Features

- Features, on page 1

Features

The following is a summary of the key features accessible from Cisco Intersight Virtual Appliance. For a complete list of features in Intersight, see the **Supported Features Matrix** section in the Help Center accessible from *<Your FQDN>/help*.

- **HyperFlex Cluster Deployment**—Intersight HyperFlex installer rapidly deploys HyperFlex clusters. Use the installer wizard to construct a pre-configuration definition of your cluster, called a HyperFlex Cluster Profile. This definition is a logical representation of the intended configuration for your HyperFlex cluster settings and HyperFlex nodes.
- **HyperFlex Cluster Expansion**—Starting from HyperFlex Data Platform version 4.0(2e), you can expand ESXi based 10/25 GbE HyperFlex Edge and Fabric Interconnect attached clusters with a minimum of 3 nodes.
- **HyperFlex Cluster Upgrade**—Starting from HyperFlex Data Platform version 4.0(1a), you can upgrade HyperFlex Data Platform,VMware ESXi and HX server firmware on HyperFlex clusters using Intersight. Currently, HX server firmware upgrade is available for HyperFlex Edge Systems only.
- **Dashboard Management**—Cisco Intersight Virtual Appliance provides a dashboard that spans Cisco UCS and Cisco HyperFlex systems. You can create, customize, rename, and manage multiple dashboard views by adding, removing, or rearranging widgets. In the Widget Library, you can select the widget(s) that you want to pin to the dashboard, preview the details for a server or a cluster, search for a widget, and add a custom title to a widget. You can add multiple instances of a widget to monitor different targets. You can add a maximum of 30 widgets per dashboard. The widgets provide a view of the health and inventory status of the managed targets in addition to reporting the following real-time data:
  - Global inventory—View information about inventory across the supported systems in the data center or at remote locations
  - License Status of your Cisco Intersight Virtual Appliance
  - Server HCL Status Summary
  - Fault monitoring—Manage faults and set up alerting for all managed systems
  - Tasks Summary for the past 24 hours

  - Firmware status—Monitor and manage firmware versions
  - Cluster Details—Details of a HyperFlex cluster, including (number of) Nodes, Capacity, Utilization, and HyperFlex version. From this widget, you can directly launch the corresponding HyperFlex Cluster Details page.
  - Custom Metric Widgets —Real-time status of a metric that you want to view.

- **Server Details and Table views**—The table view displays the details of the server. From the table view, you can launch device endpoints, perform bulk server actions, and navigate to the server details view. The details view displays additional details of the server such as server health, inventory, server profile, and hardware compliance status information of the selected server.
- **Cluster Details and table views**—Details of a HyperFlex cluster, including (number of) Nodes, Capacity, Utilization, and HyperFlex version. From the table view, you can directly launch the corresponding HyperFlex Cluster Details page.
- **Fabric Interconnect Details and Table views**—The table view displays the details of the fabric interconnect and its health status. From the table view, you can select a fabric interconnect to view further details such as management IP, firmware version, expansion module, and ports count.
- **Target Details and Table views**—The table view displays the details of the targets. From the table view, you can select a target to view additional the details such as target ID, claim, and device connector information of the claimed target.
- **Chassis Details and Table views**—The table view displays the details of the chassis. From the table view, you can select a chassis to view the additional details such as management mode, contract status, properties, and alarms of the selected chassis.
- **Context launch of Management Interfaces**—From Cisco Intersight Virtual Appliance, you can context-launch Cisco UCS Manager, Cisco IMC, Cisco UCS Director, and HyperFlex Connect, and obtain additional information as well as perform management operations on your target.
- **Installing an Operating System** —Intersight enables you to install vMedia based operating systems on the managed servers in your data center. With this capability, you can perform an unattended OS installation on one or more Cisco UCS C-Series Standalone servers from your centralized data center through a simple process. Before you begin the installation, you must select and add the required operating system and the server configuration utility images and the file share details to the Software Repository. For detailed information about installing the OS, the supported operating systems, and caveats about the installation, see Installing an Operating System and Caveats in the **Help Center**
- **Policy-based configuration through Server Profiles**—A Server Profile enables resource management by streamlining policy alignment and server configuration. You can create Server Profiles using the Server Profile wizard or you can import the configuration details of C-series servers in standalone mode and FI-attached servers in Intersight Managed Mode (IMM), directly from Cisco IMC. You can create Server Profiles using the Server Profile wizard to provision servers, create policies to ensure smooth deployment of servers, and eliminate failures that are caused by inconsistent configuration.

