Intel® Active Management Technology Setup and Configuration Service

Installation and User Manual

November 2006

Version 1.2

Table of Contents

Setup and Configuration Service Overview 1

Introduction to Intel SCS 2

Setup and Configuration Process 3

SCS Database Preparation 3

Preparation of Platform Containing Intel AMT Device 4

Setup and Configuration Steps 4

Intel AMT SCS Functional Flow 5

Setup and Configuration Operational Overview 6

Pre-Setup and Configuration 6

Setup and Configuration 7

Integration with Active Directory 7

Gathering Security Information 7

Management and Maintenance 8

Configuring Intel AMT in a Secure Environment 8

The SCS Database 10

Considerations 10

Database Security 11

Schema 11

Backup & Restore 11

SCS and Active Directory Tasks and Permissions 12

Active Directory Schema 12

Security Groups 12

AMT Object 12

Computer Object 13

Environment Prerequisites and Installation 14

System Requirements 15

Environment Overview 17

Description of Intel SCS Components 17

Intel SCS Console 17

List of Required Microsoft Components 17

Environment Prerequisites 19

.NET Framework 2.0 19

Microsoft SQL Server Express 20

Enable SQL Server and Windows Authentication Mode 22

SQL Server Verification 23

Internet Information Services (IIS) 6.0 24

IIS Verification 25

Microsoft Certificate Authority 26

Installing the Microsoft CA 27

Exporting and Installing the CA Certificate 29

Secure the Connection to IIS Using SSL 31

Installing a CA Certificate to Authenticate IIS 33

Installing an Intel AMT Client Certificate for TLS Mutual Authentication 34

Active Directory (AD) and Changes to the AD Schema 35

Installation of the SCS Server Components 36

Installing the Intel SCS Server Components 36

Upgrading the Intel SCS to a New Version 40

Silent Install 40

Installation of the Intel AMT Management Console 45

Post Installation Operations 46

Intel AMT Configuration and the DNS 46

Intel SCS 46

Intel AMT Devices 46

AMTConfig Service Verification 46

Quick Start and System Test 48

Recommended Daily Workflow 51
Intel AMT Preparation 52
Preparation Without a USB Device 53
Using a USB Storage Device for Factory Mode Setup 56
Requirements 56
Preparation 56
Initializing a Platform 56
Moving to Setup Mode 57
Preparing Intel AMT for Future Configuration 57
Intel SCS Console 58
SCS Console Overview 59
Using the SCS Console for the First time 59
Console Navigation Pane 59
Console Configuration Pane 60
Logging In 61
Configuring Main Service Settings 62
Defining General Parameters 62
Configuring Profiles 65
Viewing Existing Profiles 65
Adding a Profile 65
Configuring Pre-Setup and Configuration Security Keys 74
Configuring Users 76
Viewing Existing Users 76
Adding a User 77
New Intel AMT Systems 79
Viewing Defined Intel AMT Devices 79
Defining a New AMT Record 80
Filtering the Display 81
Configuring Existing Intel AMT Devices 82
Viewing AMT Devices and Reviewing the Details of a Device 82
Ad Hoc Operations on an Individual Intel AMT Device 83
Filtering the Display 85
Global Operations 85
Maintenance Policies 87
Intel AMT SCS Console Logs 89
Filtering a Log Display 89
SOAP API 91
Overview of the SOAP API 92
Client Samples 93
Usage 93
Input File 93
Input Binary Data 94
Output Binary Data 95
Default Values 95
SOAP Faults 96
SCS Support Content 97
SCS Tools 98
Command Line Tools 98
Add new AMT Properties 98
Database Dump 98
Administrative Tools 98
Active Directory Schema 98
Group, User, and ACL Management Scripts 99
Active Directory User and Groups 99
Active Directory ACL 101
Using a Script to Import New Intel AMT Properties 102
Environment Variables 102

Output File Format 102
Script Functionality 103
Sample Script 103
Configuring PEM Files for Redirection Applications 104
CRL XML Format 106
Troubleshooting 107
Windows Service Error Codes 109
Log Mapping 110
Glossary 111

Chapter 1

SETUP AND CONFIGURATION SERVICE OVERVIEW

This section contains:

- “Introduction to Intel SCS” on page 2
- “Setup and Configuration Process” on page 3
- “Setup and Configuration Operational Overview” on page 6
- “The SCS Database” on page 10
- “SCS and Active Directory Tasks and Permissions” on page 12

Introduction to Intel SCS

Intel® Active Management Technology's (Intel® AMT) Setup and Configuration Service (Intel SCS or SCS) provides an enterprise with the tools to set up and configure Intel AMT devices.

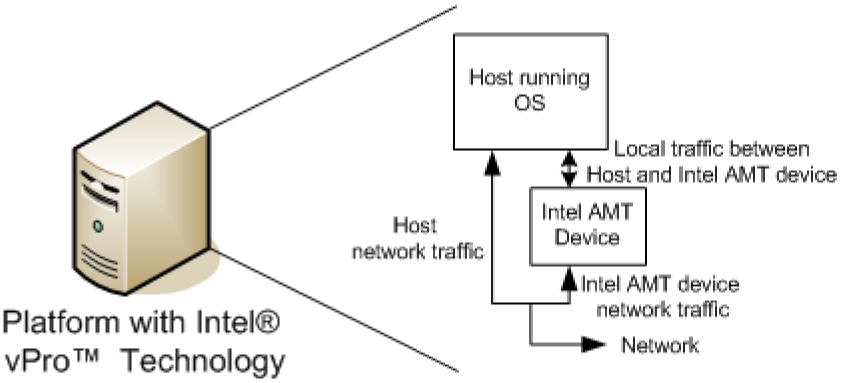
Intel AMT is an integral part of computer platforms that contain Intel® vPro™ technology. Intel AMT enhances the ability of IT organizations to manage enterprise computing facilities. Intel AMT operates independently of the platform processor and operating system. Remote platform management applications can access Intel AMT securely, even when the platform is turned off, as long as the platform is connected to line power and to a network.

