Solution Overview

Cisco Public Facilities Management: Lower Costs and Carbon Footprint While Increasing Service Levels
Cities striving toward economic, social, and environmental sustainability are finding practical solutions through the Cisco® Smart+Connected Communities initiative. This document, intended for IT, facilities, and physical security managers in public administrations, explains one aspect of Smart+Connected Communities: Cisco Public Facilities Management.

Several aspects are addressed, including:

• Consolidating all building networks on a unified IP network reduces capital and operational expenses.
• A unified network also helps cities lower their carbon footprint by automatically turning off building systems, PCs, IP phones, and wireless access points when not needed, based on policy.
• Business processes become more efficient when you can integrate enterprise applications, such as calendaring, with facility services, such as room reservation.
• Centralized physical access control and networked video surveillance can improve building security.
• Communications with building occupants becomes simpler and more effective when you use network-attached digital signage for wayfinding, emergency notification, and conference room reservation.

Cities can accomplish these goals and more when the IT, facilities, and physical security teams come together with a shared vision. The IT department builds on its existing portfolio of voice, video, and data services to offer other facilities services, starting with physical security and energy management.
Opportunity: Increase Building Efficiency and Physical Security

Municipalities need to manage hundreds of buildings distributed over multiple sites. Historically, there has been little or no collaboration among IT, facilities, and physical security departments. This led to a piecemeal approach to technology investments, with different technology and tenant services in different buildings.

As a result, many public administrations currently struggle with fragmented facility systems, including video surveillance, physical access control, building management systems, and enterprise applications such as calendaring.

Today, forward-looking public administrations are adopting a new approach. When government IT, facilities, and physical security teams collaborate, they can each deliver better services, at a lower cost, than if they continued to operate in silos (Table 1). Employees become more efficient in a variety of ways:

- Security personnel can monitor and control video surveillance cameras and physical access controls using any device, from anywhere
- Facilities engineers can monitor and control building systems such as lighting and heating, ventilation, and air conditioning (HVAC), through a unified interface.
- Automatic enforcement of energy policies helps cities work toward environmental sustainability while reducing energy costs.

<table>
<thead>
<tr>
<th></th>
<th>Traditional</th>
<th>Traditional</th>
</tr>
</thead>
<tbody>
<tr>
<td>Systems</td>
<td>Closed and proprietary</td>
<td>Open and standards-based</td>
</tr>
<tr>
<td>Teams</td>
<td>Siloed</td>
<td>Collaborative and converged</td>
</tr>
<tr>
<td>Processes</td>
<td>Disconnected and manual</td>
<td>Integrated and automated</td>
</tr>
<tr>
<td>Infrastructure</td>
<td>Separate</td>
<td>Converged on IP network</td>
</tr>
<tr>
<td>Technology</td>
<td>Analog and hardwired</td>
<td>Digital and virtualized</td>
</tr>
<tr>
<td>Deployment</td>
<td>Local</td>
<td>Regional or national</td>
</tr>
</tbody>
</table>
Solution Overview

The Cisco Public Facilities Management solution addresses three high priorities for public administrations:

- **Energy management**
  - IT endpoints, such as PCs, phones, and wireless access points
  - Data center power efficiency
  - Building management systems from Cisco partners, including lighting and HVAC

- **Physical safety and security**
  - Video surveillance
  - Physical access control
  - Communications systems, such as digital signage

- **Unified IP network infrastructure**
  - Adequate bandwidth for all building systems
  - Mobility services
  - Security
  - High availability
  - Quality of service (QoS)
  - Management and visibility

**Vision and Strategic Goals**

The vision of the Cisco Public Facilities Management solution is to integrate and automate facilities and physical security processes in public administrations, using open, standards-based systems. Services ranging from video surveillance to enterprise applications are integrated with each other, and available everywhere in the municipality, over a unified wired and wireless IP infrastructure.

Realizing the Cisco Public Facilities Management vision requires collaboration from all stakeholders it affects, including IT, facilities management, physical security departments, estate management, financial operations, and outsourced partners.

The Cisco Public Facilities Management solution helps cities achieve six strategic goals:

- Reduce capital expenses
- Reduce operational expenses
- Increase workforce effectiveness
- Strengthen physical security
- Communicate effectively with people in the facility
- Minimize energy consumption
Goal 1: Reduce Capital Expenses

Today, most facilities systems connect to a central management console over a separate network. That means municipal buildings have different networks for each building management system, video surveillance, physical access control, and energy monitoring and management (Figure 1).

