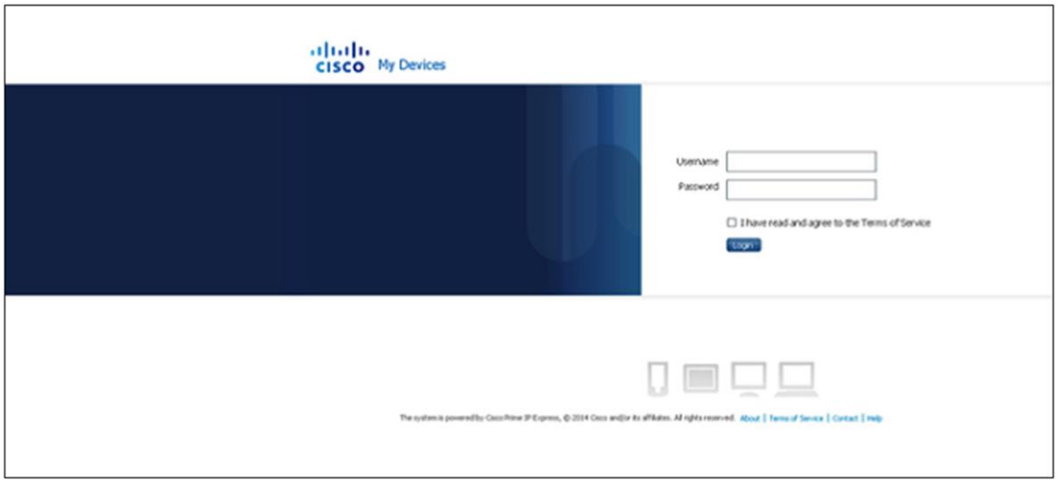
	User Id	Device Id	Device Type	Device OS	Device
1	byod	1,6,01:02:03:04:05:...	smart phone	Windows	Samsu

The User Login page allows users to delete their registered devices. To login to the User Login page, users need to provide their login credentials, such as username and password and also need to accept the terms of service. Upon successful login, the BYOD Registered Devices page opens.

This page is used to manage registered devices, such as deleting a device.

