Service Description: Cisco Hosted Identity Services

This document describes the Cisco Hosted Identity Services.

Related Documents: This document should be read in conjunction with the following documents also posted at www.cisco.com/go/servicedescriptions/: (1) Glossary of Terms; (2) List of Services Not Covered; and (3) Severity and Escalation Guidelines. All capitalized terms in this description have the meaning ascribed to them in the Glossary of Terms.

Direct Sale from Cisco. If you have purchased these 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. If not already covered in your MSA or equivalent services agreement, this document should be read in conjunction with the Related Documents identified above. 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 these Services through a Cisco Authorized Reseller, this document is for description purposes only; is not a contract between you and Cisco. The contract, if any, governing the provision of this Service will be the one between you and your Cisco Authorized Reseller. Your Cisco Authorized Reseller should provide this document to you, or you can obtain a copy of this and other Cisco service descriptions at www.cisco.com/go/servicedescriptions/.

Cisco shall provide the Cisco Hosted Identity Services 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 Services ("Quote") setting out the extent of the Services and duration that Cisco shall provide such Services. Cisco shall receive a Purchase Order that references the Quote agreed between the parties and that, additionally, acknowledges and agrees to the terms contained therein.

Service Summary

Cisco Hosted Identity Services ("Service") is a security service designed to provide Cisco Identity Services Engine (ISE) as a hosted, cloud based security service. This Service allows an organization to enable network-based authentication (802.1x, MAC address based and Captive web portal) on their network. This initiative will include 4 phases which shall be completed within six (6) months from the start of the project kick-off meeting:

1) Network Readiness Assessment and Customer Workshop
2) Design & Documentation
3) On-Boarding/Activation
4) Cisco Hosted Identity Services Operations

Each phase has a progressive focus as outlined below:

Network Readiness Assessment: The Service network readiness assessment phase helps the Customer understand any potential infrastructure (hardware or software) gaps that need to be addressed before initiating the onboarding process.

Customer Workshop: The workshop phase helps the Customer understand how the Service would be implemented in their organization; including what changes are required to complete the installation of the Service. In addition, the Cisco consultant(s) will be gathering the necessary details that are required to implement ISE for the organization, which includes a network readiness assessment.

Design & Documentation: The Cisco consultant will produce a Hosted Identity Design Document (HIDD) based on the requirements and design considerations set forth during the on-site workshop. These documents will be used as the basis for the implementation going forward.

On-Boarding/Activation: The On-Boarding phase provides a plan for the implementation of the Service, remediation of Customer network as required, provisioning of equipment for the Service, and implementation of the Service based on the design.

Cisco Hosted Identity Services Operations: For the duration of the term Cisco will operate, monitor, and maintain the Service.

Service Scope:

The Service will include elements that will be defined by the Customer's requirements as identified in the Quote and Purchase Order, those elements include:

- Network Authentication for one or all of the following; Wired, Wireless and/or VPN
- Number of endpoints/users
- Number of Customer data center sites and locations

Location of Services

The deployment of Cisco-provided on-premise hardware and software components providing coverage for the data-centers and all users, as described in the Service Scope above, must be in the same geography (country or region).

Cisco Hosted Identity Services

Project Management:

Project management will be provided for the duration of the Service term, including a project manager (PM) who will have the primary responsibilities to conduct the project kick-off meeting, develop a project plan, schedule resources, and provide change management. The Project Manager will contact the Customer to schedule the kickoff meeting within thirty (30) days from receipt of a valid Purchase Order.

Cisco Responsibilities:

- Identify project team members.
- Define the communication flow with the project sponsor and key stakeholders and document it in the project plan.
- Work with Customer to identify and document dependencies, risks and issues associated with the successful completion of the Term.
- Provide the following: a) kick-off meeting; b) schedule resources; c) project plan; and d) change management.
- Manage the project to the agreed upon project plan.
- Participate in regularly scheduled project review meetings or conference calls if required.
- Act as the focal point for the discussions related to specific areas to address or prioritize on during the Term. Activities and deliverables highlighted in this Service will be reviewed during regularly scheduled review meetings to address Customer priorities..

