



Service Description: Cisco Managed Services for Application Centric Infrastructure (ACI)

Technology Addendum to Cisco Managed Services for Enterprise Common Service Description

This document, referred to as a Technology Addendum, describes the Cisco Managed Services for Application Centric Infrastructure (ACI).

Related Documents: This document should be read in conjunction with the Cisco Managed Services for Enterprise Common Service Description <http://www.cisco.com/go/servicedescriptions>.

Direct Sale from Cisco

If you have purchased the Services directly from Cisco, this document is incorporated into your Master Services Agreement (MSA), Advanced Services Agreement (ASA), or equivalent services agreement executed between you and Cisco. In the event of a conflict between this Service Description and your MSA or equivalent services agreement, this Service Description shall govern.

Sale via Cisco Authorized Reseller

If you have purchased the Services through a Cisco Authorized Reseller, this document is for informational purposes only; it is not a contract between you and Cisco. The contract, if any, governing the provision of the Service is the one between you and your Cisco Authorized Reseller. Your Cisco Authorized Reseller should provide this document to you.

The Service

Application Centric Infrastructure (ACI) is a holistic architecture with centralized automation and policy-driven application profiles. The Application Policy Infrastructure Controller (APIC) is the unifying point of automation and management for the ACI fabric.

This Technology Addendum is designed to be read in conjunction with the Cisco Managed Services for Enterprise Common Service Description that provides a baseline understanding of and sets expectations about the Cisco Managed Services, hereinafter referred to as the Service, provided by Cisco. In addition to the activities and deliverables outlined in the Common Service Description, this Technology Addendum outlines the unique activities and deliverables for the Customer's ACI Solution that is being managed by Cisco. Both service descriptions should be read in combination to fully understand the scope of the Service being purchased.

The Service offering described herein and other optional services are intended to supplement a current support agreement for Cisco products, and only available where all the Managed Components in a Customer's ACI Solution are supported through a minimum of core services such as Cisco's SMARTnet and Solution Support (SSPT) for the APIC components. Cisco will provide the Service described below as selected and detailed on the purchase order for which Cisco has been paid the appropriate fee.

Cisco shall provide a Quote for the Service setting out the extent of the Service and the term for which Cisco will provide the Service. Cisco will receive a purchase order that references the Quote agreed between the parties and that, additionally, acknowledges and agrees to the terms contained therein. Cisco only provides support for Managed Components, unless specifically noted. For any device, component or solution element not specifically designated as a Managed Component, Cisco shall have no responsibilities whatsoever.

This Technology Addendum describes the services capabilities, supported devices, elective changes, and reports delivered.

Two service packages are available:

- Standard Managed Services
- Comprehensive Managed Services

These service packages are described in detail in the Common Services Description. In addition to activities and deliverables in the two service packages, additional Optional Services can be purchased as needed to augment the selected package. The table below outlines the specific activities and deliverables applicable to the Data Center ACI offer as well as the Optional Services available for the Service.

Activities / Deliverables	Standard Services	Comprehensive Services	Optional Services
Remote Monitoring	X	X	
Configuration Backups	X	X	
ACI Reports	X	X	
Service Level Agreement	X	X	
Third Party Southbound API Support	X	X	
Third Party Northbound API Support		X	
ACI Software Upgrade Service			X
Defined Changes			X
Custom Changes			X

1 ACI Remote Management – Standard and Comprehensive

Overview

- 24x7x365 remote monitoring by the Cisco Data Center Network Operations Center (DC-NOC) for the Cisco ACI solution components
- Incident & Proactive Problem Management for the Cisco ACI solution components
- Change Management services for remediation of Incident and Problem events as well as optional Customer Requested Change Management services
- Single Point of Contact and operations escalation for the Cisco ACI Fabric and APIC
- Single Point of Contact for Incident isolation and case management of approved Third Party Ecosystem Technology Partner components and applications
- ACI Software Upgrade Service providing customers the option to order software update services for the ACI Fabric and the APIC
- The Service provides real-time monitoring on supported ACI solution devices and components and proactively declares Incident Events for: Unified Fault and Performance Management across:
 - Application Policy Infrastructure Controllers (APIC)
 - ACI Leaf Switches
 - ACI Spine Switches

- Physical Interfaces
- End Point Groups (EPG)
- Bridge Domains
- Service Devices
- Tenants
- Fabric Pod's
- Fabric Nodes

2 ACI Configuration Backups – Standard and Comprehensive

ACI Configuration Backup includes the process and actions needed to backup and restore Cisco Nexus 9000 Series Switches and the APIC. This may include backup policies outlining retention policies, ad-hoc configuration backups and restores as well as standard backup reports. Activities include daily backup of the Nexus 9300 and Nexus 9500 series switches (ACI Fabric) and the APIC. ACI backup services do not include the backup of 3rd party devices and/or software.

