Intel® vPro™ Technology Solution Implementation Guide

Fast Call For Help / Client Initiated Remote Access

Legal Disclaimer

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

A "Mission Critical Application" is any application in which failure of the Intel Product could result, directly or indirectly, in personal injury or death. SHOULD YOU PURCHASE OR USE INTEL'S PRODUCTS FOR ANY SUCH MISSION CRITICAL APPLICATION, YOU SHALL INDEMNIFY AND HOLD INTEL AND ITS SUBSIDIARIES, SUBCONTRACTORS AND AFFILIATES, AND THE DIRECTORS, OFFICERS, AND EMPLOYEES OF EACH, HARMLESS AGAINST ALL CLAIMS COSTS, DAMAGES, AND EXPENSES AND REASONABLE ATTORNEYS' FEES ARISING OUT OF, DIRECTLY OR INDIRECTLY, ANY CLAIM OF PRODUCT LIABILITY, PERSONAL INJURY, OR DEATH ARISING IN ANY WAY OUT OF SUCH MISSION CRITICAL APPLICATION, WHETHER OR NOT INTEL OR ITS SUBCONTRACTOR WAS NEGLIGENT IN THE DESIGN, MANUFACTURE, OR WARNING OF THE INTEL PRODUCT OR ANY OF ITS PARTS.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined". Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or go to: http://www.intel.com/design/literature.htm%20

Any software source code reprinted in this document is furnished under a software license and may only be used or copied in accordance with the terms of that license. {include a copy of the software license, or a hyperlink to its permanent location}

Intel® vPro™ Technology is sophisticated and requires setup and activation. Availability of features and results will depend upon the setup and configuration of your hardware, software and IT environment. To learn more visit: http://www.intel.com/technology/vpro.

Requires activation and a system with a corporate network connection, an Intel® AMT-enabled chipset, network hardware and software. For notebooks, Intel AMT may be unavailable or limited over a host OS-based VPN, when connecting wirelessly, on battery power, sleeping, hibernating or powered off. Results dependent upon hardware, setup and configuration. For more information, visit Intel® Active Management Technology.

Client Initiated Remote Access may not be available in public hot spots or "click to accept" locations. For more information on CIRA, visit Fast Call for Help Overview

Intel, the Intel logo, and Intel vPro, are trademarks of Intel Corporation in the U.S. and/or other countries.

*Other names and brands may be claimed as the property of others.

Contents

1. Introduction

1.1 Executive Summary

Remote Access is the term describing Fast Call for Help (FCFH) or Client Initiated Remote Access (CIRA), Remote Scheduled Maintenance and Remote Alerts from outside the firewall. Fast Call for Help can also be requested from inside the firewall (CILA).

Client Initiated Remote Access (CIRA) provides a capability for Intel® vPro™ technology systems located outside the enterprise firewall, to establish a secure connection back into your organisation. Once this secure connection is authenticated and established, Intel vPro Ultrabooks, notebooks or desktops can be managed using Intel® Active Management Technology (Intel® AMT) as if they were on the corporate network, even when powered off or with a failed operating system or system drive.

1.2 Purpose of this Document

This document captures the components and requirements to implement a solution that leverages Intel vPro platform technologies and provides a secure Internet-facing service that is capable of identifying, authorising and communicating with remote Intel vPro technology systems using the Fast Call For Help interface.

1.3 Terminology

Term	Description
ACM	Admin Control Mode
Intel® AMT	Intel® Active Management Technology
APF	Intel® AMT Port-Forwarding Protocol
CA	Certificate Authority
CCM	Client Control Mode
CILA	Client Initiated Local Access
CIRA	Client Initiated Remote Access
DMZ	Demilitarised zone
FCFH	Fast Call For Help
FQDN	Fully Qualified Domain Name
HBC	Host Based Configuration
HBP	Host Based Provisioning
IDER	IDE Redirection
KVM	Keyboard, video and mouse redirection (hardware level)
LMS	Local Management Service
Intel® ME	Intel® Manageability Engine
Intel® MEI	Intel® Manageability Engine Interface
Intel® MEBX	Intel® Manageability Engine BIOS Extensions
MPS	Management Presence Server
RCS	Remote Configuration Service
Intel® SCS	Intel® Setup and Configuration Software
SOL	Serial-Over-LAN

SSL	Secure Sockets Layer
TLS	Transport Level Security
UNS	User Notification Service
VPEG	Intel vPro Enabled Gateway

1.4 References

Document/Product Name	File/Location
Intel® AMT Software Development Kit (SDK)	http://software.intel.com/en-us/articles/download-the-latest-intel-amt-software-development-kit-sdk/
Intel® Setup and Configuration Software (Intel® SCS)	http://software.intel.com/en-us/articles/download-the-latest-version-of-intel-amt-setup-and-configuration-service-scs/
Intel® vPro™ Technology Module for Microsoft* Windows PowerShell*	http://communities.intel.com/docs/DOC-4800
Fast Call for Help: Steps to create an Intel vPro Enabled Gateway by Gael Hofemeier. A fantastic how-to video, great for stunnel, MPS and Apache HTTP configuration.	http://software.intel.com/en-us/blogs/2012/11/06/fast-call-for-help-steps-to-create-an-intel-vpro-enabled-gateway

1.5 Supported Environments

1.5.1 Microsoft* Windows*

The solution supports the following client operating systems:

- Microsoft* Windows 7 Enterprise SP1 (x64)
- Microsoft* Windows 8.1 Enterprise (x64)

The reference VPEG implementation has been validated on

- Microsoft Windows Server 2003 (x86)
- Microsoft Windows Server 2008 R2 SP1 (x64)

1.5.2 Linux*

The MPS code is portable and compiles and runs on Linux* with the following limitations:

- Does not run as a background daemon.
- Does not utilise operating-system logging facilities.
- No user authentication support or provided sample authentication library.
- No automated installer.
- Fewer validation tests have been performed.

2. Detailed End-To-End Solution Overview

The Intel vPro Enabled Gateway (VPEG) consists of several software products configured as either a standalone server, i.e. Virtual Machine, or the various components can be distributed across several servers. It is recommended that the VPEG resides within the demilitarised zone (DMZ) and be available as an Internet-facing service.

The Intel vPro system initiates a connection to the VPEG via a key combination pressed by the user during system power-on (BIOS) or via the Windows Operating System or automatically. Intel AMT contact the Fully Qualified Domain Name or IP address of the VPEG using information defined during the provisioning process.

Once the VPEG has been located then Intel AMT will establish a secure session with the SSL tunneling proxy (stunnel) and verify the authenticity of the VPEG based upon a SSL certificate provided by the server. Intel AMT validates that the SSL certificate is issued by a trusted certification authority. This process is identical to that performed by HTTP clients in HTTPS.

Once a secure SSL session has been established, stunnel then forwards all traffic to the MPS component and the two peers initiate Intel AMT Port-Forwarding Protocol (APF). The Intel vPro based system provides its FQDN which is then associated with the currently active session by the MPS component.

The Service Desk can then check that a Intel vPro based system is connected to the VPEG and use VNC* Viewer Plus to establish a KVM session, after successful authentication and authorisation (using optional consent code).

2.1 Solution Design and Component Relationship

The end-to-end solution architecture incorporates the products, services and components as detailed in section 4.

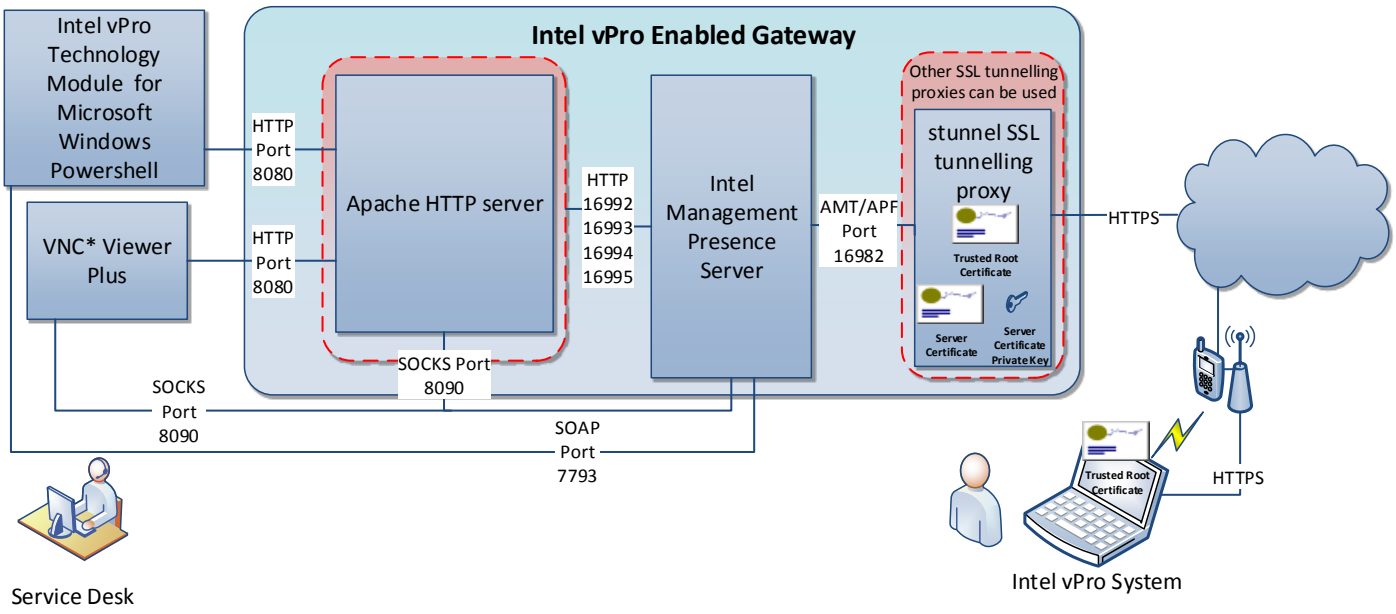


Figure 1

NOTE: When non-redirection operations are performed using Windows PowerShell and VNC Viewer Plus, i.e. power on/off, reset, etc. then HTTP via port 8080 is utilised. However when Windows PowerShell and KVM perform redirection operations such as SOL, IDE-R, KVM etc. then the redirection libraries use SOCKS via port 8090.

2.2 Service Desk and User Solution Interaction Flow

This section describes a sample interaction between the Service Desk and the remote user in the event of a failed operating system or system drive.

1. The remote user contacts into their Service Desk.
2. The Service Desk asks the user to connect their Intel vPro based system to an available port on their home router using an Ethernet cable and ensure they have AC power connected.

3. The Service Desk asks the user to power on their Intel vPro based system and press the required Fast Call for Help hot-key combination before the operating system starts.
4. The Service Desk verifies with the user that their Intel vPro based system screen shows a successful connection.
5. The Service Desk executes the *Get-AMTFCFHConnection* Windows PowerShell script with the required parameters to query the VPEG and display all currently connected Intel vPro based systems.
6. Once the relevant Intel vPro based system has been identified, the Service Desk runs VNC Viewer Plus and enters the name of the remote system identified in step 5. They then authenticate and enter any optional consent codes.
7. The Service Desk now has secure keyboard, video and mouse control even through power operations with the remote Intel vPro based system and can remediate.

NOTE: A six-digit consent code is required if Intel AMT has been provisioned using Host Based Configuration (HBC) or Client Control Mode (CCM) Consent codes are optional when provisioned in Admin Control Mode (ACM)

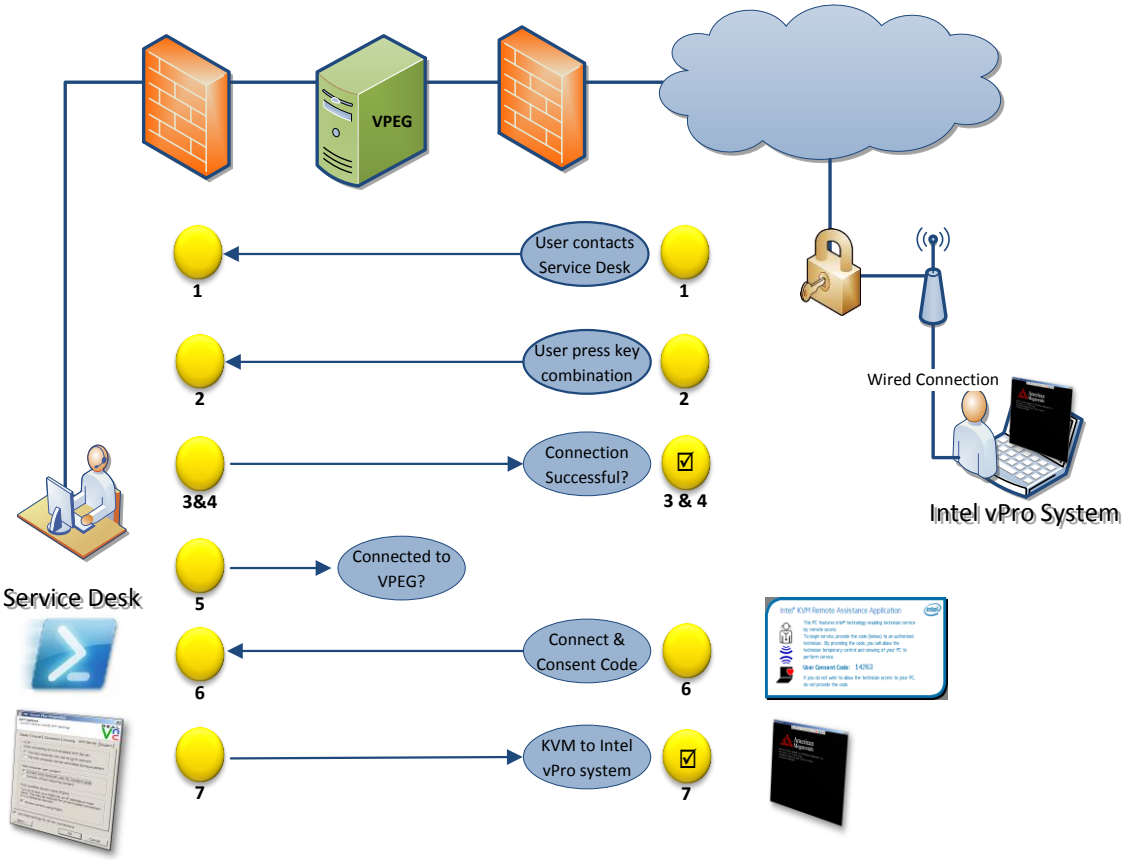


Figure 2

2.3 Solution Usage Models

2.3.1 One-to-one Remediation

The solution extends the reach of the Service Desk to connect to, and remediate remote users with Intel vPro technology enabled systems. Remote users can connect into their corporate network using a hot key-sequence during power-on in the event of a non-functioning operating system, hard disk failure or VPN issues. Authorised Service Desk personnel can then connect to the VPEG, identify the connected Intel vPro based system and take control of that system using the hardware KVM capabilities available with Intel vPro technology enabled systems to support the following use cases:

- The platform displays a blue screen and the Service Desk operator wants to view it.
- The operating system is unresponsive or is in repair mode, so other applications that run using the operating system are unavailable.

- The Intel vPro based system is asleep or powered off and the Service Desk operator wishes to power on the platform to work on it.
- The platform needs to be booted, and requires a combination of text-based BIOS and operating system graphics interaction, i.e. to unlock encrypted drives, boot an operating system and remediate it. The Service Desk operator can observe the full flow when rebooting.

2.3.2 Scheduled Maintenance

Scheduled maintenance is a capability to automatically initiate a connection from a remote Intel vPro based system back into the corporate network against a defined time period, i.e. every 48 hours. This usage model requires absolutely no user interaction as the connection is initiated by Intel AMT when the system has AC power and is connected to a WLAN or wired network. Intel AMT understands that it is not connected to the corporate network so initiates a connection to the VPEG at the defined time. Once connected it can be accessed via the VPEG as if it were sitting on the corporate network.

