Instant Access Workflow

Overview

The GUI-based Instant Access workflow in Cisco Prime Infrastructure simplifies the Cisco Instant Access deployment, interface template management, and the FEX ports configuration. The Instant Access workflow provides complete automation for deploying Instant Access networks using Cisco Catalyst 6500/6800 series switches, each connected with up to 160 compact switches. In addition, it also automates the provisioning of FEX ports for devices to be connected either statically or dynamically via automatic device detection. Applicable Cisco best practice configurations are automatically deployed by the workflow, further minimizing the deployment efforts. The workflow not only greatly reduces the time to deploy access networks, but also provides a centralized view of the network for management purpose.

The Instant Access workflow automates the following tasks:

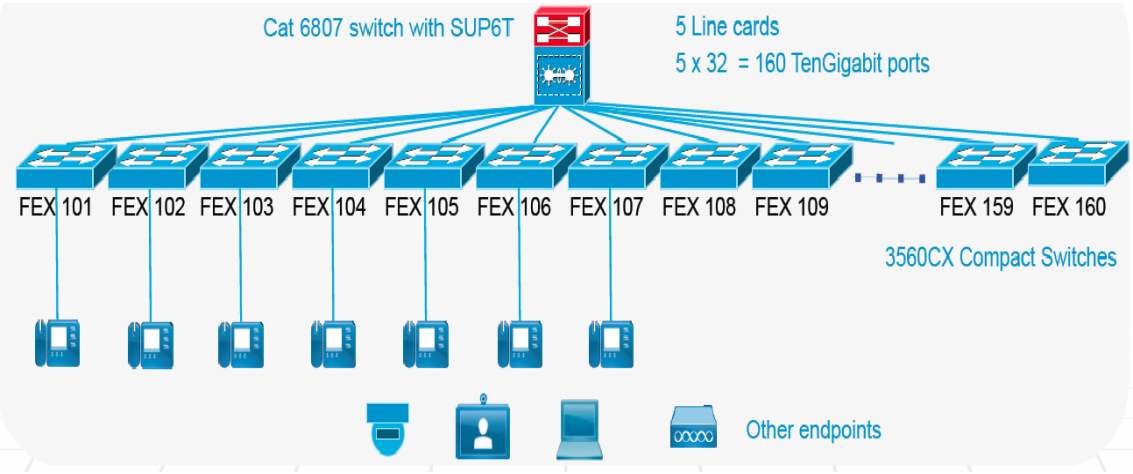
- VSS conversion—The workflow allows a 6500/6800 series switch to be converted to VSS mode. VSS mode is a pre-requisite for a switch to be configured with Instant Access.
- Configuring Instant Access on a VSS converted switch. This includes converting the ports on the parent switch to FEX mode.
- Creation and application of Templates, and VLANs to automatically provision FEX ports for accepting devices that can be detected dynamically, such as Cisco IP phones, Cisco Access Points, and Apple TVs.
- Automating the creation and application of Templates and VLANs for supporting devices such as laptops that cannot be detected dynamically.
- Automatically applying Cisco Best Practice configurations.

Text Part Number:

Instant Access Topology

Figure 46-1 shows a sample Instant Access topology that can be managed and configured by Cisco Prime Infrastructure.

Figure 46-1 Sample Instant Access Topology



The sample Instant Access topology shown in Figure 46-1, includes a single catalyst 6807 chassis with 2 x SUP6T and 5 line cards. Each line card has 32 Ten Gigabit ports. Each port is connected to a FEX switch and the FEX switches are connected to different endpoints (IP Phones). The parent switch can be any supported switch as listed in Supported Parent Switches.

Pre-requisites for Using Cisco Instant Access Workflow

To successfully use the Cisco Instant Access workflow, you must ensure that the following pre-requisites are met for the network devices and Cisco Prime Infrastructure system:

- Initial Device Setup—Parent switch is reachable from Prime Infrastructure with Telnet and SNMP configured.
- Device On-boarding—Parent switch is added to Prime Infrastructure Inventory.
- IOS Software—Parent switch has the recommended software version.
- Supported Platforms—Parent switch must be VSS mode capable. See Supported Parent and Client Switches.

