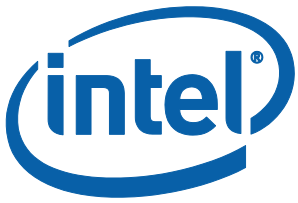


Intel® vPro™ Technology Use Case Reference Design

Find a Client's IP Address with Fast Call for Help

Revision 1.1

December 2011

Document ID: 1076

Revision History

Revision	Revision History	Date
1.0	Initial release.	December 2011
1.1	Fixed typo in script name.	December 2011

Contents

1 Preface

For a Help Desk Technician to remotely take control of a caller's PC, the technician must first identify the PC (that is, figure out its IP address). This can be a complex challenge as a caller may not know their IP address or machine name. Most solutions rely on software in the PC's operating system (OS), but that may not be helpful if the OS is not operable. However, Intel® vPro™ technology provides facilities allowing a Help Desk technician to remotely access and repair PCs without a working OS. In the case where the PC's OS is not working, alternate means must be used to identify the caller's PC. This document outlines a process, with sample code, that uses an Intel® Active Management Technology (Intel® AMT) feature called Fast Call for Help. Fast Call for Help works both inside and outside the corporate firewall. Once a Fast Call for Help is initiated by the caller, the technician can identify the PC.

1.1 Document Scope

This UCRD covers an overall process for using Fast Call for Help while in the office. It also includes sample code and documents the necessary steps to set it up demonstrate the process. Fast Call for Help while outside the office, and vPro Enabled gateways are not covered by this document.

1.2 Intended Audience

This document is intended for Information Technology (IT) professionals who develop and support help desk processes. Also, software developers working on solutions with Intel vPro technology and the Help Desk will find this document particular interest.

1.3 Related Documentation

Fast Call for Help

http://communities.intel.com/community/openportit/vproexpert/blog/2008/07/08/montevina-cira-vpro-2008-platform-users-guide

ASF specification; ASF Alert (aka PET) events sent when user requests help:
http://www.dmtf.org/standards/asf

Intel AMT From Command Line using WinRM; similar concept applies to using WinRM with vbscript, as most of this example does:

http://communities.intel.com/community/openportit/vproexpert/blog/2009/12/10/using-amt-remotley-from-a-command-line-with-winrm

Intel AMT High Level API; used in included C# code to create user account in Intel AMT. Makes programming for Intel AMT much easier. It even has PET and WS-Event support built in:

http://software.intel.com/en-us/articles/intel-amt-high-level-api-intel-manageability-library-to-manageability-webpage/

2 Introduction

Suppose, for example, that you have an Intel vPro technology based client PC (referred to throughout this document as a "Managed Client") that has been set up and configured and that the PC will no longer boot Microsoft* Windows*. In this situation, it would be natural call the help desk. The help desk technician wants to use KVM Remote Control and IDE Redirection to aid in remote troubleshooting of your system. To do that, he or she first needs to know your PC's name or IP address. Suppose that, like most people, you don't know either of those pieces of information. How can the technician get started?

This is where Fast Call for Help comes in. Starting with Intel AMT 4, Intel vPro technology has the ability to send a message to IT based on the Knowledge Worker's request (in the above example, you are the Knowledge Worker). Fast Call for Help has two modes; Inside the Office and Outside the Office.

To continue with the example above, the technician would talk you through a series of key strokes that would cause Intel AMT to send the Fast Call for Help message to IT. With that, the technician has enough information to connect and diagnose your PC's issue.

This document outlines using Fast Call for Help while inside the office to identify a caller's PC. It will cover Fast Call for Help from a high level perspective, and provide a working architecture for this use case. Then, step-by-step directions are provided to setup and use a sample Fast Call for Help implementation. This will allow readers to try Fast Call for Help first hand.

Note that Fast Call for Help may be applicable to other use cases not covered by this document such as a Self Help portal.

2.1 What is Fast Call for Help (FCFH)?

Fast Call for Help, or FCFH, is a feature of Intel AMT that allows the Knowledge Worker to request support from IT by choosing options in the OS (In Band) or during the boot process (out of band). This can augment or even replace the need to pick up the phone to call for help. This is called a User Initiated Connection and usually consists of a single mouse click from within Windows or series of key strokes during boot. Once triggered, Intel AMT will take one of two paths. If outside the office, Intel AMT established a connection to an Intel vPro Enabled Gateway. Outside the office is not covered by this document. When inside the office, Intel AMT will send alerts to IT. The alerts include information on the Knowledge Worker's system. When the alert is received, IT may respond in any fashion they see fit.

2.2 Using FCFH While Inside the Office to Find a Caller's System

2.2.1 Story

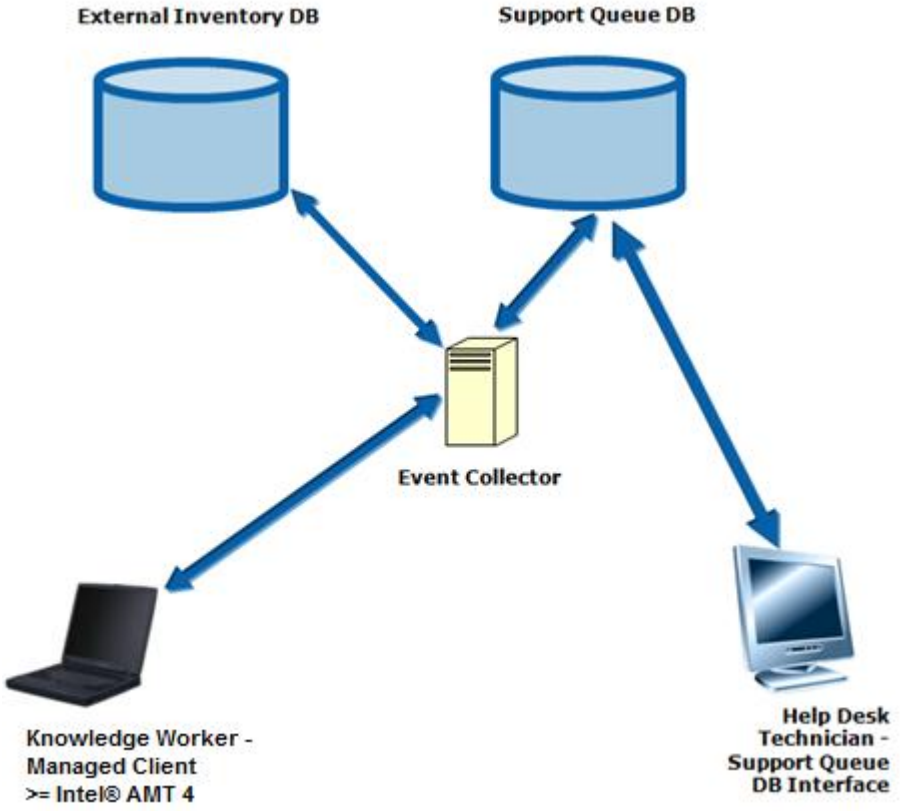
In this use case, the Knowledge Worker (KW)'s PC will not boot into Windows. The KW has already called the help desk and is speaking to a technician. The technician provides verbal instructions to the KW on how to initiate FCFH. This involves pressing a series of key strokes during the system's startup; for example ctrl-alt-f1.

