Designing the Solution

Application Traffic Flows

The focus of this release of the Urban Security solution is to integrate various physical security systems using the Cisco IP network as the platform. An open architecture framework enables various solutions to work together and provides the flexibility to integrate solutions from multiple companies. Understanding the various requirements and communication protocols that take place between those systems is critical for successful deployments.

Figure 4-1 shows the various components used in the solution and how they communicate to send/receive alerts and to enhance incident resolutions. In the center of Figure 4-1, the Proximex Surveillint receives events from multiple sources, including the Cisco Management Appliance, sensors, VSMS, ObjectVideo, and CPAM. Surveillint listens to these events and based on an individual event or correlation of the events, it triggers IPICS for first responders to collaborate or triggers AtHoc to quickly send a mass notification to a large number of users and devices.
Cisco Video Surveillance

Video Surveillance Media Server

The Video Surveillance Media Server is the core component of the solution, providing for the collection and routing of video from IP cameras to viewers or other Media Servers. The system is capable of running on a single physical server or distributed across multiple locations, scaling to handle thousands of cameras and users.

Figure 4-2 shows how IP cameras send a single video stream to the Media Server. The Media Server is responsible for distributing live and archived video streams to the viewers simultaneously over an IP network.
For archive viewing, the Media Server receives video from the IP camera or encoder continuously (as configured per the archive settings) and sends video streams to the viewer only when requested.

In environments with remote locations, this becomes very efficient because traffic needs to traverse the network only when requested by remote viewers. Remote traffic remains localized and does not have to traverse wide area connections unless it is requested by other users.

Video requests and video streams are delivered to the viewer using HTTP traffic (TCP port 80).

**Video Surveillance Operations Manager**

The Operations Manager is responsible for delivering a list of resource definitions, such as camera feeds, video archives, and predefined views to the viewer. After this information is provided to the viewer, the viewer communicates directly with the appropriate Media Server to request and receive video streams. Viewers access the Operations Manager via a web browser.

Figure 4-3 shows the traffic flow of video requested by a viewer.

After the user authenticates to the Operations Manager, the user is presented with a list of predefined views, available camera feeds, and video archives, based on defined access restrictions. From this point forward, the user interacts directly with the Media Server to retrieve video feeds. The connection remains active until the OM Viewer selects a different video feed.
The Media Server acts as a proxy between the camera and the viewer, who receives video feeds over TCP port 80 (HTTP). If another OM Viewer requests the video from the same IP Camera, the Media Server simply replicates the video stream as requested, and no additional requests are made to the camera (each feed is sent via IP unicast to each viewer).

To allow video streams to flow between the Media Server, edge devices, and viewers, the proper security must be in place to allow TCP/UDP ports to traverse the various subnets or locations.

**Distributed Media Servers**

Figure 4-4 shows a deployment with several remote locations, each with a local Media Server acting as the direct proxy and archive for local IP cameras. In this scenario, all recording occurs at the remote sites and live video streams are viewed by OM Viewers and VM (video walls) Monitors at the headquarters. OM Viewers can also be installed at remote locations to allow operators to view local camera feeds. The traffic remains local to the site, unless the viewer selects video from remote cameras.

![Figure 4-4 Distributed Media Servers](image)

A single Operations Manager is able to manage video resources from all locations.
The Media Server at the headquarters can also have parent-child proxies to each remote Media Server and request the remote streams only when required at the headquarters. This would have less bandwidth impact when the same stream is requested by more than one viewer, because the traffic would be contained locally in the headquarters LAN.

### Cisco Physical Access Control

The Cisco Physical Access Control solution benefits from a distributed architecture while lowering deployment and operational costs. CPAM is centrally located at the Command and Control center and is able to manage thousands of gateways installed at remote locations. Through CPAM, a user can configure the policy for any physical access gateway. For example, a main building entrance door may remain locked after hours while it may be unlocked during normal business.

### CPAM and Proximex Surveillint

Physical access gateways report an event, such as a forced entry or multiple invalid access attempts by the same card, to CPAM. CPAM can send events to as well as receive actions from other applications. In this design, CPAM sends events to Proximex Surveillint. Proximex Surveillint decides what actions to take based on the alerts it receives. For example, if there is a chemical leak alert in building 1, Surveillint sends "disable access for regular employees for building 1" to CPAM. **Figure 4-5** shows the interaction between CPAM and Surveillint.