Supported Parent and Client Switches

The Instant Access workflow requires a single catalyst 6500-E or 6800 switch as a parent and C3560CX-12PD-S, or C3560CX-8XPD-S compact switches as clients.

Supported Parent Switches

Table 46-1chassis and modules that are supported as the parent switch in the Cisco Instant Access workflow.

Table 46-1 Supported Chassis, Supervisors and Line Cards

Chassis	Supervisor	Line Card
C6807-XL	C6800-SUP6T-X	C6800-32P10G
C6500E	C6800-SUP6T-XL	C6800-32010G-XL
C6807-XL	VS-SUP2T-10G	C6800-16P10G
C6500E	VS-SUP2T-10G-XL	C6800-16P10G-XL
		C6800-8P10G
		C6800-8P10G-XL
C6880-X-LE	C6880-X-LE-SUP	C6880-X-LE-16P10G
C6880-X	C6880-X-SUP	C6880-16P10G

Note

- The Instant Access workflow does not support configuring uplink ports of Sup2T and Sup6T as Instant Access RSL ports.
- Only a single chassis VSS with single or dual Supervisors is supported.

Supported IOS Images

- SUP6T—15.3(01)SY, and above

For more information on the supported IOS images on the additional devices, see the *Cisco Prime Infrastructure 3.1 Supported Devices*.

Supported Client Switches

The following compact switches are supported as Instant Access Clients:

- C3560CX-12PD-S
- C3560CX-8XPD-S

Key Functions of Instant Access Workflow

The key functions of Instant Access workflow are:

- VSS Conversion
- FEX Provisioning and Pre-Provisioning
- Template/Custom Template/Workgroup Creation using Access Page
- Static Assignment of Workgroups/Templates to Ports

VSS Conversion

Instant Access configuration can only be performed on a VSS converted switch, and therefore the first step in the Instant Access Workflow is to convert a parent switch to VSS mode.

Figure 46-2 VSS Page in Instant Access Workflow

The VSS page allows you to create a deployment profile and add an Instant Access capable switch to the deployment profile along with any user specified description such as contact details of an Administrator. A switch added to one deployment profile cannot be added to another deployment profile. If a switch added to the deployment profile is in Standalone mode, you must convert the switch to VSS mode using the Instant Access workflow. As part of the VSS conversion, Prime Infrastructure automatically archives the configuration of the switch before and after VSS conversion and applies Cisco Best Practices configuration including QoS. You can also save the pre-VSS conversion switch configuration on the switch (bootdisk: or disk0:) and/or on a remote server using TFTP or FTP.

Key Functions

- Detecting VSS conversion suitability—Automatically detects if a switch is suitable for VSS conversion for Instant Access Workflow, and indicates the following issues in GUI prior to conversion:
  - Unsupported switches, chassis, and SUPs.
  - Dual SUP chassis not in SSO redundancy mode.
- Automatic saving of pre/post VSS conversion switch configurations:
  - Pre-VSS configuration is always backed up in Prime Infrastructure.
  - Pre-VSS configuration can be optionally backed up locally (bootdisk:, or disk0:), and/or remotely (TFTP/FTP)
  - Post VSS configuration is automatically backed up in Prime infrastructure.
- Automatic VSS conversion:
  - VSS conversion of a single or dual SUP switch.
  - Automatic deployment of applicable VSS Best Practice recommendations.

  - Allows to specify switch location.
  - Displays module status—You can proceed further in the workflow when all the module reach the required status.
- Automatic deployment of Cisco Best Practice recommendation:
  - System management best practices.
  - Layer 2 best practices—VTP, spanning tree and so on.
  - Layer 3 best practices.