Once this key combination is pressed, Intel AMT sends an alert (either a PET event or WS-event) to a designated alert collector. The collector will respond by querying Intel AMT and any other available data source to gather information on the caller's system. This information is placed in a support queue database. The technician is logged into the support queue so that he will see when a new system is added.

When a system is added, the technician selects it to view more information. At this point the technician can verify information about the PC with the KW; for example the make and model of the PC or the PC's serial number. This verification helps ensure that the technician has found the right system. At this point the technician has enough information to connect to Intel AMT and use all available features.

To aid in future tracking, the technician can assign a ticket number to the system in the queue. Once this is done, the system will not expire from the queue until the ticket is deleted. This provides the ability for the queue to keep the IP address information current while the issue is being worked. It also provides a relationship between a trouble ticket database and the support queue.

2.2.2 Actors



Actor	Definition
Knowledge Worker	The user using the Managed Client. Calls Help Desk for support when issues arise
Help Desk Technician	The user staffing the Help Desk. Answers calls from Knowledge Worker and attempts to solve issues over the phone or by remote access to the Knowledge Worker's Managed Client.
Managed Client	• Remotely managed Intel vPro technology based client PC • Intel AMT 4.0 or greater • BIOS support for User Initiated Connection: provides the user interface allowing a Knowledge Worker to "Call for Help" without an OS, during system boot. Often this is provided by the Intel MEBX in the form of CTRL-ALT-F1.
Event Collector	Receives FCFH alerts from Intel AMT and then takes action. The alerts may be either PET (SNMP Traps) or WS-events. The action includes gathering more information about the Managed Client and storing it in the Support Queue DB
Support Queue DB	Holds information about systems that have requested help or are being serviced.

External Inventory DB (Optional)	If an Inventory DB is available, the event collector may be programmed to gather information about the Managed Client using this DB.
Support Queue DB Interface	A user interface, used by the Help Desk Technician, to view systems in the Support Queue DB. Ideally, this interface is integrated into other support tools such as a ticketing system and/or KVM Remote Control and IDE Redirection tools.

A sample for each component, except an external inventory database, is provided. Section 3 describes setting up the example.

2.2.3 Preconditions

Infrastructure must be in place and set up. Also, Intel AMT must be configured for Fast Call for Help. This includes turning on FCFH and applying settings so that Intel AMT knows where to send alerts.

An example on how to set up and configure FCFH is provided in Section 2.3 below.

NOTE

The Help Desk Console system MUST have Microsoft .NET Framework 4 installed.

2.3 Example

This reference design includes a sample implementation of this use case. This example was written to be as simple as possible and is for the purpose of illustration only. It has not been written for scalability or vetted for security. For example, passwords are stored in clear text. As such, it not recommended for use in a production environment.

2.3.1 Example Requirements

Network with DHCP Server	
Help Desk Console	• Any PC with Microsoft* Windows 7 32 bit. • These steps outline using this PC as the Help Desk Technicians PC and the Event Collector. *The example does support separating these services. However, this document does not provide detailed steps for that.*
Managed Client with Intel vPro technology	• Intel AMT 4.0 or higher. • Must include BIOS support for Client Initiated Connections • Configured for non-TLS and Digest credentials. *The example does support sTLS and Kerberos. However, this document does not provide detailed steps for that.*

2.3.2 Process Overview

Configure the infrastructure (Precondition)

1. Copy Sample Tools to the Help Desk Console.
2. Install and Configure WinRM on the Help Desk Console.
3. Install and Configure Trap Receiver on the Help Desk Console.
4. Configure the Sample Tools.

Configure Intel AMT for FCFH (Precondition)

1. Execute the FCFH Configuration tool to remotely configure FCFH on the Managed Client.

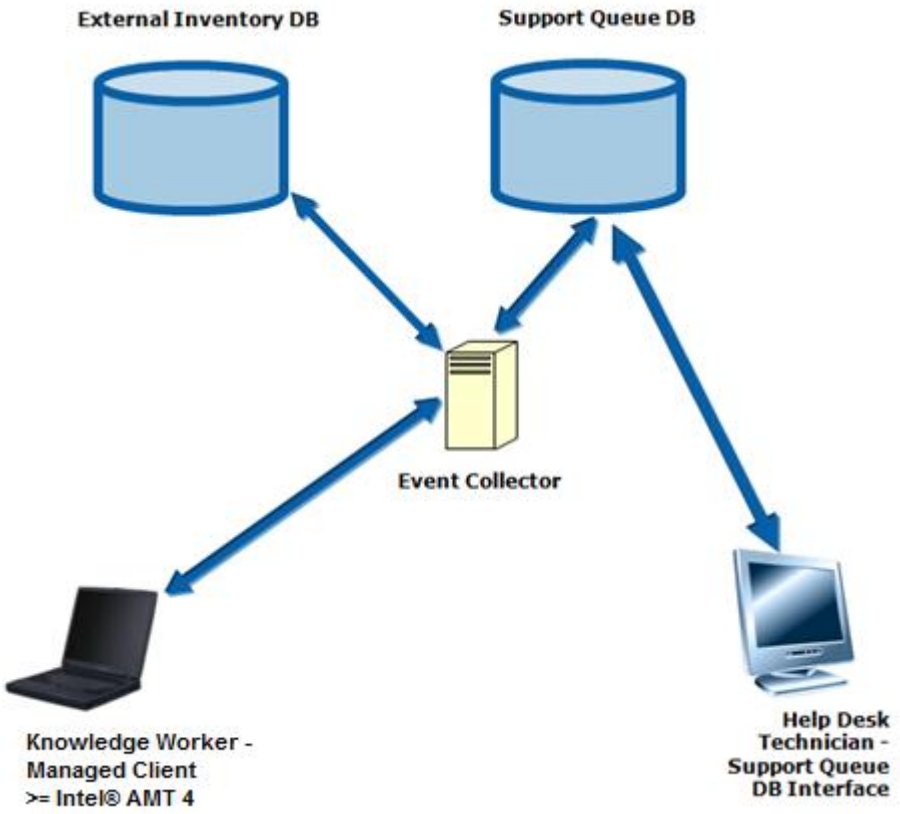
Demonstrate the Use Case

1. Open the Help Desk Queue Sample tool
2. Execute an FCFH from BIOS on the Managed Client. The Managed Client appears in the Help Desk Queue.
3. Select the Managed Client and verify it's hardware information. If there are multiple Managed Clients listed, select them one at a time until the right one is discovered.
4. Add a ticket to the Managed Client.
5. (Optional) Launch other tools from the Help Desk Queue sample tool. These tools will automatically execute against the selected Managed Client.
6. When finished, delete the client from the Queue.

3 Detailed Steps

This chapter and its subsections step you through the processes outlined above. Following these steps exactly will allow you to demonstrate the process end-to-end.

3.1 Sample Overview



The sample provided with this UCRD includes or references pieces for each actor above, except the external inventory database.