**Figure 4-5 Interaction Between CPAM and Proximex Surveillint**

The Cisco Physical Access Gateway and CPAM exchange information through an encrypted protocol over MAN or WAN. While the traffic is light, a QoS policy is required to guarantee this important traffic during congestion.

The CPAM server can have a redundant CPAM server in a Linux high-availability mode so that if the primary server fails, a redundant server is available to continue operations. However, if CPAM fails or the WAN connection goes down, the Cisco Physical Access Gateway continues providing normal card reader access. Also, the gateway will be able to perform the device I/O rules even without CPAM. Therefore, a door forced open or door held open event can cause an output alert to be triggered on the gateway locally.

Other input alerts from the gateway, such as a glass break sensor or duress signal, can trigger the output alert locally. The input alerts trigger the local output alarm using the device I/O rules similar to the door forced open example.
IPICS

This section includes specific functions of IPICS components, interactions of IPICS components, difference between policy and incident response, and high availability.

Specific Functions of Each IPICS Component

The IPICS solution is modular and each component performs a specific function. The gateway converts radio frequency to IP multicast packets, at which point the RMS mixes these packets so they can be transported over the WAN. IPICS servers control which packets are converted or mixed, and configures RMS dynamically according to the virtual talk group (VTG) configured by a user. Figure 4-6 shows the functions performed by each component.

Figure 4-6 Specific Functions of each IPICS Component

A user configures “arson response group” on IPICS server to include channel for police department and channel for fire department

An LMR gateway converts voice traffic from the police department and fire department to two streams of IP multicast packets respectively.

RMS mixes the two streams of IP multicast packets.

Select Components for IPICS

The functions that a customer chooses determine what components are needed. The list includes an IPICS server, an LMR gateway, RMS, and Cisco Unified Communication Manager (CUCM). Three scenarios are depicted below.

Scenario 1—Radios at Two Locations Need to Communicate

If a customer has two sites located in Boston and Bangalore, and the radios communicate over the same channel, only an IPICS server and LMR gateways are needed, as shown in Figure 4-7.
**Scenario 2—Multiple Channels**

If more than one channel is used, a virtual talk group is required, as shown in Figure 4-8. Various types of radios with unique frequencies go through the LMR gateway. The various frequencies of the radios are converted to IP multicast packets. RMS mixes them into one virtual talk group.

**Figure 4-8 Virtual Talk Group Consists of More than One Channel**

**Scenario 3—Push-to-Talk Service of Various Types of Phones**

Push-to-Talk (PTT) is required for this communication scenario, as shown in Figure 4-9. To support land lines and cell phones, the dial engine option is required.
Interaction of IPICS Components

IPICS server is the primary component required for deployment. It drives the interaction with the LMR gateway, RMS, and CUCM as described below:

**Step 1** IPICS server and the LMR gateway configuration:

On the LMR gateway, configure a multicast address for each channel. On the IPICS server, configure the same multicast addresses. It is not necessary for the IPICS server and LMR gateway to know the address of the other device.

**Step 2** IPICS server and RMS configuration:

On the IPICS server, configure how the authentication type for the RMS router, as shown in Figure 4-10. The RMS router does not need to know the IP address of the IPICS server.
Step 3  IPICS server and CUCM configuration:

The IPICS server and the CUCM system need to be configured with the proper IP address of the other device. Configure the IP address of CUCM on the IPICS server under “Dial Engine”. See Figure 4-11.
Step 4  In CUCM, create a SIP trunk and point to the IPICS server. See Figure 4-12.
In CUCM, create a Route Pattern. Figure 4-13 shows that extension 1010 has been created for IPICS.

When a user dials extension 1010, a SIP trunk to the IPICS server is created. When a user picks up the extension, an interactive voice response (IVR) will announce “This is IPICS calling. Please enter your credentials”. After the user enters user ID and PIN, it will announce that the user has joined VTG “first responder”, then instructs the user to “press 1 to talk; press 2 to listen”.
Deployment Models

Deployment models include single site models and multiple site models, depending on whether a WAN is used or not. For more details, refer to the Cisco IPICS Deployment Models section of the IPICS SRND listed in Appendix A, “Reference Documents.”