2.4 In Scope

This section outlines the configuration and details related to the components that form the overall solution. It does not discuss in detail any of the internal component interfaces or specific provisioning sequences.

- This solution currently only supports remote access to the Intel vPro based system using VNC Viewer Plus.

2.5 Out Of Scope

In this version of the use case reference design the following functionality is considered out of scope and not supported:

- CIRA has been available on Intel vPro systems since Intel AMT firmware versions 4.0 and 5.0. However this solution focuses on Intel vPro systems with Intel AMT firmware version 6.2 or later due to the requirement to support KVM and Host Based Configuration.
- Intel AMT version 6.0 and later supports CIRA over WLAN and wired connections. To simplify the solution the recommendation is to connect the wired interface of the Intel vPro based system directly to a home router. Some validation has been performed using CIRA over a WiFi connection and details are provided to support this.
- Provisioning of Intel vPro systems is not covered, however guidelines and examples are provided to support the required configuration using Host Based Configuration.
- Kerberos authentication is recommended, however it is not required.
- Authentication of Intel AMT, SOAP and SOCKS network traffic and notification events is configurable, however is considered out of scope.
- The ability to manually or automatically support notification events when a system enabled with Intel vPro technology connects or disconnects to a VPEG is not currently supported. The main reason was to reduce complexity although issues include the current notification messages using a proprietary SOAP protocol and the notification mechanism causing blocking I/O problems.
- The VPEG does not currently support IPv6.
- The solution supports a certificate-based SSL authentication mechanism. The Intel AMT system validates that it is communicating with a genuine VPEG based upon an embedded SSL certificate issued by a trusted certificate authority. Although the capability for the VPEG to establish trust with the Intel AMT system exists (using Mutual TLS) this is not detailed.
- CIRA does not support connections via proxy servers or where authorisation or acceptance of terms and conditions for internet access are required, i.e. public internet access points.

3. Certificate Management

This section is critical to a successful implementation and significant effort has been made to reduce the complexity associated with certificate requirements, management and configuration.

Although there are several options available to create the required certificates, the simplest method has been chosen and is detailed in this section. The ability to use an Enterprise Certificate Authority to generate these is not covered.

In summary there are a minimum of two (2) certificates required:

- Trusted Certificate (*TrustedRootCertificate.pem*)
- Web Server Certificate (*ServerCertificate.pem*) and the associated Web Server Certificate Key (*ServerCertificateKey.pem*)

The Intel AMT system requires a trusted root certificate (*TrustedRootCertificate.pem*) which is embedded within the Intel ME during the provisoning process and used to verify and authenticate that communication is established with a genuine VPEG. This validation process is identical to that performed by HTTP clients in HTTPS and checks the Fully Qualified Domain Name (FQDN) against the server certificate (*ServerCertificate.pem*) sent by stunnel to the Intel vPro based system during SSL session establishment.

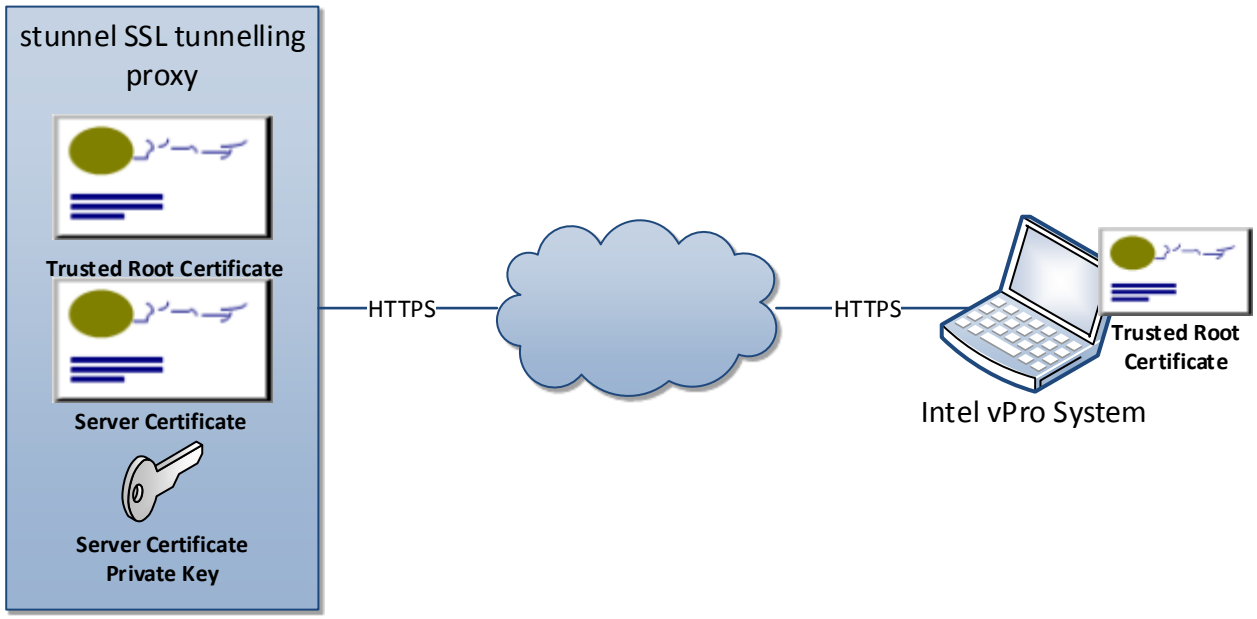
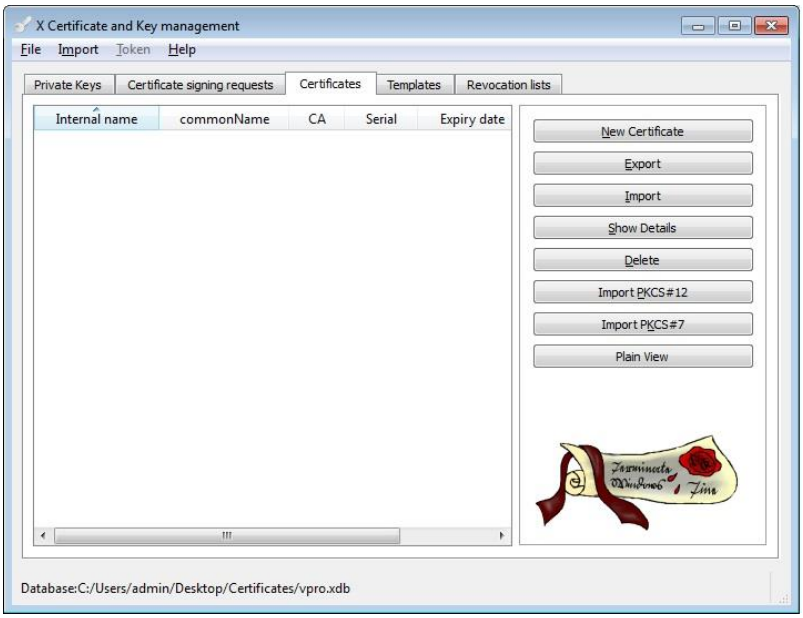


Figure 3

NOTE: Intel AMT configuration requires that the VPEG FQDN is entered into the CN field when an IP address is used. The CN is used to validate the FQDN of the system as specified in the server certificate. See section 5 for details.

RECOMMENDATION: Watch this excellent video which steps through the entire certificate management procedure: http://www.youtube.com/watch?feature=player_embedded&v=_22WYdFTxEw

3.1 Creating the Trusted Root Certificate

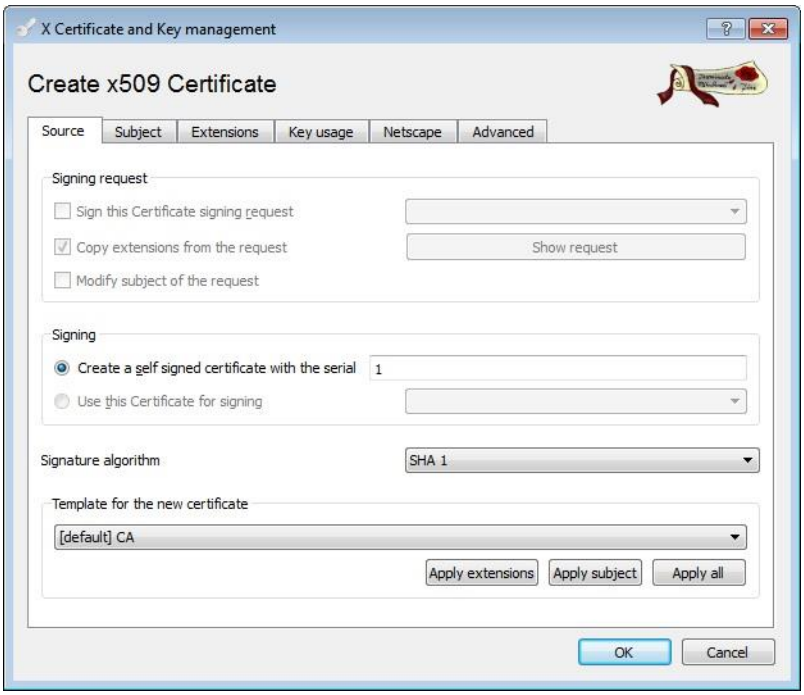


Download XCA from http://sourceforge.net/projects/xca/

Install and create a database with a password (remember this password)

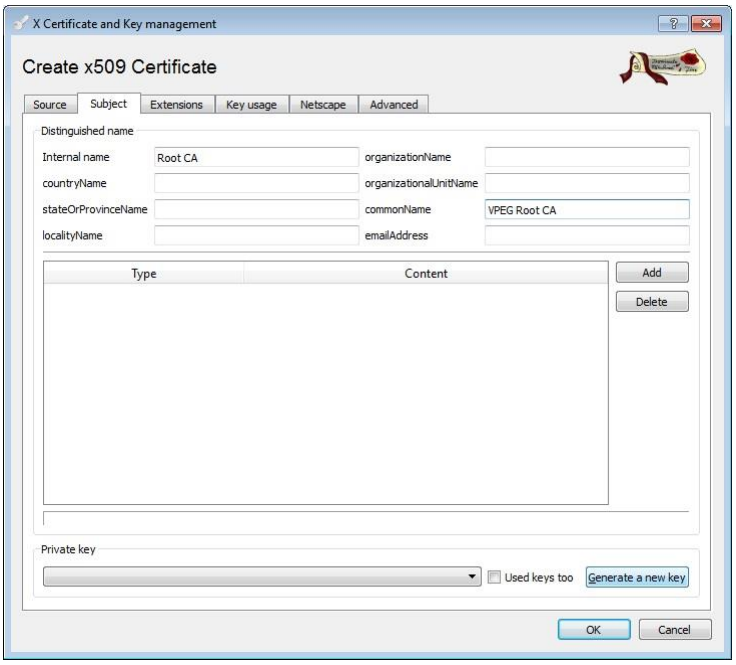
Now set up the Root CA and create the required VPEG certificates.

Click ***Certificates*** tab, then ***New Certificate*** button.



At the bottom of the panel, ensure that the "***[default] CA***" template is available.

Click ***Apply all*** which automatically fills in some of the required values under the Extensions and Key Usage tabs.



Click the Subject tab.

Type in an internal name i.e. "***Root CA***"

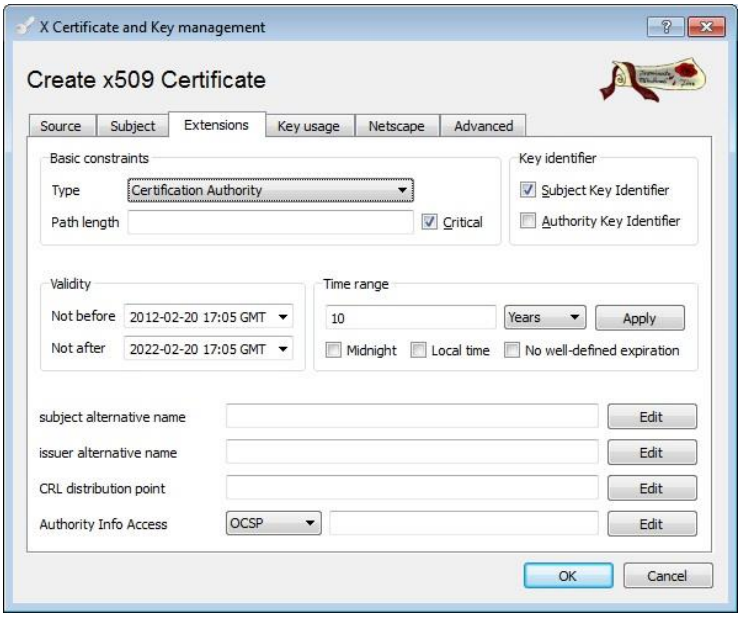
Fill in the common name "***VPEG Root CA***"

Select "***Generate a new key***"

Enter name i.e. ***RootCAKey***

Set the key size to ***2048 bit*** (recommended)

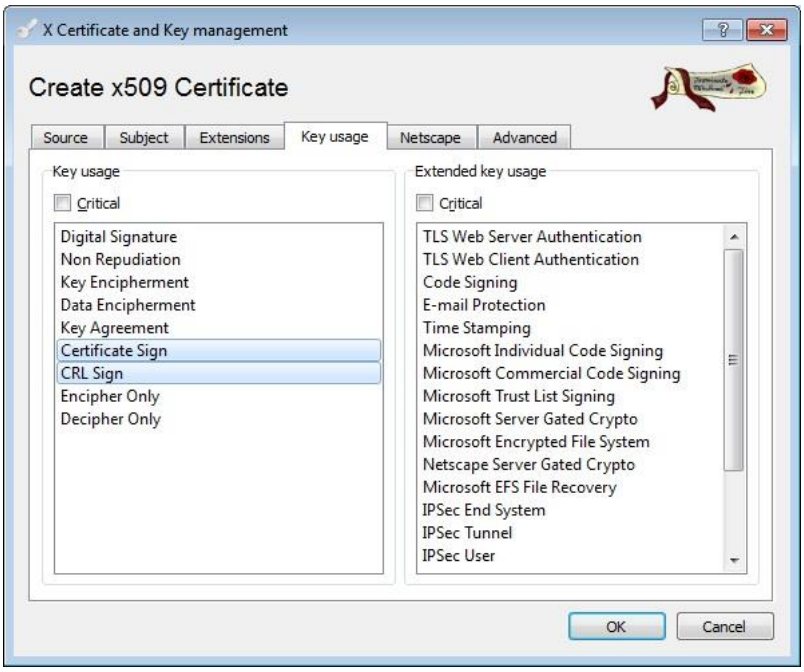
Click ***Create***.



Click the Extensions tab.

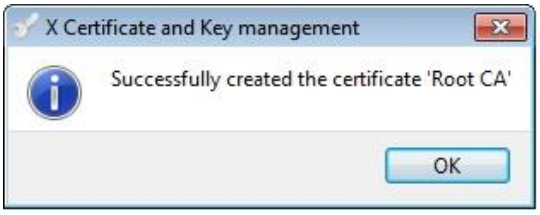
Ensure Type is set to ***Certification Authority***

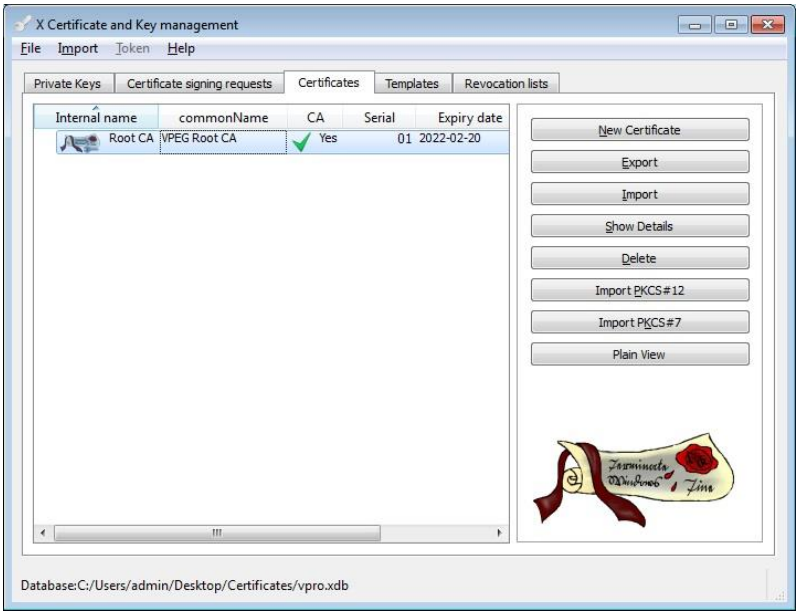
Enter a suitable Time Range, default is OK.