  The Server Profiles wizard groups the server policies into four groups namely Compute, Network, Storage, and Management Policies. After creating Server Profiles, you can edit, clone, deploy, or unassign them as required. From the Server Profiles table view, you can select a profile to view details in the Server Profiles Details view.
- **Server Actions and Bulk Server Actions**—The server actions enable you to manage a server. In Cisco Intersight, when you click on Servers, the Servers Table view is displayed. You can select one or more

servers and click the Ellipsis icon to perform server actions in bulk. You can choose to go to the Server Details page and perform server actions such as Set Certificate, Set Asset Tags, Set User Label, Launch KVM, Open TAC Case.

Note Reset CMOS and Lock Front Panel server actions are supported only on Intersight Managed Servers.

- **Update Software Packages for Intersight Virtual Appliance**—Intersight Connected Virtual Appliance provides a way to either update the software automatically when new versions are made available by the update service, or to manually update to any supported version that is higher than the running version. You must download software packages from either the Cisco Software Central site or by accessing the Appliance Account on Intersight, and then uploading them on to the appliance. Ensure that you have downloaded the required software packages as follows:
  - To download Cisco UCS Server Firmware and Cisco UCS Server Configuration Utility, go to Cisco Software Central.
  - To download Intersight Virtual Appliance, Cisco Hyperflex, and Cisco UCS Director software packages, you will need to access your Appliance Account. For more information, see Creating an Appliance Account and Downloading Software Packages for Intersight Virtual Appliance.
- **Firmware Upgrade**—Firmware upgrade in Cisco Intersight Virtual Appliance is performed using a non-interactive Cisco Host Upgrade Utility (HUU) to upgrade the BIOS, Cisco IMC, PCI Adapters, RAID Controllers, and other firmware to compatible versions. This feature requires a Cisco Intersight Essentials or above license.

  Firmware Upgrades in Intersight are supported on the following:
  - Cisco UCS C-series M4, M5, M6 and S-series M4,M5 servers that are configured in Standalone mode.
  - Cisco Fabric Interconnect-attached UCS B and C-series M3, M4, M5, and M6 servers in UCSM Managed mode (UMM).

    Note M6 servers in UMM are currently not supported for Private Virtual Appliance.
  - Cisco Fabric Interconnect-attached UCS B and C-series M5 and M6 servers in Intersight managed mode.
  - Cisco Fabric Interconnect-attached Cisco UCS S3260 M3, M4, and M5 servers in UCSM Managed mode.
  - Cisco Fabric Interconnect-attached Cisco UCS S3260 chassis in UCSM Managed mode.
  - Cisco UCS Fabric Interconnects Series 6200, 6300, 6400 and 64108 in UCSM Managed mode.
  - Cisco UCS Fabric Interconnects Series 6400 and 64108 in Intersight Managed mode.
- **Ability to Launch vKVM**—Cisco Intersight Virtual Appliance provides secure Virtual KVM capabilities for Fabric Interconnect-attached and Standalone Cisco UCS systems, and HyperFlex server nodes. You can launch the virtual keyboard, video, and mouse (KVM) console directly from Cisco Intersight. Local

network connectivity to the endpoint/server is required. This feature is available with Cisco Intersight Base and above license tiers.

