WHITE PAPER
Intel® Active Management Technology
Retail Industry

Wireless Intel® Active Management Technology for Digital Signage and Retail Whitepaper

Introduction

Digital signage and retail computing devices (vending, ATMs, POS, etc.) are everywhere, such as in stores, gas stations, airports and outdoors. Although deploying and managing these devices can be expensive and complicated, Wi-Fi connectivity and wireless Intel® Active Management Technology (Intel® AMT)[1] are being used to significantly lower system deployment costs and simplify their management.

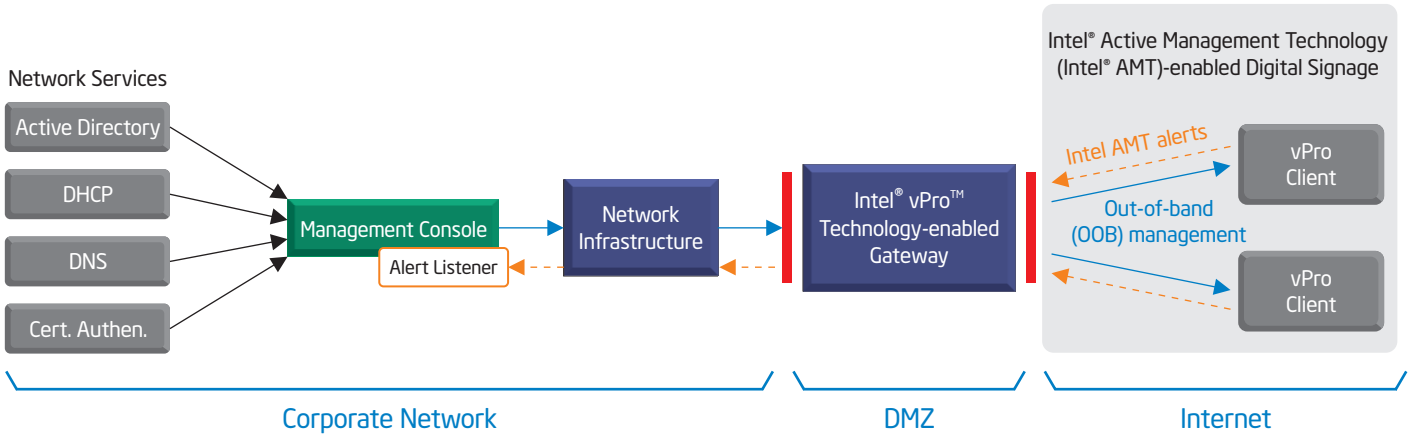
This paper is a technical 'How to' for deployment of an Intel AMT infrastructure and client configuration for digital signage and retail computing. The configuration methods, such as device set up, are not limited to the steps presented in this paper. The configurations described here are for a simple and scalable solution that is proven to work.

Benefits of Wireless Intel® AMT for Digital Signage and Retail

Before describing the technical details of this type of deployment, the following is a brief description of some of the benefits that Intel AMT, and specifically wireless (Wi-Fi) Intel AMT, can bring to your organization:

- All the features of Intel AMT, including out-of-band (OOB) communication, watchdogs/agent presence, heal, remote shutdown/turn on, 3rd Party Data Storage (3PDS) and Intel AMT security features, etc., but with the flexibility of system placement with no concern and cost of deploying LAN connectivity. In contrast, wired networks often constrain where systems can be placed in the store.
- Ability to place digital signs and retail systems, such as POS terminals, where they are most effective and not based on the infrastructure. No major infrastructure changes are needed, which reduces the number of required approvers, which could include chain management, landlords, local authorities, etc. The only requirement is an electrical connection, which is always more prevalent than LAN infrastructure.
- Ability to move signage and retail systems according to store needs at any time. Systems can be deployed anywhere within signal range of the access point, thereby increasing placement flexibility.
- Connectivity can be through the store's Internet/intranet network or via the public Internet, while maintaining full security on the systems.
- Remote management of networked embedded devices lowers IT support costs by reducing the number of onsite visits traditionally required to diagnose and fix problems. Now, with the advanced manageability and maintenance features of Intel AMT, it's possible to query, restore, upgrade and protect devices remotely, even when they are not functioning, are powered off or experiencing software failures (see link).
- Since devices can be diagnosed remotely, software issues can be repaired over the wireless connection and failed hardware components identified in advance, and technicians arrive with the appropriate parts in hand. Remote on/off switching allows companies to shut down devices after hours, thereby reducing utility costs. Software and hardware inventories can also be conducted remotely.
- Gain a reduction in total cost of ownership (TCO) with no need for local IT support. This is a big benefit when systems go into franchised retail stores that have no desire or need to manage these signs. Using wireless Intel AMT, the signage integrator or the central IT department of the parent company can remotely manage all aspects of the system. Remote diagnosis and hardware information acquisition can reduce on-site visits and system downtime.
- 3PDS access in all situations (offline/out of band) and connected online.
- For more information about Intel AMT in embedded systems, see **link**.

Table of Contents



vPro Client: Intel® vPro™ Technology-enabled Client

Figure 1. Digital Signage Deployed Outside the Corporate Network

Paper goal and target audience

This is a straightforward guide to implement Intel AMT and Intel® vPro™ technology-enabled gateway for digital signage application; however, it does not cover the entire scope of wireless Intel AMT and client initiated remote access.

After implementing this guide, you will have a working infrastructure to deploy and manage a proof-of-concept (POC) of remotely located, Intel vPro technology-enabled clients.

The target audiences are IT engineers tasked with networking and security, application engineers deploying and creating management solutions, and configuration engineers deploying remote clients for the digital signage field.

This whitepaper covers the YCD proof-of-concept only. Those following the procedure described here will configure a system that will be remotely accessible and repairable in case of a major issue previously requiring a technician visit. The paper does not cover all the available functionality of Intel AMT, CIRA, Wi-Fi and MPS; in other words, the products mentioned have much more functionality than discussed in this document. The paper covers the tools and steps required to get the system off the ground and demonstrate the potential return of investments. Readers are encouraged to seek additional information at the **vPro Expert Center**.

Architecture of a Digital Signage Solution Based on the Intel® AMT and Intel® vPro™ Technology

Digital Signage Deployed Outside the Corporate Network - Client Initiated Remote Access (CIRA)

When clients are deployed outside the corporate network, as illustrated in Figure 1, the security objective is to limit access only to authorized devices. The solution is the introduction of an Intel vPro technology-enabled gateway in the demilitarized zone (DMZ). The Intel vPro technology-enabled gateway is the traffic broker for all the client's Intel AMT management communication to/and from the enterprise. All Intel AMT management connections are initiated by the clients, referred to as "Client Initiated Remote Access" (CIRA).

Remote Access Client Connection Process Description: (see Figure 2)

1. The client calls Intel® vPro® technology-enabled gateway (aka MPS) to trigger a connection.
2. The Intel vPro technology-enabled gateway authenticates with the client and creates a secure tunnel.
3. The Intel vPro technology-enabled gateway notifies the management console that it holds an Active connection with the client.
4. The management console connects to the client through the gateway and manages/fixes the remote system.