The CRL distribution point will be part of the issued certificates, but effectively ignored by Intel AMT in this configuration.

Click the OK button at the bottom to create the certificate.



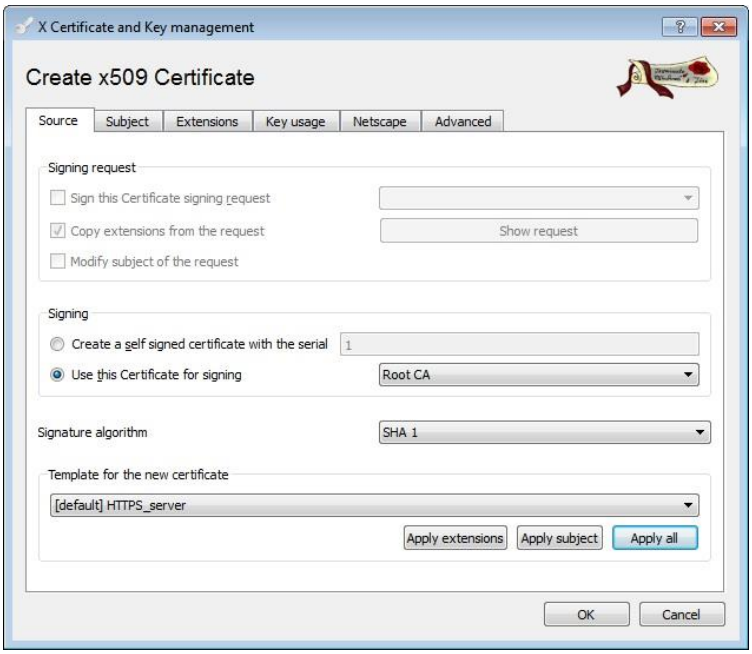


The VPEG Root CA has now been created!

Next create the required server certificate.

Click the ***New Certificate*** button.

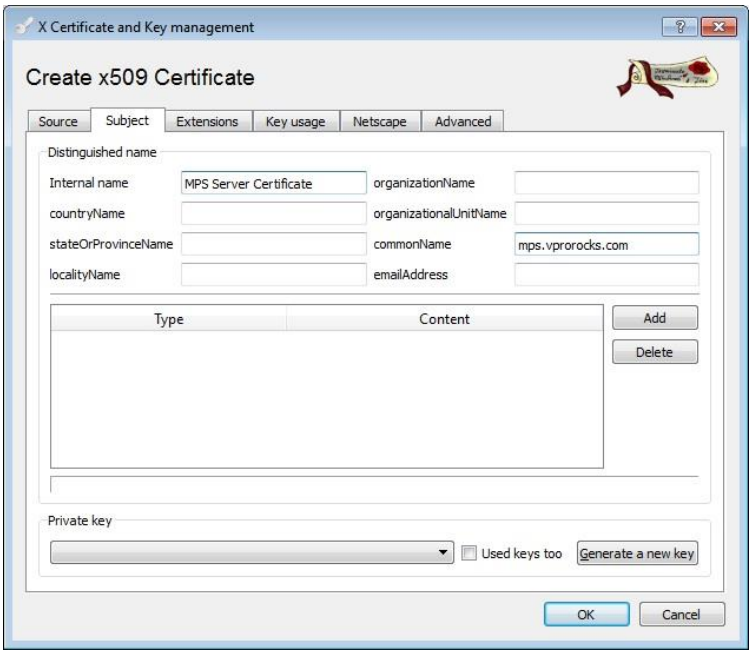
3.2 Creating the Server Certificate and Private Key



Click the Certificates tab.

Ensure the Source tab is showing and at the bottom, select the template "***[default] HTTPS_server***

In the Signing section, select "***Use this Certificate for Signing***" to ***Root CA*** (the Root CA created in section 3.1).



Click the Subject tab.

Type in an internal name.

Fill in the Common name, this is the VPEG FQDN to which Intel AMT systems connect.

NOTE: The Common Name can be anything but must match the Common Name (CN) that Intel AMT expects (see section 5.2)

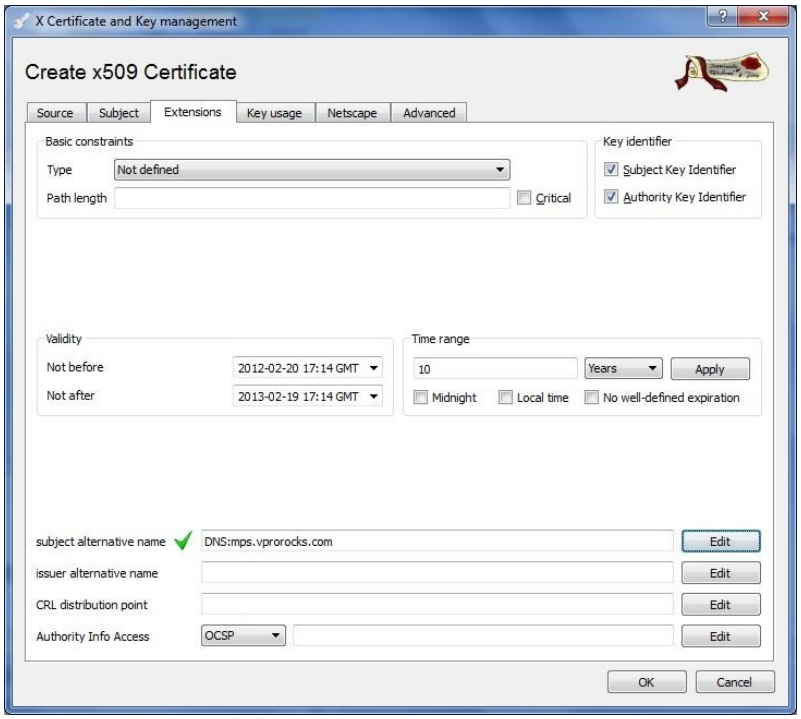
Select "***Generate a new key***" to create the required private key

Fill in a name

Select "***Generate a new key***"

Enter name and set key size to ***2048 bit***.

Click ***Create***.



Click the Extensions tab.

Under Basic Contraints set the Type to "***Not Defined***"

Uncheck the box "***Critical***"

Ensure the "***Subject Key Identifier"*** and "***Authority Key Identifier***" boxes are checked.

Select the Time Range or change as desired and click ***Apply***.

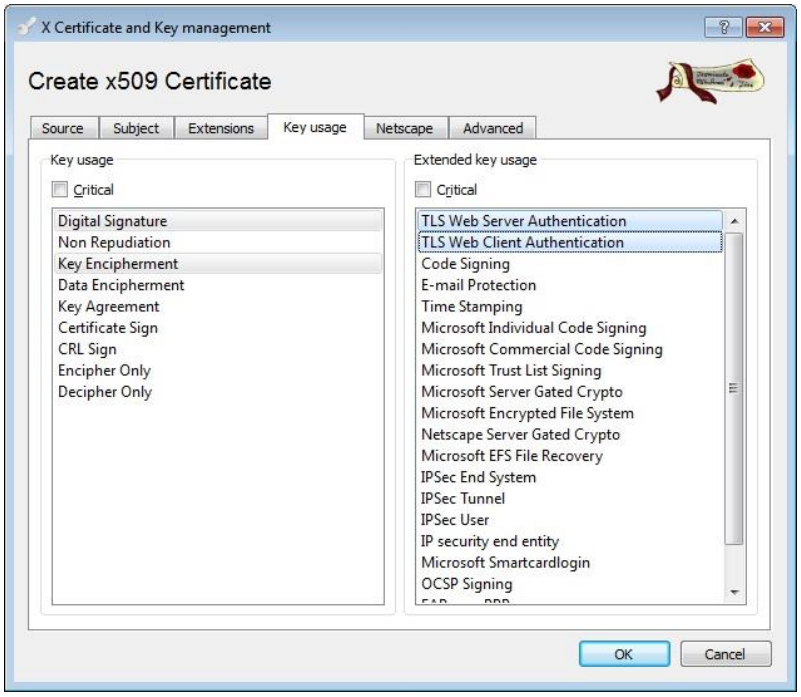
RECOMMENDATION: Set this time period according to your organisations policy.

Select ***subject alternative name*** and ***Add***, select DNS.

Enter the DNS name of the VPEG.

NOTE: This name can be anything but must match the Common Name (CN) that Intel AMT expects (section 5.2)

Click the **OK** button.



Select the Key Usage tab.

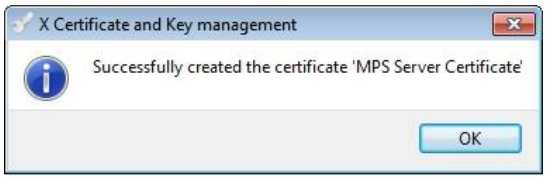
Select "***Digital Signature***" and "***Key Encipherment***" as shown.

Under Extended key usages select

"***TLS Web Server Authentication***"

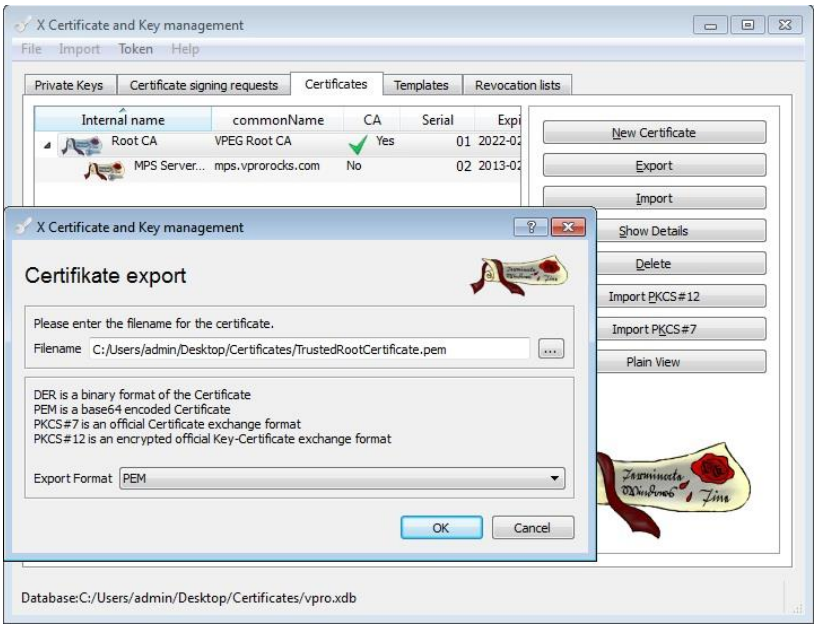
"***TLS Web Client Authentication***"

Click OK.



We now need to export the certificates and key.

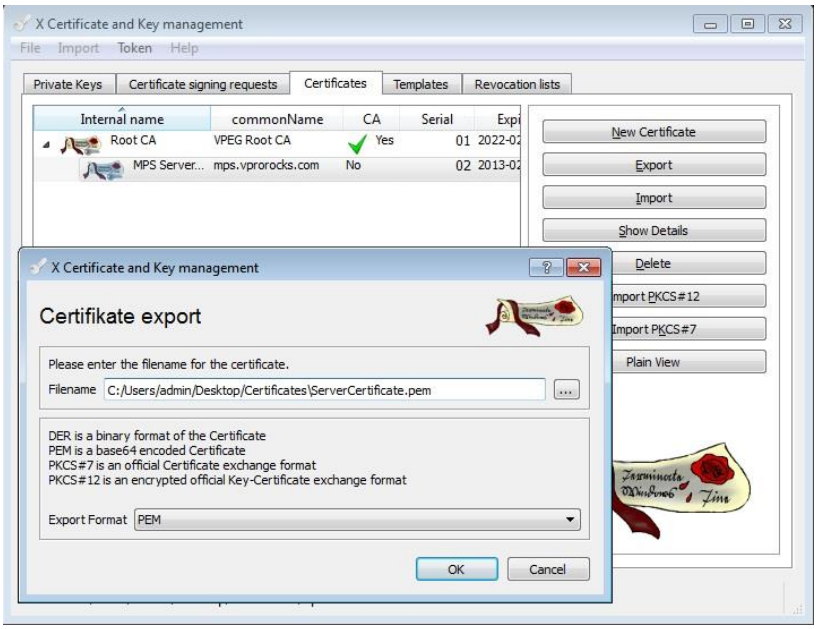
3.3 Export Certificates and Key



Under the ***Certificates*** tab, highlight the Root Certificate and select "***Export***"

Save the file as "***TrustedRootCertificate.pem***"

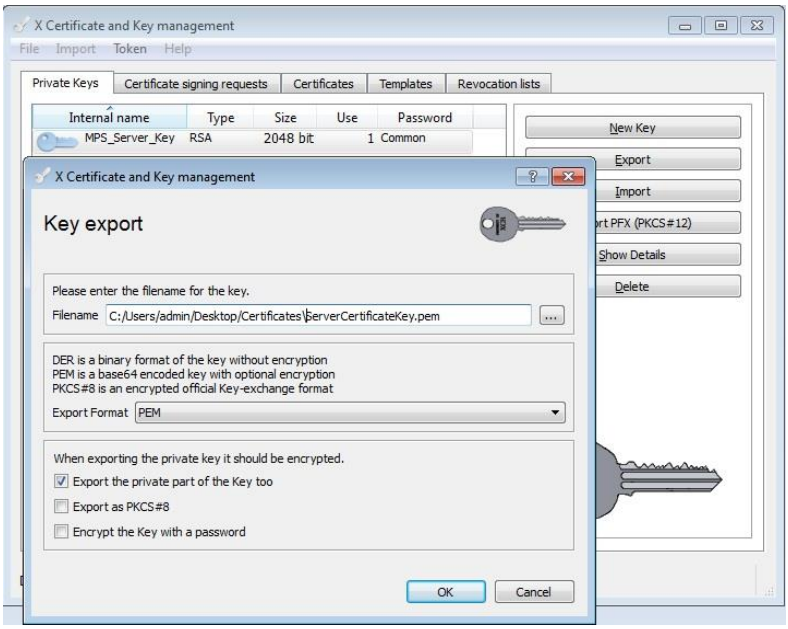
NOTE: Ensure Export Format is PEM.



Under the ***Certificates*** tab, highlight the MPS Server Certificate and select "***Export***"

Save the file as "***ServerCertificate.pem***"

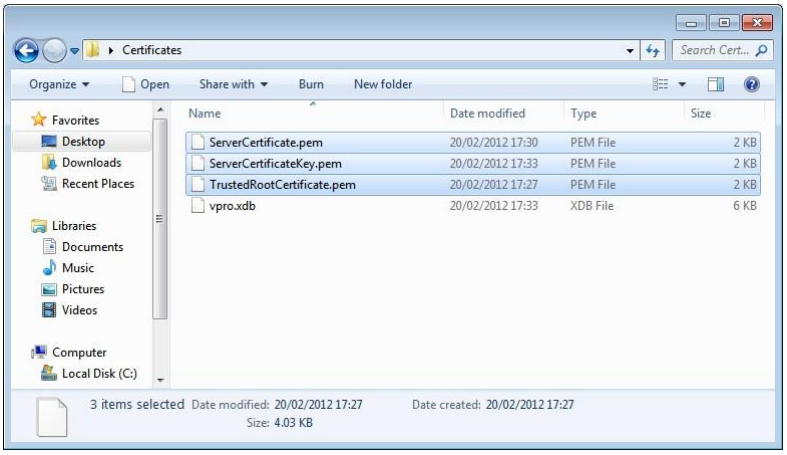
NOTE: Ensure Export Format is PEM.