3 ACI Reports – Standard and Comprehensive

The Cloud and Managed Service Platform (CMSP) constantly gathers device level information from the Managed Components covered within the Service. This information is compiled and made available via reports on the Portal and/or upon request. The available ACI Reports are as follows:

- Contracts Report
- POD Details Report
- ACI Topology Report
- L4-L7 Services Report
- ACI Fabric Ports Report
- Spine and Leaf Reports
- Endpoint Details Report
- Application Summary Report
- End Point Group (EPG) Report
- Fabric Pod Overall Health Report
- Fabric Node Overall Health Report

4 ACI Software Upgrade Service – Optional

Cisco provides an optional per ACI POD (Point of Delivery) Software Upgrade service that includes software upgrades for the ACI Fabric switches and the APICs. This is in addition to the patches or upgrades, that may be required for incident and problem resolution, included in the standard and comprehensive service packages. The service includes:

- One software upgrade, per ACI Software Upgrade Service requested, of the ACI POD specific Cisco ACI Fabric and the associated APICs.
- An assessment of the ACI POD leveraging one, all, or a combination of the following; the Cloud and Managed Services Platform (CMSP), relevant associated ACI Reports, Engineering Recommended Releases, Release Notes, Field Notices, and Security Advisories.

- A rollback process and mitigation plan in place prior to any recommended software upgrade(s) .
- Review with Customer of Cisco's findings for recommended patches or upgrade(s)
- Installation of software updates in accordance with the Customer's defined Change Management process once Cisco receives the required approval from the Customer
- Validation of ACI system health and receipt of Customer Acceptance upon upgrade completion

5 Cisco ACI Third Party Vendor Support

Standard Service Package supports Southbound APIs only, allowing you to extend Cisco ACI policies to existing virtualization and Layer 4 through 7 service and networking components.

Comprehensive Service Package supports Southbound (as above) and Northbound APIs, allowing rapid integration with existing management and orchestration frameworks.

Third Party refers to a certified Cisco ACI Ecosystem Technology Partner, a technology ecosystem to help customers use, customize, and extend their existing IT investments with Cisco ACI offerings.

- In the event Cisco determines that an escalation with an ACI third party vendor is required to resolve the issue for the Customer, Cisco will work with the ACI third party vendor in a collaborative manner to the extent allowed by the ACI third party vendor. In the event that the ACI third party vendor does not allow Cisco to work with them in a collaborative manner, the Customer may be required to engage the ACI third party vendor to resolve the issue.
- As part of the Service, it may be necessary for Cisco to disclose Customer information to the applicable ACI third party vendor. Such information may include logs and contact information.
- Cisco will provide information, to the extent allowable, to the applicable ACI third party vendor conducting diagnosis and resolution of the Customer's issue.
- Cisco will provide updates on actions taken to resolve the Customer's issue as a single point of contact.
- As needed, Cisco may open cases on behalf of Customer with the applicable ACI third party vendor.

5.1 Customer responsibilities

- Customer will ensure a service contract is active and valid for all hardware and software components of the ACI Solution for the term of the Service contract. This includes Cisco and all relevant Third Party vendors.
- Customer is responsible for approval of patches and upgrades recommended by Cisco, prior to installing in production.
- Customer is responsible for providing any required Letter of Agency in support of all ACI Solution Third Party components and to ensure Cisco Network Operations Center (NOC) Engineers have appropriate privileges with the Third Party vendor(s).

6 Customer Requested Change Management

Customers purchase a block of hours that can be used for Move, Add, Change, Delete (MACD) categories and Custom Scoped Elective Changes that a customer has under the Service. See the Common Service Description for more details of Custom Scoped Elective Change support. The customer must have a

sufficient balance of support hours on account to cover the requested change. Additional hours maybe purchased if required.

6.1 Defined Changes

Defined Changes are categorized into Small, Medium, and Large activities. A Defined Change is a change requested by the Customer and is not the result of Cisco Incident Management and Problem Management processes. The Customer identifies the needed type of change and submits a Defined Change Request on the Portal. MACD changes are considered Defined Changes.

6.1.1 MACD CHANGES

Medium MACD (Type 4)

- Create Tenants
- Create EPGs
- Configure New Fabric Node
- Configure New APIC

Large MACD (Type 8)

- Create Contract
- Create Service Graph
- Create Application Policy
- Insertion of L4-L7 Services (examples: Cisco NetScaler, Cisco ASA, etc)

6.1.2 Custom-Scoped Elective Change

Custom Scoped Elective Changes are customer requested changes that fall outside Incident and Problem (Standard) changes for restoring service. Custom Scoped Elective changes require a mutually agreed upon statement of work (SOW). See the Common Service Description for more details of Custom Scoped Elective Change support. All changes that are not pre-defined above as MACD Changes are considered Custom-Scoped Changes.