For smaller deployments, the LMR gateway and RMS typically reside in the same router. For large deployments, a best practice is to separate the functions.

If there are small numbers of radio, the LMR gateway can be installed in the data center. Otherwise, the LMR gateway should be installed near the radios. An LMR gateway can support up to six ports. Each port supports one channel. For each channel, there can be hundreds of unique end-user devices.

Use Remote IDC

In IPICS 4.0, a user can use IPICS dispatch console (IDC) installed on a laptop to interact with other radio and phone users. IDC replaces the previous Push-to-Talk Management Center (PMC) client on IPICS 2.2. In normal use, users in the field use mobile devices (a radio or a phone) while an operator uses an IDC. The IDC has two phone lines. An operator can use it to call a security officer’s mobile phone and then transfer the officer’s line to a talk group. The operator can upload video, the same as a user with a mobile phone.

A user working outside the multicast domain can still be included in the calls. In this case, the user would VPN into the network and RMS converts the unicast packets from this user to multicast IP packets. This is called Remote IDC.

Policies and Incident Responses

A user can configure a policy on the IPICS server to specify a talk group for an incident. The policy can be triggered by other applications, such as Proximex Surveillint. Configuring a policy for each type of incident allows fast response. For example, for fire, configure a policy to include the fire department and a dispatcher in the talk group; for chemical detection, configure a policy to include chemical response personnel and a dispatcher in the talk group. However, the policy-driven talk group does not allow to add additional first responders or allow video upload. The solution is to use policy and incident response at the same time. For instance, when a chemical detection policy is triggered automatically, the dispatcher creates an incident response and adds the current talk group. From that point, more people can be added to the talk group, and video sharing is also allowed.

An alternative is to report all incidents to a dispatcher. According to a specific incident, the dispatcher executes a policy or selects a collection of videos, sensor events, and access events, and then creates an incident response that displays on the IPICS Dispatch Console and pushes out to the Mobile Client.
Multicast, Quality-of-Service, Security

Multicast needs to be enabled to run IPICS. Cisco recommends using bidirectional PIM for Cisco IPICS. If the IPICS dispatch console is connected over a Wi-Fi, the Wi-Fi network does not need to support multicast.

Quality-of-Service (QoS) is recommended in LAN and WAN environments for high quality VoIP using the following best practices:

- Classify voice RTP streams as expedited forwarding (EF) or IP precedence 5 and place them into a priority queue on all network elements.
- Classify voice control traffic as assured forwarding 31 (AF31) or IP precedence 3 and place it into a second queue on all network elements.

In addition, IPICS 4.0 supports video sharing among users. For QoS on real-time streaming traffic, see the Network requirements section in the Cisco Digital Media Suite 5.2 Design Guide for Enterprise Medianet at http://www.cisco.com/en/US/docs/solutions/Enterprise/Video/DMS DG/DMS DG.html.

Integration between the IPICS server and RMS and integration between the IPICS server and CUCM are password protected. Triggering IPICS also requires authentication.

For details on multicast, QoS, and security, refer to the “Cisco IPICS Infrastructure Considerations” chapter in the IPICS SRND listed in Appendix A, “Reference Documents.”

High Availability

High availability (HA) has not been tested in this solution. This section provides an overview and points to related documents. To achieve HA, a secondary IPICS server and a secondary RMS are deployed. Because there is no redundant LMR gateway, a key first responder should be equipped with a radio and a cell phone. If the LMR gateway is down and the radio cannot be used, this person can use the PTT service of a phone, practically using a phone as radio. Because there is no redundancy for the LMR gateway, it should be monitored (for example, Cisco MAP), so that an alert can be generated in case of failure.

