Instructions for setting up the User Notification Service

The Intel® Active Management Technology (Intel® AMT) User Notification Service (UNS) runs as a Windows* service on the host of a platform that also has Intel AMT enabled. The UNS receives messages from Intel AMT and passes them to software agents running on the host. Besides installing the service as described elsewhere in this kit, IT must perform additional steps related to authentication for UNS to perform its function.

System Requirements:

The Intel(R) AMT UNS application is supported on the following Operating Systems:

- Windows* XP SP1/2 (32-bit and 64-bit)
- Windows* Vista (32-bit and 64-bit)

TLS:

If Intel AMT is configured to work with transport layer security (TLS) then any application that wants to communicate with Intel AMT must be able to verify the server certificate that Intel AMT sends. To do that, a root certificate from the certificate authority (CA) that signed the Intel AMT certificate must be installed by the IT administrator in the Windows trusted root certificate store.

Since UNS, as a service, runs in the system context (not as a user process), it does not see the same certificate store as a user process. For UNS to have access to the root certificate, the root certificate must be installed using the “mmc” tool, as described in **Step 4: Install the root certificate of the CA** at the following web page:
http://support.microsoft.com/kb/901183/

Mutual Authentication TLS:

If Intel AMT is configured to use mutual authentication TLS for communications with the local host (mutual authentication can be set separately for remote and local interfaces), when a local application tries to connect, Intel AMT will require the application to send a client certificate for verification. This client certificate must be installed in the Windows personal certificate store.

Again, since UNS is a service, the IT administrator must install the client certificate using steps 1 to 3 as described at the above link:

Step 1: Install the client certificate in the local machine store
Step 2: Configure access to the client certificate
Step 3: Copy the client certificate from the local user store to the local machine store

If the certificate store contains more than one Intel AMT client certificate, then UNS must be told which client certificate in the store to actually use. This can be done (while the service is stopped) either with the following command line argument to the

sc command: **-cert <cert name>** or in the graphical service controller window. To access the graphical service controller window, right-click on My Computer, select **Manage**, and open the **Services and Applications/Services** leaf. Double-click on the stopped UNS service and enter **–cert <cert name>** in the "start parameters" field.

HTTP Credentials:

Independent of the TLS configuration, UNS uses SOAP calls to Intel AMT and requires credentials. UNS calls two SOAP services in Intel AMT: User Notification and Endpoint Access Control. These two realms might have different access privileges (i.e. different users can be part of these realms).

By default, there is no need for credentials to access the above two realms, so UNS should just work (anonymous access). However, the administrator can decide to block this anonymous access and mandate credentials for one or both of the above realms. This can be done using the SetRealmAuthOptions SOAP command in the Security Administration interface.

If credentials are needed for these realms they need to be passed to the UNS as arguments: **-unsUser <user name> -unsPass <password>** for the User Notification realm, and **-eacUser <user name> -eacPass <password>** for the Endpoint Access Control realm. The IT administrator enters these parameters as described above, when the service is stopped, either with the **sc** command or via the graphical service controller window. When the **-clear** flag is given as command line argument to the service, the service will remove the stored credentials from the registry and will stop running.

A property of the above credentials is that UNS saves them for the next time it is run. This means that UNS can be started once with the credentials as arguments, stopped, and then re-started without the credentials, and they will still be used (as long as Intel AMT is configured to require them). This allows the administrator to run UNS without the credentials showing in the process table as the UNS process's arguments.