CHAPTER 7

Remote Operation Services

Cisco Management Appliance

Urban Security solutions require a mission-critical IP-centric network to be in place and functioning properly at all times. The network is made up of multiple pieces of equipment (video surveillance, access control, incident response, and core network components) as well as middleware software components to correlate and dispatch situational events as they occur. All network components must be in good health for the PSS system to be effective. As a result, remote management of these devices and middleware components is essential to the successful deployment of any physical safety and security (PSS) solution.

Using the Cisco Management Appliance (MAP) to manage the PSS network enables an IT or any other monitoring organization to proactively monitor the health of the network and maintain a healthy network ready to perform its primary purpose of keeping citizens safe.

Cisco Management Appliance Description

The MAP approach to managing PSS systems requires deploying one or more management appliances in the network and leveraging standard management capabilities inherent in the PSS IP devices and gateways (for example, SNMP, ICMP, Syslog, and so on) to discover and place them under management. After each of the components is placed under management, industry standard management functionality and custom Cisco intellectual property integrated into the MAP are used to monitor the health of the entire system.

The same appliance used to manage the PSS components for this effort is already in use to manage advanced and emerging technologies from Cisco such as Telepresence, DataCenter, and IronPort solutions. The appliance is field tested and proven as a management system with Cisco equipment and Cisco applications.

The Cisco MAP is able to monitor all devices in the PSS environment and generate detailed reports on their performance and availability. In addition, Cisco MAP is able to send alerts to Surveillint, allowing the operator to work through a consolidated interface. Figure 7-1 shows how the Cisco MAP is deployed in a typical PSS environment

Figure 7-1 Typical PSS MAP Deployment

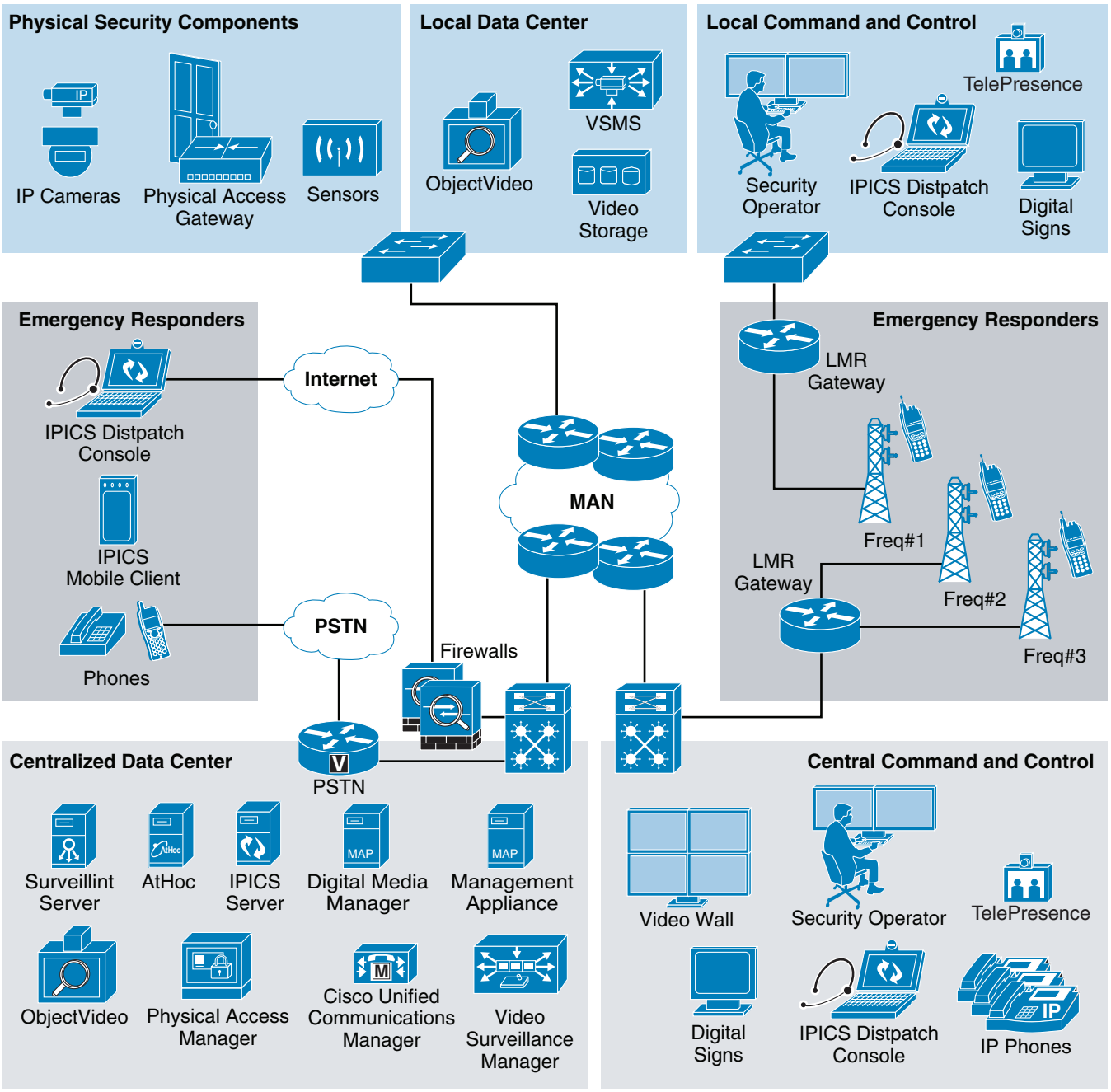
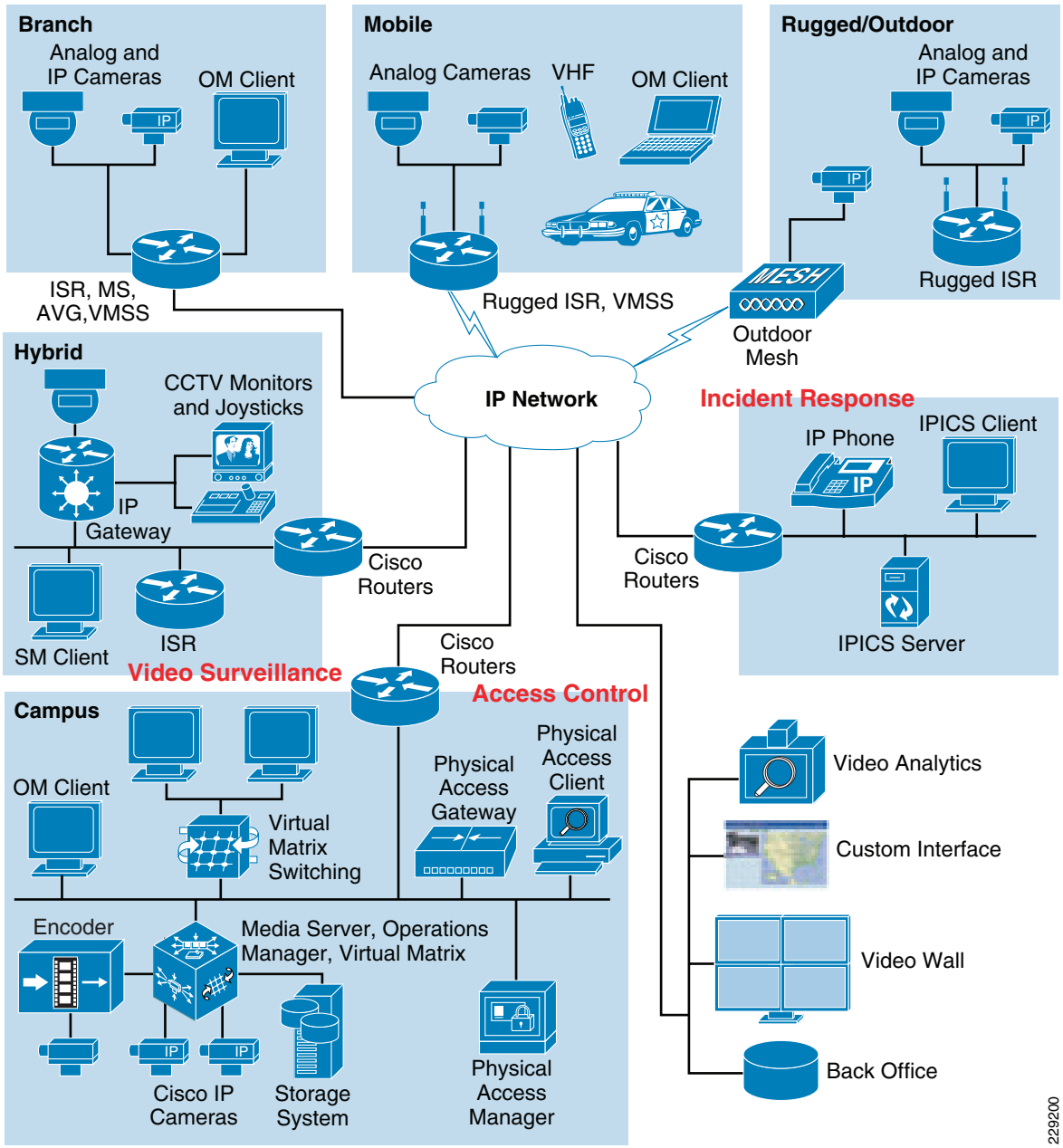


