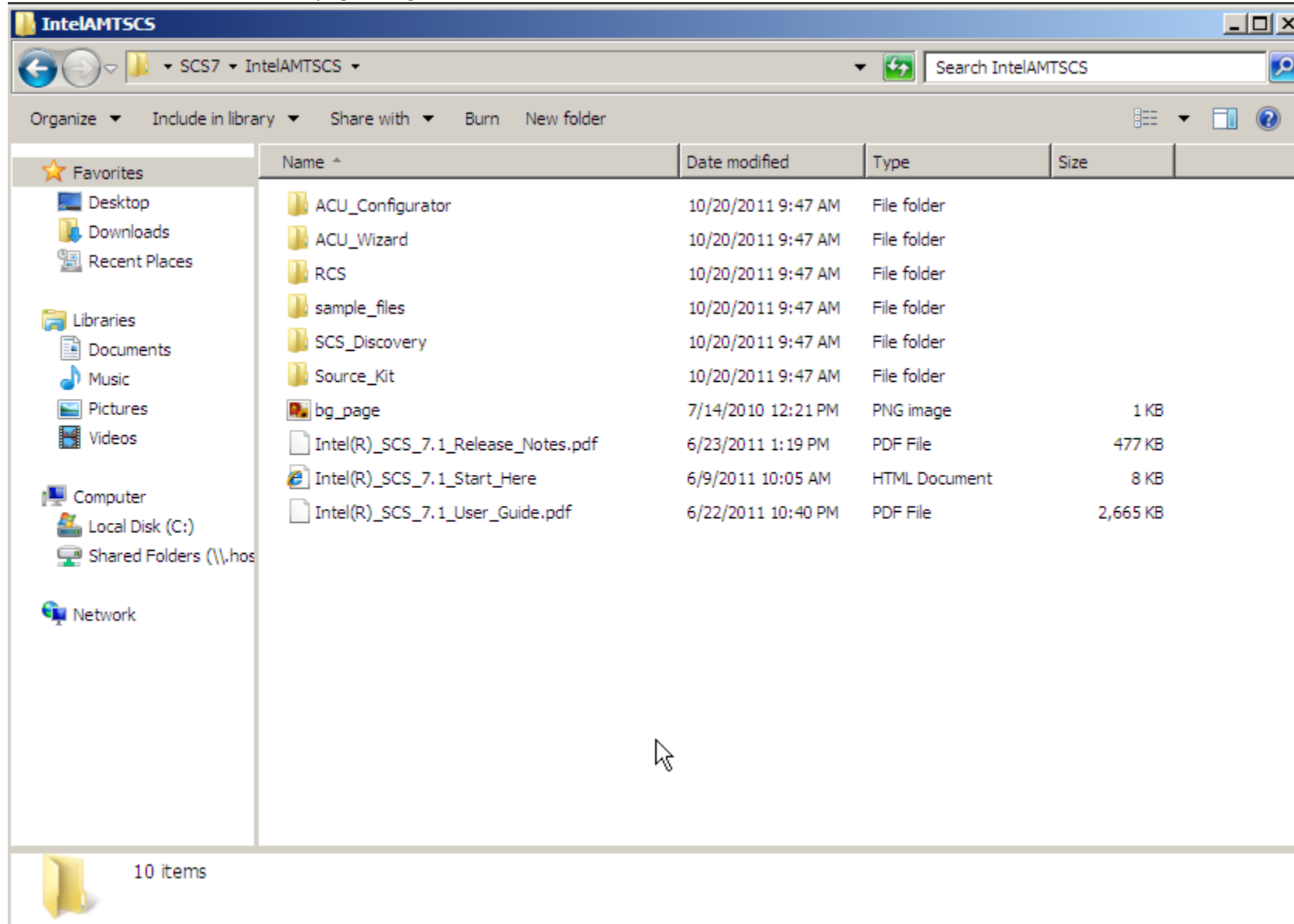Here is how I went from install to provisioning with SCS 7:

Step 1:
I went to the Intel SCS Download page and grabbed the latest version of SCS 7

Then I installed RCS on a fresh build of Windows Server 2008
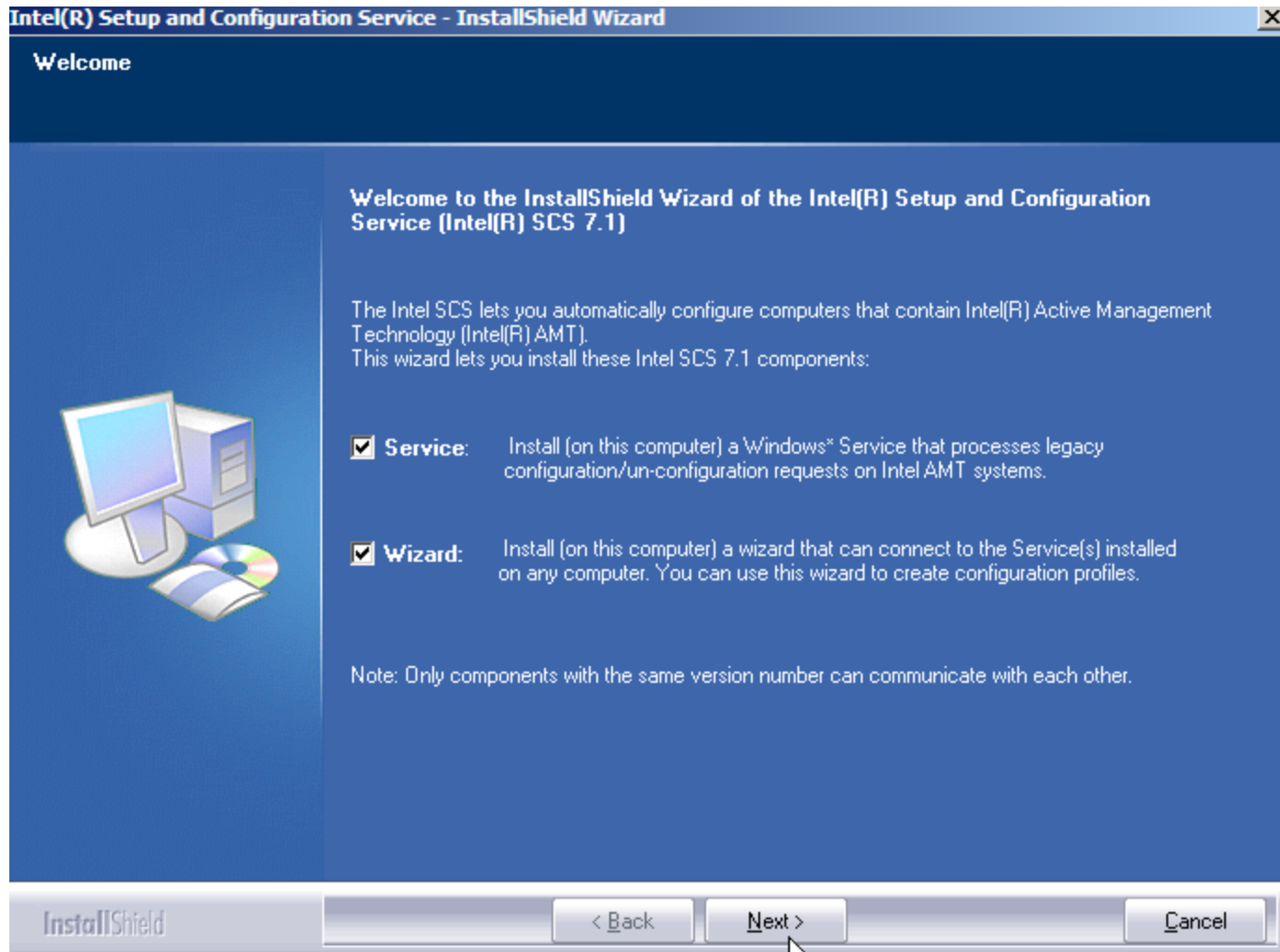
Making sure I selected both:

