Telcion Communications Group
117 S. Broadway | Turlock, CA 95380
209.632.5700 | www.telcion.com

Statement of Work

Network Infrastructure Refresh
Prepared for: City of Visalia

Authored by: Lance Reid

February 17, 2023

Client Contact Information

Client Name	City of Visalia
Project Name	City of Visalia Network Infrastructure Refresh Project
Client Contact	John Howison
Client Contact Email	

PROJECT DESCRIPTION

City of Visalia is doing a complete refresh of their entire network and computing infrastructure. This covers two separate systems, City Hall and Police, each operating independently within the same data center and connected through a firewall.

The outcomes of the refresh are as follows:

- 2 core switches in the data center for both City Hall and PD will have been upgraded to new Cisco 9606 chassis switches with redundant supervisors, power supplies, and blades to allow for redundant paths from the server farm, storage system, and remote locations if available.
- 9 distribution switches within the city network will have been upgraded to Cisco 9300 models, which then will connect to additional outlying switches.
- 75 access layer switches within the city network will have been upgraded to Cisco 9200 models, connecting to local users at various sites.
- 10 servers will be replaced with Cisco M7 models and distributed among the City and PD server farm.
- New cloud management tool for servers, Cisco Intersight, has been implemented to manage the entire server farm.
- New network management tool, Cisco DNA, has been implemented to manage the entire network infrastructure.
- New security tool, the Cisco Identity Services Engine, has been implemented and is providing additional security by way of authenticating and verifying each user or device before they are allowed onto the network.
- 3 Cisco Voice Gateways have been replaced with newer models.
- 10 analog voice gateways have been decommissioned.
- 6 weeks of Cisco IT training has been made available for the City staff.

Project Management

Telcion will assign a project manager for the duration of the project to work closely with an assigned Client representative to ensure proper project coordination and planning. These activities will include:

- Project kickoff meeting to define project resources and timeline
- Documentation of scheduled project activities
- Weekly Project Status meetings and documented updates as needed
- Coordination of Telcion and The City schedules to ensure successful implementation
- Project closure documentation to formalize the end of the project

Key Assumptions

The key assumptions for this project are:

- All work will be performed during normal business hours, Monday through Friday, 8:00 a.m. to 5:00 p.m., except holidays unless otherwise agreed to in advance for maintenance windows.
- All tasks will be performed over a consecutive timeframe unless otherwise agreed to by all parties.

Out of Scope Services

Telcion is responsible to perform only the Services described in this Statement of Work Agreement. Any additional services discussed or implied that are not defined explicitly by this SOW will be considered out of Scope. All services requested outside of this SOW as detailed above will require a "Change Order" before any services are performed. "Change Order" must be agreed upon by all parties and signed.

The City has approved a large block hour agreement to cover the hours needed to perform the services in this document. At the end of this document, each major sub-scope has been allocated a portion of these hours to accomplish the work described. It is very easy for scope creep to occur in this situation, to the extent that some sub-scopes get starved for time in lieu of other priorities. In order to help the City stay on track to accomplish the goals within this document, change orders will be issued to track changes from the original intentions of the scope and will have a potential impact on the hours required to accomplish the services described. Change this to reflect to milestones . . .

Examples:

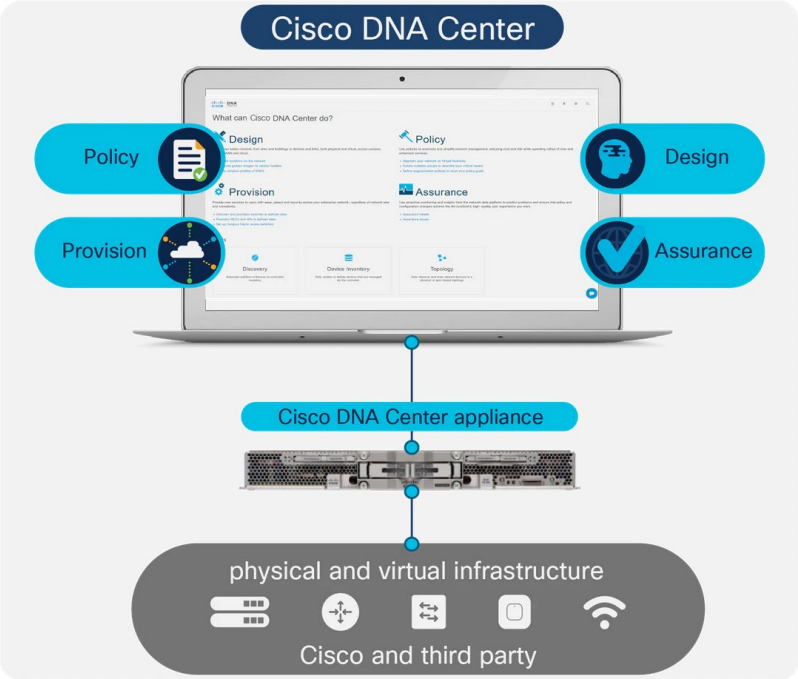
- The compute stack has been implemented, and the City has requested additional services to migrate virtual machines. A change order will be issued to indicate the amount of additional time required over and above the original intention of the scope, and the impact this may have on the overall project.
- The access switch project is underway and the City requests additional help to roll-out sites beyond what was in the scope. A change order will be issued to indicate the amount of additional time required over and above the original intention of the scope, and the impact this may have on the overall project.