Figure 7-2 shows a sample of the PSS equipment that can be managed using the MAP solution.

Figure 7-2 PSS MAP Components under Management



The MAP solution provides the following three major management functions:

- Monitoring—The MAP collects and processes events from each of the PSS and infrastructure components based on industry best practices included in the MAP appliance and Cisco product -specific intellectual property.
- Detection of faults and potential network issues—The MAP is able to determine the severity of each event received and ensure that an appropriate fault is activated in the system.
- Isolation of faults and potential network issues—The MAP provides user-friendly interfaces to the monitoring organization to allow for easy identification of faults and potential issues. In addition, the MAP must also provide operators with tools to troubleshoot problems remotely to determine the root cause of each issue.

The Cisco MAP solution provides all of these features and is designed to be deployed in a variety of configurations from hosted, onsite, and high availability environments.

Benefits of the Cisco MAP

The MAP approach to managing PSS components provides the following benefits to the PSS system:

- Proactive monitoring of the PSS mission-critical network to detect and isolate faults as they occur. This allows faults to be isolated and corrected quickly to keep the PSS system up and running and serving its primary purpose of keeping citizens safe.
- Proactive monitoring and detection of potential issues such as high memory or disk utilization to prevent faults.
- Proactive collection and maintenance of statistics to determine areas of the PSS system needing improvement. Performance degradation over time may mean the original characteristics of the system have changed and certain components may need to be upgraded.
- Minimizing legal, regulatory, and financial liability by instituting policies to measure PSS system reliability, storage requirements, and other important metrics.

Cisco MAP focuses on the management capabilities required to proactively monitor the health of the Physical Safety and Security components deployed in the Urban Security model. The management capabilities described in this section have been validated in Cisco's Urban Security lab. The lab diagram and components are highlighted in chapter 8 – Lab and test overview.

For each component to be placed under management, the device or application must support polling via ICMP, SNMP, SQL, or an API and send status asynchronously via syslog or SNMP traps.