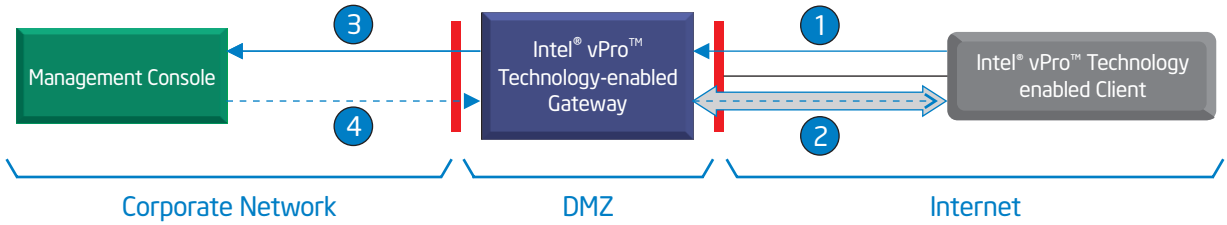


Figure 2. Remote Access Client Connection Process Description

Functionality of the Intel® vPro™ Technology-enabled Gateway

The Intel vPro technology-enabled gateway has the following functions:

1. Respond to client's connection request and create secure tunnel.
2. Notify the management console that the connection has been opened (or closed).
3. Act as a proxy to all Client<-->Management Console traffic (forward traffic).
4. Provide a list of currently connected clients.

The Intel vPro technology-enabled gateway can either be downloaded from the Intel website (as part of the Intel vPro technology SDK package) free of charge or be purchased from a third party independent software vendor (ISV).

The focus of this chapter is configuration of the Intel provided Intel vPro technology-enabled gateway. This is available to download (**link**).

The Intel® vPro™ Technology-enabled Gateway Description of Services (Figure 3)

1. Stunnel – responsible for creating secure connection with the client Intel AMT firmware.
2. Management Presence Server (MPS) – responsible for all management traffic and notifications.
3. Apache – responsible for all WS-MAN traffic.

Note: The Intel vPro technology-enabled gateway has no awareness of the content of the traffic it forwards. However, it is aware of type of traffic (WS-MAN or SockesV5) as it needs to route it to the correct service (see next item).

A few conditions must be met in order for the client to find the Intel vPro technology-enabled gateway:

1. Intel vPro technology-enabled gateway's interface to the Internet:
   a. Stunnel listening port: FQDN: Port# must be visible on the Internet
   b. The client is configured with gateway's FQDN: port during provisioning
   c. FQDN of the Intel vPro technology-enabled gateway must be resolvable via external DNS
      - Static external IP of the Intel vPro technology-enabled gateway can also be entered but requires additional info in the provisioning profile
2. Intel vPro technology-enabled gateway's Interface to the enterprise

The Intel vPro technology-enabled gateway has two separate connections for communicating with the management console.

   a. SOCKSv5 traffic for Intel AMT redirection and keyboard-video-mouse (KVM) feature
   b. WS-MAN for all web services traffic (all other are Intel AMT commands)

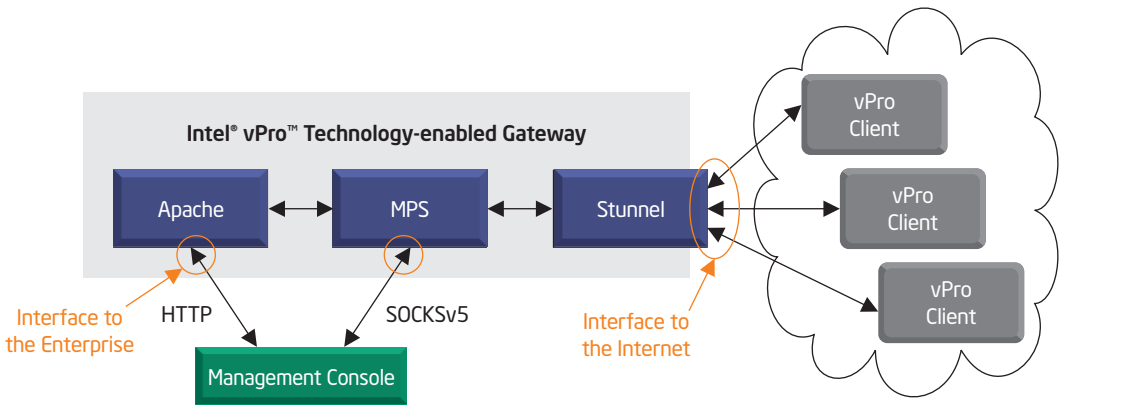


Figure 3. Intel® vPro™ Technology-enabled Gateway Description of Services

Using Intel AMT Over a Wireless Connection

For an Intel AMT-enabled device to be managed over wireless, it must be aware of the wireless network where it resides. With Profile Synchronization feature enabled, the OS automatically pushes the current wireless network parameters to Intel AMT.

Profile synchronization setup:

1. Ensure LMS service is installed
   a. LMS is the Intel AMT "Local Manageability Service" that is provided with the Intel AMT drivers package. It is usually installed by default on every Intel AMT-enabled client.
2. Download & install Intel PROSet (link).
3. The Full PROSet package (except GUI) must be installed.
   a. The 'drivers only' installation does not have the necessary API to support that feature.
   b. Install PROSet with MEPROFILESYNC=ACCEPT in the command line:
4. In the Intel AMT Provisioning profile:
   a. Check the "Enable Synchronization" box

What happens when a user profile password changed?

PROSet will NOT synchronize changes in the profile's password. The proper procedure to change profile password is:

1. First disconnect and delete the network from PROSet
   a. PROSet synchronization will remove the wireless profile from Intel AMT.
2. Create a new profile with the new password.
3. Upon connecting to that network, PROSet synchronization will add the profile to Intel AMT.

Intel AMT supports up to eight wireless profiles. What happens when the maximum number of profiles is reached?

When Intel AMT has already maxed out at eight user profiles, a newly synchronized network will override the profile that has not been used for the longest time.

Profile synchronization user acknowledgment: (Figure 4)

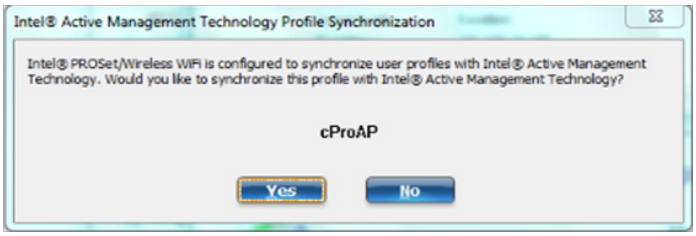


Figure 4. Profile Synchronization User Acknowledgement

Project Requirements and Preliminary Work Needed.

Background:

In this section, we'll layout the hardware, software and preliminary configuration requirements to make the POC operational.

Hardware Requirements for Intel® vPro™ Technology/ Wireless Intel® AMT-enabled Client System

In order to support Intel AMT, the client's motherboard, wireless card and processor all need to be Intel vPro technology-compliant; below is a current (October 2011) sample system/ processor configuration. Check support (link).