In all cases, it is Telcion's desire to help the City accomplish it's goals and achieve the outcomes of the scope of work described in this document, and to keep the available hours designated to each sub-scope.

DETAILED SCOPE OF SERVICES

Cisco DNA Center

Cisco DNA Center is a complete management and control platform for your network, designed, created, and implemented by Cisco. This single, extensible software platform includes integrated tools for network management, automation, virtualization, analytics and assurance, security, and Internet of Things (IoT) connectivity and can also interface with your business-critical tools. Using the Cisco DNA network controller and APIs, Cisco DNA Center provides an open and extensible platform. With Cisco DNA Center, the days of time-consuming network provisioning and tedious troubleshooting tasks are over. Cisco DNA Assurance enables every point on the network to become a sensor, sending continuous, streaming telemetry on application performance and user connectivity in real-time. This capability, coupled with automatic path trace visibility and guided remediation, means network issues are resolved in minutes—before they become problems. Integration with Cisco security solutions such as Stealthwatch® and Cisco Umbrella™ provides DNS protection, detection, and mitigation of threats, even when they are hidden in encrypted traffic. Cisco DNA Center also provides an open, extensible platform with broad support for external applications and systems to exchange data and intelligence, building upon its native functions. And it is the only centralized network controller to bring all of this functionality into a single pane of glass.



The Cisco DNA Center appliance will be deployed as the network controller at the The City offices to provide centralized enterprise network management. It will be upgraded to the latest release of DNA Center to provide the most up-to-date feature set from Cisco, in preparation for the addition of 9800 wireless controllers or other future components. DNA network deployment features such as golden image and configuration templates will be added to support future switch rollouts. DNA Assurance will be configured on the appliance and on the supported network devices to provide telemetry analysis and visibility on traffic flowing on the The City network. The selected Cisco access switches will be configured to send telemetry to the DNA Center appliance to leverage DNA Center's machine learning and root cause analysis toolset. A single DNA Center appliance will be connected to the The City network at 10Gbps.

Planning Phase

1. Cisco supplies the Cisco Digital Network Architecture (DNA) Center in a rack-mountable, physical appliance. The second-generation Cisco DNA Center appliance consists of a Cisco Unified Computing System (UCS) C220 small form-factor (SFF) chassis.
   - Review the recommended cabling and switching requirements for standalone and cluster installations. Validate the customer has rack space and power for the DNA Center appliance. Identify the 10Gbps switch connections available to attach the Cisco DNA Center network interfaces.
   - Gather the IP addressing, IP subnetting, and other IP traffic telemetry details required to complete the initial installation of the DNA Center appliance. Define the cluster virtual IP address. Identify the management network or VLAN used to access the new DNA Center appliance and confirm how to provide the DNA Center appliance with secure internet access.
   - Identify the end-users that will receive training on how to access and operate the Cisco DNA Center main features. End-user training is not a substitute for Cisco Learning but will provide details on how to start accessing the network controller.

Execution Phase

1. Rack and Network Connections
   - Rack and power the DNA Center appliance in the client data center. Connect the enterprise network interface, cluster network interface, management network interface (if required), the cloud network interface (if required), and the CIMC network interface.
2. Prepare Catalyst Switches for DNA

- Review the Catalyst switches to be managed by Cisco DNA Center. Update the software versions running on the switches and attach the switches to the The City Smart Account for DNA Advantage license consumption.

3. Prepare Appliance for Installation
   - Configure the CIMC settings to enable NTP and switch access port VLAN settings. Switch port trunk mode is not supported. Disable the Intel X710-DA4 card.
4. Initial DNA Center Configuration
   - Using the information gathered from the planning phase, run the Maglev Configuration tool from Cisco IMC and configure the primary node in the DNA Center cluster.
5. Upgrade All Modules
   - Confirm that the DNA Center can successfully access the internet. Upgrade all the Cisco DNA Center modules to the latest recommended versions. Resolve any routing or firewall issues that prevent Cisco DNA Center from accessing the internet so the upgrades are successful.
6. DNA Network Discovery Profiles
   - Configure the site and area topology for the selected locations. Add credentials for device discovery. Upload and define golden images for network devices such as routers and switches. Configure onboarding templates and network profiles before building the network information database of the network endpoints (routers, switches, firewalls). Onboard the network devices into Cisco DNA Center.
7. DNA Assurance Telemetry Profiles
   - Using the discovered devices, configure maximal telemetry profiles to enable syslog, netflow, and PoE collection from the The City network devices.
8. DNA Assurance Roll Out
   - Confirm that selected devices have been discovered and claimed in Cisco DNA Center. Confirm that the streaming telemetry configuration has been enabled in the Catalyst switching and that data is now being collected by Cisco DNA Center. Enable Netconf to capture PoE usage data on the switches.
9. Network Infrastructure Upgrades for Image Management
   - Review the latest Cisco guidelines to confirm the IOS XE releases compatible with the Cisco DNA Center running version and upgrade the golden image to obtain the latest features and bug fixes across the enterprise for routers, switches, and access points.
10. Cisco ISE Integration
    - Configure Cisco ISE integration with Cisco DNA Center via pxGrid. Validate that all endpoint information is flowing between the Cisco ISE nodes and Cisco DNA Center.

