

Part 1: Post Deployment of Intel vPro in an Altiris Environment

NOTE: This resource and the associated series are a re-post of information provided at <http://juice.altiris.com/node/4636> and related articles linked therein. Although the title and material make reference to Altiris, the core concepts apply to most Intel SCS based solutions.

Introduction: Provisioning Intel® vPro Technology After Systems Have Been Deployed

Much has been written about provisioning and enabling Intel® vPro technology, including articles such as <http://juice.altiris.com/node/4082> and <http://juice.altiris.com/node/4480> with their respective sub-linked articles. The previous articles highlighted optimal situations to provision the Intel® vPro technology, what core criteria and options must be met, and so forth.

With that base knowledge in place, this collection of articles will step into some enhanced deployment scenarios and utilities that may be of interest. Situations may arise where a ProvisionServer DNS record cannot be used, thousands of systems have been deployed without a clear indication of what Intel® AMT version is presently running on them, and so forth.

Common Scenarios: Are you experiencing one or more of the following?

In talking with various customers, partners, and associates - a common set of scenarios are frequently brought up in regards to provisioning Intel® vPro after systems have been deployed. Provided below is a brief summary of the scenarios with an indication of how to recover from each, along with a realization that some recoveries may be less desirable. The subsequent sections in this article will provide more insight to the utilities, methods, and operations to realize

Q: How do I know if systems deployed into my environment support Intel® vPro?

- **A:** By deploying the Altiris Notification Server client agent and enabling OOB Discovery, the Inv_OOB_Capability table of the Altiris CMDB will be updated. In addition, the dynamic provisioning collections within Altiris Out-of-band management will also be updated to note Intel® AMT or ASF capable systems as reported by the OOB Discovery task which requires the Altiris agent.

Q: How do we enable hundreds or thousands of Intel® vPro systems that have been deployed yet not provisioned?

- **A:** If the systems are remote configuration capable and the infrastructure will support - then refer to <http://juice.altiris.com/node/4007>. Determining remote configuration capability can be handled via the Altiris NS Agent, OOB Discovery, and OOB Task Agent. Firmware upgrades may be needed in some situations, see article <http://juice.altiris.com/node/4411>. Most major OEM systems supporting Intel® vPro have remote configuration support.

Q: Deployed systems have stopped sending hello packets. How do we restart them?

- **A:** Joel wrote a great article at <http://juice.altiris.com/node/3612>, and the target utility has been updated, renamed, and posted at <http://www.intel.com/software/activator>. If the systems were sending hello packets, then they are in a "setup" state. This means the provisioning credentials are in the client firmware, and it is attempting to authenticate to the provisioning service. If the provisioning service did not have matching credentials, configuration parameters, or a provisioning script to complete the process - then the time period for sending hello packets has expired. Checking of the provisioning service logs may reveal additional insights such as missing credentials, missing configuration parameters, and so forth. Once the provisioning service is ready to respond, reinitiating hello packets can easily be accomplished either via the Intel® vPro Activator Utility or via the Altiris OOB Task Agent. The latter is for remote configuration capable systems only.

Q: What if the system BIOS has disabled the Intel® AMT functionality or some of the options?

- **A:** Only a few instances have been seen where the system BIOS (not the MEBx) has entirely disabled Intel® AMT or some of the options for messaging, USB one-touch, and so forth. HP and Lenovo mobile systems are the main two examples where this has been experienced. Both OEMs provide BIOS configuration utilities to capture and apply the preferred settings remotely, whether via HP Client Manager, downloaded utility from the OEM, or other methods.

Q: What if Intel® AMT is disabled within the Management Engine BIOS eXtension (MEBx)?

- **A:** This has been seen on Dell, HP, Lenovo, Panasonic, and other units. The situation is easily remedied via the Intel® vPro Activator Utility or via the Altiris OOB Task Agent to transition the MEBx manageability feature from "none" to "amt" remotely. More on each will be shared later.

Q: What if the manageability feature is set to ASF? Am I able to transition to Intel® AMT remotely?

- **A:** Until recently, my answer was "no" on this one. However, in talking with associates at Intel and Symantec, and doing some additional tests in the lab, I came to realize the Altiris OOB Task Agent is able to transition from ASF to AMT manageability mode for remote configuration (e.g. delayed provisioning)

Q: What if our environment has more than one client facing Altiris Notification Server? How does this affect the ProvisionServer DNS record?

- **A:** First, with the Intel® vPro Activator Utility, the ProvisionServer DNS record is no longer mandatory. When executing the utility via a script on the client, the target server is identified within the command script. This comes in handy especially when multiple client facing Altiris Notification Servers are in the same DNS context. Second, there are advanced situations where multiple Altiris NS Servers with OOBM will use the same Intel® AMT database which retains the Intel® vPro and provisioning service settings. For those scenarios, please refer to the two linked articles at <http://juice.altiris.com/node/3771>.

Q: Similar to having multiple client facing Altiris Notification servers - What if our environment has client systems in a single DNS context, yet requiring difference management profiles and policies?