Intel AMT can:

- discover platform assets using data retained in non-volatile storage
- heal systems remotely even when the operating system is down
- protect against malicious software attacks by making it easier to keep software and virus protection consistent and up-to-date across the enterprise
- limit the effect of "malware" and platform misuse by containing outbreaks and software tampering on the managed client, isolating the infected network element from the rest of the network

The platform can be viewed as having two separate elements:

- a host processor running a general purpose operating system such as Windows* XP
- an Intel AMT device operating independently of the host. The Intel AMT firmware executes on the Intel® Management Engine (Intel® ME).


Host running OS
Local traffic between Host and Intel AMT device
Intel AMT Device
Host network traffic
Intel AMT device network traffic
Network
Platform with Intel® vPro™ Technology

When an Intel AMT enabled platform is delivered, the Intel AMT device is present but disabled. The Intel AMT device must undergo setup and configuration before it is operational. In Enterprise environments, the setup and configuration must be done over the network interface.

In addition to the term "Setup and Configuration," the process of enabling an Intel AMT device is also called "provisioning."

The Intel AMT Setup and Configuration Service performs all the necessary steps to make an Intel AMT device operational. This includes both Intel AMT Release 1.0 and Intel AMT Release 2.0/2.1 devices.

Once the Intel SCS has been installed and its database has been loaded with initial data, setup and configuration starts when an Intel AMT device sends a message called a “Hello” message to the SCS. The SCS and the Intel AMT device communicate securely as the SCS generates and sends the device:

- certificates from a public key infrastructure (PKI)
- access control lists (ACLs)
- other setup parameters, as defined in a **profile** of setup and configuration information specific to the platform or to a family of platforms

The SCS also registers the Intel AMT device in Active Directory and in its own secure database. The SCS is used for various maintenance functions, such as updating passwords and ACLs, and keeps logs of all performed transactions.

The SCS components can be distributed across several platforms. It is recommended, for performance reasons, to configure a distributed installation except for demo purposes or for small enterprise installations.

It is possible to have multiple instances of the SCS installed across an enterprise, but there is only one SCS database for the enterprise.

The major elements of the SCS are:

- a Windows service (the SCS Main Service)
- a secure database
- a SOAP API
- a console application (the Intel SCS Console)

Intended Use of this Manual

The Intel AMT SCS is provided to ISVs as a binary executable. The source code of the SCS Console is included in the product distribution, as well as a description of the SOAP API. ISVs are expected to add value to the Console or to create their own equivalent using the API. The Intel AMT SCS will not be provided to end users directly by Intel. Rather, it will be part of an ISV’s product offering, either stand-alone or embedded in a management console product. This manual is designed to be used by ISVs to learn about the SCS and its components. The manual can also be used as a basis for creating end user documentation for IT staff.

Setup and Configuration Process

For setup and configuration to proceed, the SCS database and server require preparation, as well as the platform containing the Intel AMT device. Once the preparation is complete, connecting the platform to the network starts the setup and configuration process.

SCS Database Preparation

Before setup and configuration can begin, the SCS server database must be configured with basic information:

- SCS service configuration parameters
- Profiles that define the setup parameters for the Intel AMT-enabled platforms to be configured
- Entries identifying each Intel AMT device to be configured, with a link to a profile
- A list of valid TLS-PSK keys that match what is installed on the Intel AMT devices awaiting configuration.

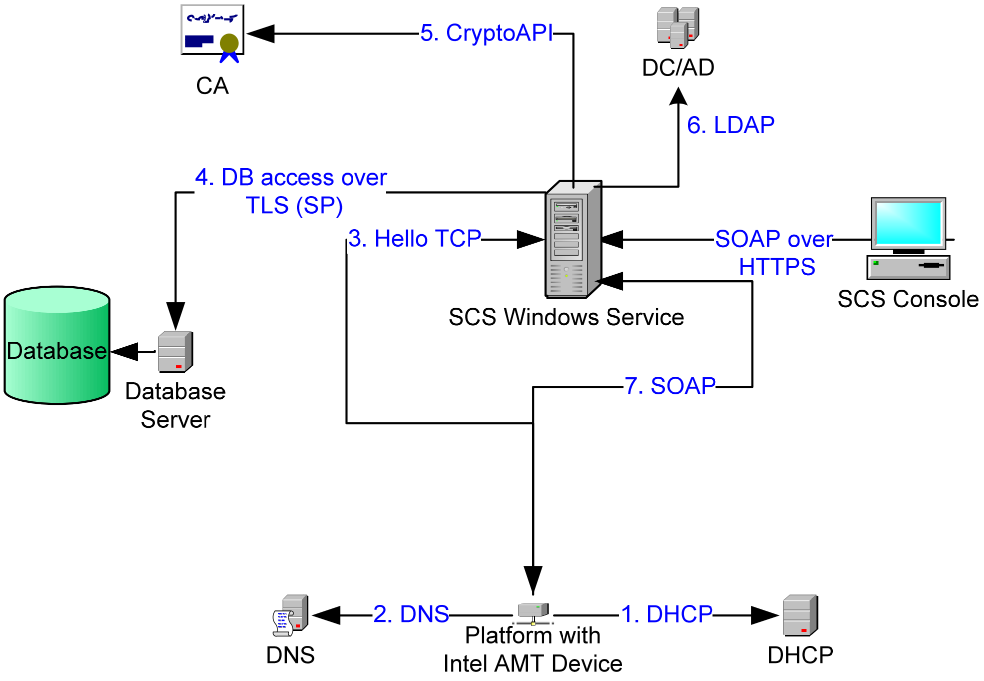
At this point, the SCS service waits for a request from an Intel AMT device.