The recommend hardware sample is:

Suppported Desktop Board for Wireless Intel AMT Note: This table contains partial information and readers should consult the first URL link for up-to-date information.	
Intel® Desktop Board DQ67EP View all compatible Intel® processor for this Desktop Board	link
Supported Processors for Wireless Intel AMT:	
Desktop	
Intel® Core™ i7-2710QE	link
Intel® Core™ i7-2715QE	link
Intel® Core™ i5-2540M	link
Intel® Core™ i5-2500 Does not support WiDi or My Wi-Fi	link
Mobile	
Intel® Core™ i7-2860QM	link
Intel® Core™ i7-2640M	link
Intel® Core™ i5-2557M	link
Intel® Core™ i5-2540M	link
Wireless Card	
Intel® Centrino® Ultimate-N 6300, Dual Band	link
Intel® Centrino® Advanced-N 6205, Dual Band	link
Wireless Access Point Intel recommends using the 5 GHz spectrum band[1]	

Table 1. A Sample of Recommended Hardware Components

Intel vPro Technology-enabled Gateway Management Presence Server (MPS) requirements

The MPS gateway is a networking and CPU-focused server, storage is needed only for logfiles and OS need:

- Required KVM bandwidth needs to be 512 Kbps symmetric connection for each active KVM session.
- OS is Microsoft* Windows* 2003.
- 1 TCP/TLS port need to be open to the outside (firewall rule).[3]
- 2 HTTP/SOCKS need to be open from the local network to the MPS (firewall rule).
- SNMP and HTTP ports need to be open from the MPS to the alert management servers (firewall rule).
- An external DNS entry needs to point to the MPS.
- A web server certificate is needed, pointing to the above DNS FQDN and signed by a known CA.[4]

Certificate Authority requirement for Remote Access:

Client authentication with the Intel vPro technology-enabled gateway is TLS (certificate based).

1. A Certificate Authority (CA) must generate a web server certificate for the Intel vPro technology-enabled gateway, and the root certificate of that CA must be installed on each Intel vPro technology-enabled client.
2. If the optional Mutual Authentication is selected, an authentication certificate must be generated also for each client.
3. For IT environments with CA already in production, simply generate the certificates from the CA
4. For environments without CA, a temporary CA must be installed. Generate and save the two required certificates: Web Server Cert for MPS & Root Cert. Once the certificates are generated and saved to a file, the temporary CA can be shutdown. If certificate-based mutual authentication is selected, this CA must be available any time a new client is provisioned (since it needs to generate an authentication certification for that client).

Provisioning area / Staging area requirements

In order to support provisioning of the Intel AMT-enabled device in the staging area (before the Intel vPro technology-enabled device is shipped to the final external location):

- Intel SCS installed
- Windows AD enterprise certificate authority
- DHCP server
- An externally purchased Provisioning Certificate matching the SD Vendor provisioning server fqdn
- For more information about obtaining Intel AMT provisioning certificates, see **link**.

  This is a show stopper – start getting this certificate now!

  The Provisioning Certificate needs to be installed on the provisioning server OS certificate store on the OS account private store that runs the SCS service.

  - http://www.symantec.com/connect/articles/obtaining-and-applying-verisign-remote-configuration-certificate
  - http://technet.microsoft.com/en-us/library/cc431417.aspx

Configurations Walkthrough – Server Side

Background:

In this section, we'll discuss the necessary environment components to setup a digital signage solution for OOB management of clients that are either inside the IT network environment or outside the IT network (i.e, behind the corporate firewall). Since digital signage devices are by definition a non-user attendant device, response to issues must be triggered by automatic alerts generated on the client when an issue has been detected (for example, faulty HW, security breach, critical SW agent is down etc.). How these alerts are configured and generated will be discussed in the Use Case section.

Networking and firewall configuration overview:

Incoming TLS port: The MPS listens to the remote client via a TLS/SSL TCP port. This port needs to be open to all internal addresses (Authentication is managed in the MPS). This port is defined in the next section.

Incoming ports: The MPS listens to two ports for management traffic coming from the internal network: one is a HTTP port and the other is a SOCKS V5. These ports should be open to management traffic coming from the internal network and can be limited according to internal security procedures.

Alert Traffic: The MPS forwards Intel AMT alerts (SNMP and SOAP/WebService) to management watchdog/deamon servers. This traffic needs to be open from the MPS to the internal management servers (SNMP and configurable HTTP ports).

Notification Traffic: The MPS can send connect/disconnect messages to an internal management server. This traffic needs to be open from the MPS to the internal management servers (configurable HTTP ports).

Status Query traffic: The MPS can be queried via HTTP/WebService from the internal management servers. This traffic needs to be open to the MPS from the internal management servers (configurable HTTP ports).

All the above ports are fully configurable in the MPS, Stunnel and Apache configuration files – see the following for configuration walkthrough on how to manage those.

Preparing Certificates for Intel® vPro™ Technology-enabled Gateway:

Obtaining the required certificates:

1. Gateway Certificate:
   a. If obtained from an external vendor, ask for a Web server certificate with generated for the server FQDN that is running the Intel vPro technology-enabled Gateway.
   b. If generated in the local CA, see the following detailed steps.
2. Trust root certificate of the CA – download from the CA in PEM format.
   a. The Trusted Root certificate will be installed on every client during provisioning; this will be discussed in the Provisioning section.
   b. The same Trusted Root certificate will be installed on the Intel vPro technology-enabled gateway (MPS).

Generating Gateway web server certificate on local CA.

1. The CA need to be able to export the certificate private key – usually available only on Windows* 2003/2008 enterprise versions!
2. Open the certificate authority manager from the administrative tool.
3. Right click on "Certificate templates" and select manage.
4. Create a new template which is a copy of Web Server – mark the checkbox "Allow private key to be exported" and save the new template under a new name.
5. Go back to the certificate authority manager, right click on the Right click on "Certificate templates" and select new, then select the new template created just now.
6. On the CA server, open browser, type: HTTP://<My CA server FQDN> /certsrv
7. Select: Request a Cert —› Advanced certificate Request —› Create & Submit to this CA.
8. A form opens, in Certificate Template select "Copy of Web Server" in Name field, Enter the FQDN of the server for which this cert is created.
   a. Select key size 2K
   b. Make sure the box "Mark key as exportable" is checked
   c. Give a friendly name
   d. Submit
9. Once the CA server generates the certificate - click on "Install certificate".
10. Open Browser, go to certificates ->Personal contailer, select the cert, go to view —› details tab —›"copy to file".
    a. Select "Yes' to export private Key
    b. Select "Save as PFX" (none of the boxes checked)
11. Enter password.
12. Save file to a known location (file is saved in *.pfx format).
13. Run any script that converts pfx to PEM (various tools are available on the Internet).
14. Using wordpad, split the PEM file to two separate PEM files:
    a. The certificate itself (which includes Public key)
    b. Certificate with Private key only
    Note: Files include the header & trailer:
    "----BEGIN CERT----" & "-----END CERT----"
15. These two files will be copied to the Stunnel once the Intel vPro technology-enabled gateway is installed.
16. Export the CA trusted root certificate. This part does not require the private key and can be exported directly to a PEM file/format (use 'base-64 encoded X.509" format).