You can eliminate duplicate expense for wiring, switch ports, and management by converging multiple networks onto the building’s existing IP network. Some forward-looking cities have already done this. However, in most cases the IT team did not get involved in the deployment, so the deployments do not follow practices for security, high availability, QoS, bandwidth, and management.

The Cisco Public Facilities Management solution provides the technology as well as the best practices for connecting facilities systems to the IP network to minimize costs and create new efficiencies through integration.

How can CIOs cost-justify the network upgrade needed to support multiple facilities systems? In many cases, the investment pays for itself in a short time by eliminating the costs of a separate video surveillance network. Return on investment grows when the IT department offers physical access control and building management services to the facilities department, minimizing operational costs while increasing higher service levels.

In addition, studies show that building a converged network pays dividends if you later sell the property, increasing property values by up to 7.5 percent.¹

---

Goal 2: Reduce Operational Expenses
Converging facilities systems onto the building’s IP network can also reduce operational expenses through:

- Centralized building management and facilities services. A study by McGraw Hill reported up to 9 percent lower overall operating costs in organizations that converge IT and facilities applications, devices, and solutions on a unified IP network. Savings include support, maintenance, and operational costs. CIOs that provide these services help to save money and increase the value of IT to facilities and other municipal departments.
- Lower equipment maintenance costs because of more efficient operation and ability to give technicians detailed, up-to-date information. For example, seeing that the heating system is using more than the usual amount of energy for one floor of a building, the facilities team can call maintenance to repair the heating system before energy costs rise further.
- Automated adjustment of heating and cooling systems in response to environmental monitoring.
- Reduced energy consumption, using built-in network intelligence to turn off unused Power over Ethernet (PoE) devices (PCs, IP phones, and wireless access points) as well as lighting and other buildings systems (Figure 2). The McGraw Hill study showed up to 40 percent lower building energy costs from using PoE devices.
- Centralized physical security services.
- Improved decision-making from creating a central data repository of building management and security data.
- Capital cost avoidance by extending the life of existing equipment. You can keep equipment longer if you find out right away if it needs repair.
- Headcount savings or reallocation by shifting responsibility for operations and maintenance from internal staff to an outsourcing company. The goal is to decrease costs while retaining control of strategic decisions to optimize facilities management.

Figure 2
Typical Building Energy Consumption

- Atypical commercial building’s IT assets consume 25% of total power usage
- The majority of IT’s power consumption occurs outside of the data center

Goal 3: Increase Workforce Effectiveness

Connecting facilities systems to the IP network also helps to optimize municipal government business processes. The reason is that you can integrate the facilities systems with HR and enterprise resource planning (ERP) systems, making municipal processes more efficient.

For example, you can:

- Provide a common operator interface so that facilities staff can manage multiple systems at the same time. For instance, if a fire alarm sounds, the facilities team can check other environmental sensors and video surveillance cameras to determine if it is a false alarm. If it is real, facilities can just click a button to invoke policy for notifying building occupants, such as displaying instructions on digital signage and IP phone displays and broadcasting audio instructions on IP public address systems. Similarly, receiving a forced-door alert, the security team can view real-time video feeds to see whether the cause is an intruder or someone simply holding the door for a package delivery. If an intruder has entered the building, the team can quickly locate the closest security guard and share video and alerts to provide situational awareness.

- Integrate building management systems with communications and collaboration tools such as email, instant messaging, and calendaring. Early awareness of events such as outages helps facilities staff take action to minimize energy bills and make sure the workplace remains healthy and comfortable.

- Integrate physical access control system with your HR database. Instead of adding and deleting employees to multiple databases, you add and delete them just once, in the main HR database. Changes automatically apply to all building system databases. This integration saves time for staff and avoids the risk of terminated employees retaining building access privileges.

- Integrate physical security systems, HVAC, elevator control, and fire systems to automate response to emergencies, such as opening emergency exits and turning off the ventilation system.

- Enable centralized security personnel to collaborate with mobile guards, sharing real-time video feeds and communicating directly using any radio, smartphone, or other device. Partnerships like these let you increase physical security levels without increasing headcount.
Goal 4: Strengthen Physical and IT Security

Physical security in public buildings is becoming a regulatory requirement. But traditional analog video surveillance and physical access control systems make it costly to comply because each building needs its own network, servers, and management software.