Preparation of Platform Containing Intel AMT Device

An Intel AMT Release 2.0/2.1 device must have its MEBx password changed from the default password. A TLS-PSK key and identifier must be loaded into the device. The values are entered manually by the IT administrator through the BIOS extension, or the administrator can use a USB key with values exported from the SCS; or the values may have been preloaded by an OEM. This is the minimum requirement, although other parameters may be required. See "Intel AMT Preparation" on page 52 for more information. The platform can now be connected to a network in common with the SCS server.

Setup and Configuration Steps

The following diagram illustrates the major setup and configuration steps. The numbered steps are described below.



1. An Intel AMT device that is ready for setup requests an IP address from a DHCP server.
2. The device performs a DNS lookup with the default SCS service server name.
3. The Intel AMT device sends a TCP/IP "Hello" message.
4. Based on the UUID in the "Hello" message, the SCS service searches the database to locate the Profile and host name to be used to setup and configure the device. If the SCS is configured to do so, it may execute a script to acquire the necessary parameters from sources outside the database, and then store the information in the database.
5. The SCS service requests a certificate for the device from a Certificate Authority server. This step is optional. It is required for installations using Transport Layer Security (TLS) and Mutual TLS.
6. The Intel AMT device is defined as an AMT object in the Active Directory domain controller, when integration with Active Directory is enabled.
7. The SCS service completes setup and configuration using SOAP commands.

All critical parameters are kept in the secure database. The Administrator configures the SCS service, defines profiles, updates individual device parameters, and so on from the Intel SCS Console. The console communicates only with the SOAP API, which queries and updates the database. All instances of the SCS service poll the database periodically or query and update the database as needed as part of the setup and configuration process.

All of the above steps are described in this guide.

Intel AMT SCS Functional Flow

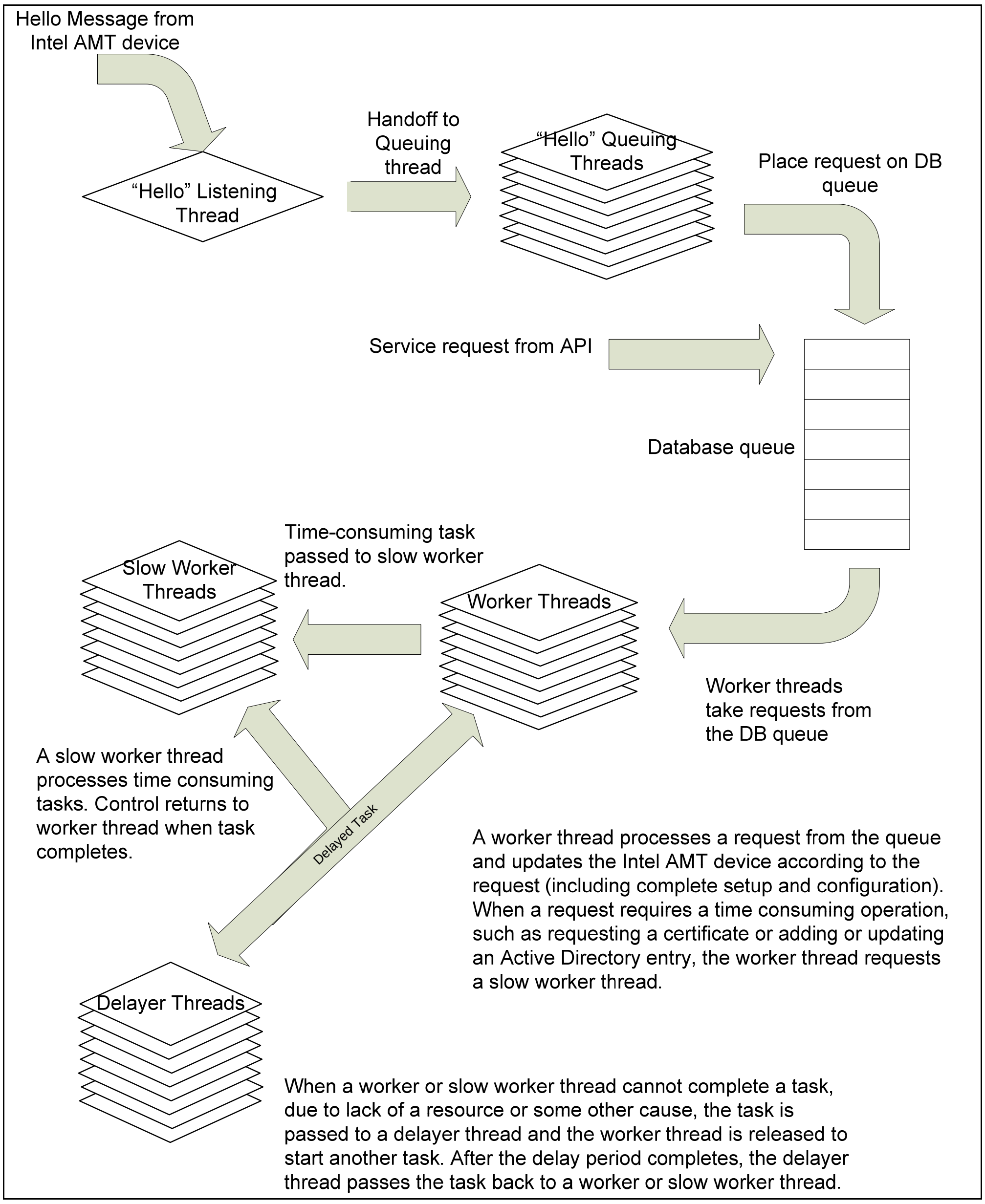
The SCS is designed to perform setup and configuration of multiple Intel AMT devices simultaneously. All requests to the SCS for service are maintained in a queue in the SCS database. A “thread” performs the processing for each portion of a task. A single thread waits for “hello” messages from Intel AMT devices. This thread passes the message to a queuing thread, which then adds this request for setup and configuration to the database queue. Requests via the SOAP API to perform an update to an Intel AMT device are added to the queue directly by the API.