- **A:** This commonly happens in university, mixed deployments, migration scenarios, recent acquisitions, or due to corporate divestiture. The crux of the problem is that a default provision profile or policy as defined in Resource Synchronization or other settings do not apply to all client systems within one location. Directing where the Altiris agent and Intel® vPro provisioning event

occurs may require some scripting. In addition, if multiple clients with different Intel® vPro provision profiles are associated to a single Altiris Notification Server, either a post provisioning event must occur to re-assign them to the correct profile or the advanced features of the Intel® vPro Activator Utility can be used to designate the correct profile assignment during the initial provisioning event. More on this approach will be addressed in this series.

Q: What if the target provision profile or Microsoft Active Directory OU depends on the client being provisioned?

- **A:** Although the Resource Synchronization settings are handy to ensure every client provisioned will receive a default profile and optionally a designated Microsoft AD Organizational Unit assignment, some environments require a little more flexibility. Directly specifying the provision profile and Microsoft AD OU settings can be accomplished via the Intel® vPro Activator Utility. However - this will require some additional configuration and setup such as installing the Intel® SCS console, defining a Configuration Client, and other advanced topics that will be discussed later.

Q: What if our Intel® vPro systems are not remote configuration capable, cannot be upgraded to support remote configuration, the environment cannot support remote configuration, and the systems have not been prepared with pre-shared keys?

- **A:** This is perhaps one of the most difficult and painful situations. In short, the systems are not in a "setup" mode and must be individually touched to at least perform a USB one-touch for pre-shared key (e.g. PID\PPS) distribution. Future systems being introduced into the environment can be intercepted to prepare them, yet already deployed systems may require a desk-side visit. The above options should be explored and tested before resorting to a brute force provisioning and enablement method - yet sometimes the preferred methods are simply not an option.

Q: After provisioning the Intel® vPro technology, the provisioning logs report "Cannot connect to system" with an accompanying IP address. When attempting to reprovision, unprovision, or perform maintenance tasks systems listed under Intel AMT Systems - a variety of SOAP, cannot connect, or related errors are occurring. Similarly, when the Altiris Real-Time Console attempts to connect, the Intel AMT options are not shown. What is happening?

- **A:** There are a variety of reasons these errors are happening, yet the most common is to ensure the DNS to IP mapping of the target client system is correct. Dynamic DNS for client systems is fairly common, especially for environments supporting DHCP. Clients should be joined to the domain. If unsure whether a client is registering DNS updates, run **ipconfig /registerdns** from the client. Similarly, to ensure the Altiris server has the correct updates within the local DNS cache, run **ipconfig /flushdns** on the server.

Q: What if the Intel® vPro systems were deployed in Small-Medium Business (SMB) mode? How do we remotely change to Enterprise mode and commence provisioning?

- **A:** As noted in a previous post (<http://juice.altiris.com/node/4480>), whether an Intel® vPro™ system is provisioned in SMB or Enterprise mode, the core functionalities and usages are the same. In addition, the Altiris Real-Time Systems Manager and Task Server have features and options to manage collections of Intel® vPro systems configured in SMB mode. However, SMB mode does not support the advanced configuration options of Kerberos, TLS, 802.1x, and so forth. In these situations, the utility **unprovision.exe** or **Intel® AMT Reflecter** ([Intel® AMT Reflecter](#)) can be used. More will be provided in a future article.

Q: What if the Intel® vPro systems were provisioned by a different client management console? Is there a way to co-host the communications to the Intel® vPro systems? What about migrating from a foreign solution to Altiris Out of Band Management?

- **A:** Short answer - yes. Once an Intel® vPro client is provisioned, any properly authenticated and authorized request can be applied to use the technology. The key is for all client management consoles to have awareness that the system is capable and configured, along with knowing the authentication details to access. Similarly, migrating the configuration or moving from one client management environment to another can be accomplished by sharing access to the configuration database, unprovisioning systems and directing the provisioning activity to the target environment, and so forth. Much more can (and hopefully will be) written on this...