- Username
- Password
- Terms of service

Figure 6. User Login Page



My Devices

Username

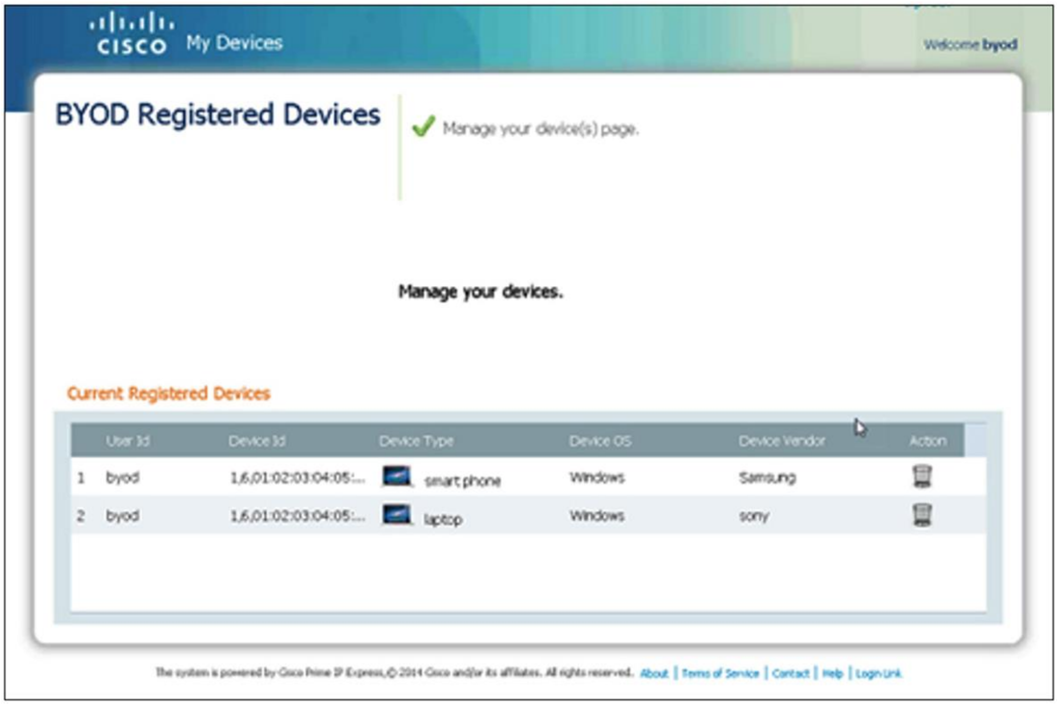
Password

□ I have read and agree to the Terms of Service

Login

The system is powered by Cisco Prime IP Express, © 2014 Cisco and/or its affiliates. All rights reserved. About | Terms of Service | Contact | Help

Figure 7. Device Management Page



My Devices

Welcome byod

BYOD Registered Devices

✓ Manage your device(s) page.

Manage your devices.

Current Registered Devices

	User Id	Device Id	Device Type	Device OS	Device Vendor	Action
1	byod	1,6,01:02:03:04:05:...	smart phone	Windows	Samsung	🗑
2	byod	1,6,01:02:03:04:05:...	laptop	Windows	sony	🗑

The system is powered by Cisco Prime IP Express,© 2014 Cisco and/or its affiliates. All rights reserved. About | Terms of Service | Contact | Help | Login Link

Lookup Expression

Lookup expression identifies whether the device is an existing device or is unregistered. It determines client-class for the client-class-lookup-id attribute of the DHCP server, and the server executes this expression on every incoming packet to determine the client class of the packet. It returns a string (client-class name for the packet, or the distinguishing string indicating that no client-class value was considered for the client request) as per the specified expression value. The goal of lookup expression is to ensure that each client receives its appropriate class of service across the same network.

Setting up Lookup Expression

After BYOD is configured, the lookup expression can be set up by following the steps:

- Enter Expert mode by clicking **Expert**.
- Open the List/Add DHCP Client Classes page, (Navigation: **Design** > **DHCP Settings** > **Client Classes**).
- Create or select an already created class in the Client Classes pane on the left.
- On the Edit DHCP Client Class created client page, under Create New Embedded Policy, enter expression in client-lookup-id and override-client-id; for example, enter (request option "relay-agent-info" "remote-id") in the client-lookup-id text box and (request option "relay-agent-info" "remote-id") in the override-client-id text box.
- Click **Save** to save the settings.
- Open the Manage Server Page (Navigation: **Operate** > **Servers** > **Manage Servers**).
- Click the **Local DHCP Server** link in the Manage Servers pane on the left.
- Click the **Edit Local DHCP** Server tab.
- Enter the created client class name in the client-class-lookup-id text box.
- Restart the local DHCP server to make these changes effective.

LDAP Client Create Support

The BYOD web server enables "LDAP client create" support when the Cisco Prime IP Express DHCP server is enabled with the LDAP client option.

If the DHCP server is enabled with client-look-up in the LDAP then Regional Server LDAP configuration is required for the BYOD to create the client in LDAP.

To create and configure the LDAP client in regional server, follow the steps below:

1. Enter Expert mode by clicking **Expert**.
2. Open List/Add LDAP Remote Servers page, (Navigation: **Deploy** > **DHCP** > **LDAP**).
3. Click the **Add LDAP** icon in the LDAP pane on the left. The Add DHCP LDAP Server window opens.
4. Enter the LDAP name and hostname in the name and hostname text boxes, and then click **Add DHCP LDAP** Server. The DHCP LDAP server gets added with the given name in the LDAP pane on the left.
5. Click the newly added LDAP link in the LDAP pane on the left. The Edit LDAP Remote Server Page opens, in which name and hostname are auto-populated.
6. Enter IP address, port values, and username and password in the respective text boxes.
7. Set the value for **enable** to **True**.
8. Set the value for **can-create** to **Enabled**.

9. Set the value for **can-query** to **Enabled.**
10. Set the value for **can-update** to **Enabled**.
11. Under Query, enter the **Search Path** value.
12. Under Query, keep the default value **SUBTREE** for **search−scope**.
13. Under Create Settings, enter the **dn-create-format** value.
14. Under Create Settings, enter the **create-dictionary** value.
15. Under Create Settings, enter the **create-object-classes** value.
16. Click **Save** to save the settings.
17. Open the Manage Servers page (Navigation: **Operate > Servers > Manage Servers**).
18. Click the **Local BYOD Web Server** link in the Manager Servers pane on the left.
19. Restart the local BYOD web server by clicking the **Restart Server** icon to make the changes effective.