For the service account, I just used my admin account:
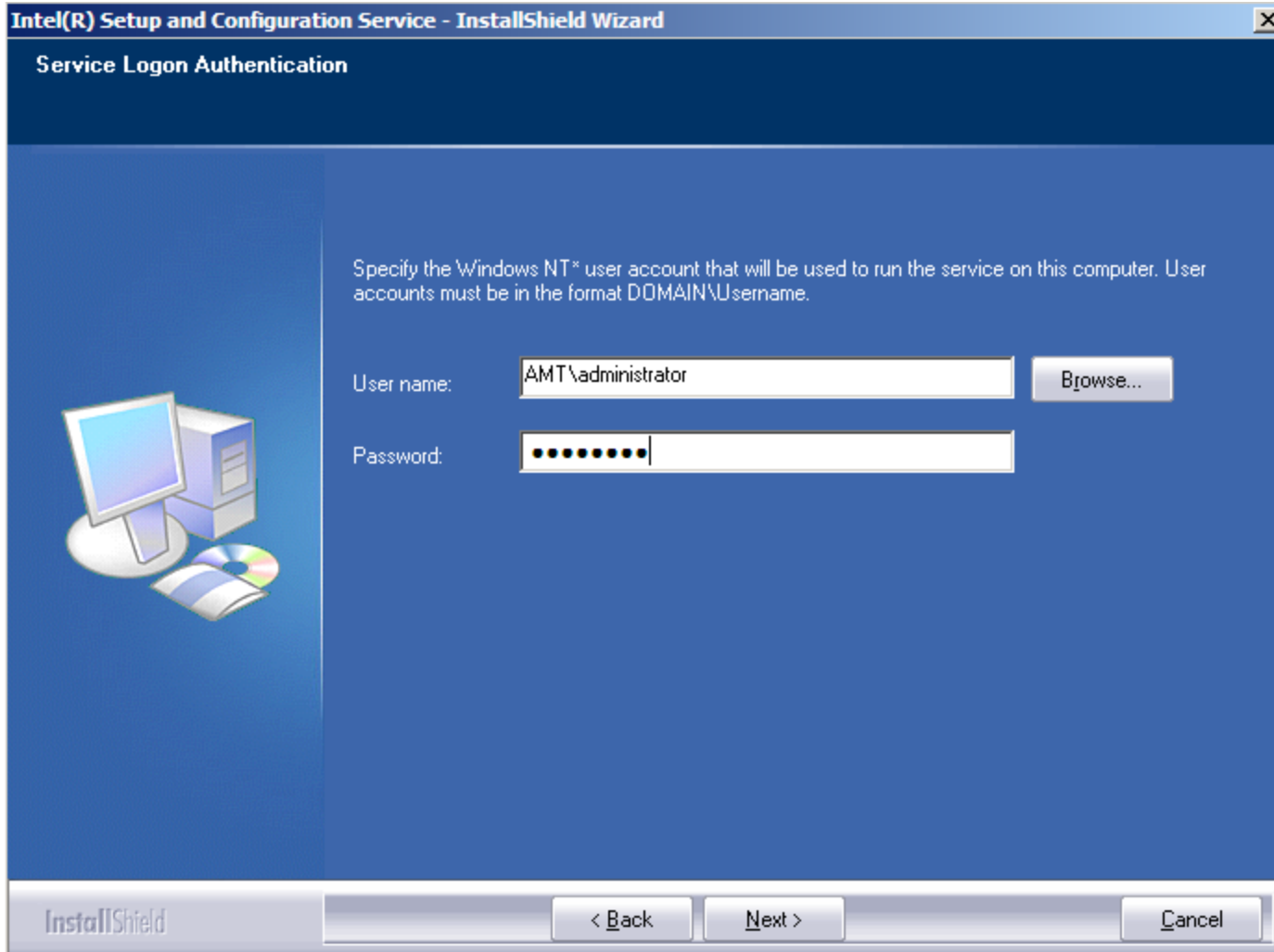
Clicked through the next few pages:

Then clicked finish:

Next you will see a few services starting, and finally the Intel SCS wizard will appear:
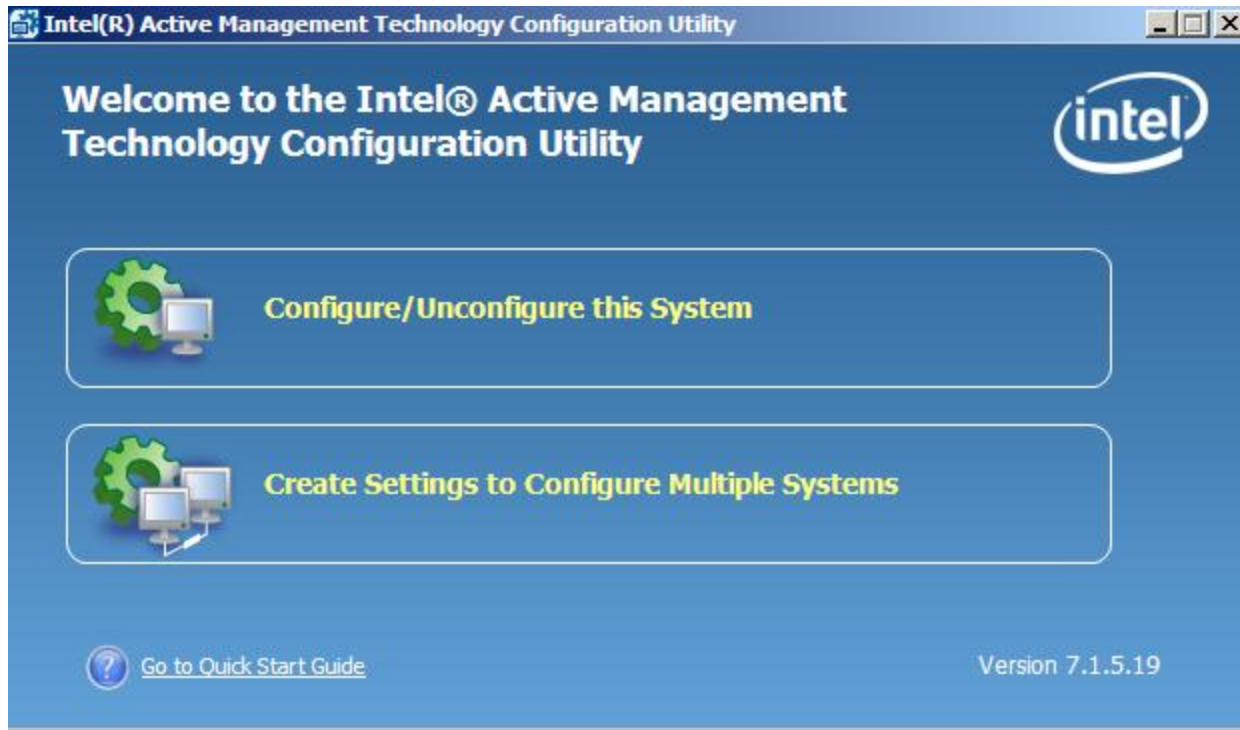
Since we are on the server, we will ignore "Configure/Unconfigure this system"
And just select "Create Settings to Configure Multiple Systems"