IPICS 4.0 supports HA of the IPICS server. If there is more than one data center, a secondary IPICS server should be placed in the secondary location. This ensures recovery not only from hardware failure of the primary IPICS server but also from a building failure (such as a power loss). To configure HA for IPICS, a user specifies the IP address of secondary IPICS server, as shown in Figure 4-14. The IPICS servers periodically synchronizes configuration changes. When there is no heartbeat from the primary server, the secondary server takes over.
For RMS HA, see the section “Redundant RMS Configuration” in the “Cisco IPICS Infrastructure Considerations” chapter of the Solution Reference Network Design (SRND) for Cisco IPICS (listed in Appendix A, “Reference Documents”).

For IPICS compatibility with CUCM, IP phones, applications, see http://www.cisco.com/en/US/products/ps7026/products_device_support_tables_list.html.

**Digital Media Player**

Digital Media Players (DMP) decode and display unicast VoDs and multicast live streamed video as well as Flash content. DMPs connect directly to large format displays through HDMI. Other output connections are available but normally not used. DMPs may be centrally controlled by a Digital Media Manager (DMM) or can be used in a standalone mode, receiving content directly from a Web Server.

**DMP Specifications**

Table 4-1 shows the different capabilities and differences between two Cisco DMP models: the 4305G and 4400G.
Jitter buffer—The jitter buffers in the DMPs are sufficient to deal with even extreme cases of jitter for live streams. The only reasonable scenario for failures resulting from exceeding the jitter buffer is when the jitter from streaming HD VoDs exceeds 1000 ms. A properly designed network should not allow this threshold to be exceeded.

Multicast support—The DMPs join multicast MPEG-2 and H.264 streams as the only method of displaying live streaming video. DMPs support Internet Group Management Protocol (IGMP) v3, although a multicast source cannot be defined when defining multicast streams or channels within the Cast interface. This means that source-specific multicast cannot be fully implemented directly from the DMPs, and that all multicast join messages are sent as (*,g) messages.

Video support—The following are common video formats:

- MPEG-4 Part 2—A video compression technology developed by the Moving Picture Experts Group (MPEG). It belongs to the MPEG-4 ISO/IEC standard (ISO/IEC 14496-2). It is a discrete cosine transform compression standard, similar to previous standards such as MPEG-1 and MPEG-2. Several popular codecs, including DivX, Xvid, and Nero Digital, are implementations of this standard.
- MPEG-4 Part 10 (H.264)—H.264 is a standard for video compression, and is equivalent to MPEG-4 Part 10 or MPEG-4 for advanced video coding (AVC).
- WMV9/VC-1—Windows Media Video 9 (WMV9) is a common Windows media format now supported for VoD playback only. WMV9 supports variable bit rate, average bit rate, and constant bit rate, as well as several important features including native support for interlaced video, non-square pixels, and frame interpolation.

These formats are supported by the various Cisco DMPs as follows:

- Cisco DMP 4305G—Supports standard MPEG-2 streams (HD or SD) as well as the rarely used MPEG-4 Part 2. DMP 4305G does not support H.264.
- Cisco DMP 4400G—Supports standard MPEG-2 streams (HD or SD) as well as MPEG-4 Part 10, also known as H.264. WMV9 is also supported for VoD playback only.

The bandwidth requirements range between 1.5 and 25 Mbps, depending on several factors including whether the video is SD or HD and what codec is used.

Flash application support—Flash applications are used with Cisco Digital Signs to display content. The DMP 4400G introduces Flash 10 support, while the 4305G is limited to Flash 7.
Bandwidth Requirements

Digital Signs use the DMP to deliver live and pre-recorded streaming content to displays. Bandwidth used per stream is 1.5 to 5 Mbps for standard definition streaming video content, and 8 to 25 Mbps for high definition streaming video content. With Cisco Digital Signs, streaming video content may be placed on a portion of the screen, with the remaining screen being used by Flash or media content such as information tickers, advertisements, images, or any other non-streaming content supported by the DMPs.

Video resolution can be reduced for partial coverage of the screen. Reducing displayed video resolution allows the reduction of encoded stream resolution, lowering the bandwidth requirements.

Latency Requirements

For live streaming content, moderate latency does not have a significant impact. Significant latency is rarely encountered with the large multicast streams sent to the DMPs because they are normally implemented in a campus environment.