With IP-based video surveillance and physical access control, you only need to invest once in servers and management software, no matter how many buildings you have. For all buildings after the first, the only investment you need to make is for cameras and door hardware.

Public administrations also need a strategy for information security. Practically every country has regulations for managing databases containing citizen data to prevent leaks or misuse of this information. An example is the U.K.’s Data Protection Act of 1998.

Fortunately, centralized physical access control systems can also strengthen IT security. When someone enters a username and password to log on to the network from within the building, the network grants the request only if the physical access control system shows that person is in the building. This prevents hacking attempts from the outside, as well as attempts to log in under someone else’s username.

The Cisco Public Facilities Management solution lets you implement best practices for physical and IT security, including:

- Implementing a uniform badge management system for all buildings. Employees gain access to building areas appropriate to their department and role.
- Granting network access to employees only if the physical access control system indicates they are physically inside the building.
- Linking alarms on building entrances to video surveillance images.
- Using video analytics software to detect tailgating, which is when one person enters a building directly behind someone else who used a card. Upon detecting tailgating, the video analytics software sends an alert to the security staff.
Goal 5: Communicate Effectively with People in the Facility
IP-based digital signage provides eye-catching communications with employees and citizens:

- Wayfinding for visitors, such as how to get to the reception area from the parking garage.
- Emergency notifications and instructions for a smooth evacuation, such as using an alternate exit to stay away from a fire outside the building.
- Meeting room schedules and reservations.
- Reports of building energy use, a technique shown to motivate employees to reduce their consumption.

Goal 6: Minimize Energy Consumption
Energy consumption has grown in the public sector, fueled by low energy costs and, until recently, a lack of awareness of the environmental costs of greenhouse gas emissions.

Today, public administrations worldwide are striving to make their buildings environmentally sustainable. Spurring these efforts is legislation to track building energy consumption to demonstrate improved usage over time. An example is the U.S. Leadership in Energy and Environmental Design (LEED) standards for designing, building, measuring, and reporting.

The Cisco Public Facilities Management helps cities meet social and legislative requirements for environmentally sustainable buildings and lower energy costs in the following ways:

- Decreasing energy consumption by PCs, IP phones, and any other PoE endpoint by automatically turning them off when not in use, according to policy.
- Providing the network foundation to replace PCs with thin clients as part of a virtual desktop infrastructure (VDI). Not only do thin clients use less energy than PCs, they often cost less and have a longer life.
- Providing earlier awareness of failing systems that are consuming more energy than usual. When building systems connect to the IP network, you can monitor real-time energy usage from a web browser.
Operational Models and Use Cases

In many municipalities, facilities and IT are different buying centers, with different concerns. The Cisco Public Facilities Management approach requires bringing together all stakeholders to agree on strategy and operations. This is essential for success. Collaborative decision making also creates an opportunity to pool budgets, meeting both organizations’ goals at less cost.

Stakeholders include:

- CIO, whose role is to support the facilities department
- Facilities director, motivated to maximize building efficiency
- Director of asset/estate management, concerned with minimizing capital expense and maximizing property value
- Chief financial officer
- Chief security officer
- Partner ecosystem, including service providers, building management system (BMS) vendors, security consultants and integrators, Cisco technology partners, and other technology providers

Following are three use cases illustrating the benefits of the Cisco Public Facilities Management solution.

Use Case Scenario 1: Streamlined Operations

To make efficient use of building space, Municipality A has consolidated multiple departments in a few buildings. Anne, an administrator working for the municipality, works from two locations depending on the current task. By presenting her badge to a door reader, she can enter her department’s areas in both buildings.

When Anne arrives in the morning, the physical access control system initiates several actions. It turns on her IP phone, desktop PC, and office lighting and heating, and begins logging her hours by recording when she enters and exits each building. When Anne presents her badge to leave the building, the physical access control system turns off IT systems and building systems, or places them in standby mode.

Anne’s colleague Aaron, who uses a wheelchair, previously needed a long time to open the door for visitors throughout the day. Now he can simply press buttons on his IP phone to see video of the person requesting entry, and remotely open the door. This capability has enabled the city to comply with the Disability Discrimination Act (DDA) requirements.

When contract workers arrive for work, Aaron issues them a temporary badge granting them access to allowed areas of the building. Access automatically expires at the end of the day or the end of the contract.
Use Case Scenario 2: Enhanced Physical Safety and Security

The main lobby and parking lot have recently been vandalized. As a result of staffing reductions, one security guard employed by an outsourced service provider has been left to patrol the grounds alone. The guard, Benito, receives support from Brigitte, who works in the city’s security operations center.