Actor	Definition
Managed Client	Provided by the reader
Event Collector	• Trap Receiver. - This may be freely downloaded. When AMT send the FCFH alert, Trap Receiver receives it. It then passes the data in the alert to ip.bat, which processes the data. • c:\fcfh\Alert_Collector\– Included. — Ip.bat, ip.vbs, and other files process FCFH alerts, gathers information from Intel AMT, and stores it in the

	Support Queue DB. — Settings.hta – GUI to define ip.vbs behavior.
Support Queue DB	c:\fcfh\ Support_Queue_DB\ - Included. Empty folder for Support Queue DB. All data is stored in .xml files.
Support Queue DB Interface	c:\fcfh\Support_Queue_gui\ - Included. • servicedesk.hta. GUI that accesses the Support Queue DB for use by the Help Desk Technician
Prerequisite	Configure FCFH • c:\ fcfh\amt_cfg\ - included — FCFH_user_credentials.vbs – command line tool used to configure FCFH — Configure FCFH on AMT.hta – GUI tool used to configure FCFH. Executes FCFH_user_credentials.vbs — Settings.hta – GUI to configure FCFH_user_credentials.vbs behavior (e.g. Intel AMT admin password to use).

3.2 Configure the Infrastructure

3.2.1 Copy Sample Tools to the Help Desk Console

This UCRD includes files in a folder named FCFH. To begin, place all files in FCFH on the Help Desk Console's folder **c:\fcfh**.

Next, download the HLAPI DLLs from here: http://communities.intel.com/docs/DOC-19140

Extract the downloaded files and copy all .dlls to **c:\fcfh\amt_cfg\util**.

NOTE

The Help Desk Console system MUST have Microsoft .NET Framework 4 installed.

3.2.2 Install and Configure WinRM

WinRM is used by this sample to send WS-Man commands to Intel AMT.

NOTE

WinRM is included with Windows Vista, Windows 7, and Windows 2008. If you have Windows XP or Windows 2003 Server, you must download and install WinRM. If you download it, be sure to check the requirements page so that you have the proper service pack and hot fixes. Use the following link to download and install WinRM.

http://www.microsoft.com/Downloads/details.aspx?FamilyID=845289ca-16cc-4c73-8934-dd46b5ed1d33&displaylang=en

Once WinRM is on your console system, it must be configured.

1. Open a command prompt (**Start -> Run** and enter **cmd**). If you have User Account Control enabled, **right-click cmd** and sele**ct Run as Administrator**.
2. At the command prompt, type **cd /d c:\FCFH**.
3. Type **WinRMcfg.bat**.
4. Exit the command prompt by typing **exit** and pressing the Enter key.

WinRMcfg.bat contains the following three commands:

Command	What it does
`Winrm quickconfig`	Enable WinRM
`winrm set winrm/config/client @{AllowUnencrypted="true"}`	Allow Unencrypted traffic
`winrm set winrm/config/client @{TrustedHosts="*"}`	Allow all hosts as Trusted

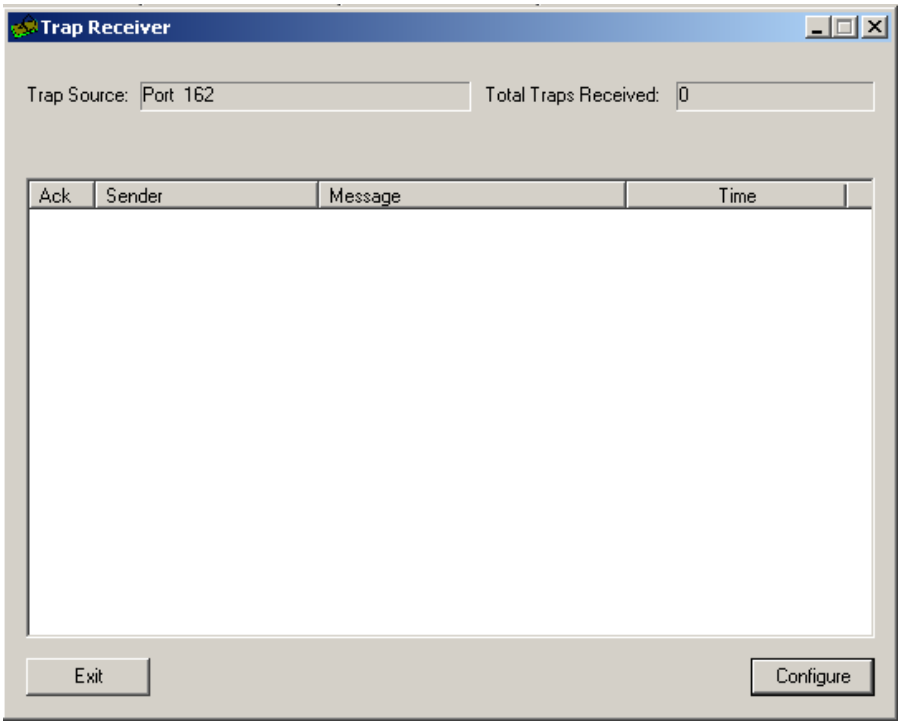
3.2.3 Install Trap Receiver on the Help Desk Console

1. Disable Windows Firewall. If it is not disabled, it will block incoming alerts. **Note**: As an alternative, you can set a rule to allow UDP traffic to port 162.
2. Ensure no other SNMP trap listing software is running as follows:
   a) **Start -> run -> cmd** (run as administrator if on Windows Vista or Windows 7)
   b) **netstat –a –n | find /i ":162 "**
   c) The above command should return no results. If it returns any results, something is listening on port 162 (the standard port for SNMP traps). This must be removed first. Details on this cannot be covered as they vary based on what service is listening. Often, this is a service called "SNMP Trap". To check for this, do the following:
      - Right-click **Computer -> Manage**.
      - Expand **Services and Applications -> Services**.
      - Scroll down and look for SNMP Trap. If listed, it may be disabled here. Double click it. Click **Stop**. Then set **Startup Type** to **Disabled**. Click **OK**.

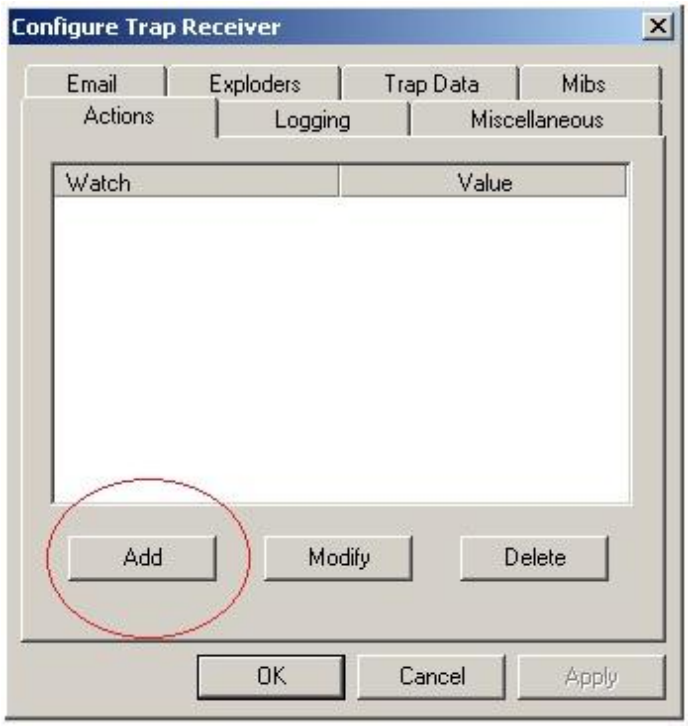
3. Download the latest Trap Receiver from http://www.trapreceiver.com/. At the time of this writing, the latest is 7.20.
4. Unzip and install trap receiver with the defaults.