For pre-recorded video content, moderate latency does occur. Pre-recorded content is streamed through HTTP or RTSP-T, with large bandwidth demands because of the TCP mechanisms for transport. This process reduces the throughput maximum as latency increases, regardless of how much bandwidth is available.

With TCP parameters set to optimal levels, tolerances for latency are still quite stringent because of the throughput needed. For SD video, latency must be less than 100 ms round trip. For HD video, latency must be less than 60 ms round trip. Delay beyond these thresholds causes the TCP data stream to slow because of the two-way acknowledgement-based communication.

Packet Loss Requirements

For live streaming content, lost packets are not retransmitted, and with the amount of compression used by the video codecs, even a single packet lost results in degraded video quality. Avoiding any packet loss is the highest priority for live streaming video. With certain configurations, packet loss of 0.001 percent may be considered unacceptable over an extended period of time.

The avoidance packet loss is the single most important factor when implementing live video with Cisco Digital Signs. Any packet loss may be visible and severely impact the video and audio quality of all DMPs experiencing that packet loss.
ObjectVideo

ObjectVideo monitors video feeds for events and generates alerts in real time as events take place. The ObjectVideo Intelligent Sensor Engine (ISE) server receives the video feeds from the Media Server for monitoring through the available DirectShow filter. The components listed below could be run on the same or on separate machines. Components talk with each other through the communication layer provided by ObjectVideo Communication Daemon software.

Server software:

- **ObjectVideo Server**—The ObjectVideo Server software routes information among the components. The ObjectVideo database stores alerts and other system data and is typically installed on the same machine as ObjectVideo Server.
- **ObjectVideo ISE**—The ISE software runs on a server that meets the ObjectVideo recommended minimum hardware requirements. Video is fed to the ISE “sensors” to process the video stream in real time and monitor the video for events based on the rules defined. Once the Cisco 4500 Video Surveillance IP Camera supports the embedded analytics, the overall server count will be reduced, providing more flexible deployment architectures.
- **Alert Bridge**—The Alert Bridge software is the service that runs URL forwarder plug-in which enables real-time http triggers to VSOM.

Client software:

- **Alert console**—The Alert Console displays alerts as events occur and allows for searching of alerts.
- **Rule management tool**—The Rule Management Tool is used to set up rules for the sensors. The rules define the security policies that, when violated, generate events.

Figure 4-15 shows how video feeds from IP cameras are sent to the Cisco Media Server for live viewing and archival. The ISE server in turns analyzes the video streams for specific events and generates alerts.

*Figure 4-15 System Components*
Figure 4-16 shows how servers may be deployed to support a large number of locations. In this case, video feeds are analyzed by each local ISE server and when alerts are generated, they are sent to the central command and control location, where alerts may be reviewed or sent to other systems, such as Proximex Surveillint or VSOM.

ObjectVideo provides several applications that provide guidance for planning and maintaining an ObjectVideo system. These tools include the following:

- **ObjectVideo Integrator Toolkit**—The ObjectVideo Integrator Toolkit contains several software applications used by customer support personnel and integrators to plan for, maintain, and troubleshoot the ObjectVideo system. The ObjectVideo Integrator Toolkit applications are also used to improve event detection and reduce false alarms.

- **Camera Placement Tool**—Used to determine the ideal camera location and settings to optimize event detection.

- **Object Sizing Tool**—Used to determine the size (in pixels) of objects within a camera’s field of view. It allows you to determine whether objects of a certain size will be reliably detected by a sensor.

- **Parameter Configuration Tool**—Used during advanced troubleshooting tasks to improve event detection. The Parameter Configuration Tool allows you to access parameters that determine how events are detected by each sensor. The Tool is also used for some advanced configuration tasks.

**Video Feed Requirements**

By default, ObjectVideo software processes video at QVGA or CIF (NTSC or PAL). Other sizes are also supported; however, processing larger video frame requires more resources. IP video is being processed using DirectShow multimedia framework.

Table 4-2 shows the recommended system options for ObjectVideo deployments. The number of sensors or channels supported by a server is critical when designing new systems.
Proximex Surveillint

Proximex Surveillint serves as central command and control center of the security environment. It integrates information and data from each component of the Cisco physical security solutions suite, including Cisco Video Surveillance Manager, Physical Access Manager, Cisco IPICS, and ObjectVideo. Surveillint provides an open platform to enable new technologies and systems to be integrated together as needed.