Worker threads in the SCS poll the queue for tasks. A worker thread will perform all steps required for setup and configuration except those that are relatively time consuming, such as a request to a Certificate Authority for a certificate or a request to add an entry to Active Directory. These tasks are handed off to a slow worker thread. If a task cannot be completed due to unavailability of a resource (for example, configuration cannot proceed because there is no profile associated with an Intel AMT device that sent a “hello” message), the task is passed to a delayer thread to wait for a defined period before retrying. As processing for requests completes, threads are freed up to process subsequent requests.

The SCS logs all transactions so that if the service is interrupted, the service can recover partially completed tasks.

IT administration can configure the number of worker and slow worker threads, the queue size, and various times to maximize performance of the SCS. In an enterprise installation that has the potential of many Intel AMT devices requesting setup simultaneously, the number of worker threads can be increased, consistent with the number of processors and the amount of memory installed in the server platform. See “Defining General Parameters” on page 62 for the tuning parameters accessible from the SCS Console.

The figure below presents a simplified flow within the SCS.


Hello Message from Intel AMT device
"Hello" Listening Thread
Handoff to Queuing thread
"Hello" Queuing Threads
Place request on DB queue
Service request from API
Database queue
Time-consuming task passed to slow worker thread.
Slow Worker Threads
Worker Threads
Worker threads take requests from the DB queue
A slow worker thread processes time consuming tasks. Control returns to worker thread when task completes.
Delayed Task
A worker thread processes a request from the queue and updates the Intel AMT device according to the request (including complete setup and configuration). When a request requires a time consuming operation, such as requesting a certificate or adding or updating an Active Directory entry, the worker thread requests a slow worker thread.
Delayer Threads
When a worker or slow worker thread cannot complete a task, due to lack of a resource or some other cause, the task is passed to a delayer thread and the worker thread is released to start another task. After the delay period completes, the delayer thread passes the task back to a worker or slow worker thread.

SCS Operational Flow

Setup and Configuration Operational Overview

The primary purpose of the Intel SCS is to deliver the Intel AMT Setup and Configuration settings to the Intel AMT devices. Intel AMT devices can be located on, for example, a desktop computer, or a workstation.

This process includes pre-setup and configuration; setup and configuration; integration with Active Directory, gathering security information, and maintenance.

Pre-Setup and Configuration

Intel SCS generates data used to configure Intel AMT devices. This data includes:

- PPS, PID and MEBx password generation
- USB key file containing a list of PPS, PID and MEBx password sets

Setup and Configuration

Intel SCS delivers initial values to Intel AMT devices. Before Setup and configuration begins, administrators add these initial values to the database. The administrator enters the values into Profiles, or into descriptions of individual Intel AMT devices, or the information is generated automatically: The information includes:

- Administrator account credentials (Username and password)
- Access control list (ACL) entries for Digest and/or Kerberos user accounts
- Networking settings (Host Name and domain name)
- RSA key pair and X.509 certificate for TLS (TLS Certificate and RSA private key) (automatic)
- Pseudo Random Number Generator (PRNG) value
- Intel AMT Kerberos secret key, SPNs, operational parameters
- Time and date (automatic)
- Trusted root certificates (Mutual TLS)
- Trusted domain name suffixes (Mutual TLS)
- Certificate Revocation Lists (CRLs)
- Power-policy options
- Replacement PID/PPS
- Third-party data storage parameters (not implemented in this release)

The information is used to communicate securely with an Intel AMT device to configure it and to create an Active Directory entry.

Integration with Active Directory

Intel SCS integrates the Intel AMT device with Microsoft Active Directory by creating a directory entry based on the Intel-Management-Engine class. The SCS installation includes scripts used by the administrator to:

- Extend the Active Directory schema to support the Intel-Management-Engine class
- Populate the Intel-Management-Engine attributes

During **setup**, Intel SCS:

- Creates an Active Directory object representing the Intel AMT device
- Creates an attribute for connecting the AD computer object to the AMT object.

Gathering Security Information

Intel SCS collects required operational security parameters.

- As part of setting up the SCS, the administrator defines Active Directory users and permissions for those administrators and operators that will work with Intel SCS. The administrator uses scripts to define the necessary groups and users within Active Directory, and then uses the SCS User commands to define which users have specific permissions to operate the service.
- When TLS is enabled, the SCS interfaces with the Microsoft Certificate Authority to obtain a TLS certificate each time it sets up an Intel AMT device.