Customer Responsibilities:

- Identify Customer's project executive sponsor, point of contact, and key stakeholders and define their roles in supporting this project.
- Coordinate with Customer internal departments and bring in as needed key resources to ensure the success of the pilot. Ensure approval is obtained for Service requirements from the key stakeholders.
- Work with the Cisco PM to ensure the Customer's project sponsor, key stakeholders and all project team members receive project communications and are included in regularly scheduled communications sessions.
- Work with Cisco to schedule the kick-off meeting, and communicate the meeting schedule to the Customer-identified stakeholders.
- Review the project schedule, objectives, services, and roles and responsibilities with Cisco.
- Schedule the necessary facilities for on-site meetings (such as: conference rooms, projectors and conference bridges).
- Participate in regularly scheduled project review meetings or conference calls.
- Coordinate any third party activities (such as in country carrier/telco activities).
- Notify Cisco of any scheduling changes related to this Term at least ten (10) business days of the scheduled activity.

Network Readiness Assessment and Customer Workshop:

The workshop is highly interactive and includes the following: interviews, review of network and infrastructure diagrams, review of supporting documentation, business and technical discussions, and white boarding sessions at the Customer's site.

Cisco Responsibilities:

- Conduct a requirements workshop with key Customer personnel to gather and review some or all of the following: a) design goals; b) business, technical and operational requirements; c) system and application interoperability requirements; d) network design/topology documents; e) network information and reports; f) existing and planned security devices, code versions and configuration files of appropriate devices; and/or g) current and planned security policies.
- Cisco and Customer shall mutually agree on requirements and information collected.
- Analyze the potential effects of integrating ISE with the Customer's existing IT infrastructure.
- Assess the readiness of the Customer's limited production network to determine its ability to adopt the ISE system.
- Recommend a software version for use and any hardware upgrades that maybe required.
- Identify the gaps in the Customer's existing and planned infrastructure with the potential to prevent the ISE system from performing optimally and develop recommendations for correcting the gaps.

Customer Responsibilities:

- Customer key personnel participate in the workshop
- Customer will provide IP addresses (public and private) required to successfully design the Service.
- Customer will provide information and review with Cisco during a requirements workshop: a) design goals; b) business, technical and operational requirements; c) system and application interoperability requirements; d) network design/topology documents; e) network information and reports; f) existing and planned security devices, code versions and configuration files of appropriate devices; and/or, g) current and planned security policies.
- Customer and Cisco shall mutually agree on requirements and information collected.

Design and Documentation:

Cisco will analyze and document the implementation requirements for the Service and assess the readiness of

Customer's network architecture, operations, security policies, and devices to support the Service.

Cisco Responsibilities:

- Assess the capabilities of the Customer's network infrastructure to support the Service which may include some or all of the following: architecture, hardware, software, features, configurations, security policies, process, and procedures, industry compliance requirements and/or local laws that may alter the local design specifications, maintenance and/or change control requirements.
- Create the HIDD requirements which may include some or all of the following: a) design goals; b) business, technical and operational requirements; c) identified gaps and assessment findings; and d) recommendations.
- Review the HIDD with the Customer to ensure that all the Customer use cases are being fulfilled by the design based on the features available within the Service.
- Develop HIDD design for the Service based on the inputs from the workshop and HIDD requirements.
- Provide the HIDD to the Customer for review and approval.

Customer Responsibilities:

- Review and approve the HIDD.
- Remediate gaps identified by Cisco in the HIDD prior to Cisco continuing with provision of the remainder of the Services.
- Review and approve the HIDD.

On-Boarding/Activation:

Provisioning and implementation of the Service for activation.

Cisco Responsibilities:

Provisioning:

- Provision all of the necessary services associated with the Service to include components, accounts, and capabilities.

Implementation:

- Create test plan, which includes: test cases and success criteria needed to validate successful test results.
- Review implementation procedures with Customer, which may include: rollback procedures, post-implementation activity exit criteria; implementation schedule that meets the Customer's change and release management processes and Cisco's consultant's availability.
- Execute the implementation activities on the Cisco Hosted CPE device, which may include: a) implementation and configuration as specified in the Design document; b) executing the test cases identified in the Test Plan; c) documenting test results; and d) evaluating the test results against success criteria.
- Assist Customer in deploying the Hosted CPE components.

Customer Responsibilities:

Provisioning:

- Provide any necessary information to assist Cisco in the provisioning of the Service; including but not limited to a) appropriate IP addresses, b) network connectivity to establish required communication channels, c) access to appropriate authentication systems.