Under the ***Private Keys*** tab, highlight the Server Key and select "***Export***"

Save the file as "***ServerCertificateKey.pem***"

NOTE: Ensure Export Format is PEM and the box "***Export the private part of the Key too***" is selected.



4. Intel® vPro™ Enabled Gateway Requirements

The Intel vPro Enabled Gateway (VPEG) acts as a standard HTTP and SOCKS proxy server. The HTTP proxy is used to mediate manageability protocols such as WS-MAN whilst SOCKS is used to route the KVM, IDE-Redirection and Serial over LAN protocols. The VPEG performs three major tasks:

1. Provides an secure Internet-facing service that identifies, authorises, and communicates with remote systems hardware using Intel vPro technology.
2. Moderates the flow of manageability operations to and from manageability consoles and applications.
3. Notifies enterprise management servers whenever a system enabled with Intel vPro technology connects or disconnects to the VPEG.

NOTE: Item 3 is currently not supported within this design.

NOTE: Installation and configuration of the VPEG should be performed before it is connected to the DMZ.

4.1 VPEG Platform Dependencies

The base operating system used is Microsoft Windows Server 2008 R2 SP1 X64 configured as a standalone server, i.e. no Domain join and with a single network interface that has a static IP address.

Throughout this document the default network ports used by the VPEG are: 443, 7793, 8080, 8090 and 16992-16995, 16982.

4.1.1 VPEG Components

The VPEG is comprised of three products that provide the required services and this section covers the installation and configuration of each one.

1. The Management Presence Server components are provided in the Intel® AMT Software Development Kit (SDK)
    a. Management Presence Server (MPS.EXE version 1.2.0.21 from the AMT SDK)
    b. Replacement Intel proxy modules for Apache HTTP Server; ***mod_proxy.so*** and ***mod_proxy_connect.so***
2. SSL Tunneling Proxy: stunnel multiplatform SSL tunneling proxy
3. HTTP/HTTPS/SOCKS Proxy: Apache HTTP Server 2.2.8
4. Microsoft Visual C++ 2008 SP1 Redistributable Package (x86) or (x64) is required.
5. XCA: X Certificate and key management: Used to create, modify and manage the required certificates that both the SSL tunneling proxy and Intel AMT client require. A fantastic product that removes much of the complexity associated with certificate and key management.

4.2 Stunnel TLS Tunneling Proxy

The default Transport Layer Security (TLS) provider used within the solution is stunnel. This is a general purpose, multi-platform SSL encryption wrapper that provides SSL functionality between remote clients and local (or remote) servers. Stunnel was chosen as it allows encryption of arbitrary TCP connections inside SSL and is available for both UNIX and Windows operating systems.

Stunnel for Windows is used to establish a SSL session with remote Intel AMT devices and performs authentication, based on a standard server certificate validation process. No check is made for certificate revocation (CRL). Once an SSL session has been established all traffic sent between Intel vPro systems and stunnel is encrypted using SSL

This overall solution has been architected so that SSL connections are completely separated from the MPS core module. To support different deployment environments and provide product choice, stunnel is not hard-wired into the MPS. For example the MPS the solution can utilise any SSL provider and some testing has been performed with other products and SSL VPN appliances.

4.2.1 Installation

RECOMMENDATION: Watch this excellent video which steps through the configuration of the stunnel component: http://www.youtube.com/watch?v=Fy7jNsk2k58&feature=player_embedded

Use default settings during installation.

1. Create the directories ***cert/*** and ***logs/*** under the stunnel installation folder.
2. Copy the certificate files ***TrustedRootCertificate.pem***, ***ServerCertificate.pem*** and ***ServerCertificateKey.pem***, created in the Certificate Management section to the ***cert/*** directory
3. Configure the file ***stunnel.conf*** within the stunnel installation folder as shown in figure 4 below.
4. Install STUNNEL as a service by running **All Programs->stunnel->Service install**.
5. Use regedit and add a **DependOnService** multi-string value to the registry under **HKLM\SYSTEM\CurrentControlSet\services\stunnel**
6. Set this to **Tcpip** to ensure stunnel depends upon the Tcpip service during service start-up.
7. Use **All Programs->stunnel->Service start** to start the stunnel service.

4.2.2 Configuration

The ***stunnel.conf*** file should be edited to include a service definition similar to below. The other parameters and service definitions i.e. pop3, imaps, ssmtp etc. can be disabled by commenting them out of this file.

Detailed descriptions of the required parameters can be found in the following table. Additionally this diagram illustrates the relationship between ports and services.

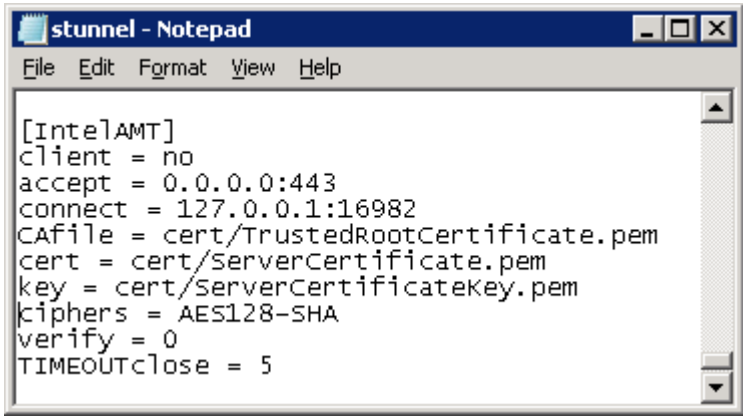


Figure 4

4.2.3 Stunnel SSL Tunneling STUNNEL.CONF parameters

Parameter	Description
Client	The default setting for server mode: ***client = no***
accept	Accept connections from Intel AMT to the MPS component: ***accept = 0.0.0.0:443***

Parameter	Description
connect	This parameter is the IP address and port that stunnel uses to receive data from Intel AMT platforms to the MPS once an SSL tunnel has been established. This must match the address and port configured in MPS.config (***AMTListenIP*** and ***AMTListenPort***) The IP address and port will be ***127.0.0.1:16892*** if stunnel runs on the same platform as the MPS component, or ***localhost:port***. If there is more than one MPS instance then this setting can be used to resolve to multiple addresses and multiple connect options can be specified. The MPS will be chosen using a round-robin algorithm. **NOTE:** No more than one instance of an MPS can run on a single server. ***connect = 127.0.0.1:16982***
CAFile	This is the path of the trusted root certificate used to validate the Intel AMT device's client certificate. ***CAFile = cert/TrustedRootCertificate.pem***
cert	The certificate chain PEM file name ***cert = cert/ServerCertificate.pem*** The certificates must be in PEM format and is always required in server mode (see client parameter above) The file must be sorted starting with the certificate to the highest level (root CA)
key	This is the path to the private key associated with the certificate above and is required to authenticate the certificate owner. **NOTE:** This file should be protected as only readable by owner. ***Key = cert/ServerCertificateKey.pem***
ciphers	This is a list of ciphers (algorithms used for performing encryption) to allow in the SSL connection. **NOTE:** Only AES 128 ciphers are supported by Intel AMT. **ciphers = AES128-SHA**
verify	This is used to verify the peer certificate and is for access control, not authorisation. As only the VPEG provides a certificate set ***verify = 0*** which means the peer certificate is requested but ignored.
debug	Use ***debug = 7*** for highest debug output. **Default 5**
TIMEOUTclose	Use ***TIMEOUTclose = 10***

Table 1

4.2.4 Resilience

The SSL proxy is used to listen for incoming connection requests, over the Internet from Intel vPro systems located outside the enterprise firewall) This can be load balanced using a virtual IP address and during provisioning of Intel vPro systems this virtual IP address should be specified to connect to the VPEG. The load balancer monitors and detects failed server instances and hands off incoming connection requests to functional servers.

4.3 MPS Core Component

4.3.1 Overview

The Manageability Presence Server (MPS) is a reference design implementation that is designed to work in a production, enterprise environment and provide a 24X7 service. The main MPS component (MPS.EXE) acts as a SOCKS proxy for the interface facing the corporate network and provides a TCP APF tunnel for each Intel AMT machine connected to it on the external network.

All information is logged to a regular text file and the MPS has a configurable logging level which controls the amount of information logged.

NOTE: No more than one instance of an MPS can run on a single server.

RECOMMENDATION: Watch this excellent video which steps through the configuration of the MPS component:
http://www.youtube.com/watch?feature=player_embedded&v=SM-XpcQrg0w

4.3.2 Installation

Download and install the Intel AMT Software Development Kit (SDK) from here. Extract the contents into a directory i.e. *<SDK_Root>*

The resulting components, binaries and modules can be found in *<SDK_Root>\Windows\Intel_AMT\Bin\MPS*

1. Download and install Microsoft Visual C++ 2008 SP1 Redistributable Package (x86) or (x64).
2. Manually create the directory ***C:\Program Files (x86)\Intel\MPS*** as the MPS installation folder.
3. From the Intel AMT SDK copy the directories ***conf*** and ***logs*** and their contents into the installation folder.
4. Copy the files *License.txt*, *MPS.exe*, *MPSInterfaceClient.exe* and *ACE.dll* into the installation folder.

NOTE: The MPS binaries provided in the Intel AMT SDK do not support MPS.EXE being started as a Windows service athough this functionality can be provided by third party applications. The user context for the service is local system. Additionally the MPS component does not currently support a graceful shutdown mechanism therefore it is necessary to manually kill the process.

4.3.3 Configuration

This section deals configures the MPS component to listen for incoming connection requests and to connect to the MPS management interface using the SOAP protocol.

NOTE: Detailed descriptions of the required parameters can be found in the table within the next section. Additionally the diagram here illustrates the relationship between IP addresses, ports and services.

Edit the ***mps.config*** file found in the ***conf*** directory. Locate the *[Network]* section and modify the following parameters appropriate to your environment.

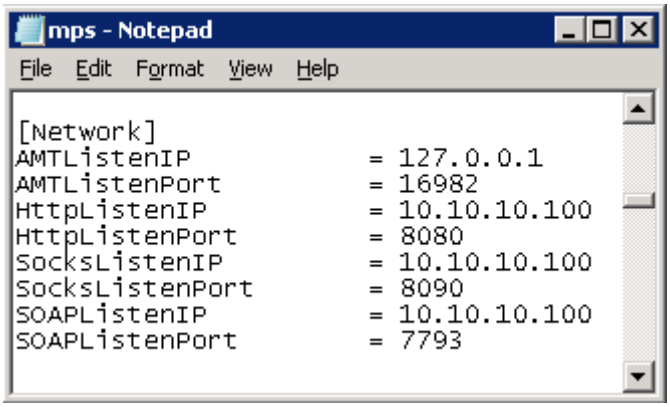


Figure 5

4.3.4 Management Presence Server MPS.CONFIG parameters

Intel vPro systems access the MPS using the ports defined during configuration (***mps.config***). Within this solution the following table lists the required configuration parameters.

Parameter	Description
AMTListenIP	This is the IP address or FQDN address that the MPS uses to listens for Intel AMT connections. The tunneling proxy (stunnel) uses this to forward connections from the Intel AMT platform. The IP address MUST equal the one entered in ***stunnel.conf connect*** parameter When the tunneling proxy runs on the same platform as the MPS, this will be: **Default 127.0.0.1**
AMTListenPort	This is the port that the MPS uses to listen for connections from Intel AMT platforms. The tunneling proxy (stunnel) uses this to forward connections from the Intel AMT platform. This port MUST equal the ***stunnel.conf connect*** parameter. **Default 16982**
SocksListenIP	This is the IP address or FQDN address of the intranet facing MPS network interface and is the address that the MPS listens to for new SOCKS connection requests. This address MUST be equal to the one entered in ***httpd.conf*** in the ***ProxySocksIP*** parameter
SocksListenPort	Port used in SOCKSv5 connections from redirection applications or traffic from the proxy server. This port MUST equal the one entered in ***httpd.conf*** for the ***ProxySocksPort*** parameter. **Default 8090**
HttpListenIP	This is the IP address or FQDN address that the MPS listens to for new HTTP connection requests from Apache. This address MUST equal the one entered in ***httpd.conf*** in the ***Listen*** parameter.
HttpListenPort	This is the port used in HTTP/HTTPS proxy connections from management consoles. This address MUST equal the one entered in ***httpd.conf*** in the ***Listen*** parameter. **Default 8080**
SOAPListenIP	This is the IP address or FQDN used by Intel MPS to listen for incoming connection requests from internal management consoles and software to connect to the MPS management interface using the SOAP protocol. IP or FQDN address that the MPS listens to for new SOAP connection requests.
SOAPListenPort	Port that the MPS listens to for new SOAP connection requests. **Default 7793**

Table 2

4.3.5 Resilience

Intel AMT firmware can be configured to maintain the names or IP addresses of up to two VPEG's to allow Intel vPro systems to connect into the enterprise network, even when one VPEG is unavailable. DNS round-robin could be used or an SSL terminator configured to choose a VPEG based upon load, however configuration of this is outside the scope of this solution design.

4.4 Apache HTTP/HTTPS/SOCKS Proxy

Apache HTTP server acts as an HTTP/HTTPS proxy server and enables connections to Intel AMT systems through the MPS, via a standard HTTP proxy interface. Intel have added the MPS software modules (***mod_proxy.so*** and ***mod_proxy_connect.so***) to the Apache HTTP server to support outgoing HTTP and HTTPS requests to be redirected through a SOCKS v5 proxy server.

RECOMMENDATION: Watch this excellent video which steps through the configuration of the Apache HTTP Server component: http://www.youtube.com/watch?v=B1bXwRjTS_A&feature=player_embedded

4.4.1 Installation

1. Install Apache HTTP server version 2.2.8 or compatible.
2. Make a backup copy of the two existing shared object modules **mod_proxy.so** and **mod_proxy_connect.so**.
3. Copy the **mod_proxy.so** and **mod_proxy_connect.so** files supplied in the Intel AMT SDK to the **modules** directory under the Apache installation folder. These files can be found in the following directories:

   <SDK_Root>\Windows\Intel_AMT\Bin\MPS\Apache\mod_proxy.so

   <SDK_Root>\Windows\Intel_AMT\Bin\MPS\Apache\mod_proxy_connect.so
4. Modify ***httpd.conf*** as described in the configuration section below.
5. Restart Apache HTTP Server.