11. DNA Center Feature Validation
    - To validate the Cisco DNA Center operation, view application traffic to confirm network performance. View the "Application 360", "Device 360", and "Application Health" dashboards to validate legitimate data is being gathered from the network.
12. Admin Training
    - Provide admin training on how to access Cisco DNA Center, view the "360" dashboards, view network inventory, and perform network troubleshooting. This training is not a substitute for official Cisco Learning as Cisco DNA Center is a very broad topic.

Telcion Responsibilities

- Telcion will provide the engineering resources to install the new DNA Center appliance in the The City network, connecting it at 10Gbps in the network core. Telcion will upgrade the DNA Center appliance to the latest version for the newest feature set from Cisco. Telcion will upgrade the attached Cisco switching infrastructure to the recommended IOS-XE versions that work with DNA Center for features such as automated network deployment and DNA Assurance. Telcion will add the selected City network devices into DNA Center for management. Telcion will upload the recommended Cisco images into DNA Center and switch configuration templates for future deployments. Telcion will push out DNA Assurance configuration to the selected access switches to provide optimal visibility into the operations. Cisco ISE will be tied into Cisco DNA Center via pxGrid.

Client Responsibilities

- The City will need to provide access to the network core to install the DNA Center appliance via 10Gbps. The City will need to provide the rack space and power for the DNA Center appliance. The City will need to provide credentials for configuration changes to the selected access switches for DNA Center management and image upgrades. The City will need to provide maintenance windows for all the required software updates to the network infrastructure.

Out of Scope Services

Telcion is responsible to perform only the Services described in this Statement of Work Agreement. Any additional services discussed or implied that are not defined explicitly by this SOW will be considered out of Scope. All services requested outside of this SOW as detailed above will require a "Change Order" before any services are performed. "Change Order" must be agreed upon by all parties and signed.

Examples:

- Software-defined network access requires Cisco ISE with TrustSec and is not included. DNA Center feature sets on older non-IOS XE devices will be limited.

Caveats

The intention is to use a single DNAC deployment to manage devices in both City and PD entities. This requires traversing a firewall which will require configuration changes that may or may not be acceptable. A successful deployment on the PD side will be dependent on the level of connectivity that is allowed to exist through the firewall. The priority on the deployment will be on the City side, with remaining hours available going towards PD functionality across the firewall. There are no hours allocated for troubleshooting the firewall configuration, and Telcion will rely on City IT staff to configure the firewall per DNAC deployment guidelines.

Core Switch Upgrade

The City and the PD each have a pair of existing Cisco Catalyst 6800 chassis switches. Each of these switch pairs will be replaced with a single Cisco Catalyst 9606 chassis switch with redundant supervisors, power supplies, and blades, with the goal of providing redundant paths wherever available.

- All ports will be operating at 25G wherever available.
- Some fiber optic modules are being purchased as new, and some optics will be reused from the existing deployment.
- The core chassis configurations will be transitioned from the old to the new. It is anticipated the core configuration will remain largely the same, with all layer 3 routing happening within the core, and multiple VLANs operating at the access edge. This is in large part due to the way traffic moves within the City and mostly terminates in the data center or out to the Internet. There is minimal traffic within each site.
- The core switch environment includes advanced DNA licensing and 24x7x4hour Smartnet replacement coverage.
- When all connections to the old core have been transitioned, the old core will be decommissioned and removed from the rack.

Caveats that need to be considered prior to deployment:

- Power will likely need to be upgraded to support the multiple 220v connections from the new core.
- The new core and the old core may need to be interconnected for a time. This is to provide a smoother transition for devices and remote locations as they are swung over to the new core.
- Spare 10G fiber optic modules are available from the City, but there are limited 25G optics being purchased. The City may purchase 3rd party optics on their own to aid in this transition, however, careful planning prior to make sure the right connections get the right optics on the first try.

Responsibilities

- Telcion will install and configure this appliance, and bring it into production use.
- The City will purchase additional 3rd party optics at their discretion.

Distribution and Access Switches

There are two types of switches being deployed: Cisco Catalyst 9300 and 9200 series switches. The distribution layer will be handled by the Cisco 9300 at strategic aggregation points within the city that already exist and is limited to about 6 switches.