Installing the Intel vPro technology-enabled gateway:

Intel vPro Technology-enabled gateway installation involves the following steps:

1. Ensure the organization has an externally known FQDN with static IP that can be resolved and accessed from the Internet. (add an "A" record in the external DNS and open a TCP port in the Firewall). This is the address the client will connect to in order to request a connection.
2. Prepare certificates for Client Authentication (this will be discussed next).
3. Install all three components of the Intel vPro technology-enabled gateway (Apache, MPS, Stunnel)
4. Configure the TCP ports on all vPro Enabled Gateway components.

Installing the Intel vPro technology-enabled gateway components:

The gateway comprises three components:

Software piece	Function	Download from:	Version
Stunnel TLS	SSL tunnel provider	link	4.47
MPS.exe	Intel SDK provider of TCP/ Tunnel managememt & notification provider	link	7.0
Apache	Web server and Socket V5 translator	link	2.2.21

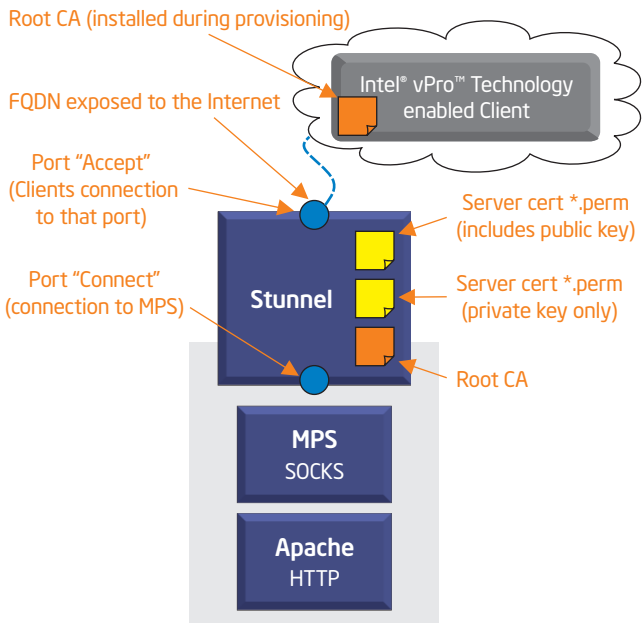


Figure 5. Stunnel Install and Configuration

Stunnel install & configuration: (Figure 5)

1. Run the supplied installer and select the default installation options.
2. Locate & edit the **Stunnel.conf** file under c:\program files\ STunnal

The file already contains most of the configuration parameters, excluding the following parameters that need to be configured:

a. **CAfile** = <path to the CA trusted root certificate file>
b. **cert** = <path to web server certificate *.pem file>
   See section above how to create that *.pem file
c. **key**= <path to certificate key *.pem file>
   See section above how to create that *.pem file
d. **accept**= <port that AMT device uses to connect to MPS>
e. **connect**= <ip:port that Stunnel will use to send the received data to MPS.exe>
   This address is also configured in MPS.config (see next section)

3. More details about Stunnel and its parameters can be found in http://www.Stunnel.org/

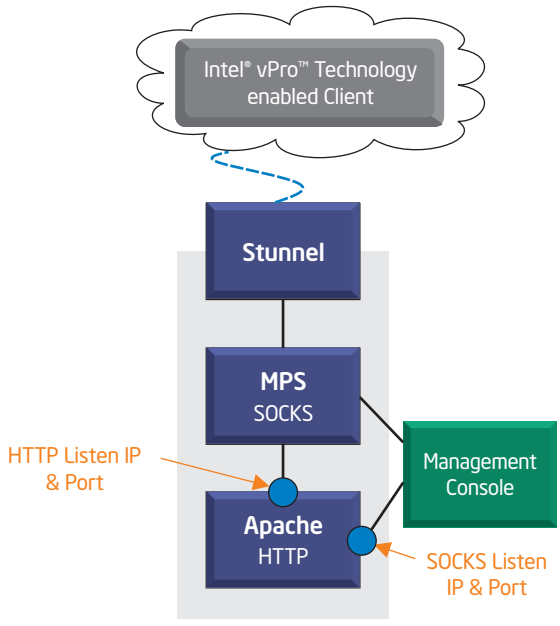
Stunnel.conf configuration sample

```
;Note: this config sample is all you need.
;debug = 7
;output = stunnel.log

cert =   c:\mps\CARootCert.pem
Key =    c:\mps\MyKey.pem
CAfile = c:\mps\MyPublic.pem
options = NO_SSLv2
options = SINGLE_ECDH_USE
options = SINGLE_DH_USE

[FromAMT]
accept  = 16994
connect = 127.0.0.1:16993
TIMEOUTclose = 10
```

Apache install & configuration: (Figure 6)

1. Run the supplied installer and select the default installation options.
2. From the Intel AMT SDK "Windows\Intel_AMT\Bin\MPS\" folder, copy (and overwrite if needed) **mod_proxy.so** and **mod_proxy_connect.so** files into the modules folder of the Apache installation path.
3. Edit httpd.conf: add / change the settings for:
   - Listen <IP : port> Binds apache to specific IP & port
   - ProxySosksIP=< listening IP addr for new SOCKS connection requests>
   - ProxySocksPort=< Listening port for new socks connection requests>
   - ProxySocksDnsMode <Remote/Local>
   - ProxySocksAuth <off/on>

Apache Configuration Example	
Listen	**8080**
ProxySocks	**On**
ProxySocksIp	**192.168.1.104**
ProxySocksPort	**4322**
ProxySocksDnsMode	**Remote**
ProxySocksAuth	**off**



Apache Configuration

Figure 6. Apache Install and Configuration

MPS installation (Figure 7)

1. **OS install:** The MPS was tested on Windows 2003. Install the OS and patch this according to your procedure. Note the MPS will be in a DMZ located machine; therefore, take appropriate steps to patch and protect it accordingly.
2. Copy the MPS directory from the SDK zip file (location: \Windows\intel_AMT\bin\MPS) to your server hard drive (c:\MPS)

MPS Configuration

1. Locate the MPS.config file under c:\MPS\conf
2. In the networking section:

[Network]

1. **AMTListenIP**=<listening IP addr for new connection requests>

   Same address entered in STunnel.conf in the "connect" parameter
2. **AMTListenPort**=<listen port for new Intel AMT connection

   Same port entered in STunnel.conf in "connect" parameter
3. **SocksListenIP=**<listening IP addr for new SOCKS connection requests>

   Some of the incoming SOCKS connections come through Apache. Use the same address as one entered in httpd.conf in the ProxySocksIP parameter
4. **SocksListenPort=**<Listening port for new socks connection requests>

   Same port entered in httpd.conf in the ProxySocksPort parameter
5. **HttpListenPort=**<Listening port for new HTTP connection requests>

   The incoming HTTP connections come through Apache

   Same address as one entered in httpd.conf in the Listen parameter
6. SOAPListenIP / SOAPListenPort = The MPS has an interface to query the MPS for connected Clients.