The core management capabilities validated in this solution guide are as follows:

- Device and application availability
- Receipt of asynchronous faults
- Generation of custom faults
- Collection of performance information
- Collection and storage of inventory information for each component in the system

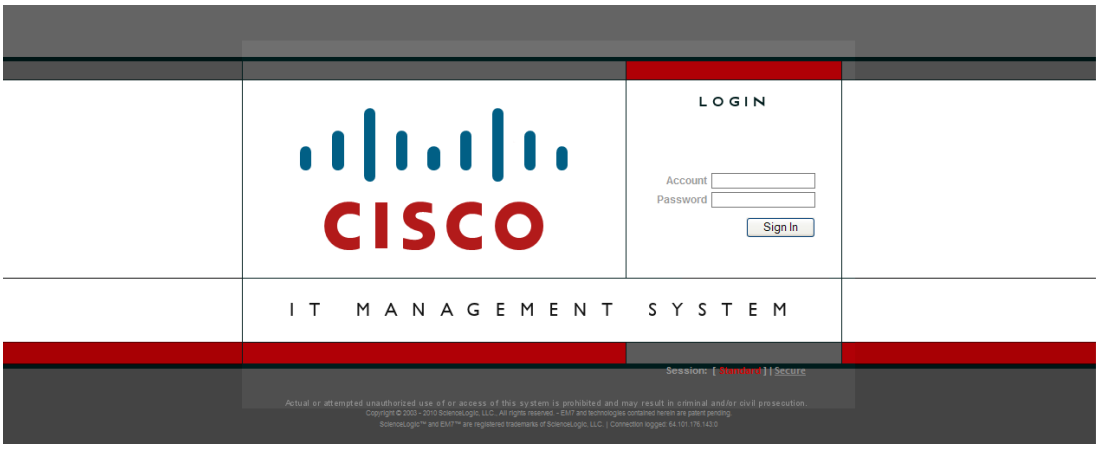
Cisco MAP Features

Several use cases were validated for this solution. The base line set of use cases required for successful remote management of the PSS system are also included.

Discovering PSS Components

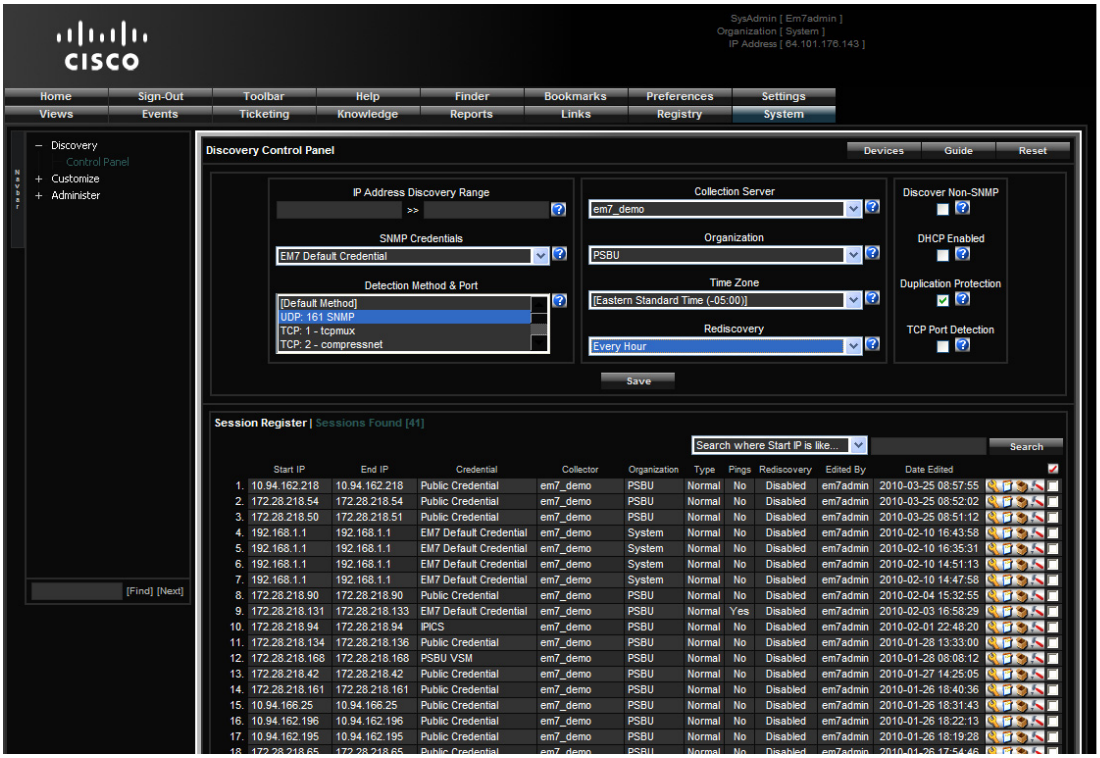
The MAP appliance must discover each PSS component to begin monitoring the health of the system. This can be done easily using the industry standard best practice discovery capabilities built into the MAP appliance. First, the user must log into the MAP appliance web portal and navigate to the System discovery screen, as shown in Figure 7-3.

Figure 7-3 MAP Web Portal Login Screen



After the user is logged into MAP appliance, it is simple to navigate to the System Discovery interface by selecting the System tab and then selecting the Discovery option on the left hand tree view, as shown in Figure 7-4.

Figure 7-4 MAP Discovery of PSS Video Surveillance Management Appliance



In this case, the MAP appliance is set up to discover a Video Surveillance Management appliance (VSM) using the SNMP protocol. The MAP appliance can discover any device or application that supports ICMP or SNMP.