- The aggregation points today include switches such as a 3750-12 fiber switch which act as an MDF core switch for a given location in terms of fiber aggregation. All aggregation sites have less than 8 ports of fiber terminating into the switch. In the new design, we are eliminating a single fiber switch and combining that with a 9300 model that includes an 8-port fiber uplink module. The uplink module will facilitate the fiber aggregation, and the copper ports on the 9300 will facilitate the access devices within the MDF. The purpose here is to reduce the total number of switches required in each of these MDF aggregation points.
- All other IDF locations will have new C9200 swithes installed to replace the existing models. In some cases, the port count has been increased or decreased to accommodate the current situation. Reference the design worksheet to see the allocation made. The City has confirmed the number of devices and ports being put into production.
- There are 2 C9200 spares and 3 C9300 spares that have been purchased to accommodate hardware failures that may arise.
- Smartnet has not been purchased on these access switches. The intention is to leverage the limited life time warranty of the switches as a mechanism for replacement. All software updates and TAC assistance are covered under the DNA license.
- Deployment of these switches must include DNAC so that they are properly deployed at the start of the implementation for use with DNAC services.

Responsibilities

The City will be responsible for a large majority of the access switch implementations, with assistance from Telcion as needed for configuration help.

Generally speaking, Telcion will configure up to 5 sites with varying configurations to illustrate how the migration takes place and how to use DNAC to facilitate the implementation. The City will then deploy the remaining units on their own schedule. Telcion can be used for more of the deployment if needed, however the time allocation to the entire project needs to be mostly focused on other areas.

Caveats

Confirm what fiber optic modules will be needed with which sites.

Where possible, use switch stack configurations.

The DR Site will have a couple 9300 switches to facilitate redundant paths for compute and storage for both the City and PD. There is also an existing C6500 at this site acting as a layer 2 aggregation switch and will be replaced with a stack of C9200.

One site has a large number of camera’s using POE power and will require an additional power supply (in the BOM).

Compute and Storage

The existing compute stack consists of servers dedicated to the City, PD, and DMZ and are part of separate VMware environments. The City has chosen to purchase the Cisco C240 M7 model servers to replace the existing compute stacks. The intention is to combine the DMZ into the City cluster of hosts for a total of 6 servers. The remaining 4 servers will be used for the PD cluster. One server from each cluster may be located at the DR site, but the final intentions here are yet to be determined.

- At the primary site, the servers will be connected at 25G to the appropriate 9606 Core Switch.
- Each server has two Quad 25G NICs to provide independent and redundant physical paths for production traffic, iSCSI, and replicaton. On board 10G ports will be used for management connectivity. Twinax cables have been supplied as part of the BOM to enable the various connections.
- Each of these servers has been licensed for Intersight with Advanced licensing.
- Telcion will jointly work with IT to rack, connect, and prepare the hardware for VMware and iSCSI storage access.
- Telcion will jointly work with IT to deploy VMware images and add the new hosts to the cluster.
- Telcion will jointly work with IT to move some virtual machines to the new hosts, as desired.
- Telcion will jointly work with IT to decommission the old servers.

Client Responsibilities

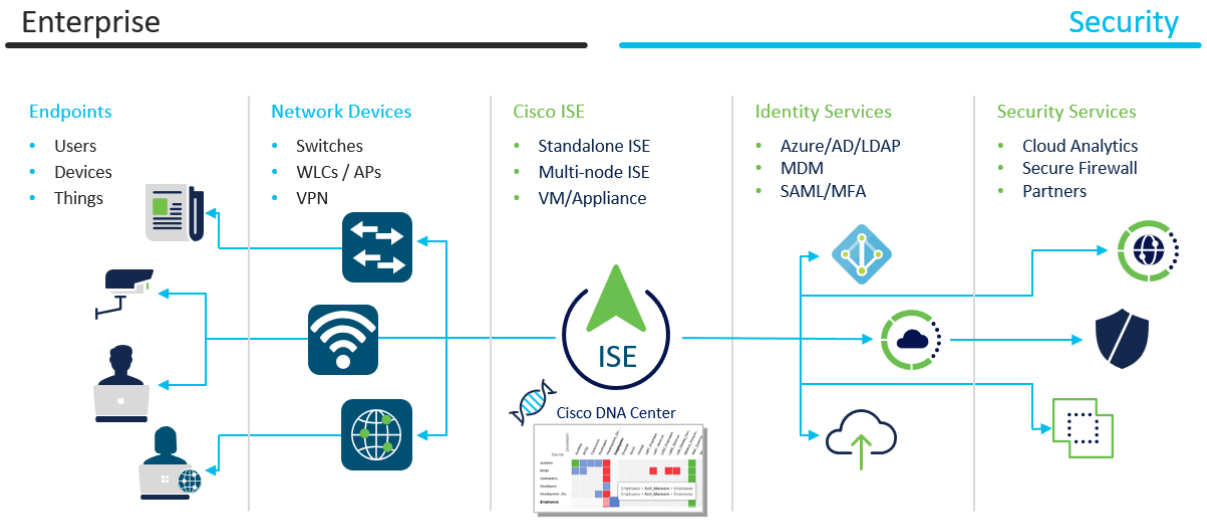
- Provide physical access to the primary data centers for the duration of the project.
- Provide remote access to primary data centers for the duration of the project.
- Provide extended hours access to the data centers, physical or remote.