Implementation:

- Assist Cisco in the creation of the test plan, which includes: test cases and success criteria needed to validate successful test results.
- Create necessary firewall rules to successfully deploy this Service in their network.
- Provide the rack space required for the Cisco-owned on-premise equipment
- Deploy Cisco-provided, Cisco-owned on-premise hardware and software components.
- Upgrade any infrastructure gap (hardware or software) before the implementation of the solution
- Review implementation procedures with Cisco, which may include: rollback procedures, post-implementation activity exit criteria; implementation schedule that meets the Customer's change and release management processes and Cisco's consultant's availability.
- Implement configuration changes to Customer owned and managed Network Devices as designed by Cisco.
- Assist Cisco in the execution of the implementation activities, which may include: a) implementation and configuration as specified in the Design documents; b) executing the test cases identified in the Test Plan; c) documenting test results; d) evaluating the test results against success criteria; e) installation of endpoint software; and f) data required for endpoint profiling

Cisco Hosted Identity Services Operations:

For the duration of the Service term, Cisco will operate, monitor, and maintain the Service.

Cisco Responsibilities:

- Monitor and report on any abnormal events or outages related to the Service that may adversely affect the availability or performance of the Service.
- Modify Cisco Hosted configurations or policies if required to ensure the Service works properly.
- Work with Customer to troubleshoot any issues that arise as a result of the Service.

Customer Responsibilities:

- Assist Cisco in the identification, troubleshooting, and remediation of any events that may affect the availability or performance of the CPE part of the Service.
- In the event of Hosted CPE equipment issues or failures that may require service or replacement, Customer will provide the resources and access necessary to Cisco in order to inspect, service, and/or replace the Hosted CPE equipment.
- Provide escalation matrix and points of contact.
- Customer will be the front line of support for its end users.

Customer Portal Reports:

The following reports may be made available through the Customer portal:

Identity Services Engine (ISE) Advanced Reporting	
Total Authentication Last 24 Hours	Presents the total amount of authentications over a 24 hour period
Current Active Endpoints	Provides the total current active endpoints in the ISE environment
Authorizations by Policy	A ranking of the top used authorizations by policy
Currently Authorized Users	A list of the current users authenticated to the network
Total ISE Failed Authentications	A list of the total failed authentications
Total Failed Authentications Last 24 Hours	A list of the total failed authentications
Total Failed Authentications By User	A ranking of the total failed authentications by individual user
Passed Authentications Last 24 Hours	A list of the total success authentications over the previous 24 hours

Assumptions and Exclusions:

- There are no Service Level Agreements (SLAs) associated with the Service or associated Services throughout the Term.
- Customer is responsible for determination and implementation of recommendations provided by Cisco to include the associated recommendations and requirements for on-boarding the Service and the recommendations associated with remediating any identified security incidents or events. In no event shall Cisco be liable for the accuracy or completeness of the information contained in the Cisco recommendations.
- Services include no more than three (3) onsite visits to one location over the course of the delivery of the Services.
- The service does not include the features and functionality that are not available in Cisco ISE.
- The service does not include monitoring of Customer infrastructure and their compliance to configuration standards.
- The service only integrates with one of the ISE supported identity stores.
- The service includes limited portal customization through what is available in ISE
- Implementation of ISE Policies is limited to policies agreed in the design (HIDD).
- Customer is responsible for providing the PKI (Public Key Infrastructure) to meet design requirements
- For certificate based authentication, the Customer is responsible for deploying the certificates to their devices
- Customer is responsible for any infrastructure upgrades (hardware or software) based on recommendations by Cisco before the implementation of the solution
- Customer is responsible for implementing configuration changes to Network Devices (routers, switches, wireless controllers, firewalls, load-balancer for example) for successful deployment of the solution.
- All Cisco-provided CPE equipment is owned by Cisco.

APPENDIX:

Glossary of Terms

Glossary of Terms should be read in conjunction with this Service Description. Capitalized terms not otherwise defined above have the meanings assigned to them in the Glossary of Terms.

ASA: Advanced Services Agreement

CPE: Customer Premise Equipment

Customer: The entity purchasing for its own internal use

Customer Premise: The physical Customer location

HID: Hosted Identity Service

HIDD: Hosted Identity Design Document

Hosted CPE: Cisco Owned Customer Premise Equipment

ISE: Cisco Identity Services Engine

MDM: Mobile Device Management

MHSA: Master Hosted Services Agreement

MSA: Master Services Agreement.

NCE: Network Consulting Engineer

SLA: Service Level Agreement

Service: Cisco Hosted Identity Services

Term: Duration of Service purchased by Customer