Management and Maintenance

Intel SCS also facilitates life cycle management and maintenance operations. These daily tasks can include:

- Entering the properties of new Intel AMT devices, such as the UUID, FQDN, profiles, and AD Organizational Unit (required for adding new Intel AMT-enabled platforms)
- Generating a dataset of PID/PPS/password data for export to a USB key
- Importing TLS-PSK lists from an OEM
- Handling certificate expirations and certificate renewals
- Delivery of Certificate Revocations Lists (CRL)
- Updating local account passwords
- Checking the logs
- Handling exceptions
- Doing ad-hoc configuration operations (Single Intel AMT device / All Intel AMT devices):
  - Performing un-provisioning
  - Performing re-provisioning
  - Updating system clock
- Doing daily database backup

In addition to these tasks, certain maintenance tasks that enhance the security of the Intel AMT devices can be performed automatically. These include:

- Reissuing digital certificates before they expire
- Updating passwords
- Updating random number generator seeds
- Synchronizing the system clock
- Performing re-configuration periodically to ensure that all Intel AMT devices have the latest profile information

Configuring Intel AMT in a Secure Environment

Intel AMT supports Transport Layer Security (TLS) for secure communications between Intel AMT devices and management console applications. Use of TLS is recommended in an Enterprise environment. TLS is a protocol intended to secure and authenticate communications across a public network by using data encryption. It depends on the existence of a public key infrastructure (PKI).

A PKI enables users of an unsecured network to securely and privately exchange information through the use of an asymmetric public and private cryptographic key pair. The key pair is obtained and shared through a trusted authority, known as a Certificate Authority (CA). The CA generates digital certificates that can identify an individual or an organization. The PKI includes directory services that can store and, when necessary, revoke the certificates.

The SCS SOAP API requires a certificate so it can be hosted by the Microsoft Internet Information Server (IIS). This is necessary even in environments when TLS will not be used. If TLS will be used with Intel AMT devices, then there must be access to the Microsoft Certificate Authority as the SCS requires it to enroll for certificates on behalf of each Intel AMT device.

The Microsoft CA can be installed as Stand-alone CA or as an Enterprise CA. An Enterprise CA can be configured only in conjunction with Active Directory. A Stand-alone CA can operate with or without Active Directory, but if Active

Directory is not present, there can be only one SCS instance and the Stand-alone CA must be installed on the same platform as the SCS.

A PKI may have a hierarchy of Certificate Authorities, with subordinate CAs and a root CA. This is beyond the scope of this discussion. IT personnel who manage a facility that depends on PKI need in-depth knowledge of PKI protocols and supporting tools. The installation example later shows how to install a single tier Enterprise or Stand-alone CA.

The SCS Database

A Setup and Configuration Domain has only one SCS database. This supports deployment of a platform containing Intel AMT in any segment of the enterprise, which may be an entire enterprise network or a subset of it. Both the Setup and Configuration Service and the SOAP API access the database directly. Thus all SCS service instances share a common set of service configuration parameters. This localizes the impact of changes in database components.

The database stores configuration data that includes:

- Shared objects that are generated, stored, and organized as Profiles before they are requested. Profiles contain values such as:
    - An Access Control List, that is, a list of authorized Intel AMT device users and their privileges in accessing device capabilities
    - Trusted root certificates
    - Kerberos options
    - TLS and mutual authentication settings
    - Power-saving options
- Per-Intel AMT device data objects defined before configuration can start. The data in these objects includes:
    - Administrator password
    - Host name, TLS settings, UUID
    - A link to one of the Profiles
- Logs of all transactions performed by the SCS, including transactions in progress and any detected errors.
- A queue containing operations used to configure Intel AMT devices.

The Intel AMT database requires Microsoft* SQL Server 2000, Microsoft SQL Server 2005, or Microsoft SQL Server 2005 Express Edition (SQL Server Express).

Considerations

For optimal performance, the Intel SCS must have adequate access to the database. These issues must be taken into consideration:

- If the database is accessed via a WAN, ensure that the areas of the database used by the Intel SCS are accessible from all installations of the SCS.
- Ensure that there is adequate bandwidth to access the database.
- The location of the database can affect performance. Attempt to locate the database at a central site.
- The database must be reliably available, so techniques such as replication, clustering, and backup and restore should be used.

Database Security

Because the data in the database is sensitive, it is recommended that the connection to the database be secure. See “Enable SQL Server and Windows Authentication Mode” step 8 on page 24 for the steps required to configure a secure database connection.

Database stored procedures may be executed only by the users that have appropriate permissions to use them. There are two types of database users, Windows Service users and API users. The console application defines SCS users and user permissions that are saved in the database.

Schema

For information about the SCS database schema, refer to the Intel document named *SCS_DB_Schema_1.0.vsd*.

The database schema is provided for information only. User applications should interact with the SCS database only by using the SOAP API. Intel reserves the right to change the schema in the future.

Backup & Restore

We recommend that an Administrator perform a daily backup of the Intel SCS database. The default name of the Intel SCS database is “IntelAMT.”

SCS and Active Directory Tasks and Permissions

Interaction between Management Console applications and the Intel AMT API is optionally authenticated with the Integrated Windows Authentication mode via the API authentication mechanisms.

The Active Directory (AD) service is used optionally to authenticate between ISV management console applications and Intel AMT devices. To enable use of AD, the following tasks have to be completed:

- Create instances of Intel-Management-Engine, which is the special class added to the AD schema each time the SCS completes setup and configuration of an Intel AMT device. These instances are called "AMT objects."
- Periodically change the password of these objects automatically.
- Delete an AMT object when it is no longer needed.

To enable Intel AMT use of AD, the following permissions have to be granted to user accounts associated with the SCS (This is the user account entered when the SCS service is started, as defined during installation on page 37):

- "Create/Delete Intel-Management-Engine objects" permission in the relevant Organization Unit (OU) where objects are created.
- Full Control over Intel-Management-Engine objects

One way to do this is by using the "Delegate Control Wizard of the Active Directory Users and Computers" MMC.

Active Directory Schema

The Intel SCS installation contains an .LDF AD schema extension definition and a script that is used to extend the Active Directory schema for Intel AMT.

For more information, see "Active Directory (AD) and Changes to the AD Schema" on page 35.