Caveats:

- Rack space during the migration, before the old hosts have been decommissioned.
- Appropriate power.
- Need to verify which servers are going to the DR site, and how those are intended to be connected, given the dedicated paths that are being used for replication and other services.

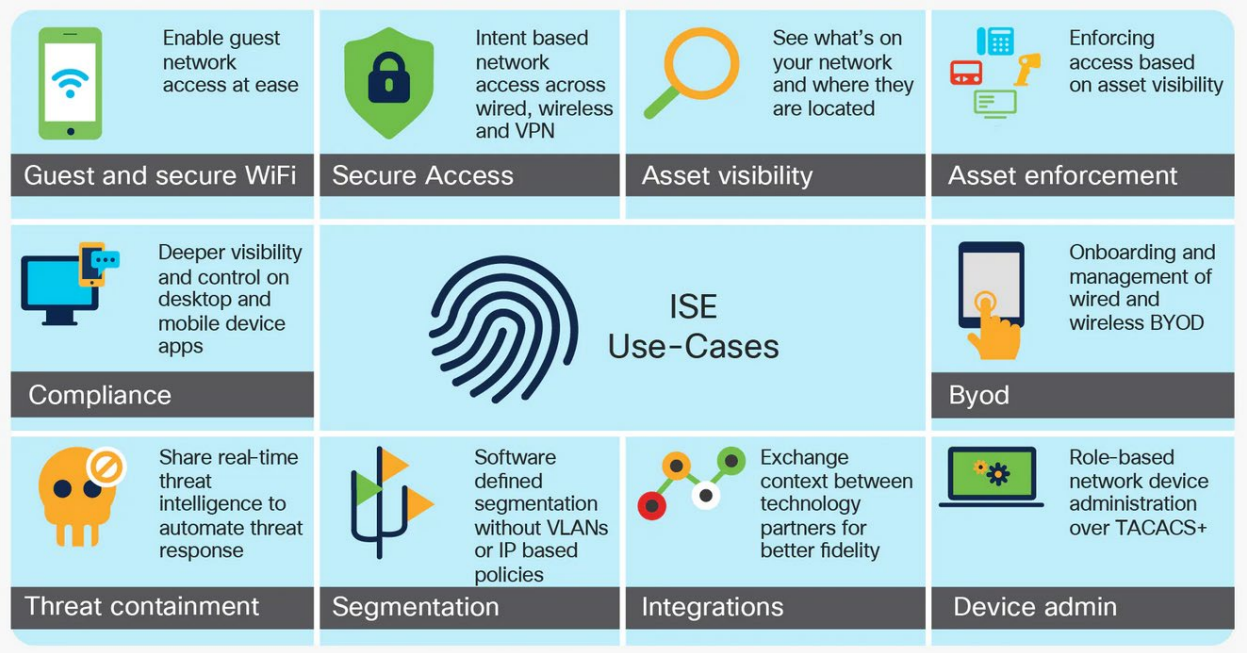
Cisco Identity Services Engine

Cisco Identity Services Engine (ISE) is a robust security product that can perform many roles in an enterprise environment. Cisco ISE has capabilities far beyond this scope of work, such as BYOD, device profiling, device posture compliance, and threat-centric network access control. These advanced features would be available after this initial project with additional configuration and licensing. The City of Visalia network infrastructure consists of Cisco switches of various models. The City would like to use the Cisco Identity Services Engine (ISE) and its RADIUS features as the central authentication source for its wired devices with 802.1x, eventually moving to utilize its more advanced policy, access control, and segmentation features in the future. This project will deploy a pair of redundant Cisco ISE virtual machines in the City data center and roll out authentication services to the wired networks to all locations.