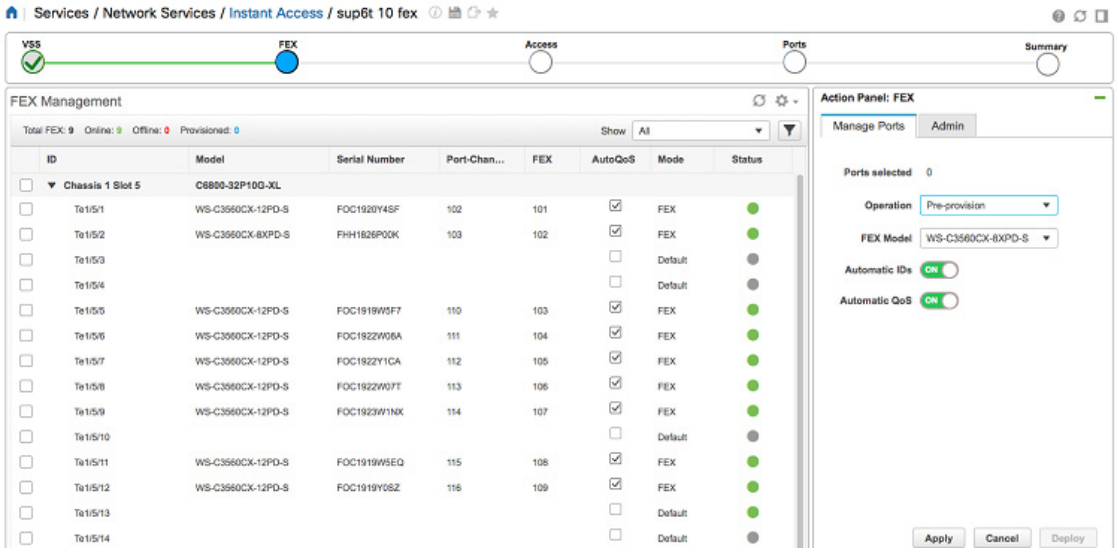
FEX Provisioning and Pre-Provisioning

After a switch is converted to VSS, the FEX Management page allows you to convert the Ten Gigabit ports of supported modules on the parent switch to FEX mode. To minimize the administration efforts, the Instant Access workflow automatically assigns the FEX IDs and port channel IDs to the ports excluding already used IDs, and provides an option to override them if needed. The Instant Access workflow automatically generates QoS and Cisco Best Practices code for the provisioned ports.

Key Functions

- Automatic filtering of non-FEX capable modules/ports to simplify deployment:
  - The GUI displays only the line card modules that can support FEX conversion.
  - The GUI does not allow to configure ports already having L2/L3 configurations, or connected to an incompatible switch.
  - A port with non-FEX L2/L3 configurations can be set to factory default settings, and then converted to FEX mode.
- Automated bulk FEX conversion/removal of FEX capable ports (Ten Gigabit ports):
  - To simplify deployment efforts, the FEX ids and their Port channel IDs are automatically generated by default. However, they can be manually assigned, if desired.
  - On a Cisco 6500E or 6807 chassis with SUP6T, up to 160 Ten Gigabit Ethernet ports can be converted to FEX mode, by a single GUI deployment activity (this creates 160 x 8 = 1280 FEX ports for 8 port compact switch, or 160 x 12 = 1920 FEX ports for 12 port compact switch).
  - Administrator can pre-provision the ports even if the compact switches are not connected to the parent switch. As and when they get connected, the compact switches will be converted to FEX mode providing PnP capability.
  - Fast boot functionality can be turned on/off in bulk for compact switches.
  - You can remove FEX mode configuration from FEX converted ports, simultaneously converting the connected FEX converted compact switches to standalone mode.
- Automated application of Cisco Best Practice recommendations:
  - Recommended best practice configurations are applied to RSL ports.
  - Automatically generates and applies both ingress and egress QoS configuration to RSL ports.
  - QoS configuration can be removed and/or re-applied to RSL ports.

Figure 46-3 FEX Management Page in Instant Access Workflow



The FEX Management page shows the operation mode and status of the 10 Gigabit Ethernet ports that are associated to the slots of the parent switch. Table 46-1 shows the possible operation modes and a brief description of each mode.