4.4.2 Configuration

Edit the configuration file ***httpd.conf*** found in the ***conf/*** directory under the Apache installation folder to enable HTTP and SOCKS proxy functionality:

LoadModule proxy_module modules/mod_proxy.so

LoadModule proxy_connect_module modules/mod_proxy_connect.so

LoadModule proxy_http_module modules/mod_proxy_http.so

LoadModule headers_module modules/mod_headers.so

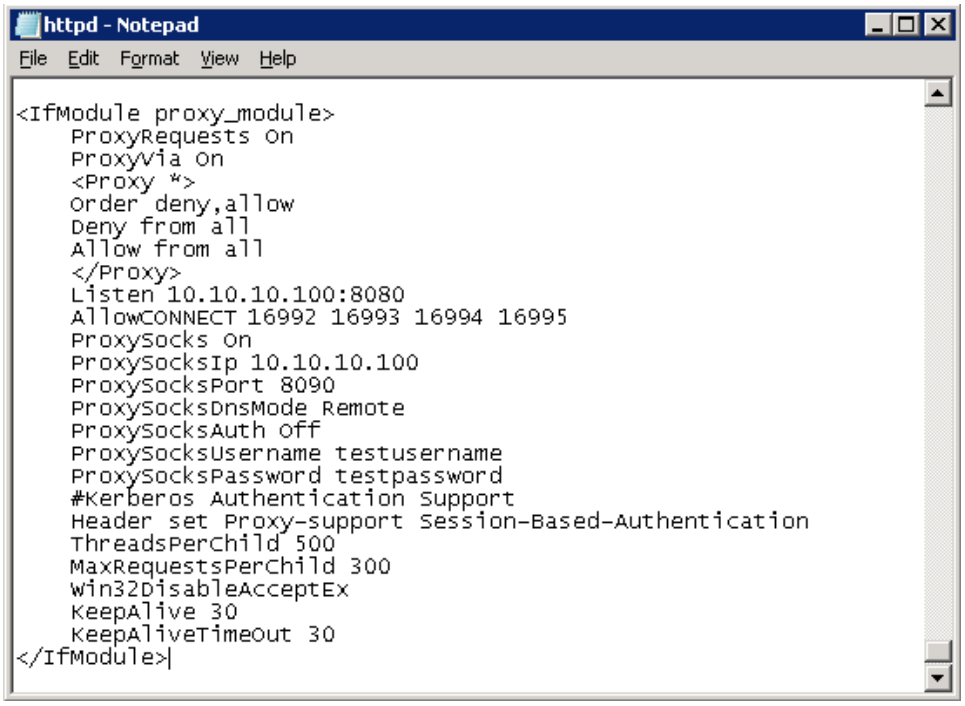


Figure 6

4.4.3 Apache HTTP Server HTTP.CONF parameters

In the following sample outgoing HTTP and HTTPS connections will be redirected through the SOCKS5 proxy server. DNS queries go through the proxy unchanged.

Parameter	Description
ProxySocks	This value turns SOCKS5 functionality on or off. Default is off, set to ***On***
ProxySocksIP	This is the IP address used by the SOCKS proxy to listen for connection requests from internal management consoles and software using the re-direction protocol to communicate with remotely connected Intel vPro systems. IP address or FQDN of the SOCKS5 proxy server MUST equal the *SocksListenIP* parameter in ***mps.config***.
ProxySocksPort	This is the port number of the SOCKS proxy to listen for internal connection requests from management consoles and software using the re-direction protocol to communicate with remotely connected Intel vPro based systems. MUST equal the parameter entered in ***mps.config*** for *SocksListenPort* parameter. Default ***8090***
ProxySocksDnsMode	This value sets the mode of hostname resolution. To pass DNS queries through SOCKS5 proxy use Remote mode. Default ***Remote***
ProxySocksAuth	Enables Username/Password authentication (RFC1929) on the SOCKS5 proxy. Default ***OFF***
ProxySocksUsername	Username to login on SOCKS5 proxy. Not required when *ProxySocksAuth* is set to ***OFF.***
ProxySocksPassword	Password to login on SOCKS5 proxy. Not required when *ProxySocksAuth* is set to ***OFF.***

Parameter	Description
Listen	This is the IP address and port number used by the HTTP proxy to listen for internal connection requests from management consoles and software using HTTP to communicate with remotely connected Intel vPro based systems. The IP address and port number MUST equal the *HttpListenIP* parameter in ***mps.config***. Default port is **8080**. Example syntax is: ***Listen 10.10.10.100:8080***
AllowCONNECT	This configures the ports to which the HTTP proxy is allowed to connect i.e. ***AllowCONNECT 16992 16993 16994 16995***

Table 3

4.4.3.1 Kerberos Authentication Support

If Kerberos Kerberos authentication is a requirement then Apache has to be configured to support this and parse the entire HTTP header. For reference the settings below are included in the example ***httpd.conf*** in figure 8:

```
#Kerberos Authentication Support
Header set Proxy-support Session-Based-Authentication
ThreadsPerChild 500
MaxRequestsPerChild 300
Win32DisableAcceptEx
KeepAlive 30
KeepAliveTimeOut 30
```

4.4.4 Resilience

The HTTP/SOCKS proxy listens for incoming connection requests from the Intranet i.e. management consoles and software located inside the enterprise firewall. However it should not be load balanced as the MPS component does not currently have the capability to share connection session information between server instances.

5. Intel vPro Client Requirements

The main components for the solution reside on the VPEG however there are several dependencies on the Intel vPro based system and configuration is required to support CIRA. The following Microsoft Windows services, system drivers and tools are required.

5.1.1 Local Management Service (LMS)

The LMS listens for and intercepts requests directed to the Intel AMT local host and routes them to the Intel Management Engine (Intel ME) via the Intel Management Engine Interface (Intel MEI) driver.

5.1.2 User Notification Service (UNS)

This Windows service registers with the Intel AMT device to receive a set of alerts. When UNS receives an alert it logs the alert in the Windows Application event log. The Event Source will be "*Intel(R) AMT*".

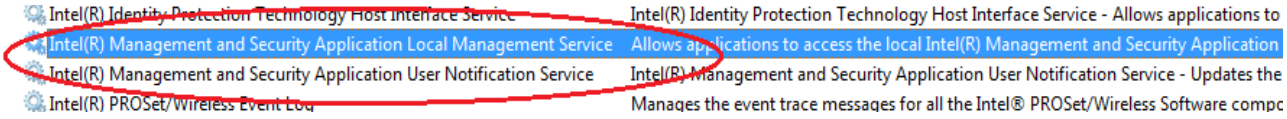


Figure 7

5.1.3 Intel® Management Engine Interface (Intel® MEI)

This operating system device driver provides access to the Intel ME and is required.

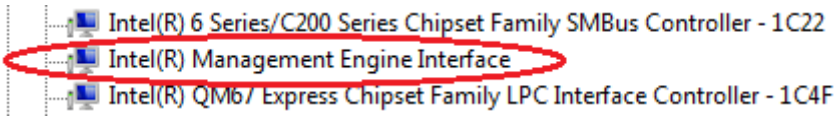


Figure 8

5.1.4 Intel® Management and Security Status (IMSS) tool

The IMSS tool is an optional component but recommended. It provides detail on the Intel services available on the platform, an event history and more advanced information. It can be accessed via the "blue key" icon in the Windows System tray.

5.2 Provisioning Intel vPro Technology

To prepare an Intel AMT platform for remote access, there are several configuration options available dependent upon the supported Intel AMT firmware version.

- For Intel AMT firmware version <6.2 then the Intel Setup and Configuration Software (Intel SCS) is required. This activity must be performed when Intel SCS and the Intel AMT platform are on the same LAN network, either during initial provisioning or afterwards as a delta configuration.
- For Intel AMT firmware version >=6.2, host-based provisioning can be used. This must be performed at the time of configuration. No delta configuration option is available.

To enable remote access for either provisioning method, you must configure the appropriate profile and provide the following information:

- Trusted root certificate (*TrustedRootCertificate.pem*) used to authenticate the server certificate (*ServerCertificate.pem)* which is sent by the tunneling proxy when setting up the TLS tunnel.

NOTE: Remote Access will fail if the Intel vPro based system does not have a trusted root certificate (*TrustedRootCertificate.pem*) for the stunnel server certificate (*ServerCertificate.pem*).

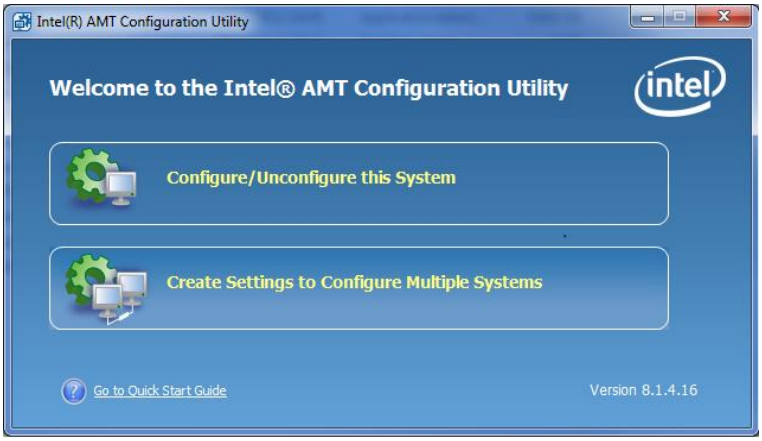
- Information on how to contact the VPEG, i.e. IP address or FQDN and port number.

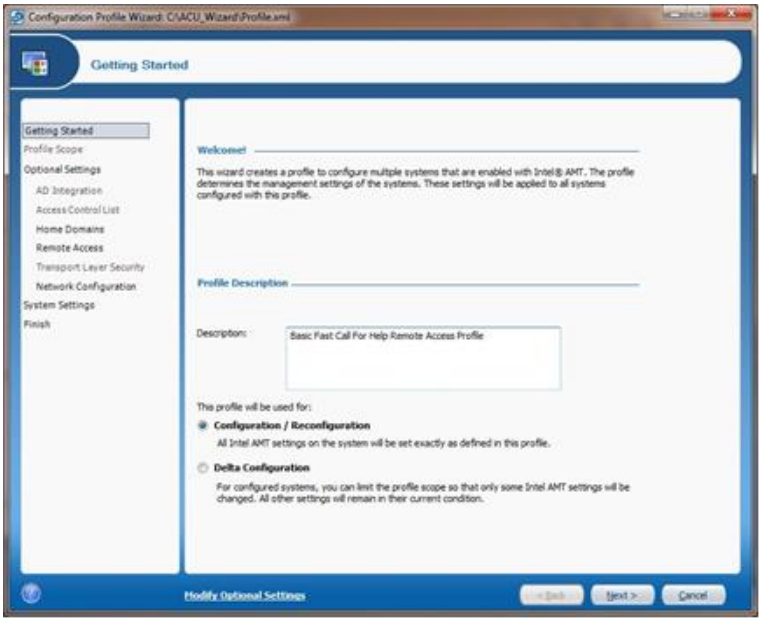
NOTE: Intel AMT platforms can be configured with up to four different VPEG instances.

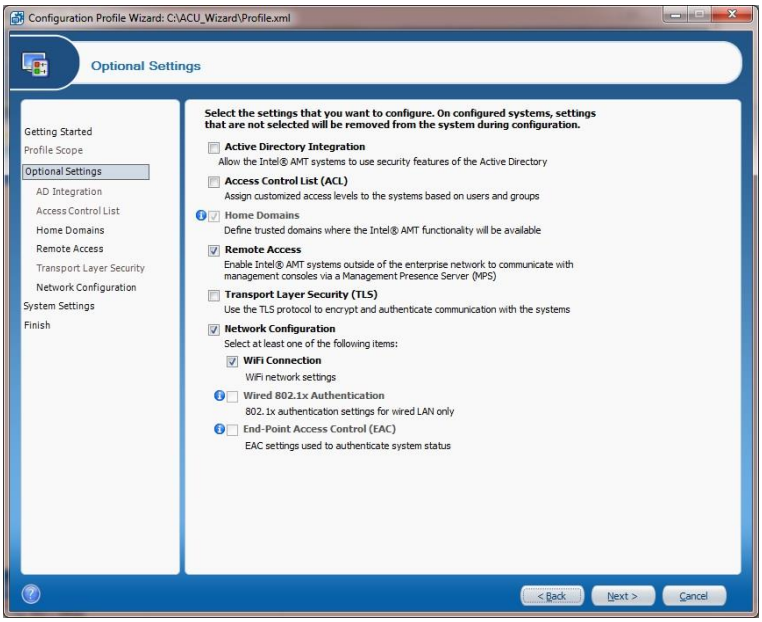
- Remote access policy, the current solution supports both the OS and BIOS interfaces policies.

NOTE: The Intel AMT firmware can maintain the names or IP addresses of up to two VPEG systems and a remote access policy can be associated with these. Intel AMT will attempt to connect with the first instance, and then the second instance. The attempt to connect will be repeated once.

The following section details a simple procedure for configuring your Intel AMT system to support CIRA (including Intel AMT over wireless).

<table>
<tr><td colspan="2">Download the Intel® Setup and Configuration Software (Intel® SCS) from http://software.intel.com/en-us/articles/download-the-latest-version-of-intel-amt-setup-and-configuration-service-scs/</td></tr>
<tr><td>Extract the directory ACU_Wizard.</td><td></td></tr>
<tr><td> 
</td><td>From the ACU_Wizard directory run ACUWizard.exe.

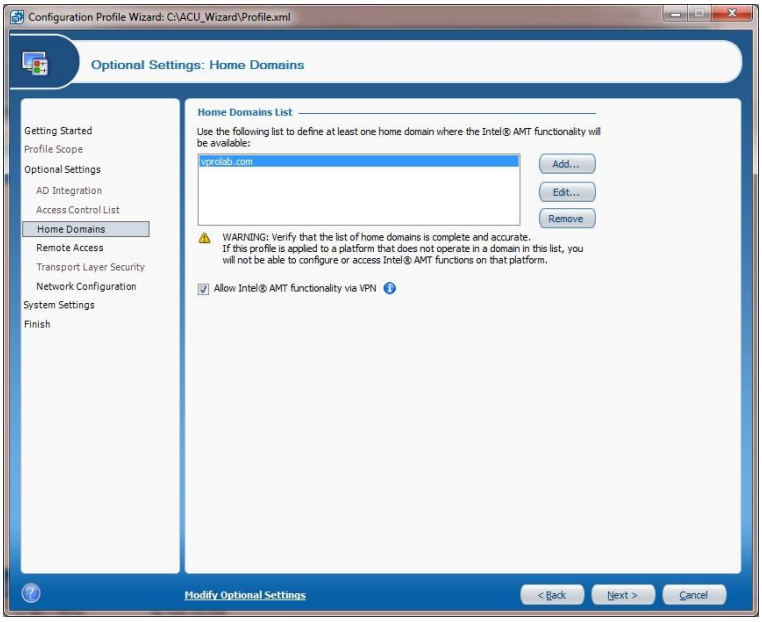
Select “Create Settings to Configure Multiple Systems”</td></tr>
<tr><td> 
</td><td>Create a new profile and enter a suitable description</td></tr>
</table>



Select the settings:

- "Home Domains"
- "Remote Access"

NOTE: The "Network Configuration and "WiFi Connection " settings are optional but not recommended during intial configuration.



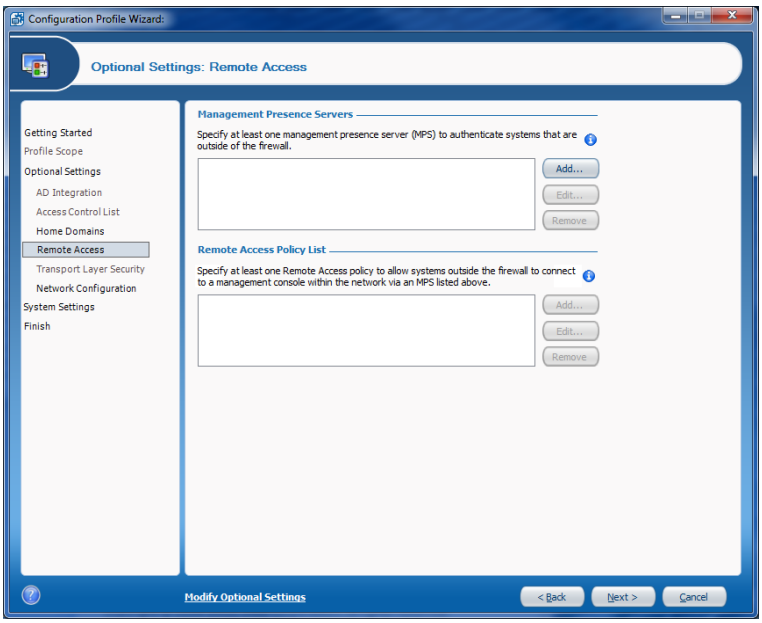
From the Home Domains list select Add and enter a DNS suffix name.

NOTE: This setting much match the DNS domain suffix provided by the corporate DHCP server.

If this profile is applied to an Intel AMT system that does not operate in a domain in this list, you will not be able to configure or access Intel AMT functions on that system.