Now that the Cisco Public Facilities Management solution is in place, Brigitte does not have to monitor multiple physical security system consoles for alerts. Instead, she is automatically notified when significant events occur, such as:

- Movement in the storage room after business hours
- More than a specified number of people waiting in the lobby, posing a risk to safety
- Forced door or door left open in a remote facility
- Person loitering in the parking lot for five minutes
- Fire alarm sounds

Brigitte can quickly view real-time video associated with any of the events. If a fire alarm sounds, for instance, Brigitte can view real-time video feeds to determine whether the event is real or a false alarm.

If the event requires investigation, she can notify Benito and stream the real-time video feed or facility maps to Benito’s smartphone. Benito, in turn, can easily update the event log with pictures from the incident or by entering comments on his smartphone.

If Benito determines that a threat is real, Brigitte can consult the physical access control system to determine who is in the building, and inform them of the nearest building exit on digital signage or the built-in displays of their IP phones. She can even stream the live video feed to the digital signage or phone display. Brigitte can also broadcast different messages to occupants of a particular floor or building.

Brigitte also has the capability to open doors to visitors in remote buildings, using the video surveillance images to assess if the person is authorized to enter.
Use Case Scenario 3: Energy Management

Carlos is a facilities manager. Environmental sustainability ranks high on the mayor’s list of priorities, and Carlos has been asked to reduce building energy consumption. He also wants to optimize facilities systems management and provide managers with reports showing progress in reducing energy consumption.

Now that all facilities systems connect to the IP network, Carlos can manage multiple systems at the same time. He can accomplish more, and more easily accommodate requests for new building services.

For example, Carlos can gain real-time visibility into all systems’ energy consumption, reported by equipment type (IT, lighting, HVAC, and others), building, and building floor. The system even provides a breakdown based on IT device type, such as PCs, servers, printers, IP phones, wireless access points, switches, and routers. Detailed reports of energy consumption by department helps departments optimize their energy consumption.

Carlos can also generate reports correlating energy consumption with the building or floor occupancy rate. If lighting system energy consumption does not significantly decrease during low occupancy, Carlos can confidently recommend occupancy-based power management. If the report shows lights remain on overnight, for instance, Carlos can then implement policies to shut off the lights automatically, turning them on again automatically when an employee uses a badge to enter that area of the building.

Connecting all facilities system to the IP network also helps Carlos more quickly find out about and remediate equipment issues. For example, if a video surveillance camera, sensor, or any other building system stops transmitting, Carlos receives an alert on his smartphone. At the same time, the system automatically creates a trouble ticket and notifies the engineer on call on the engineer’s preferred device. When the video surveillance camera or other system is back online, the system automatically notifies appropriate personnel with a text message or email.
Functional Architecture

As shown in Figure 3, the Cisco Public Facilities Management solution uses a converged network as the platform for building and physical security systems. The same network platform enables authorized personnel to communicate with facilities systems and collaborate with colleagues, using any device, from anywhere.

Figure 3
Cisco Public Facilities Management Functional Architecture
Here is a summary of services that the converged network platform provides:

- **Scalable bandwidth**: The IT team can use a variety of technologies to make sure the network provides adequate bandwidth for facilities system. These techniques range from reserving bandwidth for video surveillance to optimizing the network route taken by IP packets.
- **Mobility**: Mobility services refer to connecting people or devices to other people or devices over wired or wireless networks. These services include tracking mobile assets and roaming between subnets without losing the connection.
- **Security**: Security services help protect facilities system from attacks or unauthorized use. For example, simple access control lists (ACLs) limit access to particular devices. For more security, virtual forwarding and routing (VRF) instances create a fully isolated environment for each application or department. Identity management systems provide roles-based access to different system features.
- **Reliability**: Redundant network paths and redundant hardware, and other techniques help make sure that facilities systems can continue to operate despite a network or equipment failure.
- **QoS**: You can assign different priorities to different types of traffic. For example, video surveillance traffic might receive the highest priority because it is latency-sensitive. You can also dedicate bandwidth to specific systems, such as digital signage.
- **Management**: Management services include fault isolation, configuration, accounting, performance monitoring, and security.
Technical Components

Here are the major components in the Cisco Public Facilities Management solution:

- Physical security
  - Cisco Video Surveillance Operations Manager
  - Cisco Video Surveillance Media Server
  - Cisco IP Video Surveillance Cameras
  - Cisco IP Interoperability and Collaboration System (IPICS)
  - Cisco Physical Access Gateway
  - Cisco Physical Access Reader Module
  - Cisco Physical Access Manager
  - Third-party card reader from Cisco’s ecosystem of partners

- Energy monitoring and management
  - Cisco EnergyWise technology, which operates on Cisco Catalyst Switches and Cisco Integrated Services Routers to manage the energy consumption of IT endpoints such as IP phones, PCs, Cisco Digital Media Players, and wireless access points
  - CiscoWorks LAN Management Solution 4.0 and later, a management station for configuration, monitoring, and reporting
  - Cisco EnergyWise Orchestrator
  - Building management system from Cisco’s ecosystem of partners
  - Data center power and cooling solutions, in partnership with companies such as Schneider

- Converged network platform

Table 2 shows the services in the Cisco converged network platform that support facilities systems.
### Table 2: Capabilities in the Converged Network Platform

<table>
<thead>
<tr>
<th>Capability</th>
<th>Cisco Technologies</th>
</tr>
</thead>
</table>
| **Scalability**    | • Per flow and aggregate bandwidth policies, especially for Cisco IP Video Surveillance  
• Specific settings for ingress/egress buffers  
• Bandwidth optimization techniques, such as equal-cost load balancing, EtherChannel technology, Performance Routing (PIR) |
| **Security**       | • Network-level access control, with firewalls (stateful) or access control lists (stateless)  
• Confidentiality, through application-level or network-level encryption (IPSec VPN or SSL VPN)  
• Authentication, at packet-level (Secure Hash Algorithm [SHA] or Message Digest 5 [MD5]), or device-level, through policy control  
• Intrusion prevention and detection, at network level or device level  
• Path virtualization, using overlays (firewalling and ACLs, or IPsec VPN) or Virtual Route Forwarding (VRF) |
| **Mobility**       | • Enhanced security: Location-based authentication and precise detection, identification, and prevention of wireless threats, including rogue access points  
• Location services: Location of any Wi-Fi device or asset with an RFID tag, as well as API support for applications that consider the user’s location  
• Voice services: Delivery of voice and voicemail services to Wi-Fi clients, including smartphones, with end-to-end QoS and manageability  
• Guest services: Network access for contractors, vendors, and citizens, with privileges based on user type and physical location |
| **Reliability**    | • Network resiliency, achieved through Layer 3 technologies (Routing Protocol Convergence, Hot Standby Routing Protocol [HSRP], Virtual Routing Redundancy Protocol [VRRP], Gateway Load Balancing Protocol [GLBP]) or Layer 2 technologies (Spanning Tree, Uni-Directional Link Detection [UDLD], 802.1Q Trunking, EtherChannel, and Cisco Catalyst® 6500 Virtual Switching System [VSS])  
• Device resiliency, achieved with redundant hardware (hot standby or active-active) and redundant processors. The latter use nonstop forwarding with stateful switchover, and Cisco StackWise® and StackWise Plus technology  
• Operational resiliency, using generic online diagnostics (GOLD), In-Service Software Upgrades (ISSU), Cisco IOS® Embedded Event Manager (EEM), and online insertion and removal (OIR) |
| **Quality of Service (QoS)** | • Marking all relevant flows based on the Cisco 12-class QoS model  
• Trust boundary at the ingress edge of the network  
• Ingress/egress queuing and packet discarding to achieve desired per-hop behavior for traffic flows across LAN links  
• Policy mapping to achieve desired per-hop behavior for traffic flows across WAN links  
• Marking, remarking, shaping, and policing required to traverse a service provider network  
• Cisco AutoQoS to simplify configuration of Cisco IP Video Surveillance Cameras |
| **Management**     | • Recommendations for fault isolation, configuration management, accounting management, performance management, and security management |
Figure 4 shows how the Cisco network foundation supports energy management and physical security systems.
Case Study:
Physical Security:
City of Drancy, France

A suburb of Paris, Drancy has a population of about 66,000. To strengthen the economy, city leaders sought an innovative approach to reverse the outflow of residents, decrease crime, and attract more businesses.