All other parameters can be left with default values.

MPS.config sample Configuration

[Network]

AMTListenIP	**= 195.168.1.104**
AMTListenPort	**= 16993**
HttpListenPort	**= 8080**
SocksListenIP	**= 195.168.1.104**
SocksListenPort	**= 4322**
SOAPListenIP	**= 195.168.1.104**
SOAPListenPort	**= 1600**

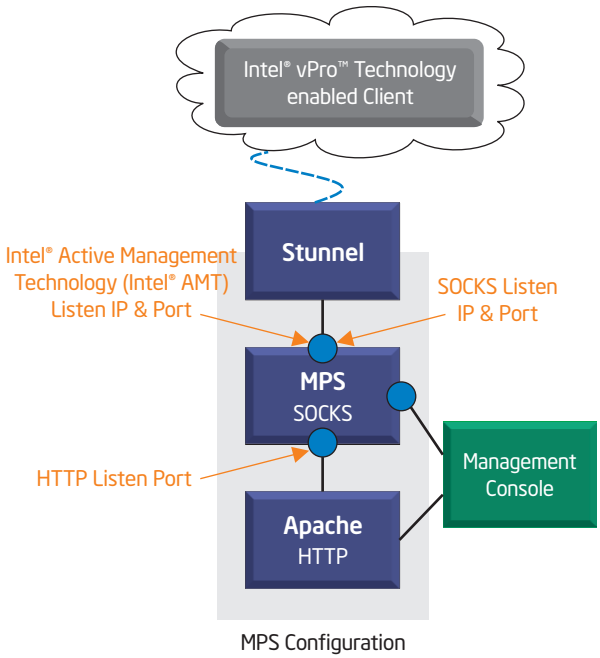


Figure 7. MPS Configuration

Example of an Intel vPro technology-enabled gateway port configuration:

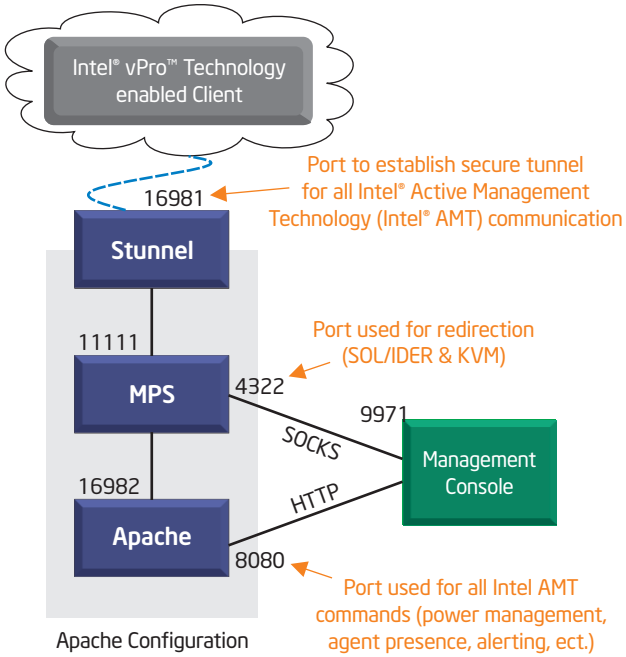


Figure 8. Example of an Intel® vPro™ Technology-enabled Gateway Port Configuration

Configuring the notification list

The MPS notification file lists the IP address of the target management console(s), where all the Intel AMT communication should be directed.

1. Locate the NotificationList.config file under c:\MPS\conf
2. Edit at least one entry:

   http://<IP address> : <port>/EventNotificationClientService

Notes:

1. IP address is the address of the management console and the port number the console is listening on.
2. At least one system has to be configured and a maximum of eight entries are allowed
3. The configuration (as above) has no authentication configured. The MPS will accept any Intel AMT machine that will attempt to connect to the MPS. The MPS supports username/password authentication and TLS certificate authentication – see the Intel AMT SDK for configuration samples.
4. For a sample web service – please look into the Intel AMT SDK.

Configurations Walkthrough-Client Staging Area-Intel® AMT Provisioning

Background:

This section describes the process that configures the Intel AMT provisioning in the digital signage vendor staging area before shipping the system out to the remote location.

This chapter focuses on provisioning the client for digital signage in a retail/remote setting, with clients outside the corporate network. The described process will enable **"Fast Call for Help"** (or FCFH).

This feature enables the Intel vPro technology-enabled client to connect to the service provider when a malfunction is detected and other means of connection are unavailable, thus allowing the support tech to remedy the issue at hand.

Note that Intel vPro technology-enabled gateway is sometimes referred to as "Managed Presence Server"; in this context, and they are the same thing.

Provisioning Process overview:

The provisioning process is performed by the Intel provided "Setup & Configuration Service" (aka SCS). Some 3rd party management consoles, such as Altiris* and Microsoft* SCCM, have the SCS integrated in their console; however, customers can use the standalone product that can be downloaded from the Intel website at no charge. Figure 9 illustrates the provisioning environment using the Intel SCS.

Download Intel SCS (**link**).

The provisioning process is described in detail in various documents (see links at the end of this document).

Intel SCS installation:

1. Use a Windows Server 2003 Enterprise OS.
2. Run the Intel SCS installer under an OS account that has permissions to obtain a certificate in the Certificate authority used.
3. Install the provisioning certificate you purchased for this server to the Private certificate store under the same OS account.

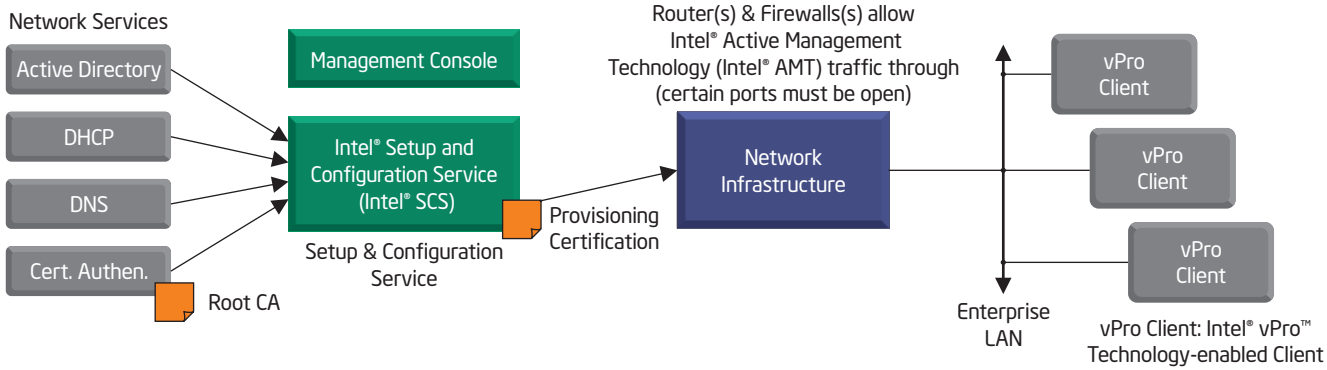


Figure 9. The Provisioning Environment Using the Intel SCS

In environments with limited IT infrastructure, an independent isolated Pod provisioning environment can be setup for the purpose of client provisioning only (Figure 10).