Surveillint’s solution includes several components that may be distributed to provide a highly available environment to support a large number of users and locations.

Server Software

Server software may be run on a standard Microsoft Windows server or on fault-tolerant servers. Surveillint can also run in a warm or hot-standby configuration providing redundancy and high availability. Additional servers can be added to provide this level of redundancy and failover.

Client Software

Multiple clients can be operated simultaneously with a server.
- Operator client
- Administrator client
- Windows Mobile PDA client
Integration Modules for Connecting with Subsystems

In addition to integrating with Cisco physical security systems, Proximex offers a library of more than 90 Integration Modules, supporting different manufacturers and models of video systems, access control systems, IT health monitoring systems, fire systems, intrusion alert systems, video analytics systems, intercom systems, computer-aided dispatch (CAD) systems, intercom systems, radar systems, sonar systems, chemical/biological sensor systems and more, as shown in Figure 4-17.

Figure 4-17 Integration Modules

Because Surveillint supports Cisco physical security technologies, a fully integrated security solution significantly improves information sharing between Cisco technologies and other related systems as part of the security ecosystem.
High Availability

Surveillint's Web Services-based Service-Oriented Architecture using Microsoft .NET technology provides operational redundancy across all of its components. To provide high availability, Surveillint supports a redundant multi-site and multi-hierarchy architecture. The redundancy is achieved by:

- **Database redundancy**—Microsoft SQL Server 2005 or 2008 failover cluster and/or database mirroring solution for SQL Server 2005 or 2008 can be used. Additionally, the Surveillint user interface communicates with the backend components using web services, which can be configured to automatically connect to another database if there is a problem with the main database. The backup database server can be at either the local site or a remote site.

- **Web services redundancy**—Surveillint's middleware components are also built on web services that can be set up to run on multiple computers for redundancy and scalability.

- **Application server components redundancy**—A cluster server approach (such as either the NEC ExpressCluster or Microsoft Cluster Server) can be used for any and all Surveillint application server components. Other approaches, such as asynchronous synchronization and scripted failover, can also be used for disaster recovery approaches.

- **Stateless user interface component**—The user interface component is stateless and multiple instances of the user interface (consoles) can run simultaneously. There is no functional limit to the number of workstations that a Surveillint solution can support. The consoles connect to the redundant web services and failover automatically as required.

Distributing Surveillint Components

Surveillint’s flexible architecture may be scaled from a single server to a large deployment, distributing components across multiple sites.

Figure 4-18 shows how the various server components may be installed in multiple instances to support multiple locations. Multiple Operation Consoles (or Administration Consoles) are supported. Each of these instances points to an instance of the Surveillint Web Service. Multiple instances of the Surveillint Web Service may be installed if required to increase load balancing for servicing requests from the Operation Console.
Multiple instances of the Surveillint Integration Modules may be deployed to service interactions with external systems such as Cisco Physical Access Manager, AMAG Symmetry, Lenel OnGuard, SoftwareHouse CCure, Hirsch Velocity, and so on.

**AtHoc IWSAlerts**

**User Requirements**

When designing an AtHoc IWSAlerts solution, the following requirements should be gathered first:

- Number of users to be supported
- Delivery speed requirements
- Type of end devices to be supported
- Whether single site or multiple sites are to be supported, and high availability requirements

**Functions of AtHoc IWSAlerts Servers**

The AtHoc solution is quite modularized and is comprised of both server- and client-side components. The servers include: IWSAlerts DB server, IWSAlerts Unified Notification System (UNS) Application server and IWSAlerts Notification Delivery System (NDS) servers.

AtHoc IWSAlerts server system configuration is composed of the following three server components:

- Database server using Microsoft SQL Server 2005/2008
- UNS application server(s) serving as a web-based application server and job processing server for all logical frameworks (platform, applications, integration, and delivery)
- NDS application server(s) serving as notification delivery gateway function to advanced communication channels, such as Cisco UCM, SMS, or SMTP

A UNS IWSAlerts application server may also be running delivery gateways (NDS) to external delivery systems and services, such as Unified Communication systems or SMTP. The separation to architectural components allows for greater deployment flexibility, depending on customer use case and existing network topology scenarios. In some cases, the NDS function can also be served from the cloud, as a hosted service to provide advanced delivery capabilities.