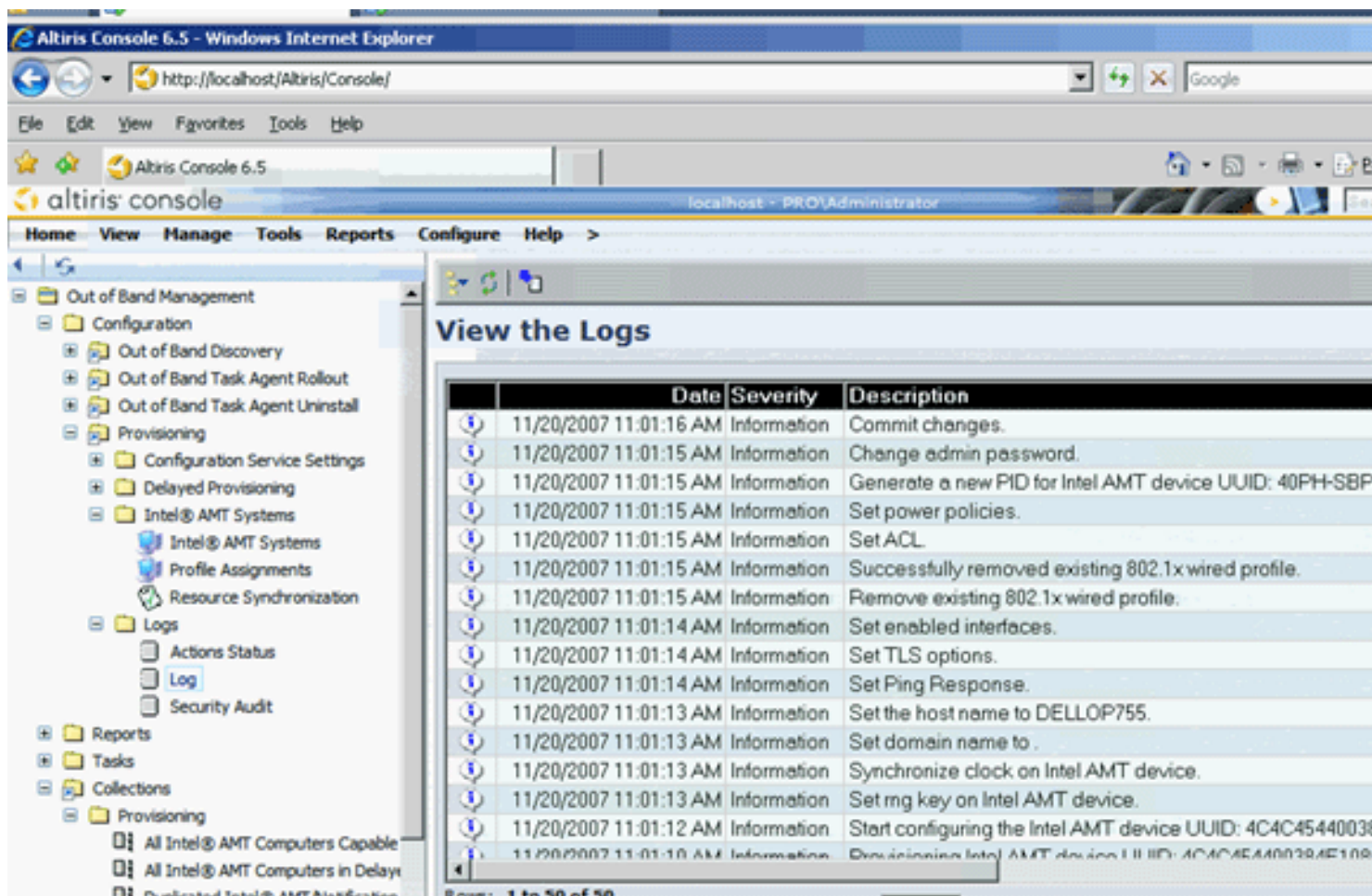
Successful Provisioning Log Sequence

In addressing many of the above scenarios and continuing on to various methods for complex provisioning situations, it may be helpful to note what a successful log sequence looks like in provisioning Intel® vPro technology. The image below provides an example of just that - a successful provisioning sequence. For all log items to appear, the logging level must be set to **Debug Verbose** in the General Service Settings located within the Provisioning menus of Out of Band Management.

The default log view shows the last event or occurrence at the top. In the example below, an Incoming connection from 192.168.0.101 occurred, followed by the start of the provisioning process. A series of SET commands then occur, which are determined by the provision profile and mapping of unique identifiers (see <http://juice.altiris.com/node/4480>).

Once the "Commit Changes" event occurs, the settings are complete and the management engine within the Intel® vPro firmware is ready to receive and respond to authorized requests.

In stepping through the scenarios and approaches, this series of articles will also expound a little more key utilities and approaches, including the Intel® vPro Activator Utility available at <http://www.intel.com/software/activator>. A previous article by Joel Smith provided a brief introduction to the predecessor of this tool, which was the Remote Configuration Tool (e.g. RCT.exe) - see <http://juice.altiris.com/node/3612>.



The third from the last event shows a new PID (provisioning ID) is set on the device. In future provisioning routines, this PID and a matching PPS which have been assigned to the client and the Altiris OOB Setup and Configuration service are used as part of the provisioning authentication routine. For those familiar with pre-shared key provisioning of Intel® vPro technology, this is the same concept. For environments using a pre-provisioning service where the same PID\PPS is initially set on all systems, it may be reassuring to know that during the initial provisioning process, a new and unique pair is assigned to the client. To take this one step further, if using remote configuration for the initial provisioning sequence, all sequence provisioning or configuration changes use the generate pre-shared key method until the system is fully unprovisioned.

Part 1 Summary

There are a variety of deployment scenarios that go beyond the basic understanding of Intel® vPro provisioning. Many of the common scenarios and inquiries were mentioned above, and there are likely more that will come forward. The next set of articles may address many, or provide sufficient pointers and resources for you to be effective in your respective environments. However, if there is a burning question or scenario that is not addressed - please ask.

The next article in this series is <http://communities.intel.com/docs/DOC-1918>