The wizard now connects to the local "RCS" and we are ready to start creating the profile that will be used to configure our systems:
I hit new:
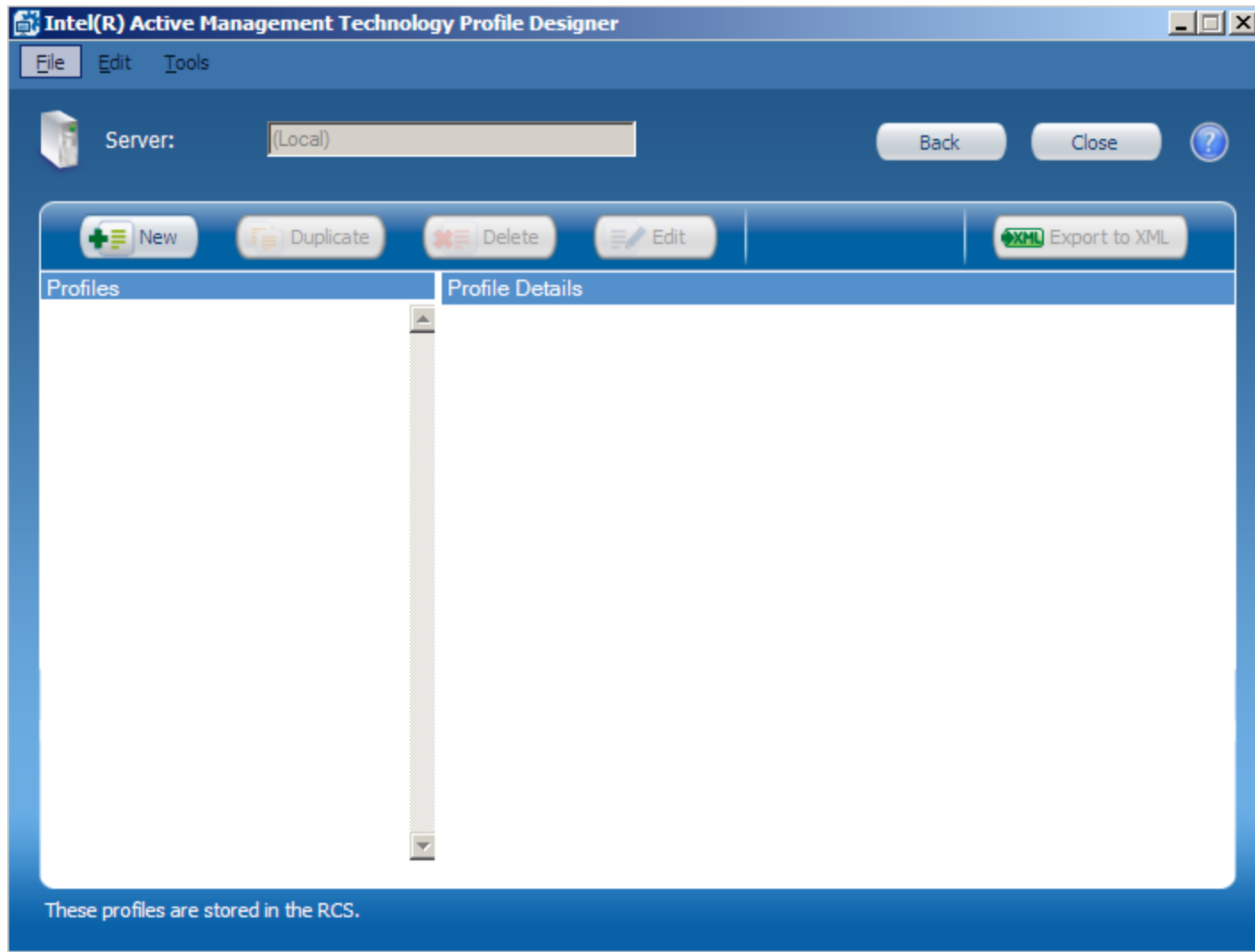
And now we can start creating the profile:

I will leave the settings at default:
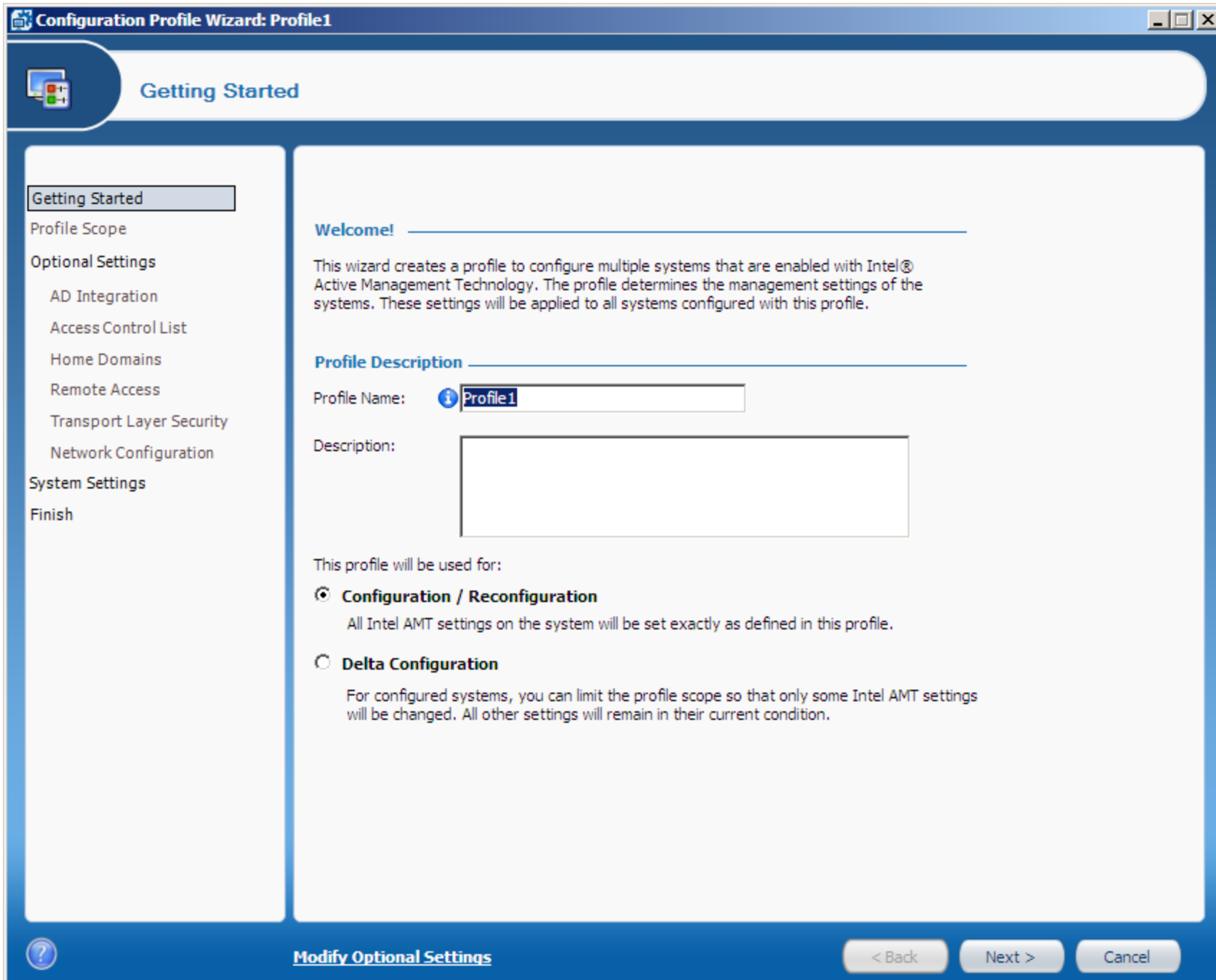
The next screen allows you to select all the features you want to enable / configure:

For my test case (since you mentioned you were using AD) I will check that box

I will also create an ACL

Optional Settings

Getting Started

Profile Scope

Optional Settings

   AD Integration

   Access Control List

   Home Domains

   Remote Access

   Transport Layer Security

   Network Configuration

System Settings

Finish

Select the settings that you want to configure. On configured systems, settings that are not selected will be removed from the system during configuration.