Although all components can be installed on the same machine, in production environments the database server and the application server are usually separated, and several application servers are deployed in a web farm fashion for scale and redundancy.

Figure 4-19 shows the AtHoc IWSAlerts architecture diagram with CUCM integration.

In a high availability (failover) architecture, a similar AtHoc IWSAlerts server system will be installed and configured in a remote site, to provide service upon failure of the primary system.

Additionally, AtHoc IWSAlerts architecture contains the following elements:
- Communication services—AtHoc provides hosted alert delivery services to deliver voice telephony and text messaging (E-mail and SMS) via scalable and highly available data centers. An account setup and provisioning is required to use the communication services.
- Desktop notifier (NAS)—Small footprint Windows and Mac compatible personal desktop notification application; this component is usually installed on every user computer (desktop, laptop) in the organization using a centralized desktop configuration management system, and provides audio/visual notifications to end users.
• AtHoc IP Integration Module (IIM)—Network appliance allowing integration with legacy non-IP supporting alert delivery systems such as indoor and outdoor public address systems; this component is installed near the interconnected system.

**Deployment Models**

AtHoc IWSAlerts system architecture is designed to support flexible deployment configurations, answering different needs and customer requirements (see Figure 4-20).

![Flexible System Architecture](image)

The flexibility is designed in multiple dimensions, covering the IWSAlerts server(s) system, the failover (alternate) system, and the alert delivery (communication) systems.

• Single site-based installation—Hardware and software applications are physically installed at the customer site, and then share specific resources within the organization. Such shared resources may be an Active Directory that is maintained centrally, or centralized telephony alerting capability (i.e., enterprise wide UCM and/or a commercial telephony alerting service).

• Site-by-site with cascading alert capability—Similar to above, but with ability to inter-connect the systems at different sites in a way that “cascades” an alert from one site to another. This capability allows a system based in Virginia to activate a system based in California and vice versa.

• Centralized enterprise—Hardware and software applications are physically installed in a centralized location. The IWSAlerts application is then configured to support multiple local instances (multi-tenancy) of the application which run on the same (centralized) servers, giving each site exactly the same operational control and functionality it would have if they were running it on their own hardware locally.

**Scalability**

By supporting web farm server configurations, AtHoc IWSAlerts UNS and NDS components cater for scaling up operations, by employing additional application servers to handle service requests and background processes.

Typically, a single AtHoc IWSAlerts system with two dual-quad core CPU application servers can handle up to 20,000 concurrent NAS (desktop alerting) users with a three minute polling period, usually equivalent to 30,000 to 40,000 actual users (considering typical network concurrency rates). In a similar way, such a single IWSAlerts system can handle up to 200,000 users when working with telephony and text alerts.
For very large organizations, more than one AtHoc IWSAlerts system can be installed, while portioning the users serviced by each system. The IWSAlerts inter-system cascade support, the multiple IWSAlerts system can be cascaded to provide single action activation across the organization in a transparent manner. This way IWSAlerts cascaded system can support alerting to hundreds of thousands to millions of users from a single unified console.

**High Availability**

AtHoc IWSAlerts application server design supports internal redundancy configuration to prevent single point of failure:

- The application servers can be installed in a web farm configuration behind a load balancer, to allow multiple application servers to service incoming requests and process background jobs in a completely transparent redundancy. The application server configurations are completely identical, and if one is down, others take over its service requests. This configuration also allows for greater scalability by distributing load across multiple application servers.
- The database server can be installed in a clustered environment, maintaining internal redundancy for high availability.
- Critical installations use other redundant components to ensure no single point of failure; these include redundant load balancer, IP switches, redundant power supplies from separate power circuits, and internal RAID storage configurations. An advanced high availability configuration uses two or more identical sites, configured in an active-passive manner with online data replication between the sites and active monitoring to start the alternate site operation when a primary site fails.