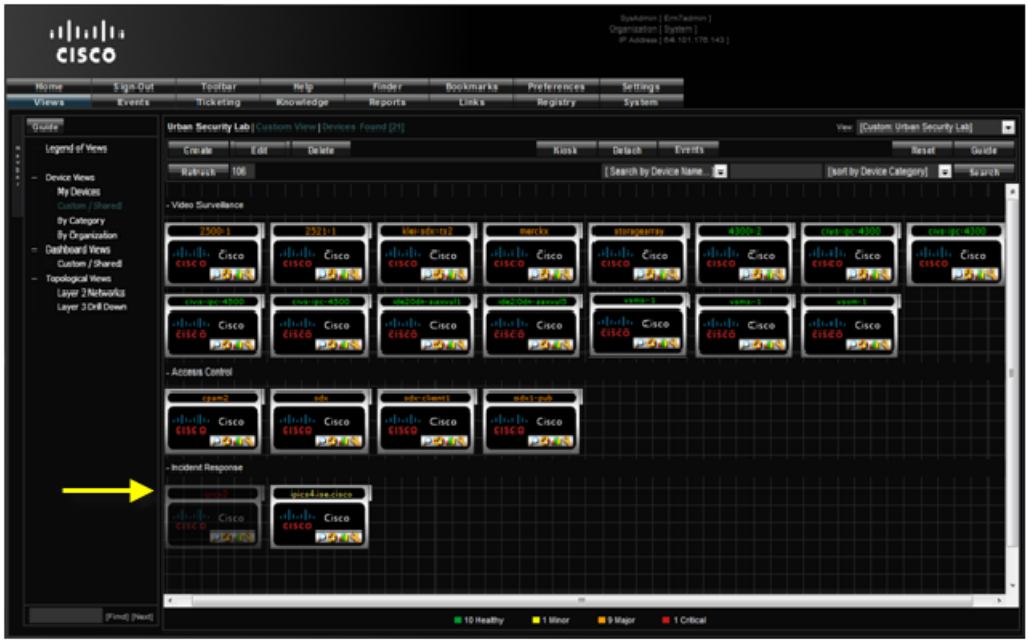
Monitoring PSS Mission-Critical Network

After the PSS devices are discovered by the MAP appliance, the entire PSS system can be monitored remotely. The MAP web portal provides multiple views of the PSS system showing the health of the system in a single pane of glass. Three sample monitoring views are displayed below.

The first view is a Cisco product specific view that allows the monitoring organization to view all of the PSS components by device category (see Figure 7-5):

- Video surveillance devices (Cisco IP cameras, AVG, VSMS, VMSS, and VSOM components)
- Access control devices (CPAG, CPAM)
- Incident response devices (IPICS, RMS)

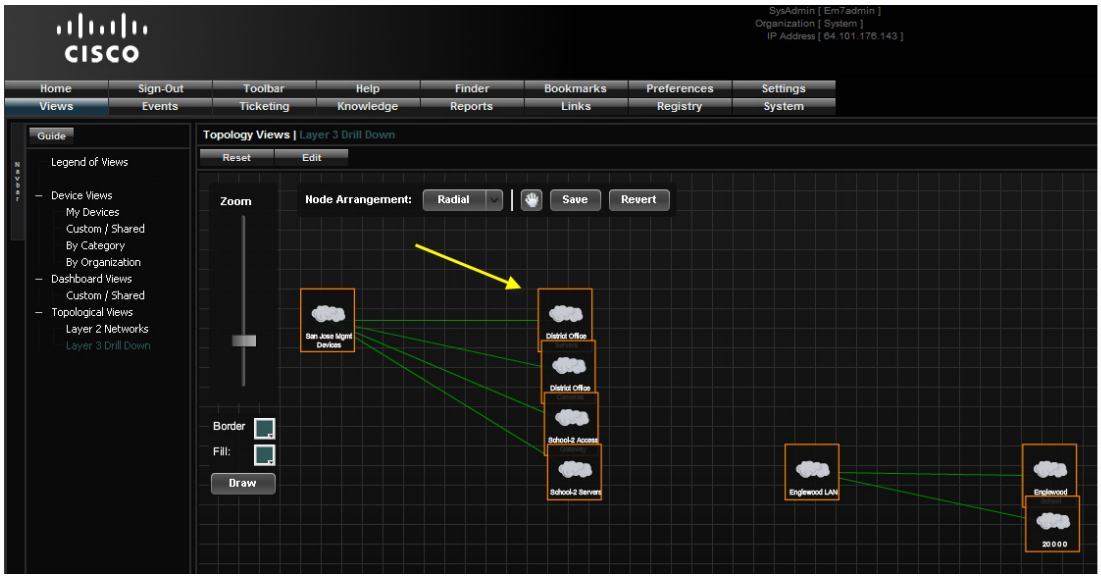
Figure 7-5 MAP Monitoring—Device Category View



In this view, the operator can quickly see any issues needing attention. The arrow in Figure 7-5 points to the first icon under Incident Response, which appears grayed out. The icon is actually blinking on the screen giving the administrator a visual cue that there is some kind of communication failure on that particular IPICS server.

The second view is graphical representation of the Layer 3 PSS network as shown in Figure 7-6. The Layer 3 PSS network includes an icon for each sub-network and shows a topological view of the status of the entire sub-network (a switch or router and all of the components connected to it in a downstream hierarchy). A color-coded box is drawn around each sub-network. The box color indicates the current state of each sub-network (green indicates no problems, yellow indicates a minor condition, orange indicates a major condition, and red indicates a critical condition). A sub-network icon with any color other than green indicates that at least one device in that sub-network is having problems.

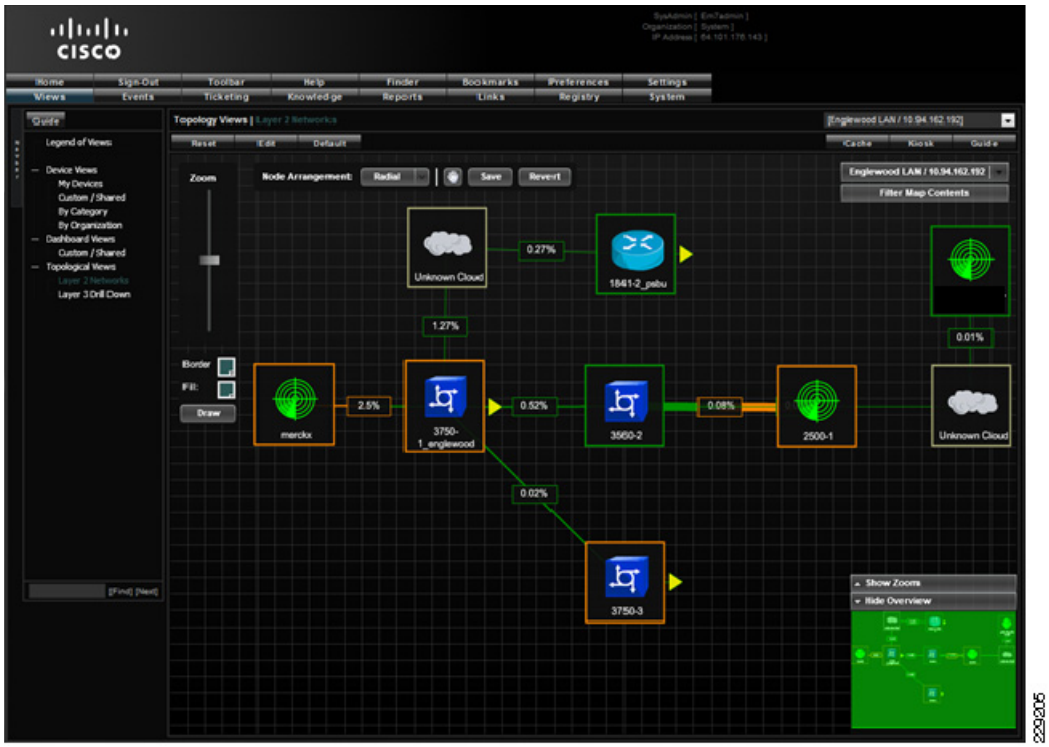
Figure 7-6 MAP Monitoring—Level 3 PSS System View