Security Groups

The Intel SCS installation contains script that are used to create security groups for the SCS user context (per Active Directory forest – a forest is a hierarchical collection of domains, and a large enterprise may have more than one forest). This task includes:

- creating an Intel SCServers local security group in each domain in the forest
- creating an Intel SCServers global security group domain in the root domain of the forest

The installation also provides scripts to define users within the groups and to give them privileges such that when they activate the SCS Windows service, the privileges required to manage the service has the proper access.

AMT Object

The Intel SCS Active Directory BuildSchema script, when executed by the administrator, creates the new object class **Intel-Management-Engine**. Objects created with this class, called **AMT objects**, are used to represent the Intel AMT device itself.

For more information, see "Active Directory (AD) and Changes to the AD Schema" on page 35.

Computer Object

Deploying a platform containing Intel AMT creates a new object in the AD which identifies the host on the Intel AMT enabled platform. This occurs independently of the Intel AMT setup process, and happens when the host joins the local domain.

For more information, see “Active Directory (AD) and Changes to the AD Schema” on page 35.

Chapter 2

ENVIRONMENT PREREQUISITES AND INSTALLATION

This section contains:

- “System Requirements” on page 15
- “Environment Overview” on page 17
- “Environment Prerequisites” on page 19
    - “.NET Framework 2.0” on page 19
    - “Microsoft SQL Server Express” on page 20
    - “Internet Information Services (IIS) 6.0” on page 24
    - “Microsoft Certificate Authority” on page 26
- “Active Directory (AD) and Changes to the AD Schema” on page 35
- “Installation of the SCS Server Components” on page 36
- “Installation of the Intel AMT Management Console” on page 45
- “Post Installation Operations” on page 46

System Requirements

In a typical installation, components of the Intel AMT Setup and Configuration Service (SCS) can be installed on more than one computer or on the same computer, depending on the enterprise requirements. This section lists the system requirements for the computers supporting various components of the SCS.

If Active Directory is not used, the Certificate Authority must be installed on the same platform as the SCS. The database must be accessible and the database credentials known to the person installing the Intel SCS.

Table 1: Requirements for Computer Running the SCS Windows Service, the SOAP API, and the IIS

PC Processor	Intel® Pentium® 4 processor - 1.5 GHz minimum 2.4 GHz or faster is recommended
Memory	512 MB minimum 1 GB or more is recommended
Operating System	Windows Server 2003 with Service Pack 1
Hard Disk	525 MB
Platform	.NET Framework 2.0 Internet Information Services (IIS) 6.0
Networking	Minimum Ethernet 10BASE-T

Table 2: Requirements for Computer Running SQL Server

PC Processor	Intel® Pentium® III processor - 600 MHz minimum 1 GHz or faster is recommended
Memory	192 MB minimum 512 MB or more is recommended
Operating System	Windows Server 2003 with Service Pack 1
Hard Disk	525 MB
Platform	.NET Framework 2.0
Networking	Minimum Ethernet 10BASE-T

Table 3: Requirements for Computer Running the Console

PC Processor	Intel Pentium 4 processor or higher (or compatible)
Memory	256 MB minimum
Operating System	Windows 2000, XP, or 2003
Hard Disk	80 MB
Platform	.NET Framework 2.0
Networking	Minimum Ethernet 10BASE-T
USB ports	For export of security keys
Internet Browser	Microsoft IE 5.5 or 6

Environment Overview

The Intel SCS includes several components. They can be installed on a single computer or on separate computers.

In addition, the environment must include several pre-installed and configured Microsoft components.

Description of Intel SCS Components

The following are components of the Intel SCS.

Main Service

This is the software component that processes Setup and Configuration Service requests from Intel AMT devices and is implemented as a Windows Service. For complete details, see “Setup and Configuration Operational Overview” on page 6.

SOAP API

This is the Application Programming Interface (API) that Independent Software Vendors (ISVs) use to create and productize a User Interface. It is used by the SCS Console to interact with the Main Service indirectly via the database server.

Database Server

This is the repository that stores the Setup and Configuration data, organized according to the SCS database schema, and installed as a database instance in Microsoft SQL Server.

Client Samples

This component includes miscellaneous reference files that demonstrate use of the SCS SOAP API functions. For complete details, see “Client Samples” on page 93.

Tools

The tools include an Add User tool and other miscellaneous tools. For complete details, see “Command Line Tools” on page 98.

Administrative Tools

Active Directory Schema

These are scripts that extend the Active Directory schema for Intel AMT. See “Active Directory (AD) and Changes to the AD Schema” on page 35 and the script description on page 98.

Active Directory User and Groups

These are scripts that enable the definition of Users and Groups. See page 99.

Active Directory ACL

These scripts allow the Administrator to create permissions for users to access resources. See page 101.

Intel SCS Console

The Intel SCS Console is an application that is installed separately from the SCS. It is an open application that uses the SCS SOAP API to manage the SCS and the SCS database. The source is distributed with the SCS. An ISV can take the source, add value to it and integrate it into a Management Console product.

List of Required Microsoft Components

The following Microsoft components must be installed and configured for the Intel SCS to function.

- .NET Framework 2.0 is a prerequisite for the installation of SQL Server or SQL Server Express, the Intel SCS Main Service, and the SCS console.

- Either Microsoft SQL Server 2005 or Microsoft SQL Server 2005 Express Edition (SQL Server Express) is required. This manual describes installation of the Express edition, but if the full edition is exists, it may be used. The Express Edition is a data management product for embedded application clients, light Web applications, and local data stores.
- Intel SCS requires that Microsoft's Internet Information Services 6.0 (IIS 6.0) be installed and configured. IIS is Microsoft's HTTP server. IIS adds full HTTP capability to the Windows operating system. IIS should be installed before the Certificate Authority is installed.
- If TCPIP Layer Security (TLS) is required in an installation, then Intel SCS requires that Microsoft's Certificate Authority (CA) be installed.