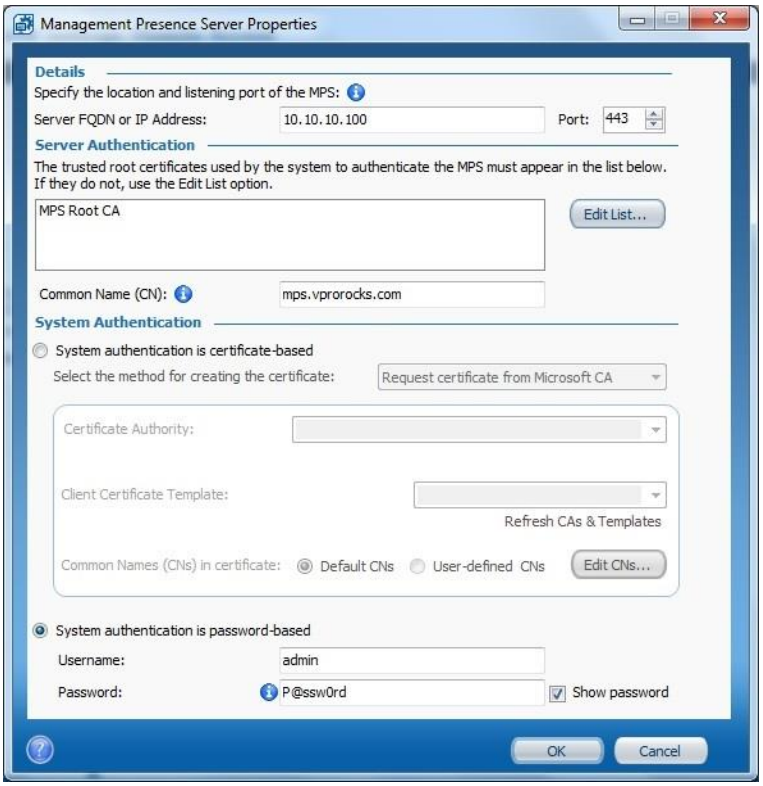
Select **Allow Intel® AMT functionality via VPN**

This permits access to Intel AMT (HTTP/HTTPS) over an operating system level Virtual Private Network when it is connected via a VPN to a domain in the Home Domains list.



From the Management Presence Servers section of the Remote Access window, click **Add**.

The Management Presence Server Properties window opens.



Enter the FQDN or IP address and port that stunnel listens on for connections from Intel AMT systems.

Click **Edit List** and add the trusted root certificate, see additional detail below.

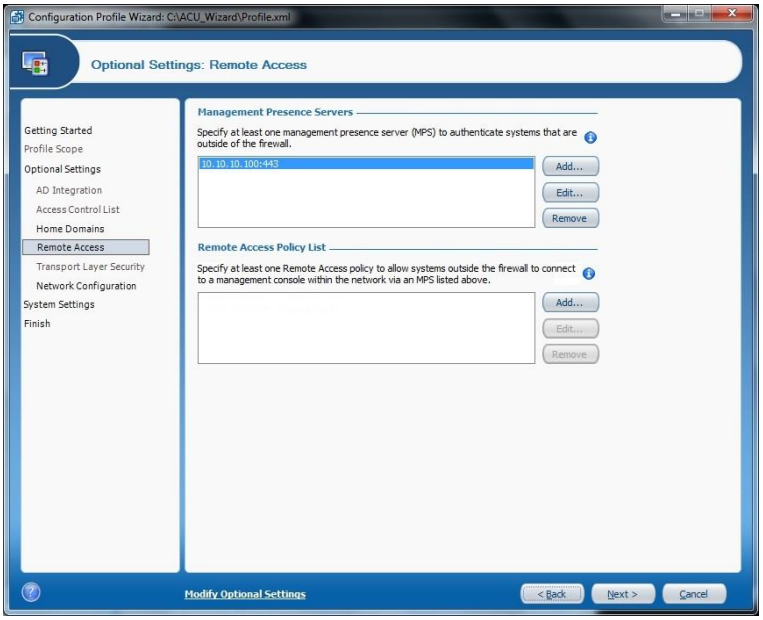
If you entered an IP address in the Server FQDN or IP Address field, enter the FQDN in the Common Name (CN) field.

Select **System authentication is password based** and enter a username and password.

Additional detail for adding the trusted root certificate (*TrustedRootCertifcate.pem*) created in section 3.

Select **From File** and enter the path to the file or Browse to locate and select the trusted root certificate.

Click OK.



Now define at least one Remote Access policy.

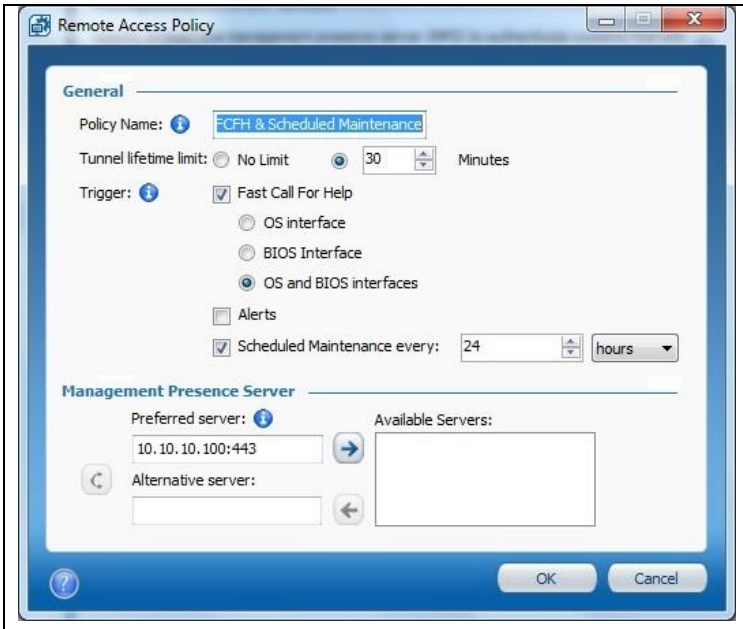
From the Remote Access Policy List section, click **Add** and enter a policy name.

Set the Tunnel lifetime limit to an interval in minutes. When there is no activity in an established tunnel for this period of time, Intel AMT will close the tunnel.

Selecting No Limit means the tunnel will not time out but will stay open until it is closed by the user or when a different policy with higher priority needs to be processed.

In the Trigger section, select the **Fast Call For Help** and **OS and BIOS interfaces** (default)

Remote Access policies also support scheduled maintenance and alerts. Scheduled maintenance is a capability to automatically initiate a connection from a remote Intel vPro based system back into the corporate network against a defined time period, i.e. every 48 hours.

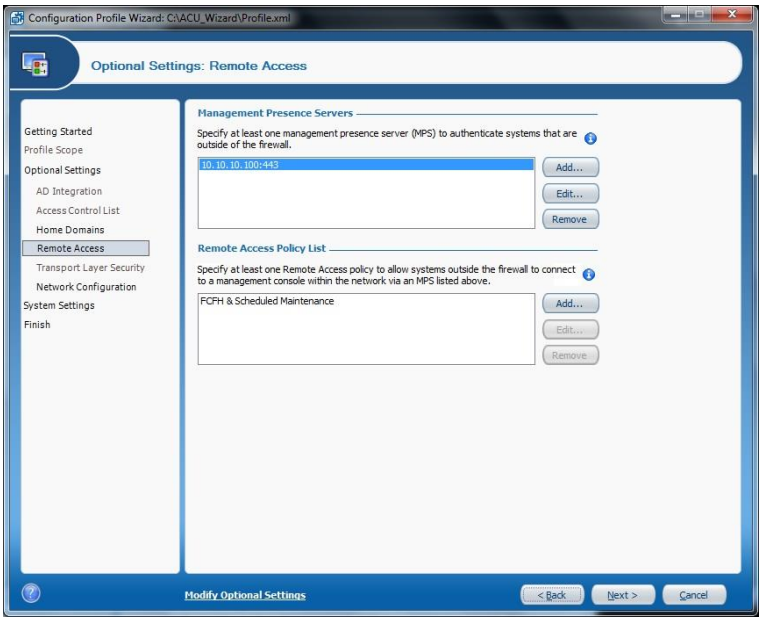


Within this solution **Scheduled Maintenance** is configured as a trigger and will automatically to connect every 24 hours.

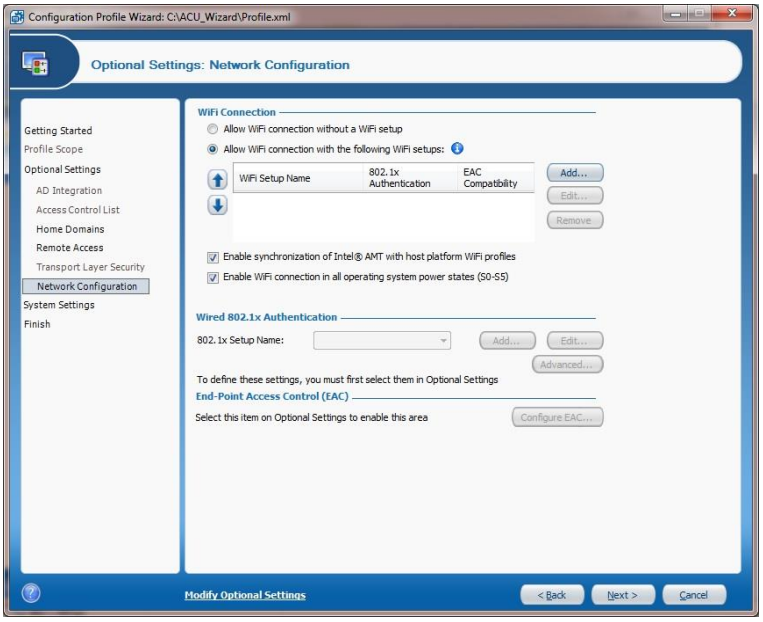
NOTE: A policy can include one or more triggers, but two different policies cannot contain the same trigger.

In the Management Presence Server section, select up to two VPEG's that apply to the policy.

When a trigger occurs, the Intel AMT device attempts to connect to the server listed in the Preferred server field. If that connection does not succeed, the device tries to connect to the server listed in the Alternative server field, if one was specified.



Click OK to close the Remote Access Policy window.

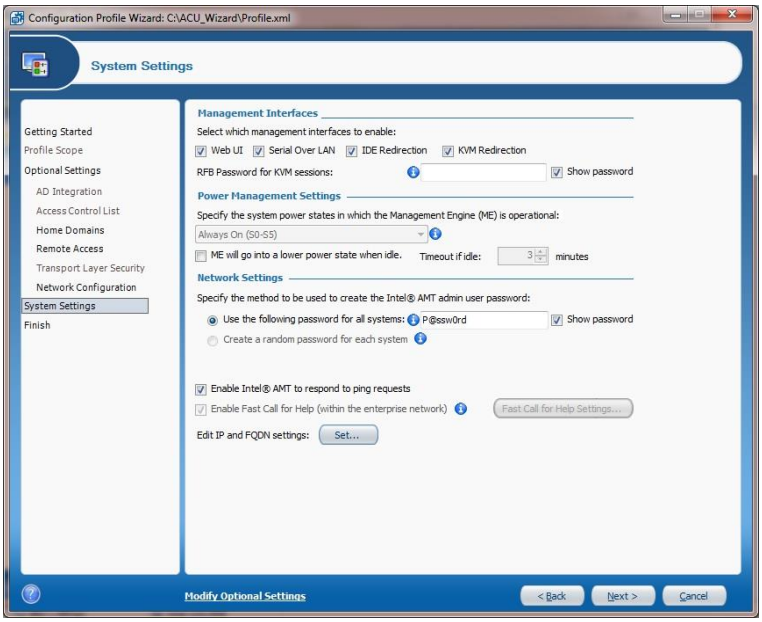


RECOMMENDATION: Return to this step once you've got CIRA working successfully! Initially connect using the standard wired Ethernet interface.

Select **Allow WiFi connection without a WiFi setup** to allow WiFi connection using OS WiFi settings.

Select **Enable Synchronization of Intel® AMT with host platform WiFi profiles**

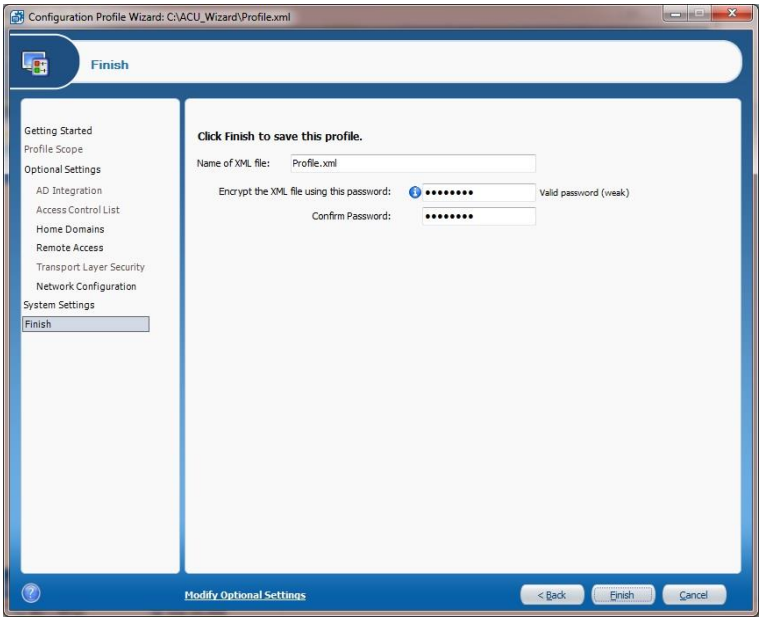
Intel AMT 6.0 and higher supports synchronisation of the WiFi profiles present on the host platform with the WiFi setups defined in the Intel AMT device. Intel® PROSet/Wireless Software is used to support this capability.



The System Settings window of the Configuration Profile Wizard lets you define several settings in the Intel AMT device.

You cannot make changes to the setting **Enable Fast Call for Help (within the enterprise network)** as a Fast Call For Help trigger was defined in a Remote Access policy.

The setting in the policy is used for remote and local connection requests.



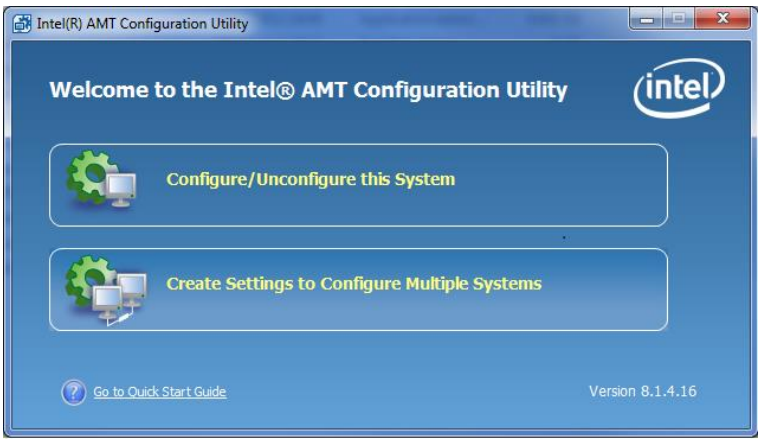
The Configuration Utility uses XML files for host-based configuration.

These files can contain information about your network and to protect this data, each profile created or edited by the Configuration Utility is encrypted with a password that you must supply (and remember!).

The XML profiles are encrypted using this format:

- Encryption algorithm is AES128 using SHA-256 on the provided password to create the key
- Encryption mode: CBC
- Initialize Vector (IV) is the first 16 bytes of the Hash

Save the resulting ***Profile.xml*** file to ***C:\ACU_Wizard***.



From the ***ACU_Wizard*** directory run ***ACUWizard.exe***.

Select "**Configure/Unconfigure this System**" and "**Configure via Windows**", enter the password and Intel AMT will configure itself using the above profile.

5.3 CIRA over WiFi

Although CIRA over a WiFi connection is not the focus of this solution, basic validation has been performed.