3.2.4 Configure Trap Receiver

1. **Start -> Programs -> Trap Receiver -> Trap Receiver GUI**. The Trap Receiver GUI is displayed, as shown below. Click the **Configure** button at bottom right.



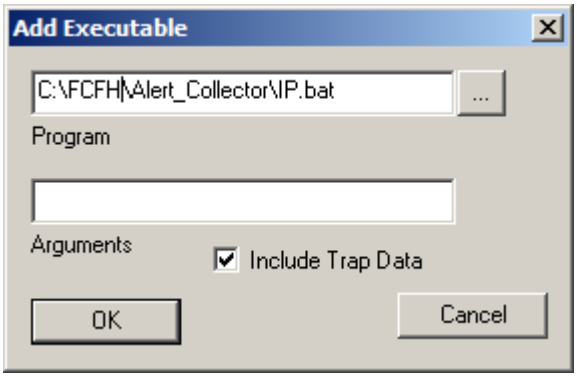
2. The Configure Trap Receiver dialog is displayed. On the Actions tab (shown below), click **Add**.



3. Select **Community** for Watch and enter **vpro** for Value, as shown below (**Note**: the Intel AMT Configuration application sets the Community string to **vpro**):

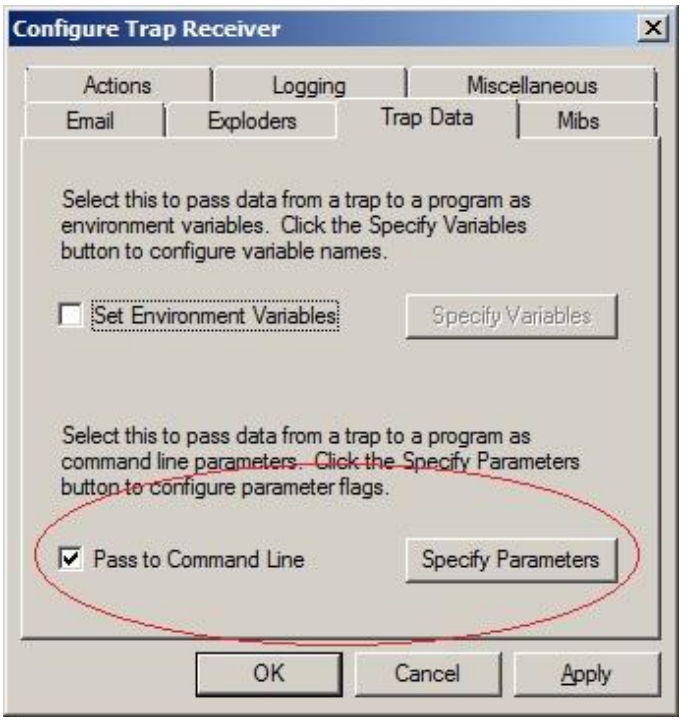
4. Select **Execute** and click **Configure** as shown below.

5. For Program enter **c:\fcfh\alert_collector\ip.bat**; select **Include Trap Data** and click **OK**.



6. In the Trap Receiver Action Add screen, click **Add**.

7. Select the Trap Data tab (shown below). Select **Pass to Command Line** and then click **Specify Parameters**.



8. Select **IP Address**, **Specific Type**, and **Varbind Data**, as shown below; then click **OK**.

9. Click **OK**.
10. Click **Exit**.

3.2.5 Set the Trap Receiver Service to Run as a Local Administrator

This is required so that processes run by the trap receiver have access to write to the local file system. This is used to write to XML files to the help_queue_db folder.

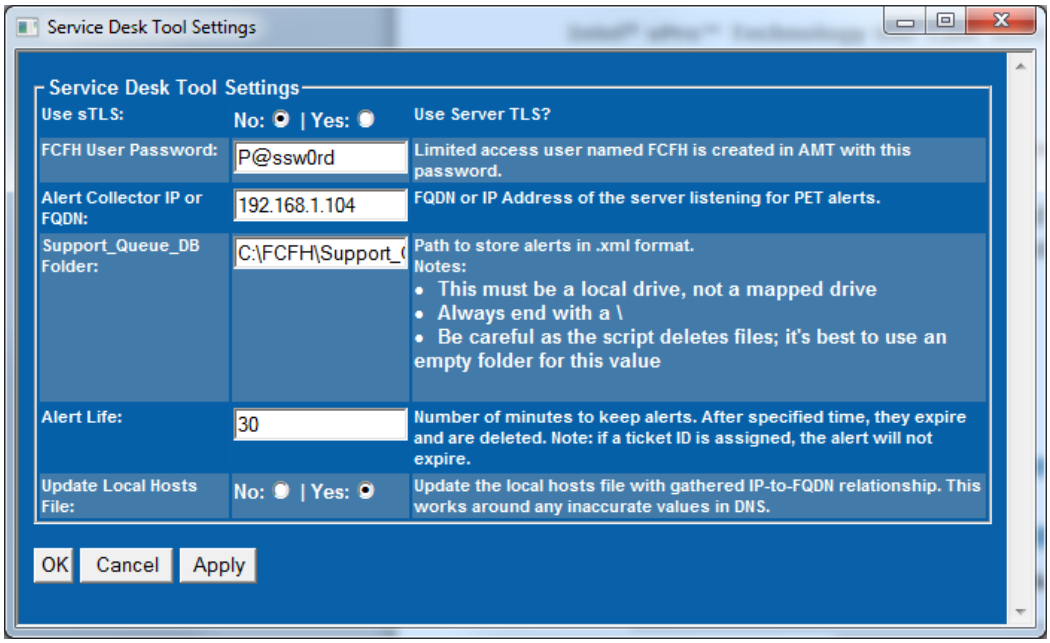
1. Right-click **Computer**.
2. Select **Manage**.
3. Expand and select **Computer Management -> Services and Applications -> Services**.
4. Scroll down and double-click **TrapRcvr**.
5. Select the **Log On** tab.
6. Set **Log on as** to **This Account**.
7. Enter parameters for an account that has local administrator rights. This may be a local account or an active directory account. For example, vprodemo\itproadmin. Be sure to set the password correctly.
8. If prompted, accept the warning that the account was granted "Log on as a service" rights.

9. If prompted, accept the warning that the service must be restarted.
10. Click **OK**.
11. Right-click **TrapRcvr** and select **Restart**. Be sure it is listed as "Started" when the task completes. If not, the account credentials you provided may be incorrect.
12. Close the MMC Snap-in.