Microsoft's Active Directory (AD) is a directory service that is integrated with Windows 2003 Server. AD is an optional environment pre-requisite. Intel SCS uses AD for:

- Kerberos authentication using AMT objects
- User lists

The Intel AMT installation adds a script that extends the AD schema for Intel AMT and that creates several new attributes.

Environment Prerequisites

This section details the environment required by the various Intel AMT Setup and Configuration Service components. The section “System Requirements” on page 15 specifies which components require which environment elements.

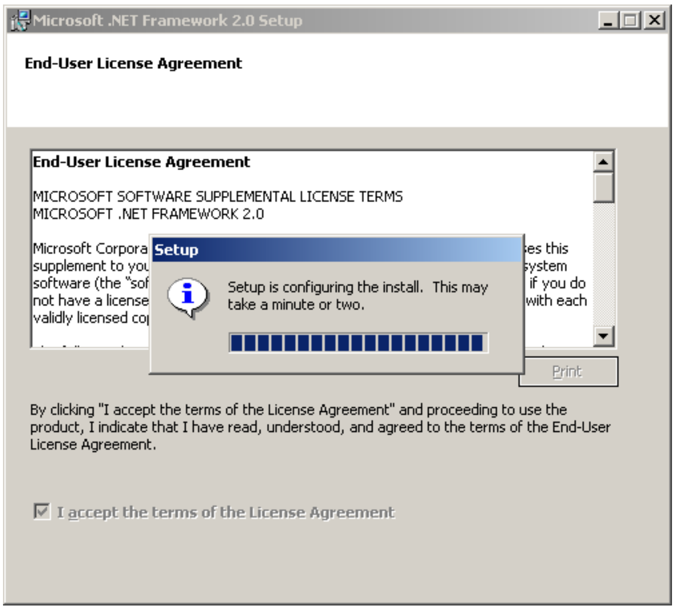
.NET Framework 2.0

.NET Framework 2.0 is a prerequisite for the installation of both SQL Server Express and the Intel SCS Windows Service. For summary information about .NET Framework and a download link, see:

http://www.microsoft.com/downloads/details.aspx?familyid=0856eacb-4362-4b0d-8edd-aab15c5e04f5&displaylang=en

To install .NET Framework 2.0:

1. Ensure that all instances of Microsoft Internet Explorer are closed.
2. Double-click the installation file named `dotnetfx.exe`. The installation files are extracted and the Welcome to Setup screen is displayed.
3. Click **Next**. The End-User License Agreement is displayed.
4. Select the **I accept the terms** checkbox and click **Install**. A message is displayed indicating that “Setup is configuring the install.”


Microsoft .NET Framework 2.0 Setup
End-User License Agreement
Setup
Print

End-User License Agreement

MICROSOFT SOFTWARE SUPPLEMENTAL LICENSE TERMS
MICROSOFT .NET FRAMEWORK 2.0

Microsoft Corpora ... es this supplement to you ... ystem software (the "sof ... if you do not have a license ... with each validly licensed co

Setup is configuring the install. This may take a minute or two.

By clicking "I accept the terms of the License Agreement" and proceeding to use the product, I indicate that I have read, understood, and agreed to the terms of the End-User License Agreement.

☑ I accept the terms of the License Agreement

Setup then installs the components. An installation progress bar is displayed. Installation may take a few minutes. Upon completion, the Setup Complete screen is displayed.

5. Click **Finish**.

Microsoft SQL Server Express

Microsoft SQL Server 2005 Express Edition (SQL Server Express) is a data management product for embedded application clients, light Web applications, and local data stores. Designed for easy deployment and rapid prototyping, SQL Server Express is available at no cost.

There are various editions of Microsoft SQL Server. For an overview, see: *http://www.microsoft.com/sql/prodinfo/features/compare-features.mspx*
This manual only describes installation of the Express edition. An Enterprise solution will require the full SQL Server 2005 or SQL Server 2000 application.

For detailed information about SQL Server Express and a download link, see:

http://www.microsoft.com/downloads/details.aspx?familyid=220549b5-0b07-4448-8848-dcc397514b41&displaylang=en

For summary information about SQL Server Express and a download link, see: http://msdn.microsoft.com/vstudio/express/sql/download/

To install the SQL Server 2005 Express Edition:

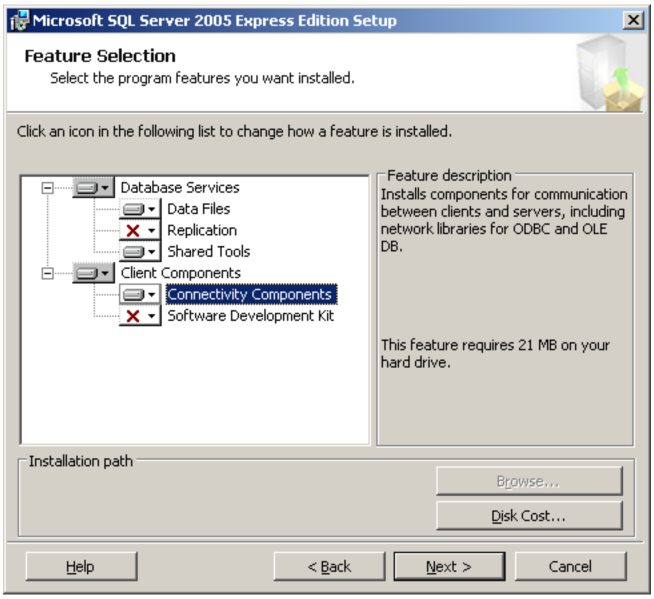
1. Ensure that .NET Framework is installed.
2. Ensure that the server meets the system requirements listed in Table 2, “Requirements for Computer Running SQL Server” on page 15.
3. Double-click the installation file named `sqlexpr.exe`. The installation files are extracted and the Installation Options screen is displayed.
4. Select **Install SQL Server 2005 Express Edition** and click **Next**. The End-User License Agreement is displayed.
5. Select the **I accept the licensing terms** checkbox and click **Next**. A message is displayed indicating that “Setup is configuring the install.” The Installing Prerequisites screen is displayed.
6. Click **Install**. Setup installs the necessary components. A message is displayed indicating that “The required components were installed successfully.”
7. Click **Next**. The Welcome to the Microsoft SQL Server Installation Wizard screen is displayed.
8. Click **Next**. The System Configuration Check screen is displayed and the Wizard inspects the system.