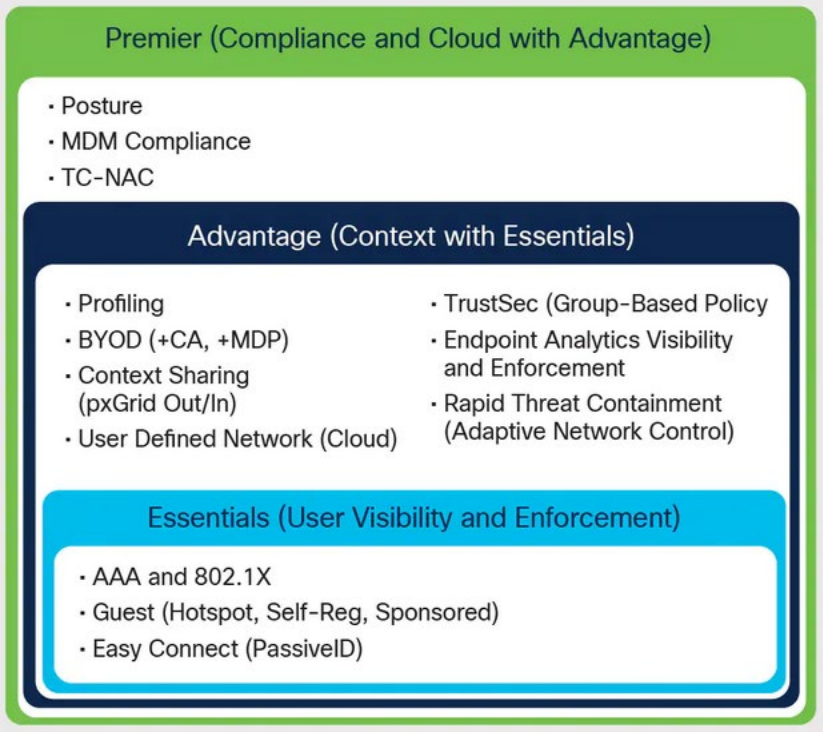


Cisco ISE has many use cases in the enterprise. The City will benefit from deploying Cisco ISE for guest and secure WiFi, secure wired access, asset visibility, integrations with existing mobile device management platforms such as Microsoft Intune and JAMF, device administration of network devices, and much more.

Here are some of the overall use cases that make Cisco ISE so beneficial for the enterprise:

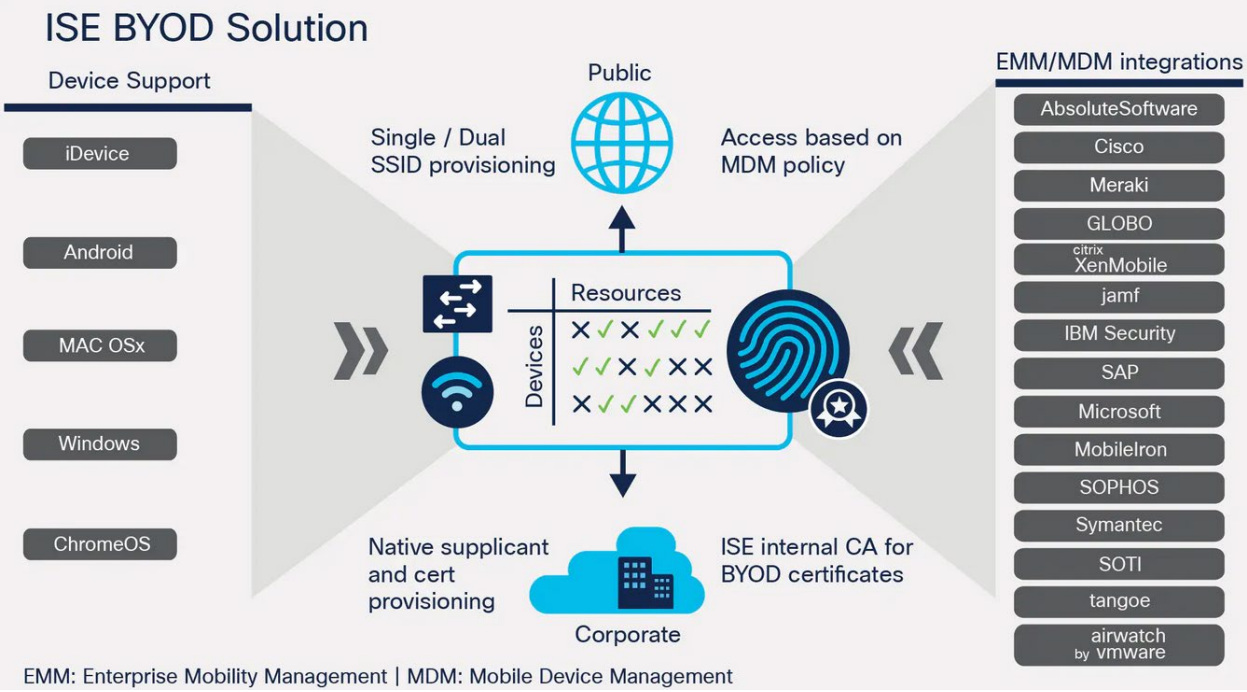


Cisco ISE licensing is divided into three primary nested subscription tiers. With this flexible model, you can select the number and combination of licenses to get the features that best fit the City. The Bill of Materials that accompanies this scope includes 1000 Advantage and 1000 premium licenses.