The arrow above is pointing at a sub-network with a major condition (orange box). This sub-network contains at least one device reporting a major condition that needs attention.

The third view is a graphical representation of the Layer 2 PSS network (see Figure 7-7). The Layer 2 PSS network can be viewed by clicking on one of the level 3 icons in Figure 7-6. An icon for each PSS component in the system (CPAM, CPAG, VSM, VSMM, IPICS, and so on) is present in the level 2 view with a color-coded box drawn around each component. The box color indicates the current state of the component (green indicates no problems, yellow indicates a minor condition, orange indicates a major condition, and red indicates a critical condition). In addition, each box is connected with color-coded lines representing the network links between components.

Figure 7-7 MAP Monitoring—Level 2 PSS System View



Each line includes a number inside a box, representing the current link utilization. Link utilization data is collected automatically by the MAP appliance and is used to determine the color of each link (utilization data is compared to Cisco product specific thresholds defined in the MAP).

Note The thresholds were set artificially low to induce the error conditions shown with orange-colored link lines. In a standard PSS system, the link thresholds are set based on Cisco product-specific recommendations.

Detecting and Isolating Faults

One of the primary functions of the MAP appliance is to allow the monitoring organization to detect and isolate faults and potential issues in the PSS system. There are several ways the MAP appliance allows detection of issues. The views described above are the starting point for the fault detection use cases. Figure 7-8 shows the PSS component view by category with additional reference points.

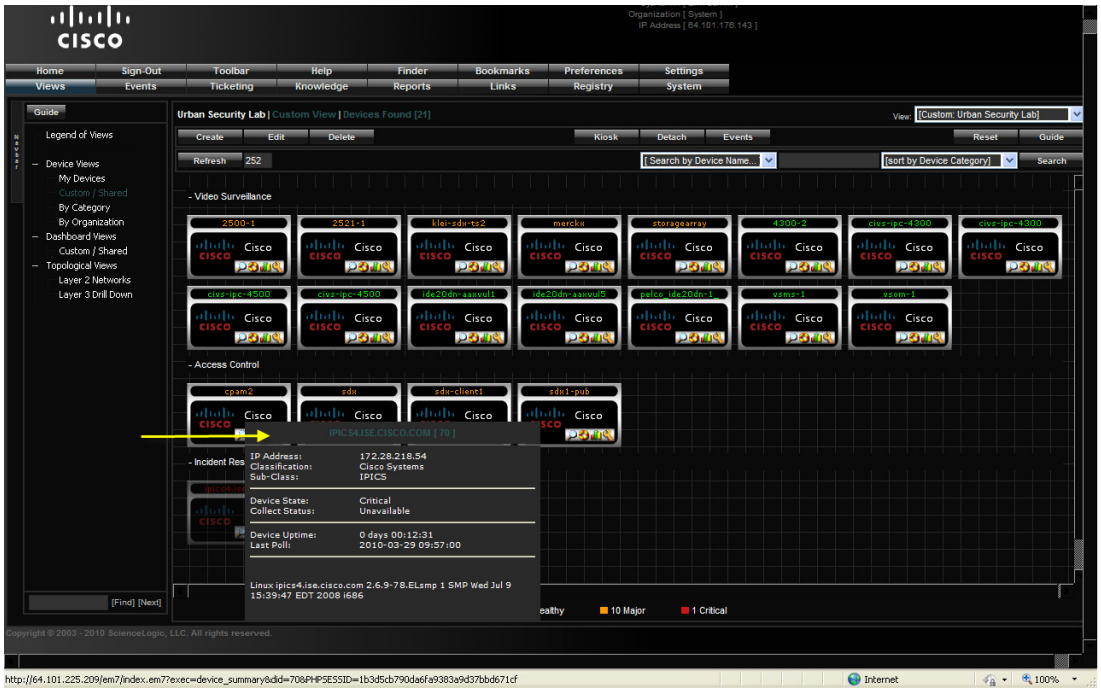
Figure 7-8 PSS Faults—Category View

Note the numbered arrows on the diagram. Arrow #1 shows a summary of the state of all of the PSS components in the system. The number of devices in each state is displayed at the bottom of the web portal user interface allowing an administrator to see the overall health of the PSS system at a glance.

Arrow #2 shows the first icon under Incident Response as grayed out. The icon is actually blinking on the screen giving the administrator a visual cue that there is some kind of critical communication failure on that particular IPICS server. Arrow #3 shows the label of one of the Video Surveillance components (a Cisco 2500 series IP camera) is orange indicating this PSS component has a major condition present. The label color indicates the health of each component in the system and provides an at a glance health status for the system administrator. Each of these cues serves as a starting point for detecting and isolating faults in the system.

Moving the mouse over the IPICS server pointed to by Arrow #2 above brings up a more detailed status dialog showing the vital statistics for the server (see Figure 7-9).