☑ **Active Directory Integration**
   Allow the Intel® AMT systems to use security features of the Active Directory

☑ **Access Control List (ACL)**
   Assign customized access levels to the systems based on users and groups

☐ **Home Domains**
   Define trusted domains where the Intel® AMT functionality will be available

ⓘ ☐ **Remote Access**
   Enable Intel® AMT systems outside of the enterprise network to communicate with management consoles via a Management Presence Server (MPS)

☐ **Transport Layer Security (TLS)**
   Use the TLS protocol to encrypt and authenticate communication with the systems

☐ **Network Configuration**
   Select at least one of the following items:

   ☐ **WiFi Connection**
      WiFi network settings

   ☐ **Wired 802.1x Authentication**
      802.1x authentication settings for wired LAN only

   ⓘ ☐ **End-Point Access Control (EAC)**
      EAC settings used to authenticate system status

< Back   Next >   Cancel

Now I hit next:

Configuration Profile Wizard: Profile1

Optional Settings: Active Directory Integration

Active Directory Integration

Getting Started
Profile Scope
Optional Settings
  AD Integration
  Access Control List
  Home Domains
  Remote Access
  Transport Layer Security
  Network Configuration
System Settings
Finish

◉ Active Directory OU: [   ] [..]

○ Path to file containing ADOU information: [   ]

Modify Optional Settings

< Back   Next >   Cancel

It's now asking me for an OU to store the AD objects that will enable Kerberos Authentication

I now have to go to my Domain Controller and create a unique OU to hold the objects.
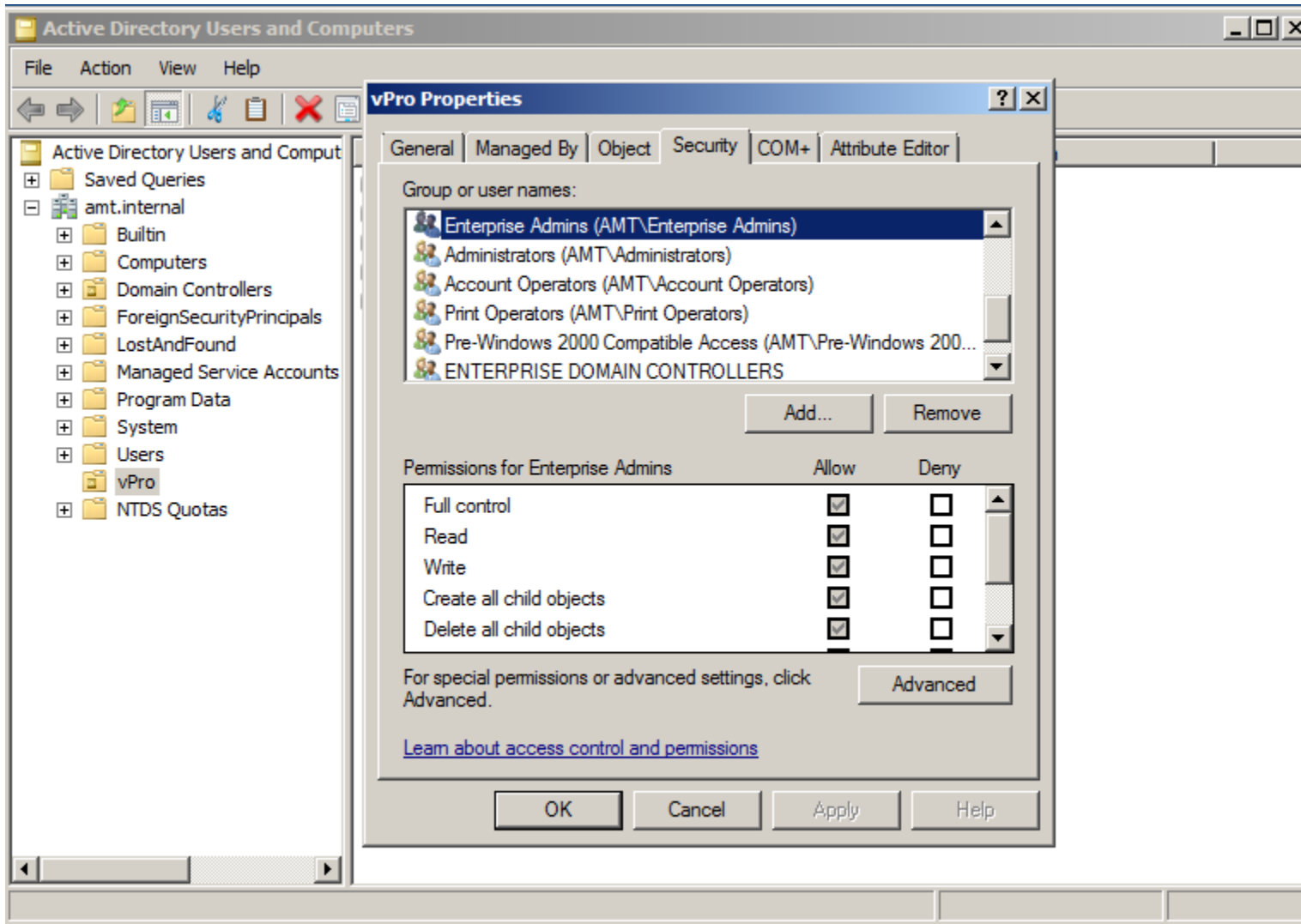
Here we can see that I created an OU called "vPro" and I made sure to grant Full Control to the account we used to run the RCS Service (in this case I used a domain admin account, but in a real environment you would simply create a process account and grant it permissions)

Now that we have our OU, we can select it:

Optional Settings: Active Directory Integration

Getting Started

Profile Scope

Optional Settings

    AD Integration

    Access Control List

    Home Domains

    Remote Access

    Transport Layer Security

    Network Configuration

System Settings

Finish

Active Directory Integration

⦿ Active Directory OU: [   ] [..]