A license is required for each endpoint on the network. For 802.1x wired and wireless authentication, only "essentials" licensing is required. To provide enhanced information about each network endpoint and enable "bring your own device (BYOD)" capabilities, an "Advantage" license for the endpoint is required. "Advantage" licensing is also necessary for DNA Center or MDM integration. A "Premier" license is required to enable endpoint compliance and remediation. For TACACS+ device authentication on network devices, the additional "device administration" license is required. Because the City uses mobile device management solutions such as Microsoft Intune, Telcion recommends a mixture of "Advantage" and Premier licensing for all the endpoints. This will allow for the integration of the existing solutions and the eventual integration of Cisco DNA Center.

Below is a diagram of how ISE can integrate with supported EMM/MDM solutions:



Planning Phase

1. Complete an ISE High-Level Design Document to identify the security policy and business objectives. The high-level design document will clearly state the desired solution capabilities, hardware, and software environment, any integrations and will quickly allow people to understand and configure ISE.

2. ISE Node design and deployment to include virtual machine sizing, licensing, Cisco Smart license provisioning, and following all Cisco pre-deployment checklists.

3. Confirm ISE 3.x virtual machine requirements for the deployment of the redundant virtual machine (small):

OVA Template Type	Number of CPUs	CPU Reservation (In MHz)	Memory (In GB)	Memory Reservation (In GB)
Evaluation	4	No reservation.	16	No reservation.
Small	16	16,000	32	32
Medium	24	24,000	96	96
Large	24	24,000	256	256

Execution Phase

- ***ISE - Base Installation***

  Subtasks include:

  a. Install ISE as redundant Virtual Machines
     - Install the Cisco ISE software package as primary and secondary virtual machines on a client-provided hypervisor (Hyper-V or VMware). Telcion is adding a second ISE node to the existing ISE installation at The City.

  b. Install ISE licensing
     - Provision a Cisco Smart Account for the Cisco ISE entitlements. Telcion will use the Cisco Smart Account to retrieve the new smart entitlements.

  c. Test failover between ISE Virtual Machines
     - Verify replication and failover functionality of the ISE virtual machines.

  d. LDAP Integration for Identity Store
     - Integrate ISE with the directory of choice for user authentication and identification. Configure ISE to accept RADIUS authentication requests. City has multiple identity stores and will need local Active Directory and Microsoft Azure Active Directory configured as identity stores.

- ***ISE - Secured Wired Access Implementation***

Subtasks include:

e. Verify Cisco switch software loads at the City
   - Confirm each switch model and software load is compatible with deployed ISE version.

f. Update Cisco software loads
   - Perform Cisco switch IOS updates to get the highest firmware possible.

g. Build switch devices in ISE
   - Configure each switch device in ISE. Configure switches for communication with the closest Cisco ISE virtual machine. Update switch configurations.

h. Configure 802.1x authentication
   - Configure 802.1x authentication for wired devices on all ports. Initial Cisco ISE deployment will be in "monitor mode" to verify operational status before forcing new security standards across all users. This mode will also allow for visibility into devices that may need extra configuration or updates to support the use of 802.1x authentication.

i. Create ISE user authentication policies
   - Create ISE user authentication policies based on the ISE high-level design document that was created during the planning process.

j. Create MAC bypass authentication policies
   - For devices that are not associated with specific users, configure Cisco ISE with a list of MAC addresses that are allowed to access the network for authentication purposes (MAC authentication bypass). Telcion will assist in gathering device MAC addresses in each site via ARP to generate a master list of all devices accessing the network for designated locations. Device authentication by MAC address will only be used for devices that do not support 802.1x and yet still have valid operational network requirements.

k. ISE Operations in "monitor" mode
   - Operate Cisco ISE in "monitor" mode and validate how ISE sees each device connected to the switches to validate the configuration.

- ***ISE – Device Authentication***

  Subtasks include:

  l. Configure TACACS on Cisco Network Devices across all sites
     - Configure each Cisco network device to authenticate with ISE for device authentication for all Citysites.

  m. Configure ISE to accept incoming TACACS Authentication Requests
     - Configure ISE to accept incoming authentication requests for device authentication. Confirm LDAP or identity configuration for the base ISE implementation to validate TACACS operations.

- ***ISE –Integrations***

  Subtasks include:

  n. Configure Integration with Microsoft Intune
     - Configure pxGrid integration with Microsoft Intune to pass endpoint data to the Microsoft service.

  o. Configure Integration with DNA Center
     - Configure pxGrid integration with Cisco DNA Center to pass endpoint telemetry to the Cisco management solution.

- ***ISE – Production Cutover in "Low Impact" or "Closed" Mode***

  Subtasks include:

  p. Cutover ISE into production on the "low impact" or most secure "closed" mode
     - Cutover Cisco ISE into production with the new 802.1x settings on the wired network by moving from "monitor mode." Choice of cutover mode will be based on operations impact and security goals of the City.

  q. Day One support
     - Provide day one support for wired ISE operations in production.

  r. Documentation and Training
     - Provide training on the operation and administration of the Cisco ISE system to City technical staff. Provide documentation on the overall configuration of the Cisco ISE system.