The use case supports the user bringing their Intel vPro notebook or Ultrabook™ home and connecting to their home WiFi network from within the operating system. Upon successful connection the wireless profile is synchronised with Intel AMT by Intel PROSet/Wireless Software so that when the system is powered down, Intel AMT maintains the WiFi connection. This removes the requirement for a wired connection and the associated issues with locating an Ethernet cable, then having to plug this into their home wireless router.

To support this capability Intel PROSet/Wireless software must be installed on the notebook. See next section for details.

5.3.1 Intel® PROSet/Wireless Software

Intel® PROSet/Wireless[1] supports Intel vPro Technology and when used with Intel Active Management Technology (Intel AMT version 6.0 and higher) provides the capability to synchronise WiFi profiles from the host operating system and make these available as WiFi setups within the Intel AMT device.

- User-defined: When a user performs a successful connection to a wireless network with a WiFi profile that is not defined in Intel AMT, Intel PROSet/Wireless displays a pop-up message asking the user if they want to add the profile to Intel AMT and make the profile available for use by Intel AMT.
- IT-defined: WiFi profiles that are added to the host operating system through a Group Policy by IT administrators will be added to Intel AMT.

	From Windows or the Intel PROSet/Wireless WiFi Connection Utility select the appropriate WiFi network. **NOTE:** There are limitations with profile selection where when a CIRA connection is attempted out-of-band i.e. no operating system running, Intel AMT will attempt to connect to the last known associated WiFi profile. If that connection is no longer valid then the CIRA connection will fail. For example when a user brings their laptop home from work and they are unable to associate with their home network before they have a problem, CIRA over WiFi will not work. **NOTE:** Remote power control operations over WiFi can cause loss of connectivity to Intel AMT.
When prompted enter the Wireless encryption key.	
	The first time this connection is configured a window will prompt to synchronise the user profile with Intel Active Management Technology. This makes the WiFi connection profile available to Intel AMT.

[1] Intel® PROSet/Wireless version 15.3 for Microsoft Windows 7* 32-bit and 64-bit operating systems only

6. Management Components

6.1 Get-AMTFCFHConnection.ps1

This script connects to one or more Intel VPEG's and enumerates the currently connected remote Intel vPro systems.

Run the script with two required parameters, the IP address (or IP addresses, separated by a comma) of the VPEG and the SOAP port (7793) as shown below in figure 9.

If Intel vPro systems are connected then output is displayed as below, otherwise nothing is returned.

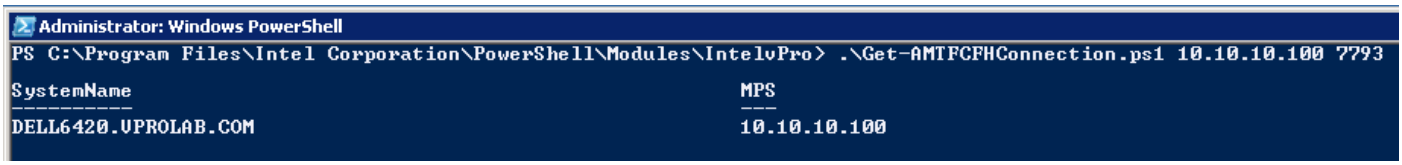


Figure 9

6.1.1 Windows PowerShell Requirements

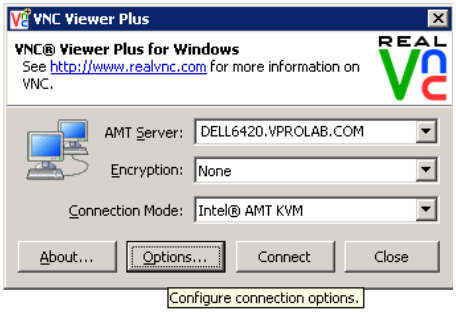
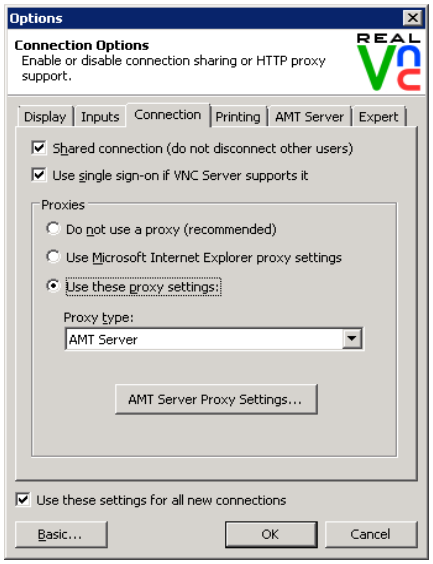
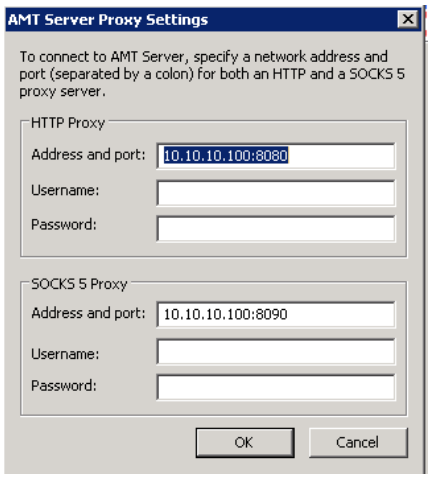
The above script is dependent upon the Intel vPro Technology Module for Windows PowerShell downloadable from http://communities.intel.com/docs/DOC-4800) Follow the instructions to install and configure the product.

Copy the Windows PowerShell script into the Intel vPro Technology Module for Windows PowerShell installation folder:

- For 64-bit Windows path = *C:\Program Files (x86)\Intel Corporation\PowerShell\Modules\IntelvPro*
- For 32-bit Windows path = *C:\Program Files\Intel Corporation\PowerShell\Modules\IntelvPro*

6.2 VNC* Viewer Plus Configuration

This section covers configuring RealVNC VNC* Viewer Plus to support connections to the VPEG and enable Intel AMT KVM connections to be established to the remote Intel vPro based system.

		
Select "Options" button from the main screen	On the Connection Tab, select "Use these proxy settings" and specify "AMT Server" as the proxy type.	Enter the IP address and port number of the HTTP and SOCKS proxy.

7. Solution Performance & Scalability

The VPEG has been tested to evaluate performance and stability capabilities. The test environment was capable of simulating thousands of Intel AMT instances with realistic response times and functional behavior. Two tests were run, the first a stability test and the second an attempt to identify a connection limit.

7.1 Stability

This test ran a simulated environment that consisted of 1000 Intel AMT devices connected to the VPEG, then began transmitting SOL data over the VPEG. The test was run over 48 hours with the following results:

The VPEG was stable and still functioning after 48 hours.

There were no disconnections or transmission failures during the 48 hours.

The maximum hardware load for the MPS.exe process was 15% CPU usage with 26 MB of RAM used and 725 KB I/O (for MPS log files).

7.2 Connection Limitations

The connection limitation test checked the maximum number of connections that the VPEG can reliably support. The test created several hundred simulated connections and then attempted to open a redirection session from an Intel AMT platform.

With approximately 500 existing connections the Intel AMT 7.0 platform connected and redirection sessions were opened successfully.

With approximately 600 existing connections Intel AMT platforms still connected, however redirection sessions failed to open and generated a "Session Closed" error.

These tests show that the VPEG is stable when managing approximately 500 active connections.

7.3 Latency

Functional testing was performed against a vPro Enabled Gateway, located at an Intel facility in Folsom, California, USA and an Intel AMT system located in Israel in an attempt to represent a worst-case scenario. The management console component was also located in Israel both behind a 1.5 MB ADSL connection.

The latency between the Intel AMT system and the VPEG was approximately 240 msec with latency back to the management console being slightly lower at 220 msec.

7.4 Redirection Performance

The following table identifies the IDER performance for wired and wireless over a CIRA connection using an IDER test application.

Bandwidth	Downlink Speed	Uplink Speed	RTT Latency	IDE-R over CIRA Throughput
High	2 Mbps	2 Mbps	80 ms	125 KB/s
Medium	768 Kbps	256 Kbps	80 ms	48 KB/s
Low	512 Kbp	512 Kbp	80 ms	32 KB/s

Table 4

8. Security Considerations

8.1 Securing the Intel vPro Enabled Gateway

With Intel AMT based systems operating outside the enterprise firewall and the VPEG operating inside, firewalls must be configured to allow traffic to flow between Intel AMT based systems and the VPEG. Further, the VPEG may be in a DMZ, with additional firewalls between it and the intranet. Dependent upon policy, the external firewall must be configured to allow packets addressed to the incoming and outgoing ports to cross the firewall. Below are example guidelines to secure the VPEG.

- Configure the network interface to disable all network services and protocols except for TCP/IP.
- Disable the interface from registering addresses in DNS.
- Disable NetBIOS over TCP/IP.
- Create an inbound firewall rule allowing incoming TCP traffic from any port to ports 443, 8080, 8090, 7793
- Create an outbound firewall rule allowing outgoing TCP traffic from any port to any port.

8.2 Incoming Ports

External Intel AMT based systems connect to the VPEG using ports defined in the SSL proxy configuration (stunnel).

8.3 Outgoing Ports

Intel AMT accepts connnections on the following ports

16992 SOAP over TCP

16993 SOAP over TLS

16994 Redirection over TCP

16995 Redirection over TLS

623 DASH over TCP

664 DASH over TLS

8.4 Apache* HTTP Server

Apache* HTTP server is used as a HTTP and SOCKS proxy and filters incoming and outgoing packets between Intel AMT based platforms and the enterprise network. Applications determine the ports for each session managed, outgoing ports are the standard ones listed.

The Apache configuration parameter ***AllowCONNECT*** lists all Intel AMT ports that Apache will accept. Within this solution the configuration parameter in ***httpd.conf*** is: **AllowCONNECT 16992 16993 16994 16995**

8.5 Stunnel

Stunnel uses OpenSSL libraries for cryptography and FIPS 140-2 support is available and enabled by default in the Windows version of stunnel used within this solution.

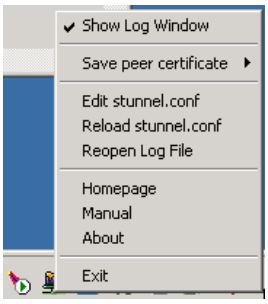
8.6 Additional Protocol Authentication

An authentication mechanism exists for providing additional security for SOCKS, SOAP and AMT data. Authentication of the user name and password from APF and Intel AMT data can take a long time and blocks threads upon which the data was received. This subsequently ends up blocking lots of threads for a long time and can use up all of the threads in the thread pool.

9. Troubleshooting

9.1 Successful stunnel log output

Find below the log output for a successful SSL connection between the Intel AMT based client and stunnel. Once an SSL session is established then stunnel simply connects to the MPS listener on port 16982.

Right-click on the stunnel system tray icon to display the log window. **NOTE:** Log output uses ***debug = 7*** and can be set in the configuration file ***stunnel.conf***	

No limit detected for the number of clients

```
stunnel 4.54 on x86-pc-msvc-1500 platform
Compiled/running with OpenSSL 1.0.1c-fips 10 May 2012
Threading:WIN32 SSL:+ENGINE+OCSP+FIPS Auth:none Sockets:SELECT+IPv6
Reading configuration from file stunnel.conf
FIPS mode is enabled
Compression not enabled
Snagged 64 random bytes from C:/.rnd
Wrote 1024 new random bytes to C:/.rnd
PRNG seeded successfully
Initializing service [IntelAMT]
Certificate: cert/ServerCertificate.pem
Certificate loaded
Key file: cert/ServerCertificateKey.pem
Private key loaded
Loaded verify certificates from cert/TrustedRootCertificate.pem
Loaded cert/TrustedRootCertificate.pem revocation lookup file
Could not load DH parameters from cert/ServerCertificate.pem
Using hardcoded DH parameters
DH initialized with 2048-bit key
ECDH initialized with curve prime256v1
SSL options set: 0x03000004
Configuration successful
Service [IntelAMT] (FD=232) bound to 0.0.0.0:443
Service [IntelAMT] accepted (FD=424) from 10.10.10.15:664
Creating a new thread
New thread created
Service [IntelAMT] started
Service [IntelAMT] accepted connection from 10.10.10.15:664
SSL state (accept): before/accept initialization
SSL state (accept): SSLv3 read client hello B
SSL state (accept): SSLv3 write server hello A
SSL state (accept): SSLv3 write certificate A
SSL state (accept): SSLv3 write certificate request A
SSL state (accept): SSLv3 flush data
SSL state (accept): SSLv3 read client certificate A
SSL state (accept): SSLv3 read client key exchange A
SSL state (accept): SSLv3 read finished A
SSL state (accept): SSLv3 write change cipher spec A
SSL state (accept): SSLv3 write finished A
SSL state (accept): SSLv3 flush data
1 items in the session cache
0 client connects (SSL_connect())
0 client connects that finished
0 client renegotiations requested
1 server connects (SSL_accept())
```

Works with the stunnel version 4.54!

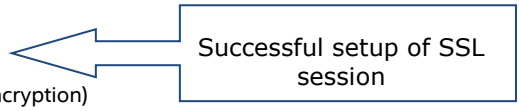
Server certificate & key loaded & verified

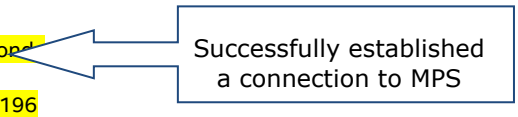
Start service & listen on 443

Incoming connection from Intel AMT

Start SSL session setup

1 server connects that finished
0 server renegotiations requested
0 session cache hits
0 external session cache hits
0 session cache misses
0 session cache timeouts
No peer certificate received
SSL accepted: new session negotiated
Negotiated TLSv1/SSLv3 ciphersuite: AES128-SHA (128-bit encryption)
"Compression: null, expansion: null"
connect_blocking: connecting 127.0.0.1:16982
connect_blocking: s_poll_wait 127.0.0.1:16982: waiting 10 second
connect_blocking: connected 127.0.0.1:16982
Service [IntelAMT] connected remote server from 127.0.0.1:49196
Remote socket (FD=444) initialized

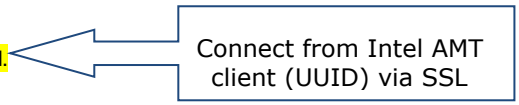


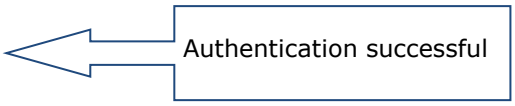


9.2 Successful MPS log output

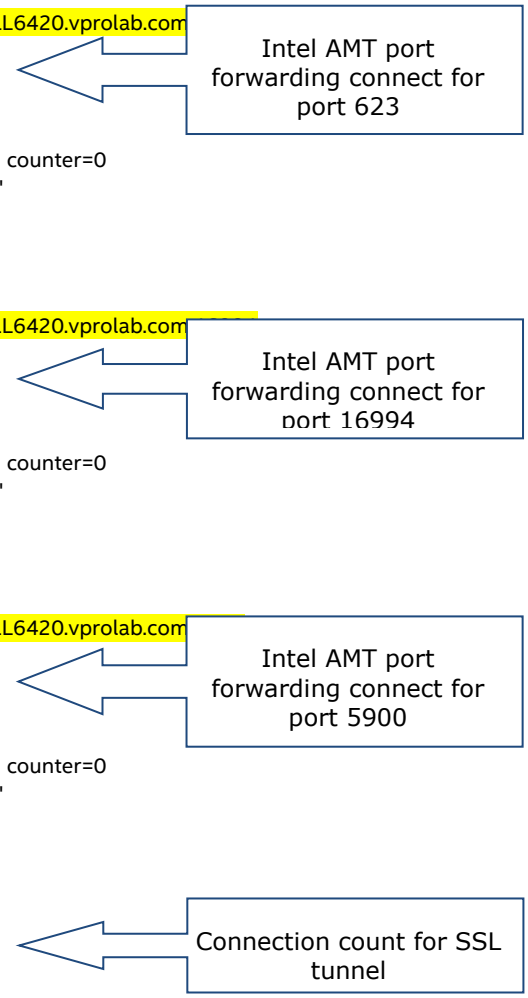
NOTE: Log output below uses ***TraceLevel = "INFO|ERROR|WARNING"*** which is dynamically set in the configuration file ***C:\Program Files (x86)\Intel\MPS\conf\mps_dynamic.config***