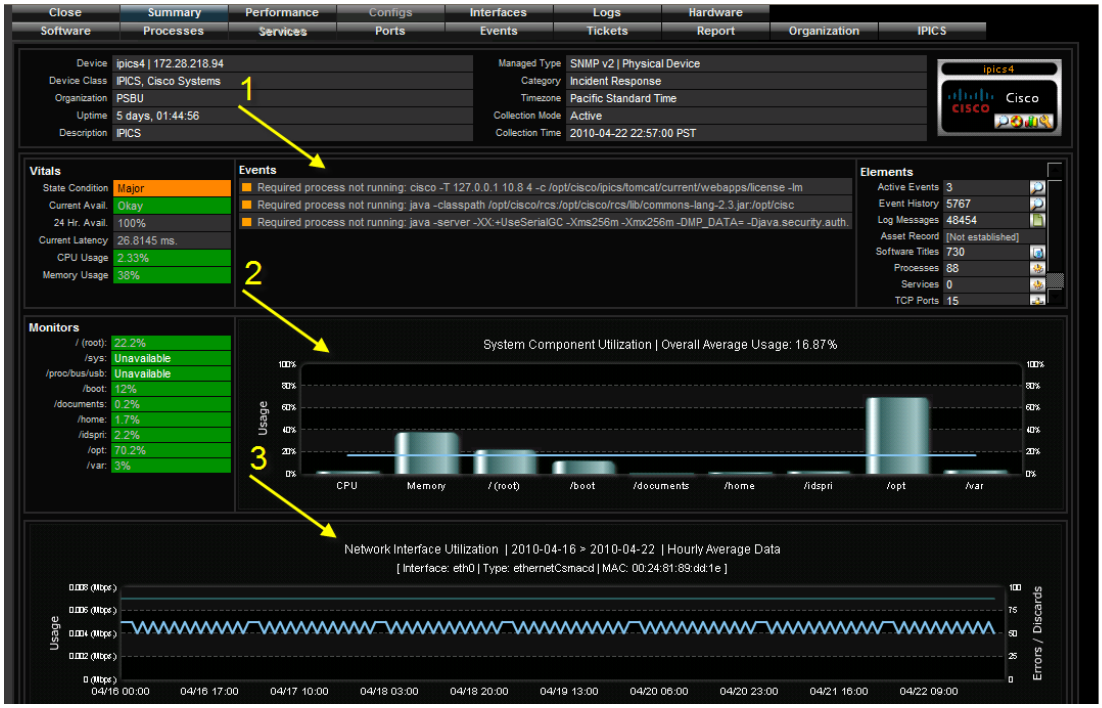
Figure 7-9 PSS Faults—Vital Statistics Dialog



The vital statistics dialog shows the last time this IPICS server was known to be operating properly and lets the administrator know it is currently not accessible to the MAP appliance.

From this point, the administrator can double-click on the IPICS server icon to navigate to the IPICS detail screen, as shown in Figure 7-10.

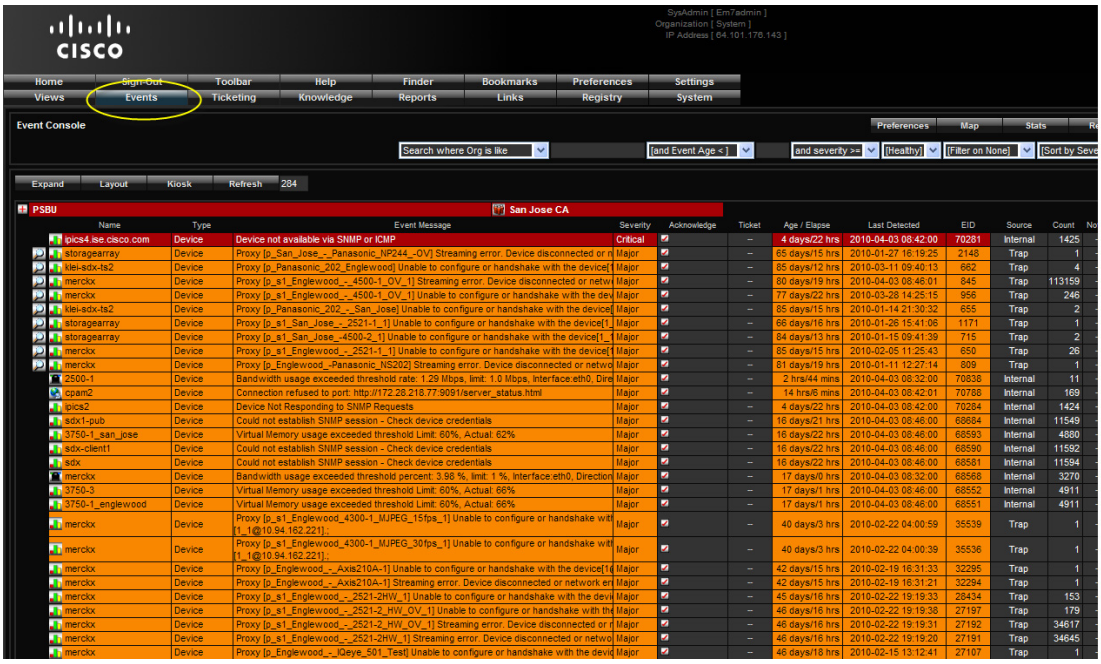
Figure 7-10 PSS Faults—IPICS Details



This view allows an administrator to review the currently active alarms and events on the IPICS server, current and historical memory utilization trends on the server, and vital network statistics. In this case, one of the alarms indicates that an important process on the IPICS server is not operating properly. An administrator can now take the appropriate actions to correct the issue on the IPICS server.

Another useful view for identifying and troubleshooting issues in the system is the Events view, as shown in Figure 7-11. This view can be started by selecting the Events tab on the main MAP menu bar.