Outcomes and Deliverables

Telcion has completed its responsibilities to this Statement of Work when the deliverables below have been completed. These will be included in the Project Completion Certificate for the final project sign-off.

1. The base installation of the redundant Cisco ISE virtual machines has been tested and is ready for production with endpoints reporting to the policy nodes. The identity stores configured are for local Active Directory.

2. Cisco ISE has been configured for user authentication and authorization. It was initially installed in "monitor" mode to validate the endpoints on the network and policy configurations.

3. Cisco ISE has been configured for protecting the wired network at City locations and was moved into final production enforcing 802.1x authentication.

4. Cisco ISE has been integrated with Microsoft Intune to provide endpoint data.

5. Documentation will be provided to City on the overall operation and configuration of the Cisco ISE network access control system.

Telcion Responsibilities

- Telcion will provide the engineering and project management resources to install the Cisco ISE software package as redundant virtual machines, one running "active" and the second as "passive."
- Telcion will integrate Cisco ISE with the local City Active Directory for user authentication and identification.
- Telcion will configure all existing Cisco switches at the City locations to work with Cisco ISE using 802.1x authentication on all ports.
- The Cisco ISE deployment will initially be in "monitor mode" to verify operational status before forcing new security standards across the various IDF's within the City.
- For devices that are not associated with specific users, Telcion will configure Cisco ISE with a list of MAC addresses that are allowed to access the network for authentication purposes (MAC authentication bypass).
- Telcion will assist in gathering device MAC addresses in each site via ARP to generate a master list of all devices accessing the network within the City. Device authentication by MAC address will only be used for devices that do not support 802.1x and yet still have valid operational network access.
- Telcion will configure the Cisco switches to allow for continued network operation in the chances that the ISE virtual machines are not reachable in the various data centers.

- TACACS will be configured on the Cisco switches, routers, and other supported Cisco devices throughout the City network.
- Telcion will integrate the Cisco ISE system with the City's Intune solution so the endpoint telemetry can flow between the solutions.
- Telcion will integrate Cisco ISE with Cisco DNA.
- Once devices are all classified, the Cisco ISE system will be put into "closed" mode for enhanced network security on the wired networks.

Client Responsibilities

- The City will need to provide the compute and storage resources to run the new Cisco ISE virtual machines in the data centers that meet the Cisco requirements.
- The City will need to work with Telcion to schedule maintenance windows to test switch features and endpoint access.
- The City will need to provide credentials to the wired network devices that will integrate with Cisco ISE. Credentials will also be required to integrate with the local Microsoft Active Directory to provide end-user identities.
- The City data centers will always need to be reachable and provide response times under 300ms round trip for the ISE system to remain operational.
- The City will need to provide access information and credentials for the MDM solutions to be integrated with Cisco ISE.

Out of Scope Services

Telcion is responsible to perform only the Services described in this Statement of Work Agreement. Any additional services discussed or implied that are not defined explicitly by this SOW will be considered out of Scope. All services requested outside of this SOW as detailed above will require a "Change Order" before any services are performed. "Change Order" must be agreed upon by all parties and signed.

Examples:

- This scope is for secured wired access, device administration (TACACS), and features of the BYOD solution for MDM integration. Asset Visibility, Segmentation (TrustSec), Endpoint Compliance, and Threat Containment are not included but available with additional licensing and labor.
- Telcion will create ISE policies for Intune, but Intune configuration is not included in this scope.
- Wireless configuration or integration is not included.
- Use of certificates on wired/wireless is not included.

Caveats & Assumptions

The intention is to use a single ISE deployment to manage users in both City and PD entities. This requires traversing a firewall which will require configuration changes that may or may not be acceptable. A successful deployment on the PD side will be dependent on the level of connectivity that is allowed to exist through the firewall. The priority on the deployment will be on the City side, with remaining hours available going towards PD functionality across the firewall. There are no hours allocated for troubleshooting the firewall configuration, and Telcion will rely on City IT staff to configure the firewall per ISE deployment guidelines.

Assumptions:
PKI infrastructure is in place, or will be the responsibility of the IT staff to configure.
Intending to use Peap/mschap for AD authentication challenge on wired devices.
The City is using Intune as their MDM solution.

SERVICES PRICING

This engagement is tied to a block of hours being purchased for the overall network refresh project.

- *Total number of available block hours:* ***667 hours***

The estimated hours assigned to each component of the project:

- *DNA Center Project: 100 hours*
- *Core Switch Project: 80 hours*
- *Access Switch Project: 80 hours*
- *Compute Infrastructure: 100 hours*
- *ISE project: 200 hours*
- *Reserved for Project change orders: 107 hours*

IN WITNESS HEREOF, the parties hereto have caused this Statement of Work Agreement to be executed by their duly authorized representatives on the dates set forth below.

Accepted: **Accepted:**

By: City of Visalia	**By: TELCION COMMUNICATIONS GROUP**
Name:	**Name:**
Title:	**Title:**
Date:	**Date:**