Table 46-1 Operation Modes of 10 Gigabit Ethernet Ports

Mode	Description
Default	The port is configured to default factory settings, if any compatible compact switch in standalone mode is not detected on the port.
Standalone	The port having the default configuration and a compact switch in standalone mode (not converted to FEX mode), is connected to the port.
Provisioned	The port is configured for FEX mode. A compact switch is already connected to the port and has been converted to FEX mode.
Pre-Provisioned	The port is configured for FEX mode before any compact switch is connected to the port. Once a compact switch is connected to the port, it will get converted to FEX mode, and the status of the port will change to provisioned from pre-provisioned.
Non-Default	The port has some existing layer 2 or layer 3 configurations. Instant Access workflow excludes these ports from FEX conversion by default, assuming that these are valid configurations for the switch to operate in the network. However, the GUI allows converting these ports to factory default mode and then configuring to FEX mode.

The operation status of each port is represented by a colored dot in the FEX page. You can view the description by hovering the mouse over the colored dot. Table 46-2 shows the description of the operation status of the FEX ports represented as a colored dot in the FEX page.

Table 46-2 Operation Status of FEX Ports

Status	Description
Red	The port is administratively down or FEX port is offline.
Green	The port is up or the FEX port is online.
Blue	The port is pre-provisioned.
Grey	The port is down (not connected).

Table 46-3 shows the tasks that can be performed in the FEX Action Panel.

Table 46-3 Tasks Performed in FEX Action Panels

Task	Description
Factory Reset	Configures the port to factory default settings. Click the **Factory Reset** radio button in the **Admin** tab in the FEX Action Panel to perform this task. The port must be in Default or Non-Default mode to perform this task.
Pre-provisioning one/more Ten Gigabit ports	Configures the port to FEX mode while no compact switch is connected to the port. This is useful when you want to configure the parent switch before the compact switches are available. To pre-provision a port, it must be in one of the following modes: • Default and shut-down (Red). • Default and unconnected. If you want to pre-provision a port irrespective of its current configuration, you must first configure the port to Factory default settings and then apply the pre-provisioning action.
Provisioning one/more Ten Gigabit ports	Configures the port to FEX mode operation while the compact switch is already connected to the port. Once the port is configured, the connected compact switch will reload itself, download the image if necessary and convert itself to FEX mode. To provision a port, it must be in one of the following modes: • Standalone mode. • The port must be up, in Default mode, and no CDP neighbor is detected through the port. **Note** The second condition allows recovery from a situation where a FEX provisioned port is changed to Factory default configuration. In this case, the connected compact switch will still be in FEX mode and hence will not be seen as CDP neighbor.
Remove FEX provision from one/more ports	The removal operation performs the following: • Sets the port to factory-default mode. • Converts the connected compact switch to standalone mode from FEX mode. The port must be in FEX mode (provisioned or pre-provisioned).
Up	Brings the port up.

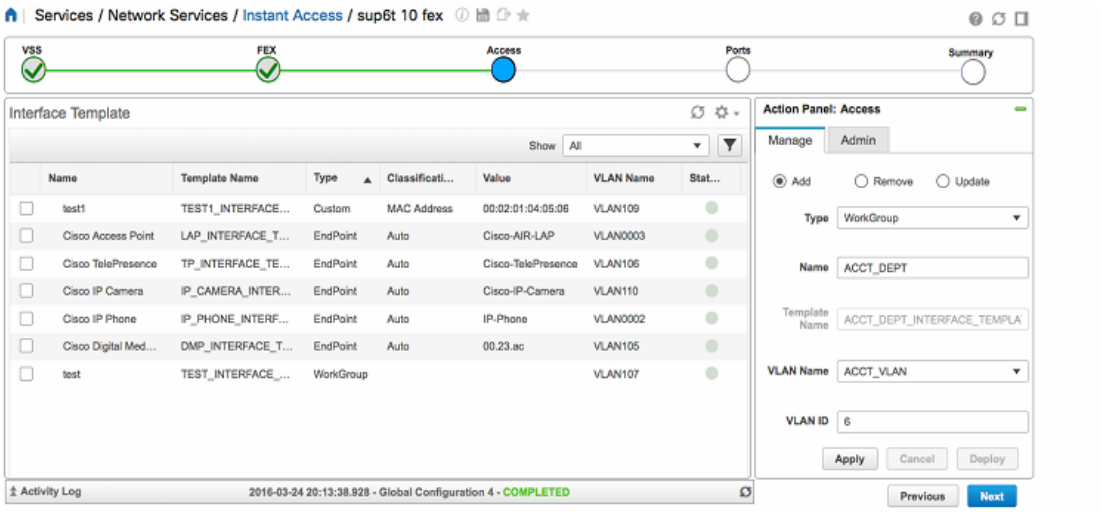
Task	Description
Down	Shuts the port down.
Reset	Shuts the port down and brings it up.