With this solution, a client is networked attached to the provisioning server, and an operator runs a script that initiates the provision process. Once the client is provisioned, it can be placed on the production network; it will be discovered and can be managed using Intel AMT.

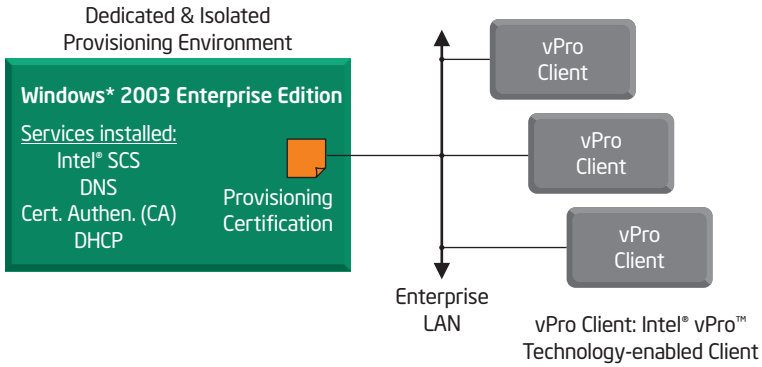


Figure 10. Provisioning Environment

Configuring the client for FCFH connection

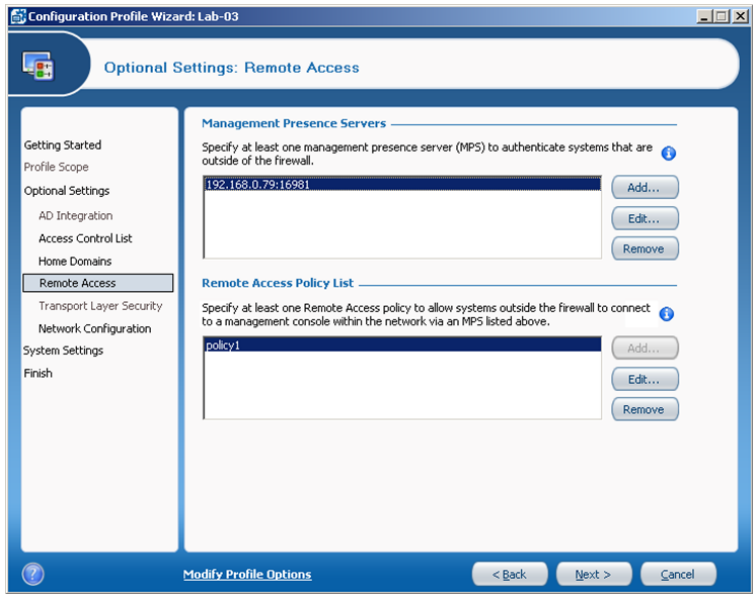
There are three scenarios by which Intel AMT can initiate a FCFH connection:

1. User Initiated connection.
2. Alert connection (triggered by some OS, SW or hardware event on the client).
3. Scheduled or periodic connection.

In addition, Intel AMT must know the IP address/DNS FQDN and the port of the Intel vPro technology-enabled gateway.

Step 1: Setup 'Home Domains':

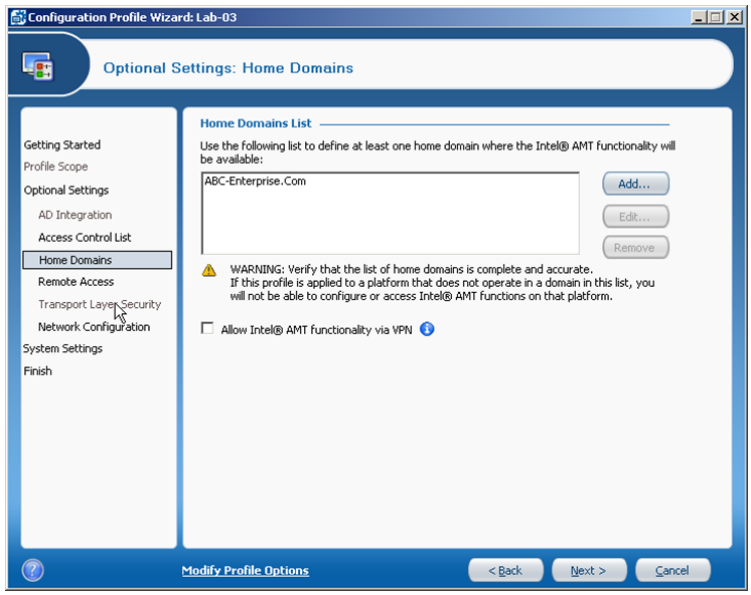
To generate a FCFH, Intel AMT must first recognize that it is outside the corporate network. The SCS configuration profile must include the list of all 'home domains', i.e., the DNS/DHCP domains that are considered "inside the network". When Intel AMT on the client detects that it is located outside the enterprise network, it realizes it is not open for direct management. In this state, Intel AMT will generate a FCFH connection request upon one of the three connection triggers: user or software initiated, alert (both hardware and software), and periodic.



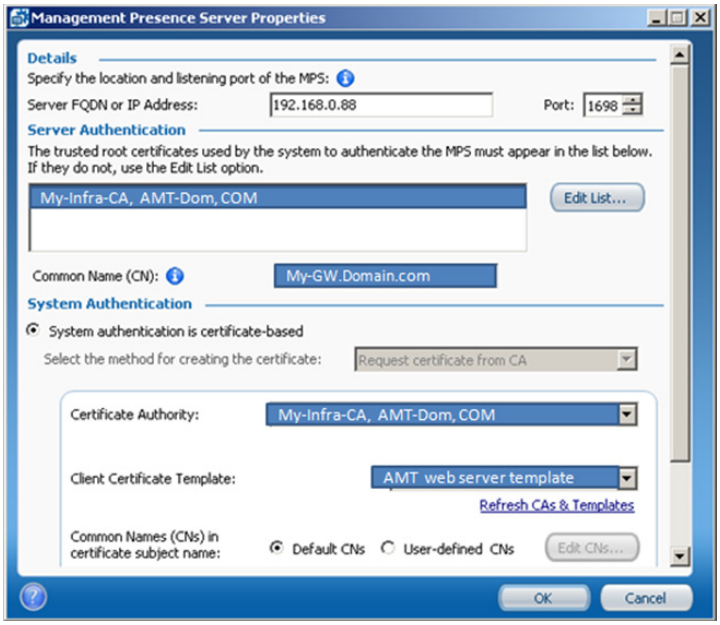
Step 2: Setup FQDN (or IP) & port number for Intel vPro technology-enabled gateway

In this screen, the administrator defines the Intel vPro technology-enabled gateway, and configures the Intel vPro technology-enabled gateway and the remote policies.