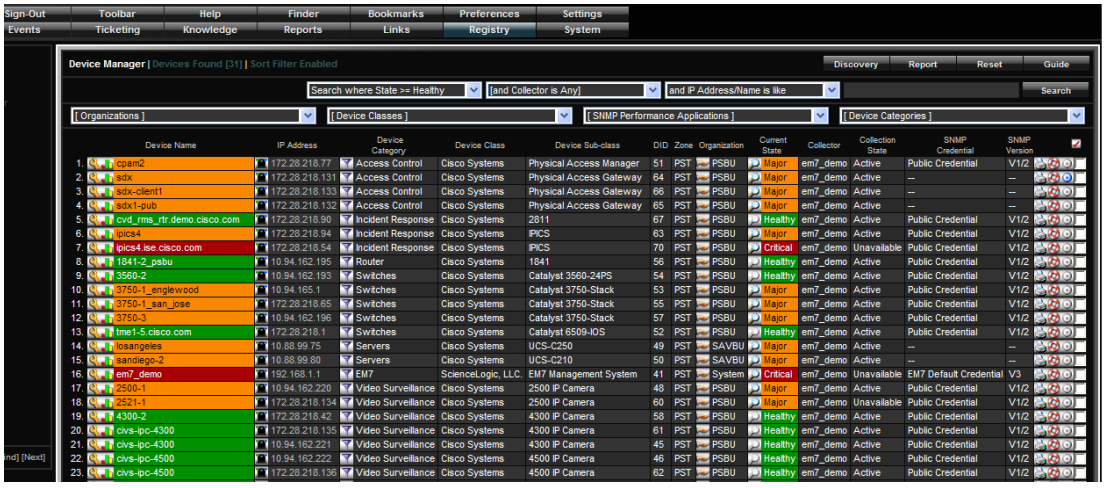
Figure 7-11 PSS Faults—Active Event View



All of the active events in the system are shown in this view. The top event in the table is highlighted red to indicate the device is in a critical condition. This event corresponds to the IPICS server from Figure 7-9. The administrator can navigate to the same IPICS details screen by selecting on the device summary icon on the left hand side of the top row.

The Registry view is another view that is very useful for detecting and isolating faults. This view can be started by selecting the Registry tab on the main MAP menu bar. Figure 7-12 shows the Registry view.

Figure 7-12 PSS Faults—Registry View



The registry view shows the condition of each of the devices under management. In this case, row 17 on the table shows a Cisco 2500 Series IP camera with a major condition (orange colored label). After the administrator has detected this fault on the camera and wants to isolate the problem, additional

information for the camera can be obtained remotely by selecting the camera device summary icon next to the camera name in the table. When the device summary icon is selected, detailed information about the camera is displayed, as shown in Figure 7-13.

Figure 7-13 PSS Faults—Component Summary View (Cisco IP Camera)

The device summary for the camera shows that it has exceeded the threshold set for bandwidth utilization. This is an example of a potential issue in the network that needs to be addressed. After the administrator is aware of the issue, corrective action can be taken before this escalates to a critical condition.

Collecting and Storing Compliance Information

Organizations that require collection and storage of information for compliance and liability reasons benefit from the MAP solution. The MAP appliance is able to collect many statistics using industry standard SNMP, SQL, or custom API calls, store the statistics, and provide standard and custom reports to show operational trends related to each statistic collected.

In the Urban Security lab on the Cisco campus, the MAP appliance has been configured to collect statistics such as memory and disk utilization. Custom thresholds have been set to allow the MAP appliance to generate alerts on behalf of PSS components when memory or disk utilization is too high. Figure 7-14 shows one of the applications created for the Urban Security lab.

Figure 7-14 MAP Application Configuration

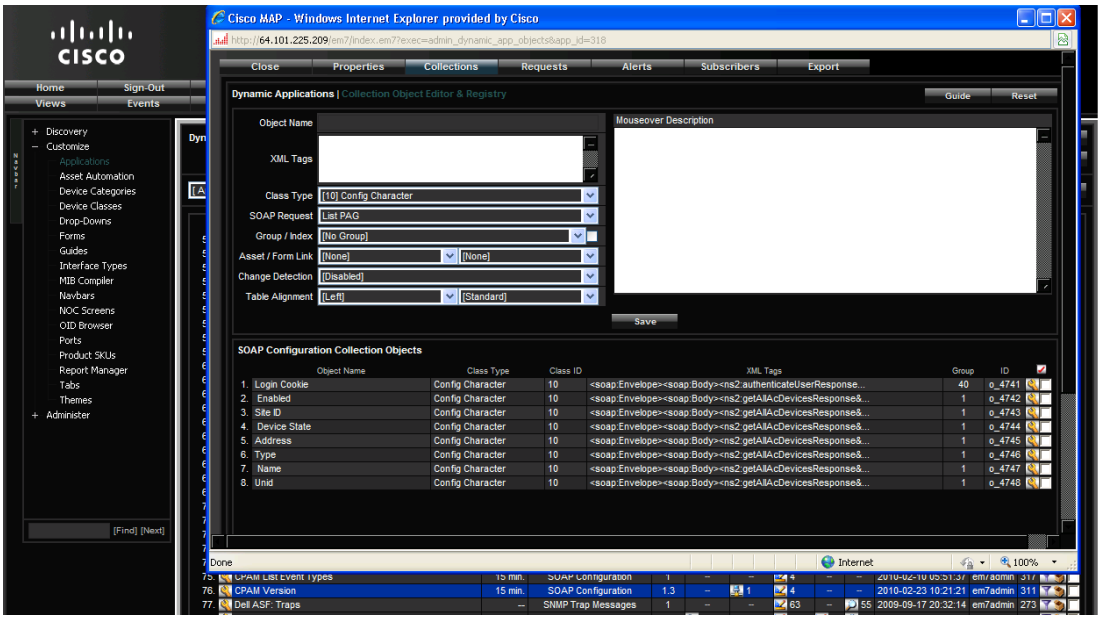


Figure 7-15 shows the physical memory utilization for a Cisco Physical Access Manager component. Reports can also be generated in a number of formats including HTML, CSV, PDF, and others.