○ Path to file containing ADOU information: [   ]

Select Active Directory Organization Unit

Select an Active Directory Organization Unit that will contain the System object:

- ☐ DC=amt (amt.internal)
  - ☐ CN=Computers
  - ☐ OU=Domain Controllers
  - ☐ CN=ForeignSecurityPrincipals
  - ☐ CN=Managed Service Accounts
  - ☐ CN=Program Data
  - ☐ CN=System
  - ☐ CN=Users
  - ☐ **OU=vPro**

[OK] [Cancel]

Modify Optional Settings

[< Back] [Next >] [Cancel]

Then I hit next:

For the ACL, I am just going to add my domain admin user and grant them full permissions
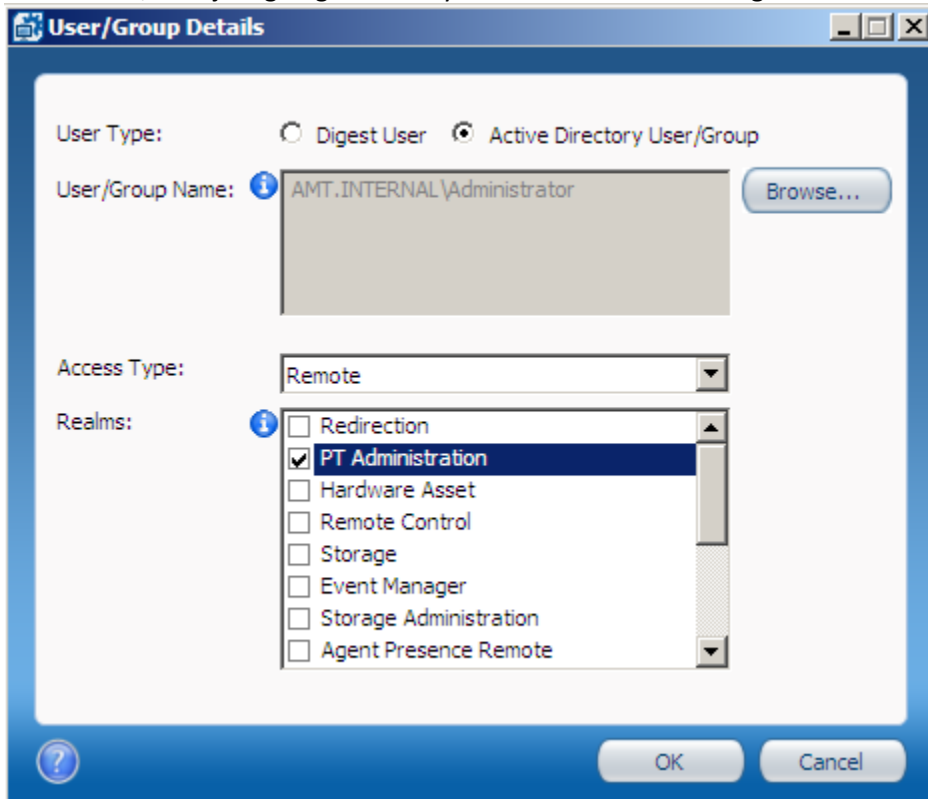
Now when I access that configured AMT system, it will only grant that account access to the AMT features.

I hit next:
And for the demo I am just going to enter the new MEBX password (used for local access)
And specify a remote admin password (you want to be sure you do not select Random option here) (Will be used to access the system remotely via digest user: Admin)

System Settings

Getting Started

Profile Scope

Optional Settings

  AD Integration

  Access Control List

  Home Domains

  Remote Access

  Transport Layer Security

  Network Configuration

System Settings

Finish

Management Interfaces

Select which management interfaces to enable:

☑ Web UI ☑ Serial Over LAN ☑ IDE Redirection ☑ KVM Redirection   [KVM Settings...]

RFB Password for KVM sessions: ⓘ [   ] ☐ Show password

Power Management Settings

Specify the system power states in which the Management Engine (ME) is operational:

[Always On (S0-S5)   ▼]

☐ ME will go into a lower power state when idle. Timeout if idle: [3 ⇕] minutes

Network Settings

ME Bios Extension (MEBx) password: ⓘ [••••••••] ☐ Show password

Specify the method to be used to create the Intel® AMT admin user password:

⦿ Use the following password for all systems: ⓘ [••••••••] ☐ Show password
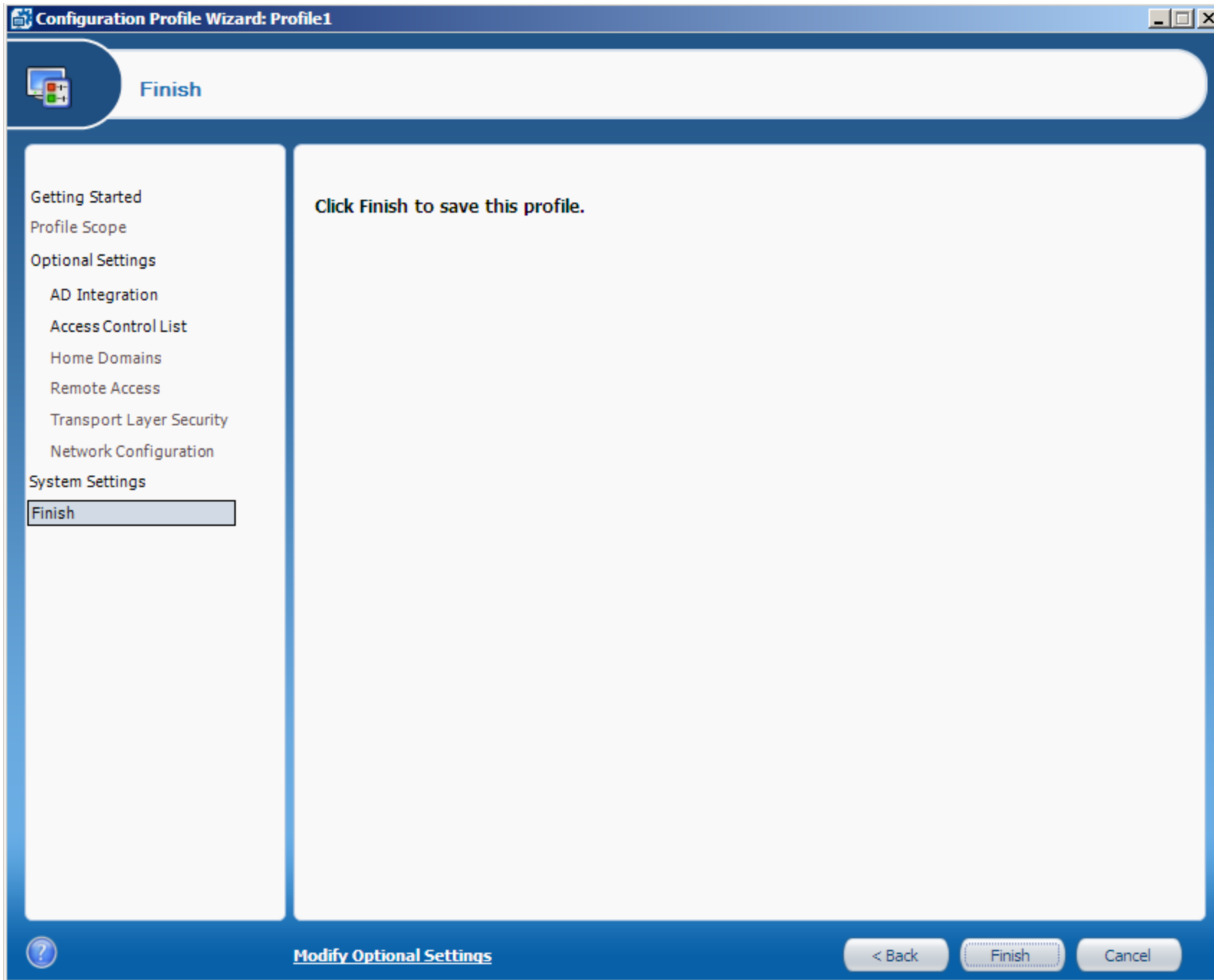
◯ Create a random password for each system