DHCP Fingerprint

A DHCP fingerprint is a unique identifier to identify specific operating system or device type.

BYOD Web Server reads the dhcp_fingerprints.conf and it has a HashMap of fingerprints (PRL) and OS description.

From the DHCPv4 lease query reply, the BYOD web server gets the user-defined attribute value on the lease and finds the appropriate OS (description value) and OS number. Using the OS number, it finds the appropriate class definition, and the description of class provides device type information.

If the OS vendor and device type can’t be identified using the fingerprint file, HTTP header user-agent data is used. Pattern matching is done with the master file which has the list of OSs.

To configure DHCP Fingerprint, follow the steps given below:

1. Enter Expert mode by clicking **Expert**.
2. Open the List/Add DHCP Extensions page (Navigation: **Deploy > DHCP > Extensions**).
3. Click the icon in the Extensions pane on the left. The Add DHCP Server Extension window will open.
4. Enter the **extension name, lang, file** and **entry** values in the respective text boxes.
5. Click **Add DHCP Server Extension**, and then **click** Save to save the settings. The new extension is added.
6. Click the extension link in the Add Extension pane on the left. The Edit DHCP Extension page opens.
7. Click the **Attach Extension Point** icon on the right. The Extension Points window opens.
8. Under Attach Extension Points, select **post-packet-decode**, and then click **Save**.
9. Or click the **DHCP Extension Points** tab and then select Attach drop-down list against ‘post−packet−decode.’ This window can also be used for de-attaching the attached extension.
10. Open the Manage Servers page (Navigation: **Operate > Servers > Manage Servers**).
11. Click the **Local DHCP Server** link in the Manager Servers pane on the left.
12. Restart the local DHCP server by clicking **Restart Server** icon to make the changes effective.

Note: Fingerprint should be configured only in the local server.

Theme Configuration

This page allows BYOD admin to edit the look and feel of the BYOD web server pages by editing the theme attributes such as specific colors or color code and logo/background images to match with their own brands.

There are two types of themes, a non-customizable-default Cisco theme and a customizable theme.

To configure the theme, follow the steps given below:

- Enter Expert mode by clicking **Expert**.
- Open List/Add Custom Theme page (Navigation: **Deploy > BYOD > Theme**).
- Click the **Add Theme** icon in the Theme pane on the left. The Add Custom Theme window opens.
- Enter the theme name, background color, login page title font color and page title font color in the respective text boxes.
- Click **Add Custom Theme**. The next page will open with the details you provided.

Note: You can use this page to upload background image, common page header image, login page logo and common page logo.

- Click the **Background Image Browse** button, and then click **Upload** to upload an image for background.
- Repeat the same procedure to upload images for common page header image, login page logo and common page logo.
- Click **Save** to save the settings.

Content Page

The Content page allows the BYOD admin to configure messages specific to the customer, such as register/login page message, about content, terms of services, contacts and help.

When the user enters the content and submits or uploads (.html) file, it generates specific HTML files for each attribute inside the BYOD web content directory with specific file names, and the content links point to the specific HTML files.

The entered content is placed in between the HTML paragraph tag to make sure the content is displayed in the same format as it was entered.

To configure the Content page, follow the steps given below:

1. Enter Expert mode by clicking **Expert**.
2. Open Content page (Navigation: **Deploy >BYOD > Content**).
3. Enter the contents for **Register/Login Page Message Content, About Content, Terms of Services Content, Contact Content** and **Help Content** in the respective text boxes.
4. Or click the respective **Browse** and **Load** buttons to import the contents.
5. Click **Save** to save the settings.

Glossary

The list below describes the acronyms for the terms that are used throughout the document.

ACL: Access control list

AD: Active Directory

BYOD: Bring your own device

CCM: Central Configuration Manager

CDNS: Caching Domain Name System

DHCP: Dynamic Host Configuration Protocol

DUID: DHCP unique identifier

LDAP: Lightweight Directory Access Protocol

RFC: Request for command

SCP: System Configuration Protocol

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C11-732499-00 09/14