AMT_Tunnel_Handler::handle_input - (5bb258)
AMT_Tunnel_Consumer::putq_wrapper - after putting in queue 5bb258
Intel remote client 4C4C4544-0038-5710-8043-B3C04F355131 is now connected.
AMT_Tunnel_Handler handle_output 5bb258
Tunnel_Consumer::handle_output - not the last dispatcher. tcp=[5bb258] state=2 counter=0
"AMT_Tunnel_Handler::handle_output inside while loop, mutex going to be taken"
"AMT_Tunnel_Handler::inside handle_output, mutex was taken!"
"AMT_Tunnel_Handler::handle_output, after loop"
AMT_Tunnel_Handler::processReturnVal - going to return 0
AMT_Tunnel_Handler::handle_input - (5bb258)
Service request: auth@amt.intel.com
AMT_Tunnel_Consumer::putq_wrapper - after putting in queue 5bb258
AMT_Tunnel_Handler handle_output 5bb258
Tunnel_Consumer::handle_output - not the last dispatcher. tcp=[5bb258] state=3 counter=0
"AMT_Tunnel_Handler::handle_output inside while loop, mutex going to be taken"
"AMT_Tunnel_Handler::inside handle_output, mutex was taken!"
"AMT_Tunnel_Handler::handle_output, after loop"
AMT_Tunnel_Handler::processReturnVal - going to return 0
AMT_Tunnel_Handler::handle_input - (5bb258)
"Got user authentication request, canceling timeout."
"User authetication request Username: admin"
authentication SUCCESS
AMT_Tunnel_Consumer::putq_wrapper - after putting in queue 5bb258
AMT_Tunnel_Handler handle_output 5bb258
Tunnel_Consumer::handle_output - not the last dispatcher. tcp=[5bb258] state=4 counter=0
"AMT_Tunnel_Handler::handle_output inside while loop, mutex going to be taken"
"AMT_Tunnel_Handler::inside handle_output, mutex was taken!"
"AMT_Tunnel_Handler::handle_output, after loop"
AMT_Tunnel_Handler::processReturnVal - going to return 0
AMT_Tunnel_Handler::handle_input - (5bb258)
Service request: pfwd@amt.intel.com
AMT_Tunnel_Consumer::putq_wrapper - after putting in queue 5bb258
AMT_Tunnel_Handler handle_output 5bb258
Tunnel_Consumer::handle_output - not the last dispatcher. tcp=[5bb258] state=5 counter=0
"AMT_Tunnel_Handler::handle_output inside while loop, mutex going to be taken"
"AMT_Tunnel_Handler::inside handle_output, mutex was taken!"
"AMT_Tunnel_Handler::handle_output, after loop"
AMT_Tunnel_Handler::processReturnVal - going to return 0
AMT_Tunnel_Handler::handle_input - (5bb258)
Intel remote client DELL6420.vprolab.com started port forwarding to address DELL6420.vprolab.com
Sending notification to management console
CONNECT
AMT_Tunnel_Consumer::putq_wrapper - after putting in queue 5bb258
AMT_Tunnel_Handler handle_output 5bb258
Tunnel_Consumer::handle_output - not the last dispatcher. tcp=[5bb258] state=5 counter=0
"AMT_Tunnel_Handler::handle_output inside while loop, mutex going to be taken"
"AMT_Tunnel_Handler::inside handle_output, mutex was taken!"





```
"AMT_Tunnel_Handler::handle_output, after loop"
AMT_Tunnel_Handler::processReturnVal - going to return 0
AMT_Tunnel_Handler::handle_input - (5bb258)
Intel remote client DELL6420.vprolab.com started port forwarding to address DELL6420.vprolab.com
Sending notification to management console
= DELL6420.VPROLAB.COM:623 - CONNECT
AMT_Tunnel_Consumer::putq_wrapper - after putting in queue 5bb258
AMT_Tunnel_Handler handle_output 5bb258
Tunnel_Consumer::handle_output - not the last dispatcher. tcp=[5bb258] state=5 counter=0
"AMT_Tunnel_Handler::handle_output inside while loop, mutex going to be taken"
"AMT_Tunnel_Handler::inside handle_output, mutex was taken!"
"AMT_Tunnel_Handler::handle_output, after loop"
AMT_Tunnel_Handler::processReturnVal - going to return 0
AMT_Tunnel_Handler::handle_input - (5bb258)
Intel remote client DELL6420.vprolab.com started port forwarding to address DELL6420.vprolab.com
Sending notification to management console
= DELL6420.VPROLAB.COM:16994 - CONNECT
AMT_Tunnel_Consumer::putq_wrapper - after putting in queue 5bb258
AMT_Tunnel_Handler handle_output 5bb258
Tunnel_Consumer::handle_output - not the last dispatcher. tcp=[5bb258] state=5 counter=0
"AMT_Tunnel_Handler::handle_output inside while loop, mutex going to be taken"
"AMT_Tunnel_Handler::inside handle_output, mutex was taken!"
"AMT_Tunnel_Handler::handle_output, after loop"
AMT_Tunnel_Handler::processReturnVal - going to return 0
AMT_Tunnel_Handler::handle_input - (5bb258)
Intel remote client DELL6420.vprolab.com started port forwarding to address DELL6420.vprolab.com
Sending notification to management console
Device = DELL6420.VPROLAB.COM:5900 - CONNECT
AMT_Tunnel_Consumer::putq_wrapper - after putting in queue 5bb258
AMT_Tunnel_Handler handle_output 5bb258
Tunnel_Consumer::handle_output - not the last dispatcher. tcp=[5bb258] state=5 counter=0
"AMT_Tunnel_Handler::handle_output inside while loop, mutex going to be taken"
"AMT_Tunnel_Handler::inside handle_output, mutex was taken!"
"AMT_Tunnel_Handler::handle_output, after loop"
AMT_Tunnel_Handler::processReturnVal - going to return 0
Handler counters:
SOAP_COUNTER = 0
TUNNEL_COUNTER = 1
TCP_COUNTER = 0
```



9.3 TCP/IP connections and Services

The netstat command can be used to validate current TCP/IP network connections. Figure 10 below shows the output from "*netstat –a –n"* and has the important VPEG IP and addresses ports circled. Adding the "*-b*" switch also displays the executable responsible for creating each connection or listening port which can be useful.

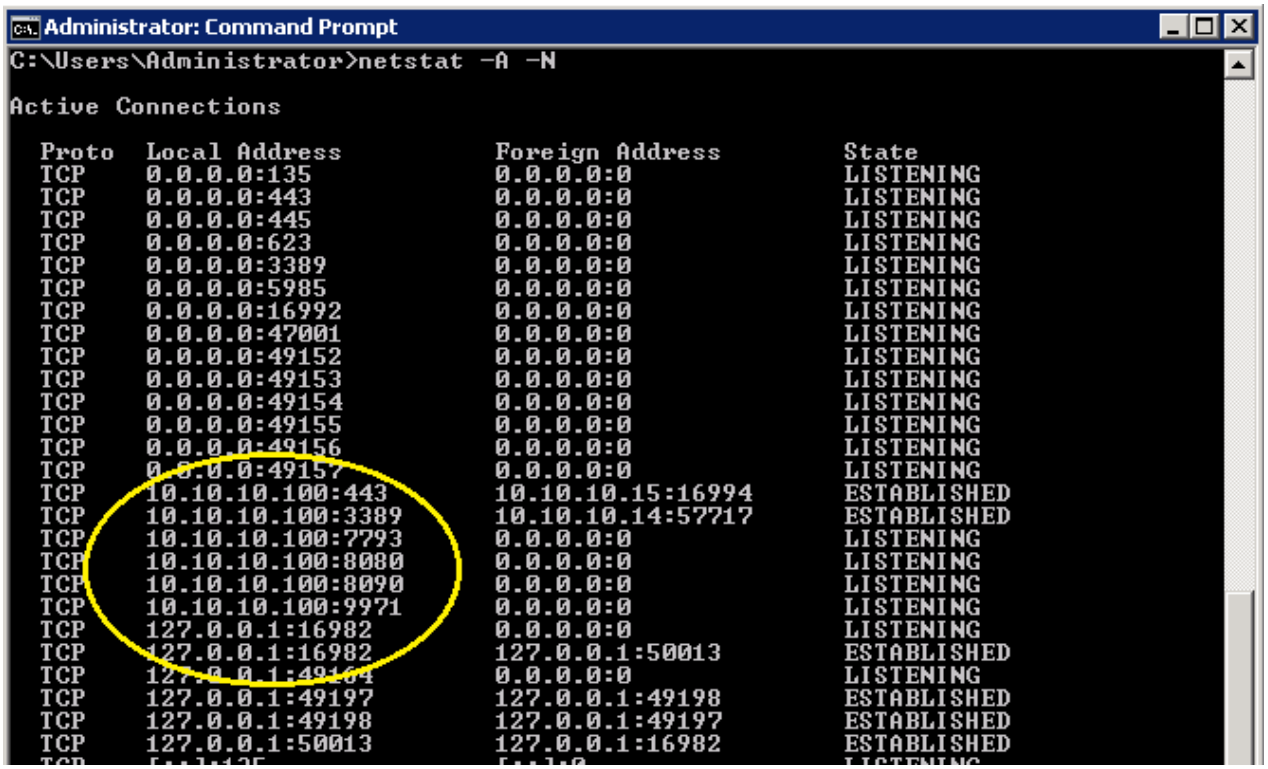

Administrator: Command Prompt
C:\Users\Administrator>netstat -A -N
Active Connections
Proto Local Address Foreign Address State
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING
TCP 0.0.0.0:443 0.0.0.0:0 LISTENING
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING
TCP 0.0.0.0:623 0.0.0.0:0 LISTENING
TCP 0.0.0.0:3389 0.0.0.0:0 LISTENING
TCP 0.0.0.0:5985 0.0.0.0:0 LISTENING
TCP 0.0.0.0:16992 0.0.0.0:0 LISTENING
TCP 0.0.0.0:47001 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49152 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49153 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49154 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49155 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49156 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49157 0.0.0.0:0 LISTENING
TCP 10.10.10.100:443 10.10.10.15:16994 ESTABLISHED
TCP 10.10.10.100:3389 10.10.10.14:57717 ESTABLISHED
TCP 10.10.10.100:7793 0.0.0.0:0 LISTENING
TCP 10.10.10.100:8080 0.0.0.0:0 LISTENING
TCP 10.10.10.100:8090 0.0.0.0:0 LISTENING
TCP 10.10.10.100:9971 0.0.0.0:0 LISTENING
TCP 127.0.0.1:16982 0.0.0.0:0 LISTENING
TCP 127.0.0.1:16982 127.0.0.1:50013 ESTABLISHED
TCP 127.0.0.1:49197 127.0.0.1:49198 ESTABLISHED
TCP 127.0.0.1:49198 127.0.0.1:49197 ESTABLISHED
TCP 127.0.0.1:50013 127.0.0.1:16982 ESTABLISHED

Figure 10

10. Appendix A

10.1 Intel AMT Certificate Store

The Intel AMT stores certificates in its own store which has the following limitations:

- 7 certificates can be stored with a maximum length each of 4100 bytes
- Server certificate supported key lengths: 1024, 1536, 2048 bits
- 4 root certificate instances with a maximum length each of 1500 bytes
- For Intel AMT releases 2.6, 3.2, 4.2, 5.1, 5.2, 6.0 and later, supported root and client certificates key sizes are 4096-bit

10.2 Certificate Revocation List (CRL)

Intel AMT can use a Certificate Revocation List (CRL) but only whilst mutually authenticating with a remote system, i.e. the Intel AMT system trusts the VPEG and the VPEG trusts the Intel AMT system through certificate exchange.

Additionally this requires the configuration of a Certification Authority (CA) to issue certificates that have a "CRL Distribution points" field. The CRL Distribution Points field should have an HTTP distribution point type, as Intel AMT does not support LDAP or other distribution point types. Intel AMT compares the CRL Distribution Point and serial number information included in the peer certificate with the contents of the stored revocation list. Intel AMT rejects certificates that match those in the CRL. Active TLS sessions are not affected by changes in CRL settings due to session caching of the TLS stack.

However this information is redundant for the conifguration of this particular solution as it requires mutual authentication which is not supported.

10.3 The Intel AMT Port-Forwarding Protocol (APF)

The remote connectivity protocol for Intel vPro technology is the Intel AMT Port-Forwarding Protocol (APF). APF provides a generic routing capability that supports all existing manageability protocols utilised by Intel vPro technology, i.e. WS-MAN and and non-HTTP protocols.

For protocols such as Intel AMT redirection protocols, i.e. SOL and IDE-R which are implemented directly over TCP or SSL, the SOCKS v5 protocol is used to provide generic routing capabilities.

The APF protocol provides TCP and UDP connection multiplexing over a single reliable transport session, typically TLS so that confidentiality and server authentication are handled by the underlying transport session.

This multiplexing presents challenges when one end of the connection is terminated, i.e. Intel AMT closes its side of the channel. The APF protocol supports keep-alive messages and the Intel AMT firmware continues to update the window size and send window size messages to ensure the management end point continues to send data, there is a non-configurable timeout of 5 minutes.

The APF protocol as implemented in Intel AMT Releases 4.0 and 5.0, is used in several scenarios. In some scenarios the protocol messages travel over the Intel MEI tunnel (Local Port-Forwarding) and in other scenarios it travels over a TLS tunnel (Remote Port-Forwarding).

Local Port-Forwarding refers to cases where protocol messages are travel over the Intel MEI tunnel. On the host side, the LMS module implements the protocol.

11. Appendix B: MPS Statistics Generator

MPSStatistics.pl is a Perl script file, used to generate statistics using the MPS generated log files.

11.1.1 Usage

MPSStatistics.pl <log file name> <number of hours to trace> <number of minutes to trace>

NOTE:A Perl script interpreter must be installed (minimum version 5.8.8) If not then you will need to run the script explicitly i.e.

Perl.exe MPSStatistics.pl <log file name> <number of hours to trace> <number of minutes to trace>

- The latest MPS log files entries are generated in the file without the numerical suffix i.e. *mps.log*. This should be the first argument passed to the MPS statistics generator.
- A smaller amount of time may be logged than the amount specified if the MPS has been operating for less time than the amount of time specified.
- If the amount of time to trace is larger than the total time recorded in the log files, than only the time frame available is traced.
- If there are many large log files, generating the statistics may take some time.

Output from the MPS statistics generator can be seen in the table below.

Field	Explanation
Report period	Amount of time for which the statistics were generated
Number of Intel clients connections opened	States the amount of Intel clients connections opened.
Number of Intel clients connections closed	The number of Intel clients connections closed (does not include unexpected or connection shutdowns)
Number of Intel management-console opened	A count of the total number of connections opened from management-consoles, i.e. KVM.
Number of Intel management-console closed	A count of the total management-console connections closed (includes unexpected or connection shutdowns)
Number of Intel AMT authentication failure	The number of Intel AMT authentication failures
Number of Socks authentication failure	The number of Socks authentication failures
Number of non-filtered (blocked) UDP connections	The number of UDP connections rejected because they weren't in the authorised servers list
Number of non-filtered (blocked) TCP connections	The number of TCP connections rejected because they weren't in the authorised servers list
Number of connection errors	The number of connection errors which includes APF protocol failures, unexpected connection shutdowns, bad messages etc.
Number of general errors	The number of general errors occurring in the MPS.

Table 5