☐ Enable Intel® AMT to respond to ping requests

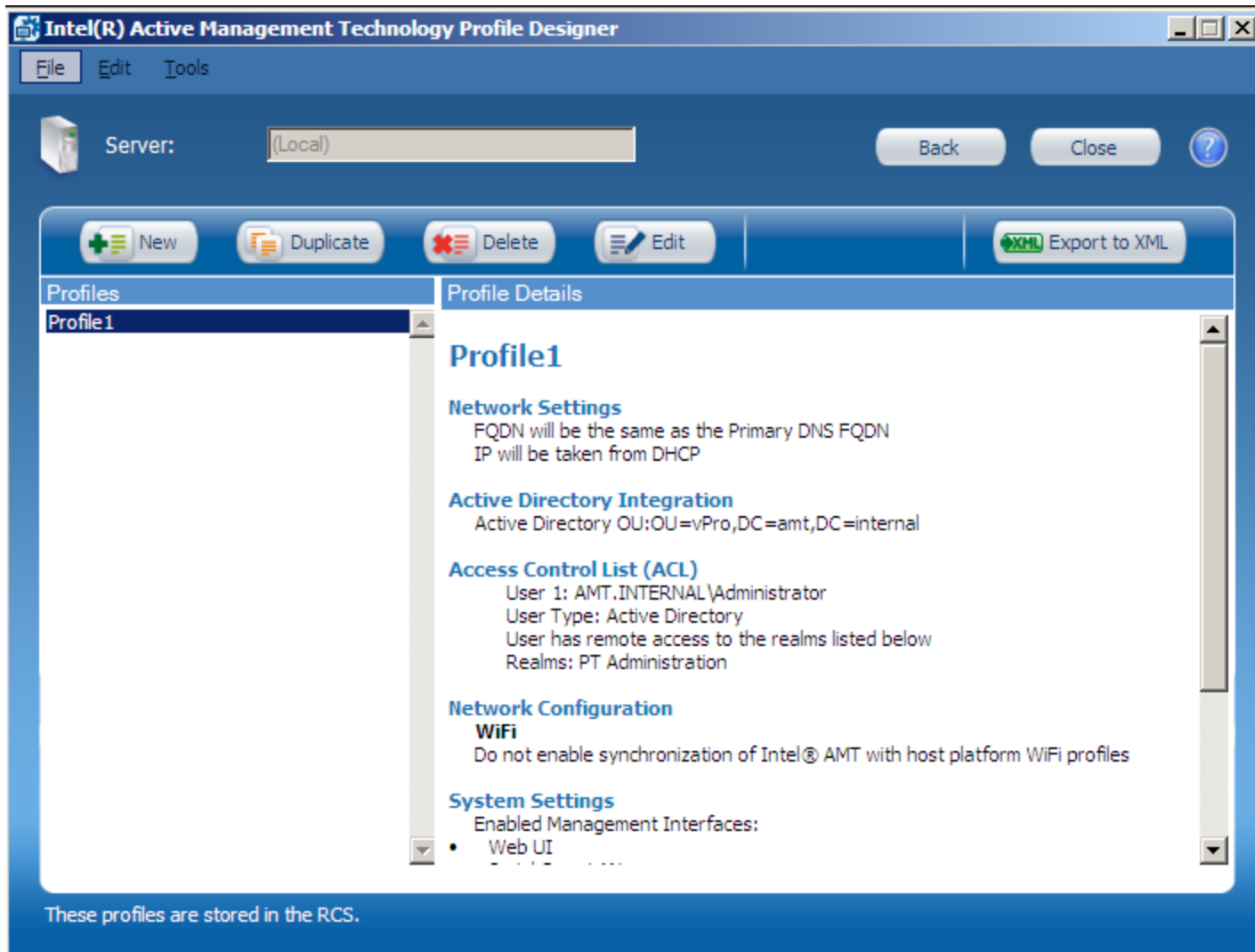☑ Enable Fast Call for Help (within the enterprise network)   [Fast Call for Help Settings...]

Edit IP and FQDN settings: [Set...]

Modify Optional Settings   [< Back] [Next >] [Cancel]

Now I click finish

Configuration Profile Wizard: Profile1

Finish

Getting Started
Profile Scope
Optional Settings
    AD Integration
    Access Control List
    Home Domains
    Remote Access
    Transport Layer Security
    Network Configuration
System Settings
Finish

Click Finish to save this profile.

Modify Optional Settings   < Back   Finish   Cancel

Now I have the profile created on the RCS server itself:

Intel(R) Active Management Technology Profile Designer

File   Edit   Tools

Server: (Local)   Back   Close

New   Duplicate   Delete   Edit   XML Export to XML

Profiles

Profile1

Profile Details

Profile1

Network Settings
FQDN will be the same as the Primary DNS FQDN
IP will be taken from DHCP

Active Directory Integration
Active Directory OU:OU=vPro,DC=amt,DC=internal

Access Control List (ACL)
User 1: AMT.INTERNAL\Administrator
User Type: Active Directory
User has remote access to the realms listed below
Realms: PT Administration

Network Configuration
WiFi
Do not enable synchronization of Intel® AMT with host platform WiFi profiles

System Settings
Enabled Management Interfaces:
• Web UI

These profiles are stored in the RCS.

One last step (because I do not want to have to touch each system) is to obtain a Remote Provisioning Certificate from an external cert vendor and install it:

SCS7

amt.internal....

Certificate Import Wizard

Password
To maintain security, the private key was protected with a password.

Type the password for the private key.

Password:

●●●●●●●●

☐ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

☑ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

☑ Include all extended properties.