3.2.6 Configure the Sample Tools

3.2.6.1 Configure the Sample Application

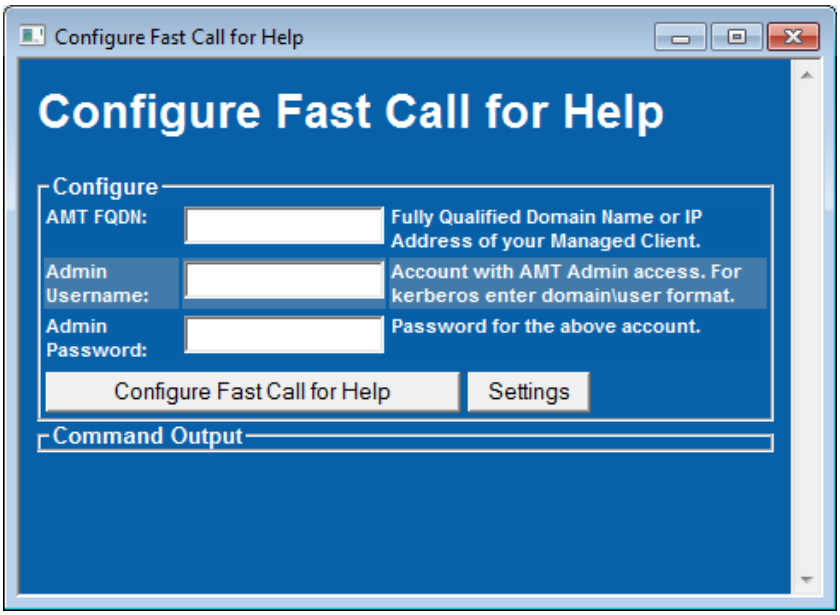
1. Double-click **c:\fcfh\settings.hta**.



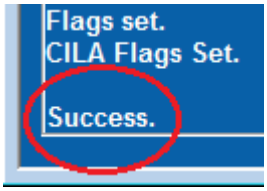
2. Rather than using the admin account for all operations, the configuration tool creates a limited access user named FCFH. Enter a password to be used with this account. It must be a strong password, containing at least 8 characters, with at least one upper case letter, one lower case letter, one number, and one special character. The tool will not check for conformance to this requirement.
3. Set the listener IP. This is the IP of the system that is running as the event collector. In this case, that is the IP of the Help Desk Console.
4. All other information is correct if you are using non-TLS as recommended by this document. If you are using an alternate configuration, adjust the settings as needed.
5. Click **OK**.

3.3 Configure Intel® AMT for Fast Call for Help

1. Open **c:\fcfh\amt_cfg\Configure FCFH on AMT.hta**. The Configure Fast Call for Help dialog is displayed as shown below.
2. Enter the FQDN or IP of the Managed Client, as well as an admin username and password. These credentials are used once, only during the configuration process, and not stored.



3. Click **Configure Fast Call for Help**.
4. Command output is displayed when the command has completed. Errors will be listed as well. To ensure success, check the last line of the output, as shown below.



This .hta file is actually running FCFH_user_credentials.vbs in the background. This can be run from a command line to aid in automation of configuring many Managed Clients. To run FCFH_user_credentials.vbs from a command line, do the following:

1. Open a command prompt as administrator.
2. Run the following command, replacing items in <> with your info.

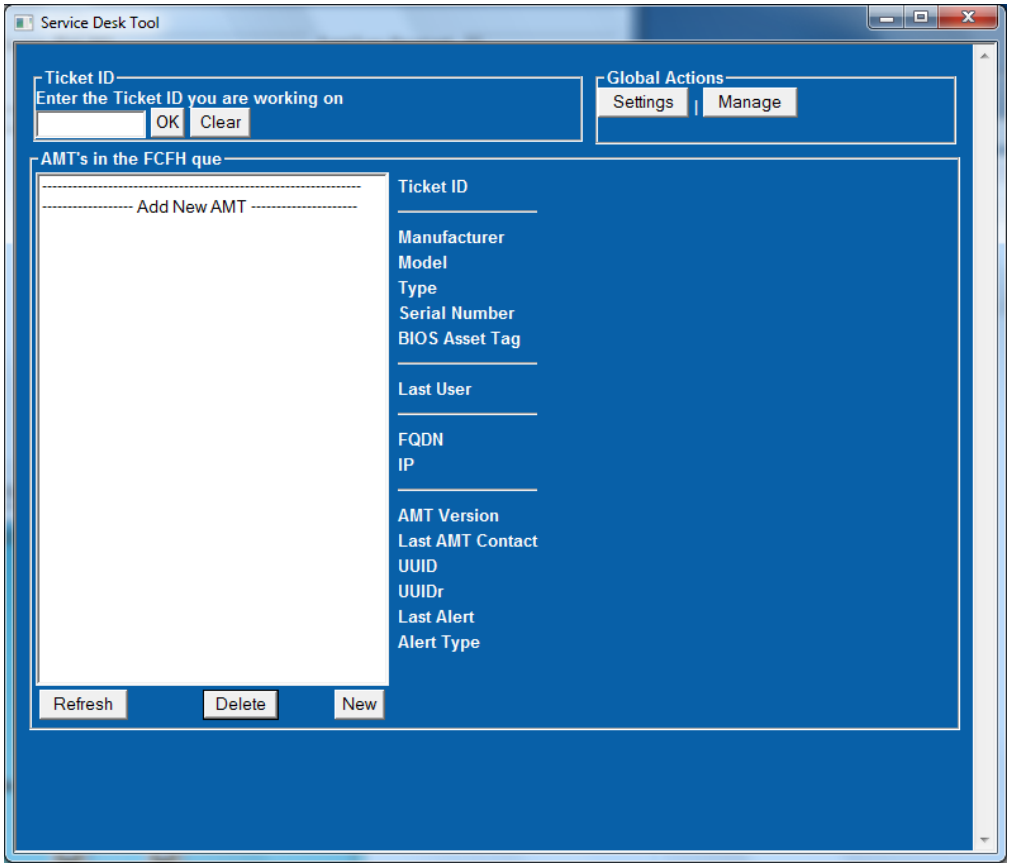
```
cscript /nologo C:\FCFH\amt_cfg\FCFH_user_credentials.vbs <IP or FQDN of managed client> <admin> <password>
```

3. All output is displayed on the command line.

The Managed Client is now ready to send Fast Call for Help messages while in the office.