- Intersight provides **Role-Based Access Control (RBAC)** to authorize or restrict system access to a user based on user roles and privileges. A user role in Intersight represents a collection of the privileges a user has to perform a set of operations and provides granular access to resources. Intersight provides role-based access to individual users or a set of users under Groups.
  - For a detailed description of the supported roles in Intersight and their associated privileges, how to add a User or Group, Create a Role or an Organization, and switch between roles, see Role Based Access Control (RBAC) in Intersight.
  - To watch a demonstration of how to create an organization, create a custom role, define a privilege for an organization, and assign a target to one or multiple organizations, see Introduction to Organizations.
  - For information about security in the Intersight platform, see Security in the Cisco Intersight Platform.
  - For frequently asked questions on Organizations and Roles, see FAQs .
- **Single Sign-On (SSO)**— SSO authentication enables you to use a single set of credentials to log in to multiple applications. With SSO authentication, you can log in to the Cisco Intersight Virtual Appliance with your corporate credentials. Cisco Intersight Virtual Appliance supports SSO through SAML 2.0, and acts as a Service Provider (SP), and enables integration with Identity Providers (IdPs) for SSO authentication. To set up SSO through the appliance, you must log in to Cisco Intersight Virtual Appliance as a user with administrator role, download the SP metadata, and register your Identity Provider (IdP) in the Intersight Virtual Appliance. For more information about how to set up SSO, see Setting Up Single Sign On Through Intersight and the SSO section in **Resources** in the Help Center. Click here to watch a video that shows how to enable Intersight Single Sign-On and set up a custom SAML 2.0 application in an external Identity Provider (IdP) with Intersight.
- **LDAP-based Authentication**—Cisco Intersight Virtual Appliance enables LDAP-based authentication for users added in your organization's LDAP server. Specifies the LDAP configuration settings and preferences for an endpoint. The endpoints support LDAP to store and maintain directory information in a network. The LDAP policy determines configuration settings for LDAP Servers, DNS parameters including options to obtain a domain name used for the DNS SRV request, Binding methods, Search parameters, and Group Authorization preferences. Through an LDAP policy, you can also create multiple LDAP groups and add them to the LDAP server database.
- **Integration with Cisco TAC**—Technical support offered by Cisco Technical Assistance Center (TAC) is included in your Essentials license. If you face any issue with the installation, set up, or operations of Cisco Intersight Virtual Appliance, open a case with Cisco TAC for assistance. The Cisco Technical Support website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies http://www.cisco.com/techsupport. For more information, see Technical Assistance.
- **Alarms**—Cisco Intersight Virtual Appliance provides fault monitoring capabilities to track and set up alarms for all managed UCS and HyperFlex systems. An alarm alerts you about a failure in the endpoint (a fault) or a threshold that has been raised. An alarm includes information about the operational state of the affected object at the time the fault was raised. The Virtual Appliance displays the total number of alarms in the Critical and Warning states next to the Alarms icon (bell icon representation). Click the icon to view the details of the alarms under the Critical and Warning tabs. For more information about alarms, see Related Documentation.

- **Manage Tags**—Cisco Intersight Virtual Appliance enables you to select and add tags to multiple objects in the Server, Clusters, Fabric Interconnects, Profiles, and Policies table view. You can edit the tags in the **Manage Shared Tags** window, accessible from **Tags** in the table view. The tags common to the selected objects are displayed by default, and you can add new tags or modify the common tags. If you modify a common tag, the existing common tag with the same key gets overridden. You can also manage the tags associated with a Server, Fabric Interconnect, Policy, or Cluster from **Tags** > **Manage** on the corresponding Details page. The existing tags for the selected object are displayed by default, and you can add new tags, or modify the existing ones.
- **Access to REST APIs and documentation**—You can automate management workflows through Cisco Intersight APIs to provision, report, track, and manage the targets. To become familiar with Cisco Intersight REST APIs, review the API resource information and functionality at API Docs.

Features