Note: Up to four Intel vPro technology-enabled gateway can be defined and active at the same time. Intel AMT will attempt to create a connection with each one in the order of the list. If it fails to successfully generate a connection, it will time out and attempt a connection with the next one on the list.



When you click the **Edit** on the Managed Presence Server the following screen appears.



1. On the first field, enter the FQDN or IP and port number of the Stunnel as configured in previous chapter.
2. Enter the location of the trusted root certificate. This certificate is installed on the client. During connection authentication, the Intel vPro technology-enabled gateway presents its web server certificate (created in previous steps) to the client and the client uses the trusted root certificate to authenticate that certificate.
3. Enter the Common name of the server hosting the Intel vPro technology-enabled gateway. This entry is necessary only if in step #1, an IP was entered. If FQDN was entered, this field is disabled.

Configure System Authentication

This section is used when mutual authentication is desired. There are two methods for mutual authentication:

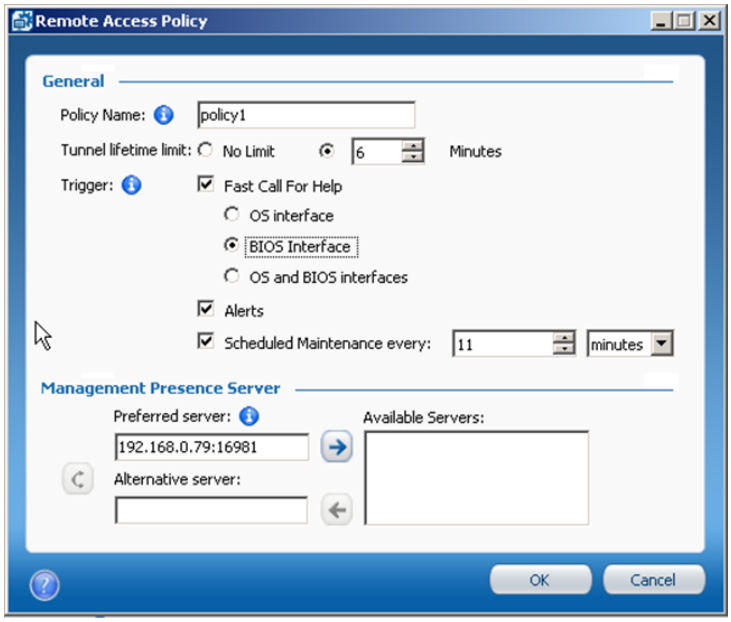
1. Certificate based mutual authentication: When Certificate based is selected, the Intel vPro technology-enabled gateway presents its web server certificate (described earlier) to the client. The client authenticates that certificate using a trusted root certificate generated by the same CA.
   a. Enter the source of the certificate.
   b. Enter the template for the certificate.
2. User credentials mutual authentication: When user credentials is selected, enter the same credentials as the user defined in Intel AMT administrators.

Step 3: Defining 'Remote Access Policies':

As mentioned earlier there are three scenarios by which Intel AMT can initiate a FCFH connection. The configuration options are setup in Remote Access Policy form.

Items descriptions:

1. Tunnel Life Time: This option determines how many idle minutes are allowed on the connection before the connection terminates. If 'no limited' is selected, the connection will never close due to idle time.
2. Trigger: Three scenarios are available, and any number of these scenarios can be selected.
   a. Fast Call For Help – this is a user initiated connection.
      The choices in this option determine which user interface will be available.
   b. Alerts - Certain platform events can be subscribed to when such an alert takes place, and an event is generated that will also request a FCFH connection.
   c. Scheduled Maintenance – Intel AMT will trigger a connection according to the timer set in this field.
   d. Preferred Servers – Enter the preferred Intel vPro technology-enabled gateway for maintenance functions. In most cases this is the same as the Intel vPro technology-enabled gateway defined in previous section.



Obtaining, Installing and configuring OS drivers:

Obtain the following from your OEM:

LAN Drivers
Platform chipset Drivers
Onboard Graphics Drivers.

Installing and configuring wireless driver

PROSet is currently the only Wireless Connection Manager that supports Profile Synchronization.

Obtain the latest PROSet driver package (link)

The Full PROSet package (except GUI) must be installed. The 'drivers only' installation does not have the necessary API to support that feature.

Install PROSet with MEPROFILESYNC=ACCEPT in the command line:

LMS is required for Profile Synchronization (PROSet communicates with Intel AMT through LMS).

The Intel vPro technology-enabled client is now ready for deployment in the final remote site.

In-site Installation Walkthrough – Client @ Remote site

Steps to connect the Intel vPro technology-enabled machine at the remote site:

1. Configure the machine according to the machine's intended usage.
2. Connect the machine to the wireless network by creating the wireless profile using PROSet.
3. The PROSet software will sync the profile to Intel AMT.

Testing the Intel vPro technology-enabled machine connection to the gateway:

Note: This test can be done ahead of the actual deployment in the lab. All that is needed is to supply the Intel AMT with a networking environment that has:

1. A connection to the external side of the Intel vPro technology-enabled gateway (the port and IP that Stunnel listens to)
2. A connection that has a different domain name that the provisioning environment (DHCP option 15)

   Example: the provisioning area has "ABC-Enterprise.com" for the domain name, so the test environment will have "AOL.com" for the domain name.

The Test:

1. Verify that the machine has a working connection to the Internet.
2. Open the Intel Management and Security Status (IMSS) by clicking on it in the notification area (Figure 11).
3. Open the Intel AMT tab.
4. Verify Intel AMT is not connected (should state "Disconnected").
5. Click on the "Get Technical Help" button.
6. Verify Intel AMT has a working connection (Should State "Connected").
7. Disconnect the "Get Technical Help" button, and it will change to "Disconnect". Click on that button to disconnect.

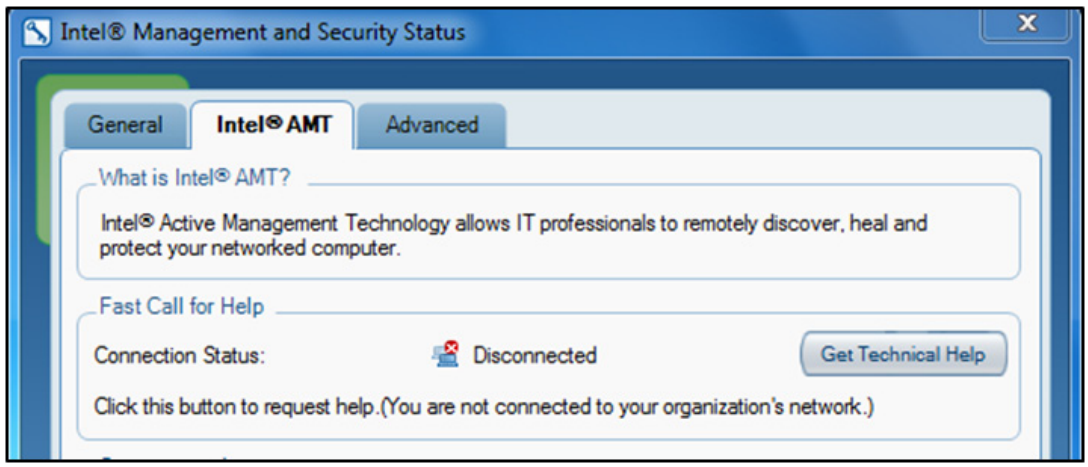


Figure 11. The IMSS Screen (initiate CIRA connections from here)

Use cases overview

KVM (Keyboard, Video, Mouse) :

Capability: Full KVM access via CIRA to the digital sign or retail computer, enabling remote access regardless of the OS status.