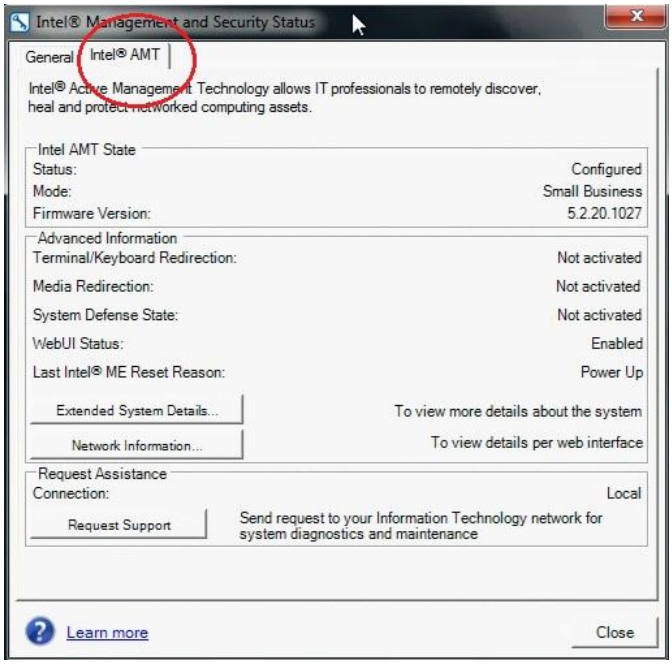
3.4 Demonstrate the Use Case

1. Open the Support Queue Sample tool (**c:\Support_Queue_gui\servicedesk.hta**).



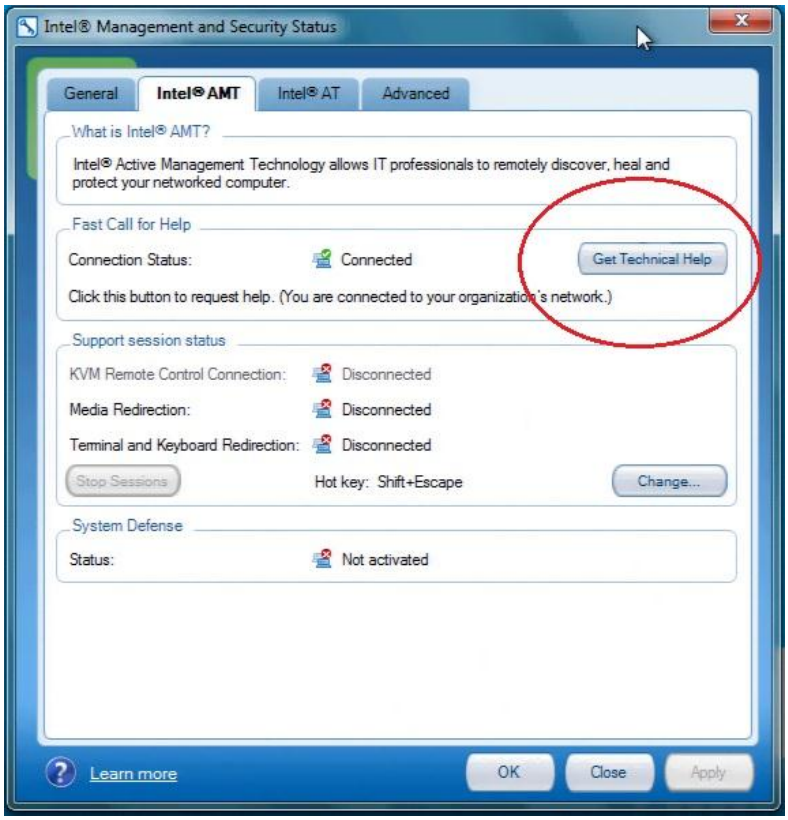
2. Execute an FCFH from the Managed Client using one of the following methods. Select one appropriate for your client:
   - **In Band (Intel AMT 4 & 5)**

     Note: Intel AMT 4 and 5 need the latest LMS driver to provide this support. Be sure you have the latest.
     - Click **Start -> Programs -> Intel Management and Security -> Intel Management and Security Status**.
     - Select the Intel AMT tab (shown below).



- Click **Request Support**. Intel AMT will send an alert to the alert collector.

- **In Band (Intel AMT 6 & 7)**
  - Click **Start -> Programs -> Intel -> Intel Management and Security Status**.
  - Select the Intel AMT tab (shown below).



  - Click **Get Technical Help**. Intel AMT will send an alert to the alert collector.

- **Out of Band**

  Steps vary based on vendor's BIOS implementation. The steps below are meant a guideline, but they may not match exactly. Check with the system vendor for specific steps.

  Generic ctrl-alt-F1
  - Reboot the Managed Client.
  - When the Intel MEBX screen is displayed press Ctrl-Alt-F1.
  - Intel AMT will send an alert to the alert collector.

  Generic ctrl-p
  - Reboot the Managed Client.
  - When the Intel MEBX screen is displayed press Ctrl-p

- A menu will appear. Choose option 2 to send an alert.
- Intel AMT will send an alert to the alert collector.

Most Dell Laptops

- Reboot the Managed Client.
- During initial BIOS load, press F12.
- A boot option menu will appear. Choose Intel Fast call for Help.
- Intel AMT will send an alert to the alert collector.

Most Lenovo* systems

- Reboot the Managed Client.
- During initial BIOS load, press enter
- A boot option menu will appear. Type Ctrl-p
- A menu will appear. Choose option 2 to send and alert.
- Intel AMT will send an alert to the alert collector.

Most HP* Laptops

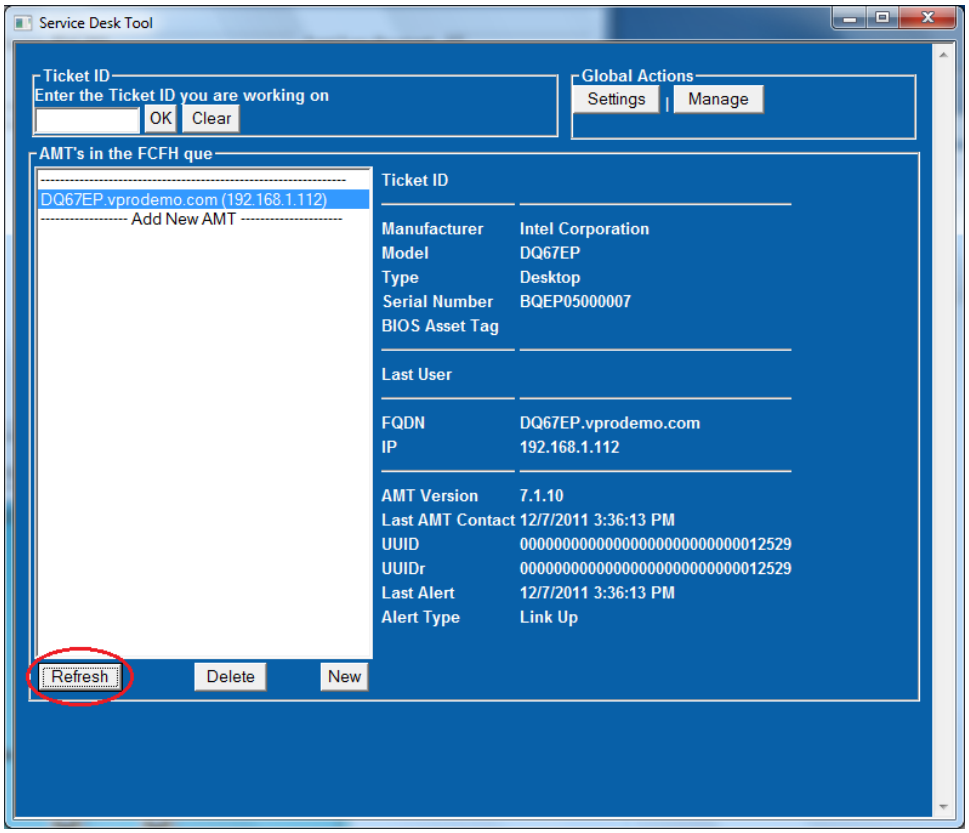
- Reboot the Managed Client.
- During initial BIOS load, press Esc.
- A boot option menu will appear. Choose the option for "Initiate Intel CIRA", usually F3.
- When prompted, select **Yes**.
- When prompted, set a timeout as desired (the default is 0).
- Intel AMT will send an alert to the alert collector.