Template/Custom Template/Workgroup Creation using Access Page

The Instant Access workflow automates the administration efforts to provision the FEX ports that are created by provisioning/pre-provisioning the RSL ports. The FEX ports can be connected to various endpoint devices such as Cisco IP phones, Access Points, Telepresence devices, DMP devices, Video Surveillance Cameras, and custom devices such as Apple TV, and laptops. The automation is performed by:

- Turning on Autoconf feature, and using Interface Template functionality of IOS to automatically detect the type of device connected to an access port and dynamically configuring the port with the device appropriate template.
- Creating VLANs required for the endpoint devices. The GUI automatically generates VLAN IDs excluding:
  - VLANs already used.
  - VLAN 1, static Internal VLANs (1002-1005), dynamic Internal VLANs (e.g., 1006-1013, and 3968-4031)
- User can override any generated VLAN ID.
- Updating/creating the templates with appropriate VLANs.
- Automatically enhancing/creating the templates with Cisco Best Practices code.
- Automating the creation of QoS configurations and enabling/disabling QoS on FEX ports:
  - Ingress QoS on that classifies and marks packets
  - Egress QoS for queuing
- Ensuring that QoS is either enabled on all ports of a FEX switch or is disabled on all the ports

Figure 46-4 Access Page in Instant Access Workflow



The Access page deals with the following type of endpoint devices connected to the FEX ports:

- Well known Cisco Endpoints—Cisco devices such as Cisco IP phones, Cisco Access Points, Cisco Telepresence device, Cisco DMP device and Cisco Video Surveillance Camera can be automatically detected by the switch. The switch comes with built-in interface templates for these devices.
- Custom Endpoints—Non-Cisco devices such as Apple TV that does not have any built-in template and cannot be detected by default. You can create new templates for such devices and configure the switch to automatically detect them via MAC address or OUI and apply the template.
- Workgroups—Devices such as laptops are not automatically detected. The Instant Access workflow allows you to create interface templates for such devices and statically apply them to interface ranges.

You can create a separate workgroup for each department (for example, accounts department, finance department, engineering department and so on) in an organization and add an exclusive VLAN for each workgroup. The Instant Access workflow also adds Cisco Best Practice code to the templates.

The Access Page allows you to do the following:

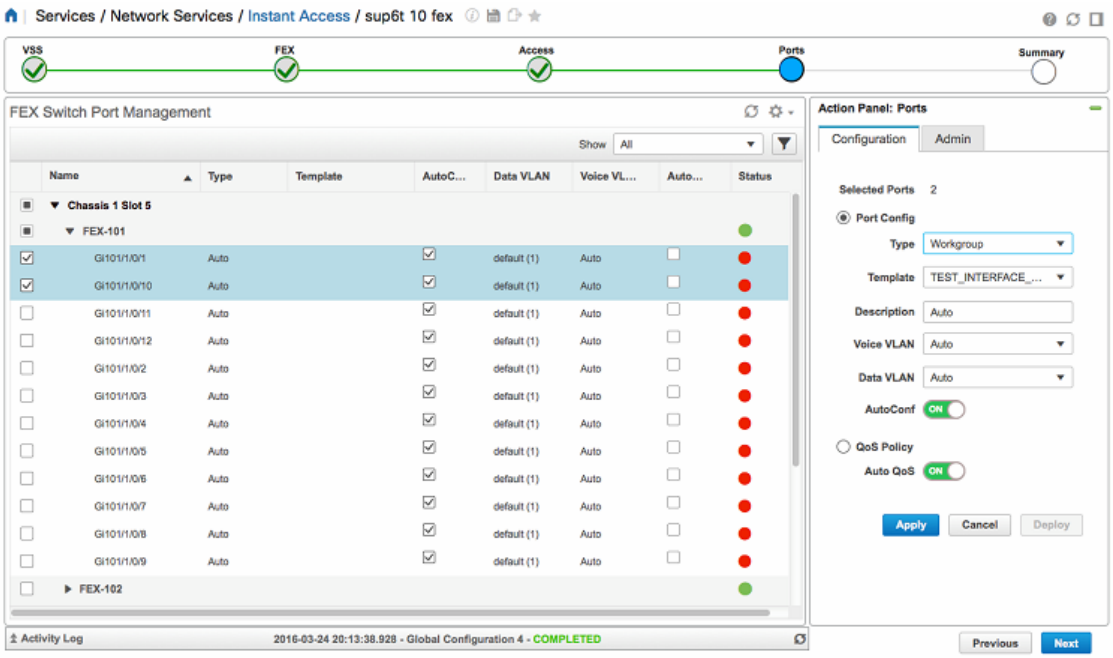
- Add/Edit/Remove the template for Cisco devices, custom device, or workgroups.
- Turn ON or OFF the LLDP based device type detection. By default, the CDP based detection is enabled.

Note The templates for the Cisco devices and custom endpoint devices are automatically applied to the ports, when such a device is connected, and the templates are removed when the device is disconnected. You need not do any reconfiguration when such devices are added, removed, or moved to a different port. For the Cisco devices and custom endpoint devices to work, the configuration is complete once we create the corresponding endpoint with the template and the VLAN in the Access page. For such dynamically detectable devices, additional functionality to statically assign a template to a port as provided by the Port page is not necessary, although such static assignment is possible.

Static Assignment of Workgroups/Templates to Ports

The ports page allows static assignment of workgroup/templates to individual FEX ports or a range of FEX ports. For example, you may assign the workgroup **ACCT_Workgrp** with Data VLAN **ACCT_VLAN** to a range of ports connected to the accounts department employees, and another workgroup **ENGG_Workgroup** with Data VLAN **Engg_VLAN** to ports connected to the engineering department employees. The ports are automatically configured with the VLANs that are associated with the department. The Port page also allows you to edit the Data and Voice VLANs for the ports.

Figure 46-5 FEX Ports Management Page in Instant Access Workflow



If an employee connects an automatically detectable Cisco device or custom endpoint to the port, the corresponding template is dynamically applied to the port in addition to any statically applied template. For example, if an employee attaches an IP phone to a compact switch port, and further attaches a laptop to the IP phone, two templates are applied to the same port. First, the workgroup template corresponding to the laptop must be applied statically to the port, and then the IP Phone template is automatically applied to the port on detection of the device.

Generally, in the Ports page, you need not apply templates to FEX ports to which the automatically detectable devices such as, IP Phones or Cisco Access points are connected. However, if you know that a Cisco Access Point or an Apple TV is always connected to a fixed port, you may statically apply a Cisco Access Point template or an Apple TV (custom) template to the fixed port.

The following operations can be performed on the Ports page:

- Add or remove a template to one or more selected FEX ports. When the type field is Auto it removes the existing template from the port.
- Turn on/off Auto Conf on the selected FEX ports.
- Add or remove QoS from the FEX ports—IOS allows QoS to be applied to all FEX ports of a client switch or remove QoS from all these ports (it is not possible to add QoS to some selected FEX ports of a client switch).

Using Instant Access Workflow

To create to an Instant Access deployment profile, do the following:

Step 1 Choose **Services > Network Services > Instant Access**.