Intel AMT enables the usage of remote KVM even in the event that the OS is down (BSOD, stuck in bios or boot, etc.). Using remote management through Intel AMT, the IT technician can manage the remote computer using normal input devices, and not only through command line instructions. Even in the case that a technician would have to physically go to the computer to repair it, there would be a need to connect a keyboard and mouse to the digital sign/retail computer, which typically doesn't have these input devices permanently connected. With Intel AMT management in the technician's 'home' location, the tech is able to use these input devices without any additional physical connections.

IDER (IDE Redirection):

Capability: The ability to resolve / boot the SD machine from a remote recovery image.

IDER is typically used to boot a remote system from a local drive (CD/DVD) and utilize the data or image on that drive to resolve issues on the remote computer, including remote imaging or file repair.

Agent Presence:

Capability: The ability to monitor system processes and trigger remote connections / alerting upon status changes to these processes.

Agent Presence has particularly important usage models for digital signage and retail computers. It is very common that digital signs are placed by vendors and manufacturers in retail stores or outlets. When there is an issue on the remote sign, such as the player stops or is not functioning, the OS freezes, etc., a local store employee may not care or pay attention. For situations like this and many others, through Intel AMT, a pre-configured agent would detect that something was wrong, send an alert to the remote IT support and provide details of the issue. At that point, the technician could remotely connect to the computer and resolve the issue the agent reported. It's like having a full time person watching the system and reporting issues in real time.

3PDS : 3rd Party Data Storage

Intel AMT provides an API to save and read data on the platform flash memory (this also holds the platform BIOS and Intel vPro technology executable images) – this 192 KB block of memory is available to the digital signage solution provider to store vital information as a backup copy of data typically saved to the local hard disk.

Critical / valuable information can be stored on this storage device and can be obtained remotely even in the case of a complete hard disk failure/crash.

For digital signage system integrators and suppliers, the 3PDS is particularly attractive. Proof of play of the ads is typically required for digital signage customers. In the event of OS or disk corruption/failure, this proof of play is sometimes destroyed as well. 3PDS can be configured to store and protect this data and maintain proof of play even in these cases. The data is not stored on the hard drive or in the operating system and is therefore protected, and fee payment for proof of play can be assured.

Another use case of 3PDS is storing the changes in the play list. Typically, when a system is re-imaged with a locally stored image, that image is from the time the system was first deployed or from a later date when it was updated. It does not necessarily reflect the changes in the playlist that were configured after that. 3PDS can be configured to store that data and upon re-image, present the updated playlist to bring the system back to a current situation. This can provide considerable time savings and reliability of the playlist.

Management software for use with Intel® AMT

Intel provided management software

Intel vPro Technology Power Shell Module (link)

Commercial 3rd party management software:

This is a current list of vendors and management software that can be used to manage Intel vPro technology-enabled systems (link) ***(LINK in word doc doesn't work)***

YCD usecase and example

Following are pictures of an Intel vPro technology-enabled YCD digital signage solution installed at a retailer end-point.

Coca Cola Israel, through system integrator YCD, sought a digital signage solution that would provide placement flexibility, minimize deployment effort and lower support cost. The company wanted to place advertisements near their product displays, which change a few times a month, using a scalable solution that could fit in small convenience stores and large supermarkets of all sizes and with different IT infrastructures.

Typical challenges of deploying remote digital sign displays:

Complex approval process: A new wired LAN connection for digital signage may require approval by the facilities manager, IT department and other groups.

Overall cost: Large pocket expenses, including deployment, energy and management, will deter retailers.

Few placement options: Wired networks constrain where systems can be placed in the store.

Solutions:

Wireless networks: No major infrastructure changes are required, which reduces the number of required approvers.

Advanced remote management: Systems can automatically shutdown during off hours, saving energy. In addition, they can be serviced remotely, reducing support costs.

Wireless connectivity: Systems can be deployed anywhere within signal range, thereby increasing placement flexibility.

YCD incorporated Intel AMT into their YCD|Platform*, a remote management and distribution platform that enables IT departments to program, schedule and distribute audio and video content in retail settings easily, quickly and accurately. With Intel AMT, the console is able to implement a real-time hardware watchdog that works even if the operating system hangs; thus, it is capable of alerting when a catastrophic failure occurs.

Location, Location, Location

Wireless has created a whole new dynamic that is bringing customers closer to retailers and their messaging. A logical progression is wireless digital signage, which allows display screens to be located and even relocated as needed – to best reach out to customers. In addition to greater flexibility, the technology reduces installation cost and effort, making it only a matter of time before wireless is a check off item for digital signage systems.

Figure 12. Digital Signage with Wireless Intel® AMT

Conclusion

This guide is not a conclusive document for deploying Intel AMT in any and all environments. Its purpose is specifically to serve as an easy to follow guide for deploying Intel AMT and wireless Intel AMT for digital signage and retail computing.

In order to simplify these types of deployments, it is recommended to view a digital signage/retail environment as separate from the company's normal IT environment, either as completely separate or partially separated through the use of dedicated management and security systems. In this way, the digital signage system integrator can deploy and manage this network with far less concern for matching it to a typical IT network made up mostly of end user computers. Digital signage and retail computers fall into the category of Machine to Machine (M2M), and as such, managing them is done almost entirely by sending a technician or ideally, by remote management without any end user on the other side.

Proper deployment of Intel AMT will provide you and/or your customers with lower total cost of ownership; remote management through the use of KVM (Keyboard, Video, Mouse) operations even in the event of system crash; having the digital sign/retail computer 'call home' for help through 'Agent Presence' when it self identifies pre-configured issues (such as system down, media player not playing); 'Proof of Play' through 3PDS (3rd Party Data Store) so that even if the system crashes, there is a log showing what has been played; power savings through remote shut-down/turn on; and the ability to boot/reboot the computer when needed or desired.

Figure 13. Digital Signage with Wireless Intel® AMT

For more information about Intel solutions in retail, visit **www.intel.com/go/ic**.

[1] Intel® Active Management Technology (Intel® AMT) requires the platform to have an Intel AMT-enabled chipset, network hardware and software, as well as connection with a power source and a corporate network connection. With regards to notebooks, Intel AMT may not be available or certain capabilities may be limited over a host OS-based VPN or when connecting wirelessly, on battery power, sleeping, hibernating or powered off. For more information, see www.intel.com/p/en_US/embedded/hwsw/technology/amt.

[2] See bandwidth recommendations in the CIRA part of this document.

[3] See configuration walkthrough regarding the needed firewall setup.

[4] See Stunnel config

Printed in USA 0312/TB/TM/PDF Please Recycle 327022-001US