Most Intel® Desktop Boards

- Reboot the Managed Client.
- During the initial BIOS load, press F9.
- Intel AMT will send an alert to the alert collector.

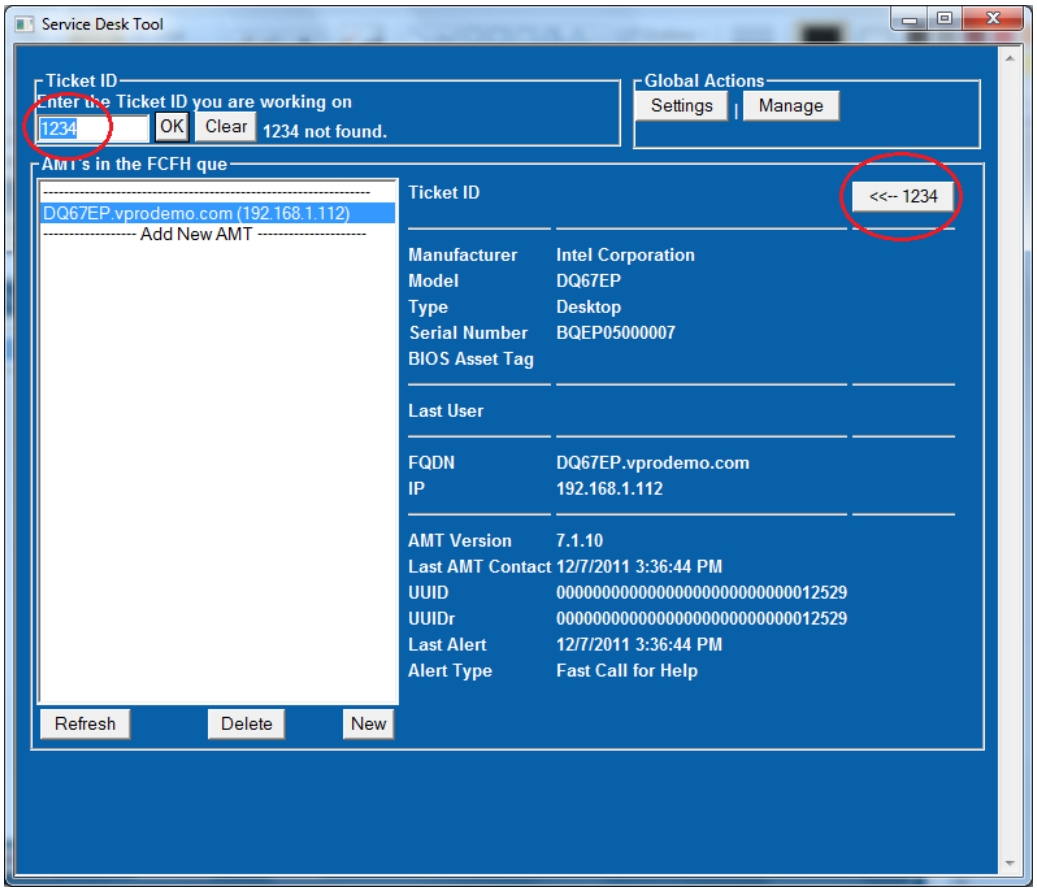
Note: Some Intel® Desktop Boards have a RPAT or FCFH header. It is possible to connect a temporary switch to this header and use it in place or pressing F9 on the keyboard.

3. On the Help Desk, in the Service Desk tool, the Managed Client should appear in the queue within 60 seconds. If it does not, click **Refresh** to force a rescan of the Support Queue Data Base.

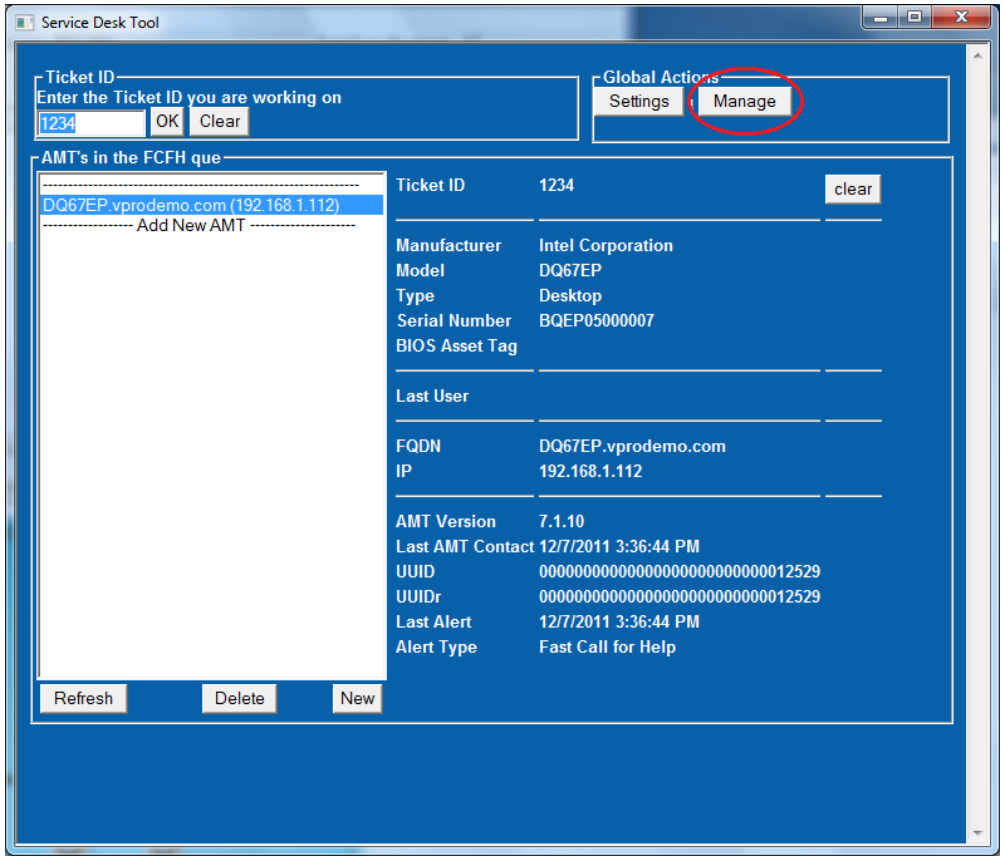


4. Select the Managed Client and verify its hardware information. If there are multiple Managed Clients listed, select them one at a time until the right one is discovered.
5. Once you have identified the right one, you may assign a trouble ticket ID. This ID is usually generated by a trouble ticket tracking tool in use by the help desk. For demo purposes, any ID may be used.