Learn more about protecting private keys

< Back   Next >   Cancel
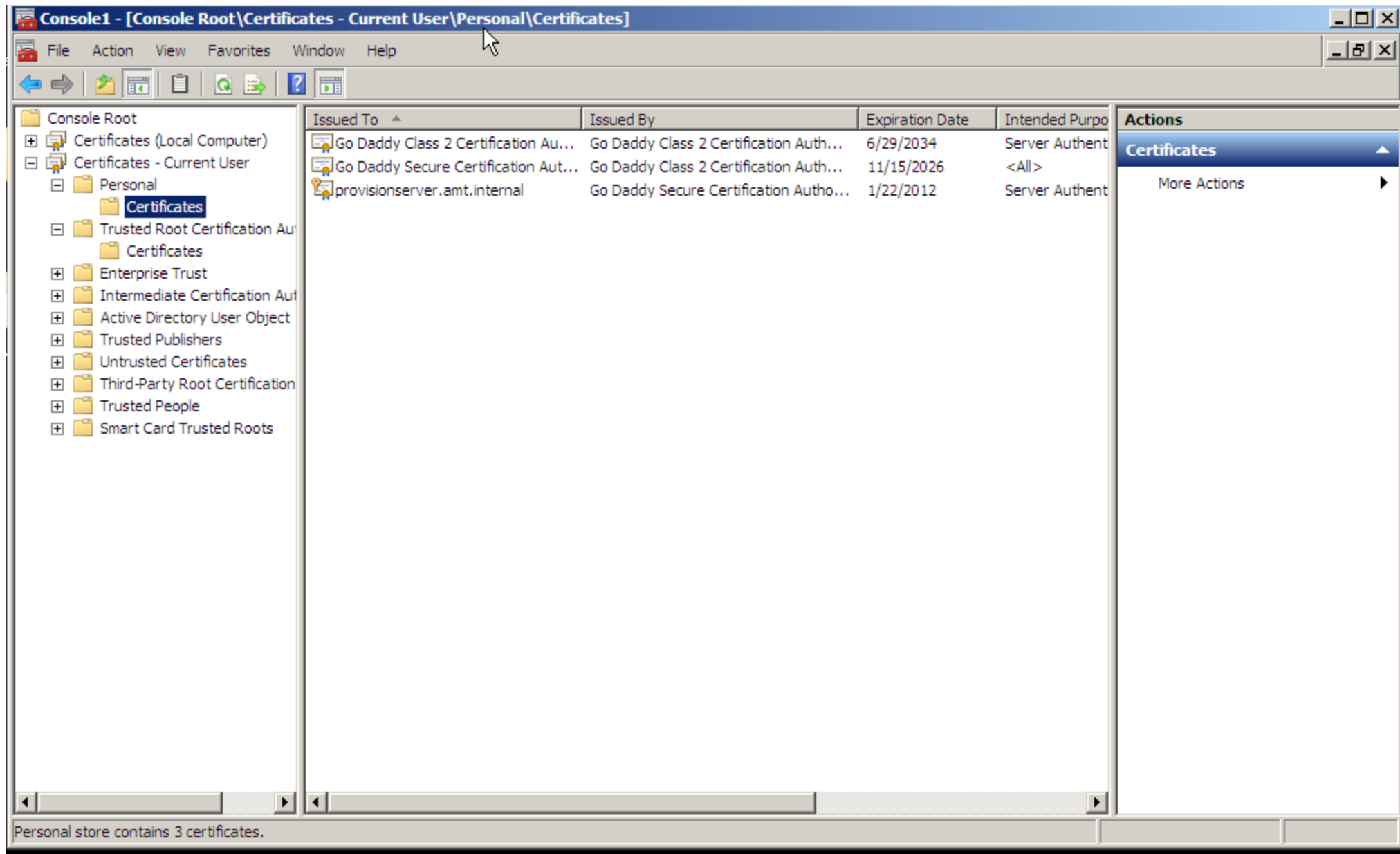
For the cert, we also want to make sure that we have the entire "Chain" in the Current User Trusted Root Certification Authority

File   Action   View   Favorites   Window   Help

Console Root	Issued To ▲	Issued By	Expiration Date	In
⊞ Certificates (Local Computer)	amt-WIN2K8X64-DC-CA	amt-WIN2K8X64-DC-CA	4/7/2016	</
⊟ Certificates - Current User	Class 3 Public Primary Certification Authority	Class 3 Public Primary Certification A...	8/1/2028	Se
⊟ Personal	Class 3 Public Primary Certification Authority	Class 3 Public Primary Certification A...	1/7/2004	Se
Certificates	Copyright (c) 1997 Microsoft Corp.	Copyright (c) 1997 Microsoft Corp.	12/30/1999	Tir
⊟ Trusted Root Certification Aut	Equifax Secure Certificate Authority	Equifax Secure Certificate Authority	8/22/2018	Se
Certificates	Go Daddy Class 2 Certification Authority	Go Daddy Class 2 Certification Auth...	6/29/2034	Se
⊞ Enterprise Trust	Go Daddy Secure Certification Authority	Go Daddy Class 2 Certification Auth...	11/15/2026	</
⊞ Intermediate Certification Aut	GTE CyberTrust Global Root	GTE CyberTrust Global Root	8/13/2018	Se
⊞ Active Directory User Object	Microsoft Authenticode(tm) Root Authority	Microsoft Authenticode(tm) Root Au...	12/31/1999	Se
⊞ Trusted Publishers	Microsoft Root Authority	Microsoft Root Authority	12/31/2020	</
⊞ Untrusted Certificates	Microsoft Root Certificate Authority	Microsoft Root Certificate Authority	5/9/2021	</
⊞ Third-Party Root Certification	NO LIABILITY ACCEPTED, (c)97 VeriSign, Inc.	NO LIABILITY ACCEPTED, (c)97 Veri...	1/7/2004	Tir
⊞ Trusted People	Thawte Timestamping CA	Thawte Timestamping CA	12/31/2020	Tir
⊞ Smart Card Trusted Roots				

Actions

Certificates ▲

More Actions ▶

Trusted Root Certification Authorities store contains 13 certificates.

Now we have the RCS server configured and waiting for clients to call in to provision..

Now we will go to one of our systems and make sure we have the Intel Management and Security Status icon on our AMT Client:

You can download the IMSS application / AMT Drivers etc.. from your OEM. for example here it is on Dell's website for this e6410 machine:

Intel AMT HECI

Release Date:	7/6/2011	
Version:	6.2.0.1022 , A05	
Download Type:	Driver	▸ Other Versions
File Format:	Hard Drive	
File Size:	10 MB	
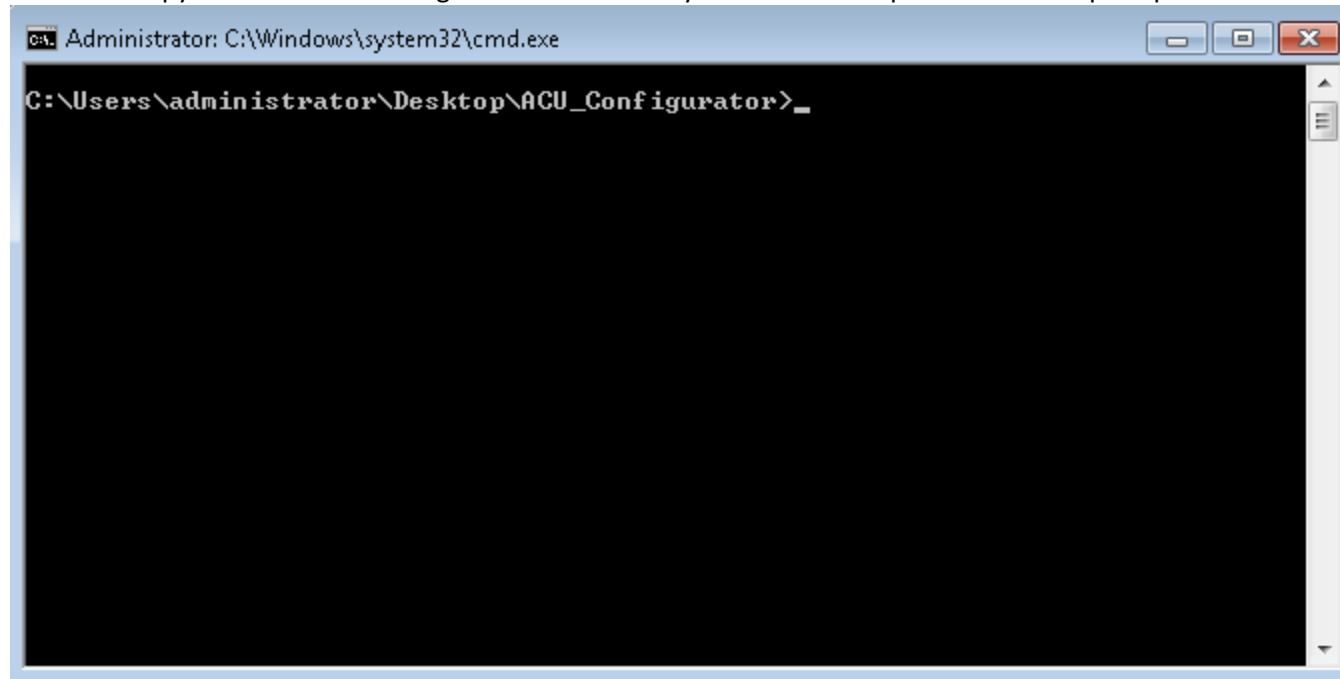
[Download]
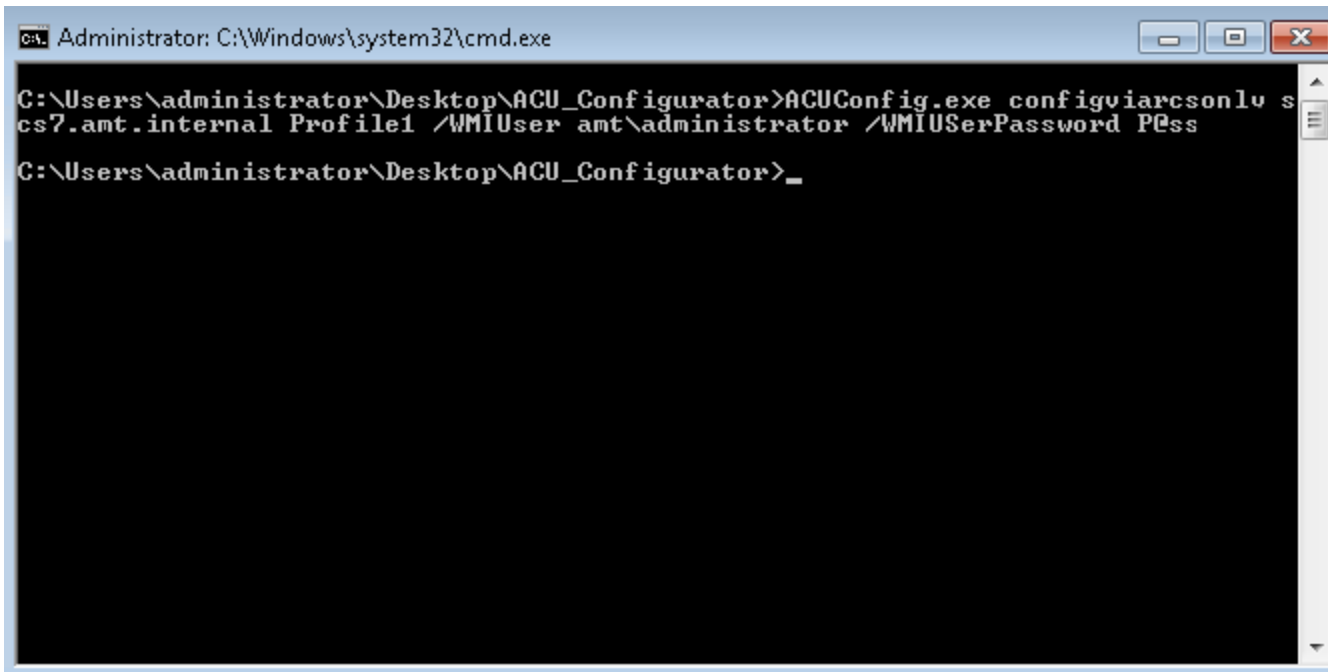
▸ Add To Download List