Step 2 Click **New Deployment** to create a new deployment profile.

Step 3 Ensure that the pre-requisites mentioned in the **Before you Begin** page are satisfied and then click **Begin**.

Step 4 Enter the **Deployment Name** (typically a name to identify a parent switch), **Description** and click **Save**.

Step 5 Click the **Plus** icon and choose the VSS compatible device you want to configure as instant access parent switch (6500-E or 6800 series switch).

Step 6 Click **OK** to view the device details in the **Action Panel**.

The action panel displays relevant details of the switch including whether it is converted to VSS or not.

Step 7 If the device is already converted to VSS mode, go to Step 12.

Step 8 If the device is not configured in VSS mode, enter the Domain ID and other required details and click **Convert** to configure the device to VSS mode.

Step 9 Click the **Activity Log** to view the VSS conversion job status.

After the VSS conversion is over, the **VSS Action Panel** displays the status of the modules as **Other** or **OK**. The modules may take more time to reach **OK** status even after the VSS conversion is completed. You must wait until the relevant modules reach **OK** status before moving to the FEX page.

Step 10 (Optional) Enter the Location in the Action Panel and click **Set Location.**

Step 11 Click the Save Profile icon at the top of the VSS Page to save the profile and the running configuration of the switch in its start-up configuration. We recommend you to save the running configuration periodically while configuring a switch.

Step 12 After the VSS Action Panel displays the status of the relevant modules as **OK**, click **Next** to move to the **FEX Management** page which displays a list of the modules. If any of the modules is disabled, wait until it becomes selectable and perform the following tasks, as required:

Pre-provisioning the Ports

a. Click the expand icon corresponding the required parent switch module to view the available ports.

b. Choose the ports you want to pre-provision.

c. Choose the **Pre-Provisioning** operation under **Manage ports** tab in the **Action Panel**.

d. Choose the type of compact switch that you want to connect to the ports.

e. Set **Automatic IDs** and **Automatic QoS** to ON/OFF as required.

f. If Automatic ID is set to **OFF**, click the port row in the **FEX Management** window and enter unique port channel IDs and FEX IDs for the ports and click **Save**.

g. Click **Apply**.

h. Click **Deploy** to convert the selected ports to FEX mode.

Provisioning the Ports

a. Choose the ports that are connected to the compact switches.

b. Choose the **Provisioning** operation under **Manage Ports** tab in the **Action Panel**.

c. Set **Automatic IDs** and **Automatic QoS** to ON/OFF as required.

d. If Automatic ID is set to **OFF**, click the port row in the **FEX Management** window and enter unique port channel IDs and FEX IDs for the ports and click **Save**.

e. Click **Apply.**

f. Click the **Admin tab** and choose the required **Admin Port** and **Fast Boot** settings.

g. Click **Deploy** to convert the selected ports to FEX mode.

Step 13 Click **Next** and do the following in the **Interface Template** page:

a. Choose the template type from the drop-down list containing workgroups, custom templates, and built-in templates.

b. Enter the **Name**. The **Template Name** gets auto-populated based on the entered Name.

c. If you choose custom template, enter the device classification type and the classification value.

d. Choose a **VLAN** from the available VLANs or enter the VLAN Name.

e. The VLAN ID gets auto-populated based on the chosen VLAN. When creating a new VLAN, you can override the auto-populated value of the VLAN ID.

f. Click **Apply**.

g. Click **Deploy**.

Step 14 Click **Next** and do the following in the **FEX Ports** page.

a. Choose the FEX ports on which you want to apply the templates.

b. Choose the template type, template name, Data VLAN, and Voice VLAN in the **Manage Ports** tab under **Action Panel.**

c. Click **Apply**.

d. Click **Deploy**.

Step 15 Click **Next** to view the configuration summary of the created deployment profile.

Related Topics

- Pre-requisites for Using Cisco Instant Access Workflow
- Supported Parent and Client Switches
- Key Functions of Instant Access Workflow