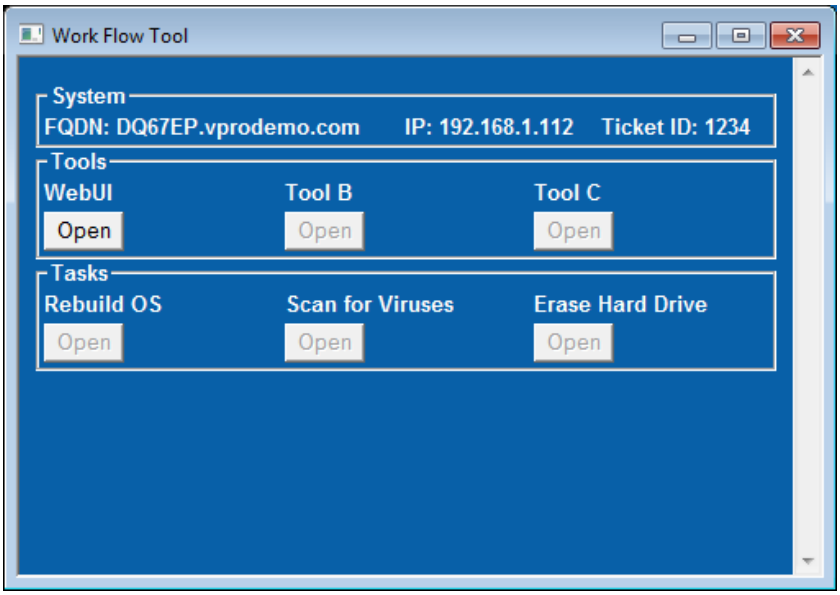
6. In the Ticket ID field, enter an ID (1234 for example, as shown below) and click **OK**. To assign the ID, click the button with the ticket ID number next to the Ticket ID field.



7. To work on this client, click the **Manage** button (shown below).



8. The figure below shows an example of integration of work flows such as Scan for Viruses. The goal is to show that, once the system has been found, a series of common help desk tasks can be integrated to make remote tasks easy for service desk personnel. Here you may click Open under WebUI to connect to this system's WebUI.



9. When done, close the Work Flow Tool.

As long as the ticket is associated to this Managed Client, the client will not be cleared from the database. Further, if the client loses and re-establishes a network link, it will send an alert with its updated IP address information. In this way a support agent may continue to work on this issue until work is complete.

If there are multiple Managed Clients in the queue, and the support agent wants to find one based on an open ticket, the agent can enter a ticket ID in the Ticket ID field and click **OK**. If a Managed Client with this ID is found, the queue will only show this client.

Once a ticket is closed, it should be cleared from the Managed Client in the queue. This will allow the Managed Client to be automatically deleted from the queue based on the configured timeout value. To clear a ticket from the queue, do the following:

1. Enter a ticket ID in the Ticket ID field, and click **OK**. If a Managed Client with this ID is found, the queue will only show this Managed Client.
2. Select the Managed Client in the queue.
3. Click the **Clear** button.

4 Considerations for Building Your Own Solution

4.1 Trouble Ticket Management

It is recommended to link the trouble ticket system to the Support Queue database so that ticket management can be automated. For example, this will allow a Managed Client to be purged from the queue automatically once a ticket has been closed.

4.2 Identifying the Caller's System

By linking customer information to an inventory database discovery of a caller's Managed Client in the queue can be made easier. For example, many support desks will collect a caller's company ID number, user name, or Managed Client serial number. By referencing data in the Support Queue to an inventory database it may be possible to identify a specific Managed Client based on information gathered as a part of standard practice.

4.3 Information Provided by the Alert

As previously mentioned, the alert sent by Intel AMT may be a PET alert, or a WS-Event. Each contains different capabilities and information. Note that this sample uses PET alerts

4.3.1 PET

PET alerts are part of the ASF standard and are SNMP trap events. There are many PET Alerts that Intel AMT can send. Part of the alert data indicates what type of any Alert is being sent. Other data includes the IP address of the sender and the UUID. Since the UUID is unique, it can be used to query external inventory databases for more information about the system.

The following are some of the drawbacks to using PET events:

- PET events are not encrypted or authenticated. This means an attacker could sniff the details of the PET event, or send a fake PET event to the alert listener.
- Due to the ASK standard, Intel AMT will always send a "link up" event. This event is sent whenever the network link comes online, including during the boot process. This means under certain circumstances, the alert collector must be able to handle a large influx of alerts. For example, in the morning when users arrive to the office, they may all turn on their systems at approximately the same time, causing a large influx of "link up" events.

4.3.2 WS-Event

WS-Events are part of the DASH standard and are SOAP based. There are many WS-Events that Intel AMT can send. Part of the alert data indicates what type of any Alert is being sent. Other data includes the IP address of the sender. The UUID is not commonly included in the alert. However, WS-Events have an advantage in that they can be setup with custom data. As such, they may be programmed to include the UUID, the FQDN, or anything else.

Another advantage of WS-Events is security. Events may be authenticated by setting the alert subscription to use digest credentials when sending the alert. Also, events may be encrypted using TLS. This makes spoofing and sniffing much more difficult for an attacker.

See the Intel AMT SDK documentation for more information.

The Intel AMT HLAPI has special provisions for WS-Events and FCFH.

4.4 Kerberos, TLS, and Intel AMT's FQDN

Using TLS or Kerberos present additional challenges. For TLS, the FQDN must be used when performing redirection (SOL, IDEr, or KVM). For Kerberos, the FQDN must be used for all authenticated operations. Using the FQDN, rather than the IP address presents a twofold challenge. First, the events sent from FCFH outside the firewall do not contain the Managed Client's FQDN, only its IP address. Second, even if the FQDN and IP address are known, most applications use DNS to resolve the IP address, meaning DNS needs to be accurate.

There are a couple options to deal with the first challenge. The obvious answer is to perform a reverse DNS lookup. Then, check any returned IP addresses against those in the alert. If this fails, the next option is to lookup the system in an inventory database. If such a lookup fails, or if this is not an option, the next option is to check in Intel AMT by connecting to the IP address. This will work so long as digest credentials are used. The included example currently always uses a digest user named FCFH, which is created during the initial configuration. If digest is not an option, the last resort for automatic discovery is to connect to Intel AMT's webUI using the IP address, and no credentials. Intel AMT will present its certificate. In the subject of the certificate is Intel AMT's FQDN. Note, this only works if Intel AMT is configured for TLS. A final option for Intel AMT 7 based systems is to ask the local user. On Intel AMT 7, when the user performs an out of band FCFH, the BIOS will show the user Intel AMT's IP addresses and its FQDN.

To deal with the second challenge, first check DNS to see if it resolves the expected IP address. If it does, just use it. If it does not, the quick fix is to temporarily update the hosts file on the help desk console. This method is optionally used by the included example. The drawback of this method is that the help desk console needs to have administrative access to be able to change this file. Also, if an alert is spoofed, the help desk technician may unknowingly be tricked into connecting to a malicious source.