▸ Sign In to View My Saved Downloads

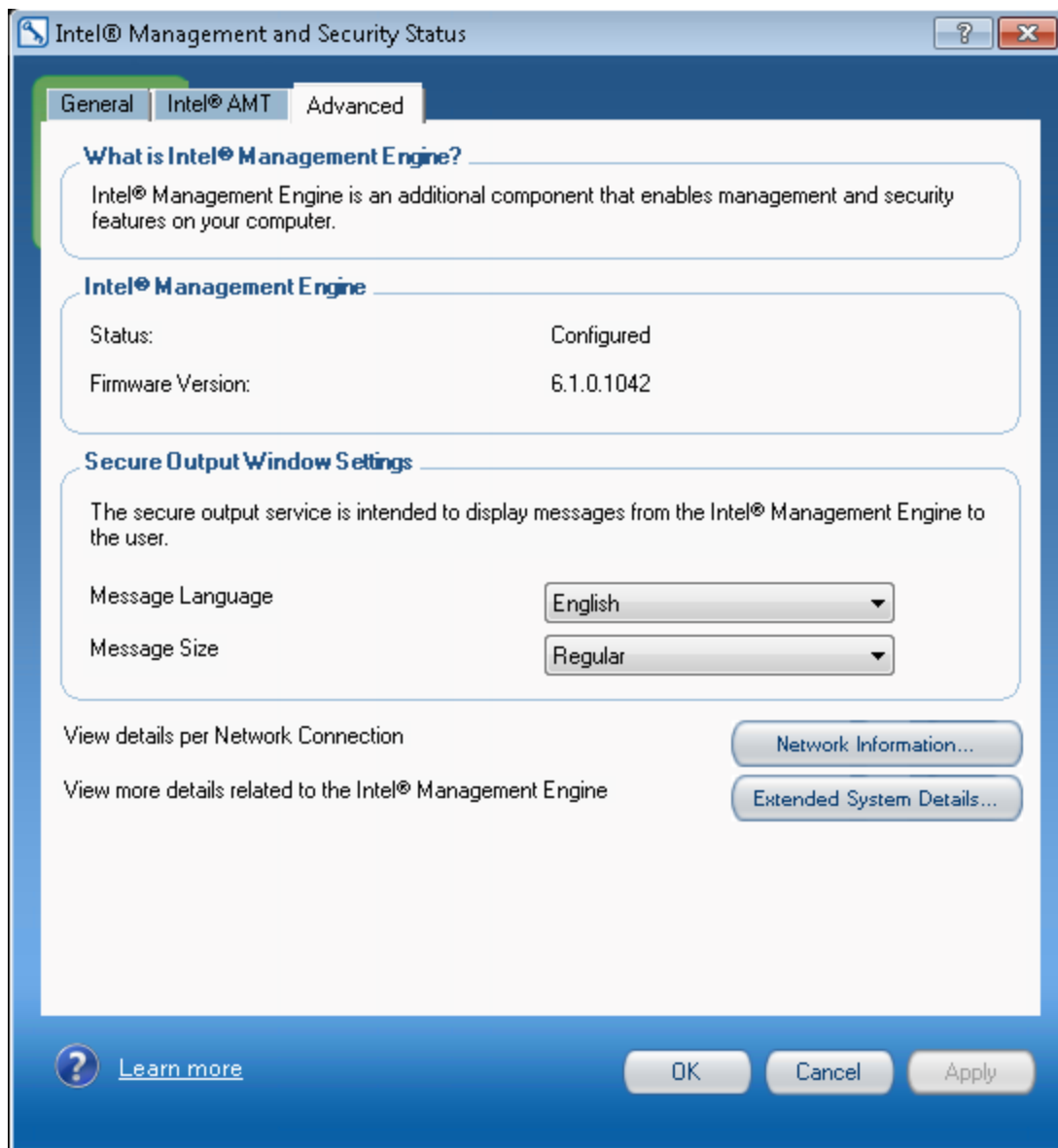Now I will copy over the "ACU Configurator" to one of my machines and open a command prompt

```
Administrator: C:\Windows\system32\cmd.exe                          ─ ▣ ✕

C:\Users\administrator\Desktop\ACU_Configurator>ACUConfig.exe configviarcsonlv s
cs7.amt.internal Profile1 /WMIUser amt\administrator /WMIUSerPassword P@ss

C:\Users\administrator\Desktop\ACU_Configurator>_
```

I run the command (specifying my user and password) and the system is configured.

I can check the status by opening the IMSS icon:

Now I can connect to the machine using PowerShell.