All municipal buildings and schools, nearby municipalities, businesses, and many residences have access to a citywide fiber network. The network supports more than 300 centrally managed IP video surveillance cameras. National and municipal police can view real-time video streams on their notebook computers, from anywhere with a wired or wireless connection.

The crime rate has decreased by 30 percent since the city of Drancy implemented Video Surveillance, making Drancy the second safest suburb of Paris. Drancy also uses the network as the foundation for Cisco Physical Access Controls, enabling centralized control of doors in all municipal buildings.

What’s more, the same investment in the IP network and Cisco data center technologies is helping the city introduce 21st century learning and compete to attract new employers.

To read the full case study, visit:
Case Study:
Energy Monitoring:
Brunel University, United Kingdom

Located in West London, Brunel University has almost 15,000 students and more than 1600 academic and professional staff. Rising energy costs and a commitment to environmental sustainability motivated university leaders to monitor and manage energy consumption more effectively.

The university already used numerous Cisco PoE endpoints, such as IP phones and wireless access points. But there were no policies to turn the devices on and off based on whether building occupants were present.

Now, using Cisco EnergyWise, a Cisco Catalyst switch feature that can be activated without charge, the university has real-time visibility into power usage. The IT team also sets policies to automatically turn devices on and off in buildings, individual offices in the building, and even individual devices.

Brunel collected energy usage data before and after using EnergyWise, and extrapolated to reflect savings in a deployment with 3000 IP phones, 300 wireless access points, 5700 PCs, 1100 printers, and 1630. Annual savings amount to £12,280 (or approximately $20,000) for PoE devices only, and £90,823 (or approximately $150,000) including PCs and printers. This equates to approximately £47 (or approximately $77.00) annually for every member of Brunel’s staff.

The network manager said, “As the full Cisco solution rolls out, we expect our savings to increase—if not quite in orders of magnitude, then certainly into significant thousands of pounds.”

To read the full case study, visit:
Located southeast of Madrid, the city of Rivas Vaciamadrid, Spain, is home to more than 68,000 residents.

In 2004, the city launched the Rivas 21.10 Digital project, designed to take advantage of IT to transform Rivas into a Smart+Connected Community.

One priority is environmental sustainability, especially minimizing building energy and water use. Using the Cisco Public Facilities Management solution, Rivas Vaciamadrid equipped 10 municipal buildings with programmable logic controllers (PLCs) integrated in the IP network. In conjunction with the centralized SCADA system, the PLCs enable facilities manager to centrally manage and monitor all building processes, including HVAC, lighting, water, power, gas, physical access control, equipment in sporting facilities, and more.

Results to-date include significantly reduced energy consumption, partly from earlier detection of energy-consuming malfunctions such as water or gas leaks. The city has also reduced building greenhouse gas emissions and reduced monthly operational costs.

To read the full case study, visit:  
www.cisco.com/web/strategy/docs/gov/Rivas_cStudy.pdf
Next Steps

To discuss how your organization might begin taking advantage of the Cisco Public Facilities Management solution, contact your local Cisco account manager. Questions to consider when planning the solution for your city include:

- **Energy efficiency**
  - Is environmental sustainability part of the public administration’s mission? Is the CEO or CFO looking to reduce budgets and considering energy-saving technologies?
  - What processes are in place to deal with energy inefficiencies?
  - Does your facilities master plan document best practices regarding the electrical infrastructure, such as a preferred BMS partner?
  - What processes and measures do you use to benchmark energy efficiency across the IT and facilities infrastructure? How do you assess overall building energy efficiency?
  - Do you report the findings to any national organizations, or make the information publicly available?

- **Physical security**
  - Which regulatory requirements apply to the municipality regarding physical safety and security for people in the facility?
  - Which regulatory requirements apply for protecting the confidentiality of paper and electronic data in the facility?
  - Do you outsource all or part of your security staff? Are you looking for ways to improve efficiency of security personnel?
  - Are building tenants concerned with vandalism, petty theft, or other minor physical security incidents?

- **Infrastructure convergence**
  - Do you have a strategy to eliminate duplicate expense for wiring and devices used for building management systems, physical security, and energy monitoring and management?
  - Do you see any benefits from integrate office application (such as calendaring) with facility systems (such as room reservation) or physical security (such as physical access control)?
  - Do you have plans to use digital signage for communications with people in the building?
For More Information

To learn more about Smart+Connected Communities, contact your local Cisco account representative or authorized Cisco partner, or visit:
www.cisco.com/web/strategy/smart_connected_communities.html