Figure 7-15 MAP Memory Utilization Trends

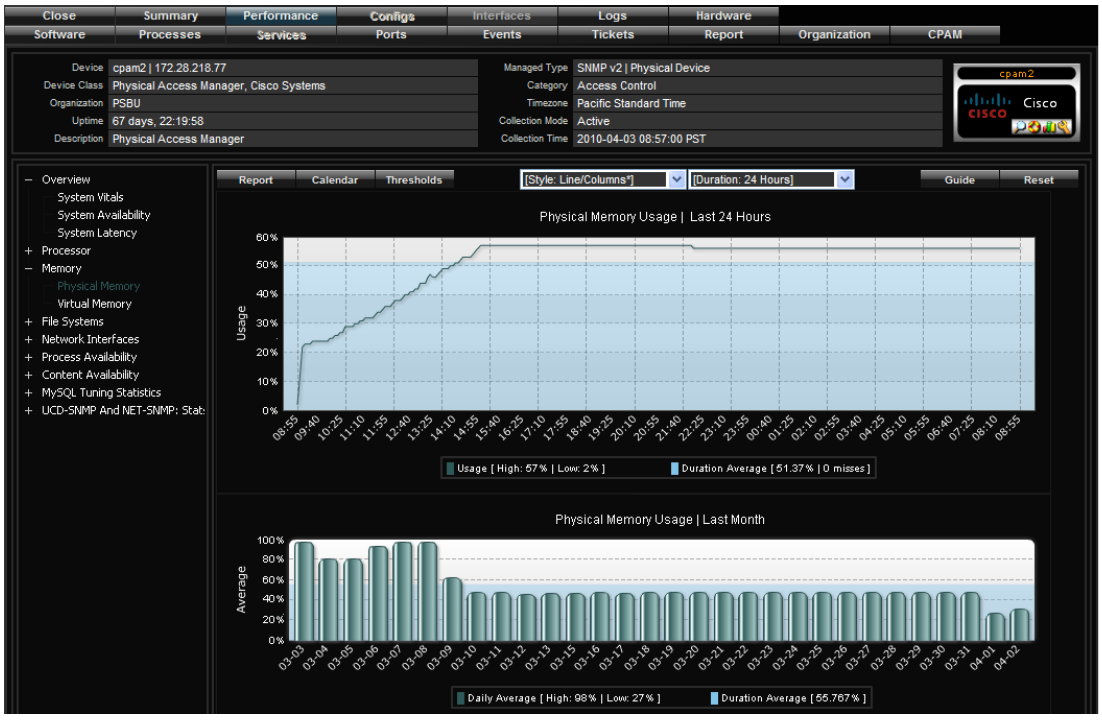
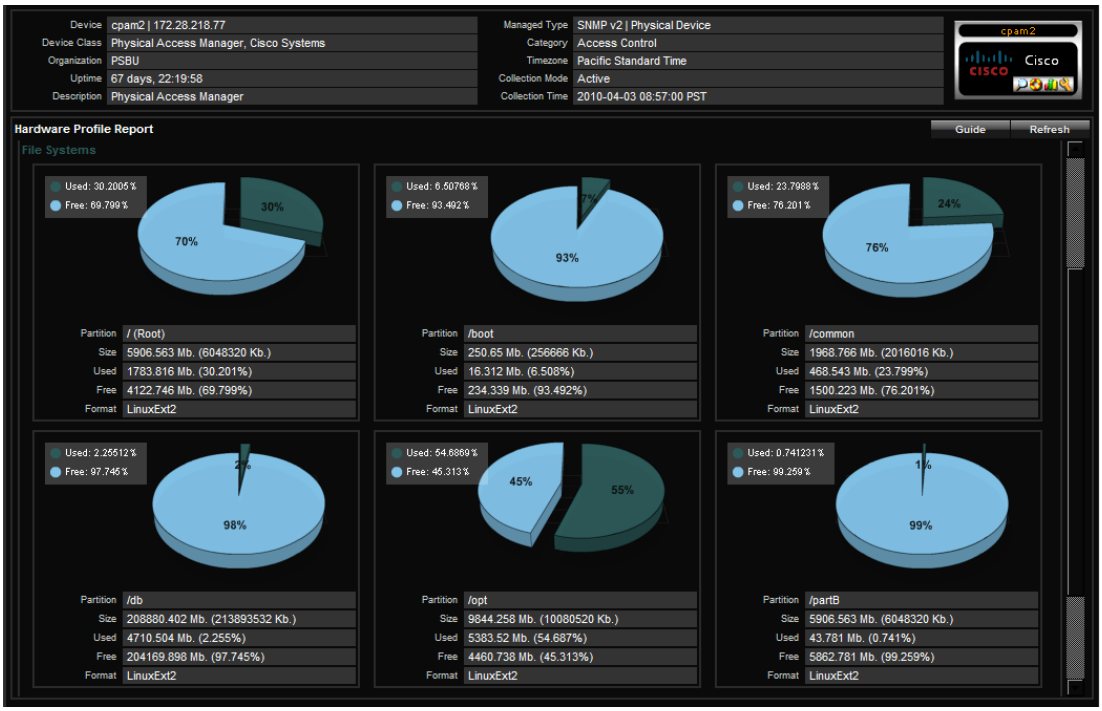


Figure 7-16 shows the disk utilization for a Cisco Physical Access Manager component. Reports can also be generated in a number of formats including HTML, CSV, PDF, and others.

Figure 7-16 MAP Disk Utilization Trends



Cisco MAP Deployment Options

The MAP appliance allows flexible deployment in the PSS system. It can be deployed as an all-in-one single appliance in a central location to monitor devices across the entire PSS system, or it can be distributed across the PSS system network with collectors in each branch or local office. It can also be configured in a redundant fashion to provide a highly available collector service.

This flexibility in deployment allows Cisco to provide remote monitoring capabilities tailored to meet each customer's needs based on individual sophistication and expertise levels. Following are a few potential deployment options for the MAP appliance:

- As a traditional Remote Managed Service (RMS) with proactive management of the PSS system provided as a service by Cisco where Cisco continuously monitors the PSS system on behalf of the customer
- As a light RMS deployed on-site or remotely where PSS components are monitored by the MAP appliance and notifications are automatically generated and sent to key customer personnel in the event of system failures
- As an integrated component of other Cisco smart services

The MAP appliance can be deployed as a distributed system with collectors in one or more of the remote locations. The configuration of the MAP solution can easily be tailored to meet the needs of each PSS solution developed to maximize the return on investment.