If the Wizard detects problems, it will display the status of the problem and, possibly, a message. The status “Warning” will usually allow the installation to continue. However, the status Error indicates that the installation cannot continue. View the accompanying message and click Exit. Then, correct the error and try again.

9. If all checks are successful, click **Next**. The Registration Information screen is displayed.
10. Enter your name and the company name.
11. Select or clear the **Hide advanced configuration options** checkbox. When the checkbox is cleared, the Instance Name, Service Account, User Instances, and Collation can also be configured.

Select the “Hide advanced configuration options” checkbox and accept the default settings. This manual does not document the advanced configuration options.

12. Click **Next**. The Feature Selection screen is displayed.



Microsoft SQL Server 2005 Express Edition Setup

Feature Selection

Select the program features you want installed.

Click an icon in the following list to change how a feature is installed.

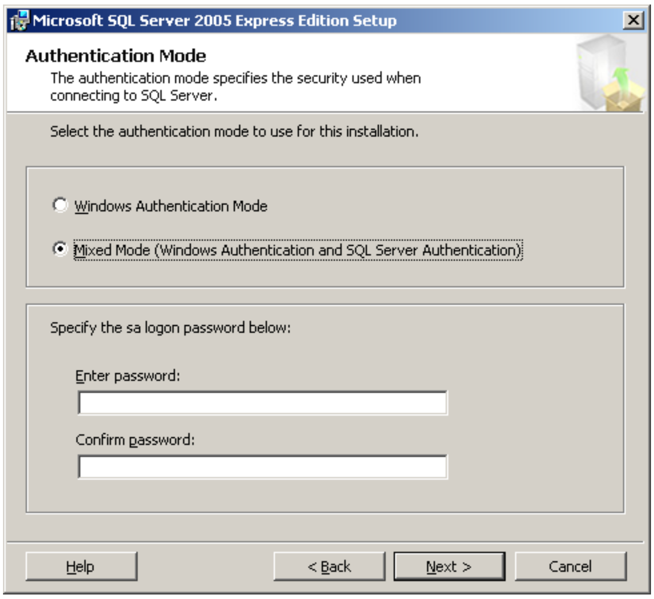
- Database Services
  - Data Files
  - ☒ Replication
  - Shared Tools
- Client Components
  - Connectivity Components
  - ☒ Software Development Kit

Feature description

Installs components for communication between clients and servers, including network libraries for ODBC and OLE DB.

This feature requires 21 MB on your hard drive.

13. As pictured above, select the following features:
    - Data Files
    - Shared Tools
    - Connectivity Components
14. Click **Next**. The Authentication Mode screen is displayed.



Microsoft SQL Server 2005 Express Edition Setup

Authentication Mode

The authentication mode specifies the security used when connecting to SQL Server.

Select the authentication mode to use for this installation.

○ Windows Authentication Mode

● Mixed Mode (Windows Authentication and SQL Server Authentication)

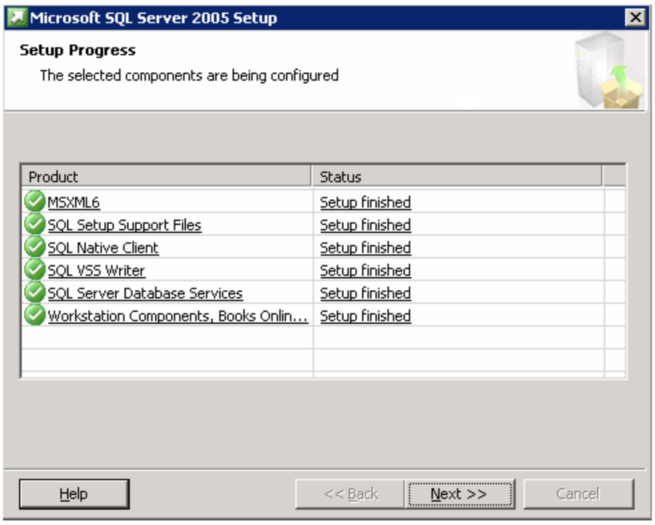
Specify the sa logon password below:

Enter password:

Confirm password:

Authentication is the process of verifying the identity of the person logging on to a network.

15. Select **Mixed Mode**.
16. Enter the **sa logon password**, confirm the entry, and click **Next**. The Error and Usage Report screen is displayed.
17. Select or clear the error handling options and click **Next**. The Ready to Install screen is displayed.
18. Click **Install**. The Setup Progress screen is displayed.



Microsoft SQL Server 2005 Setup

Setup Progress

The selected components are being configured

Product	Status
✓ MSXML6	Setup finished
✓ SQL Setup Support Files	Setup finished
✓ SQL Native Client	Setup finished
✓ SQL VSS Writer	Setup finished
✓ SQL Server Database Services	Setup finished
✓ Workstation Components, Books Onlin...	Setup finished

19. Click **Next** when the setup is finished.
20. Click **Finish**.

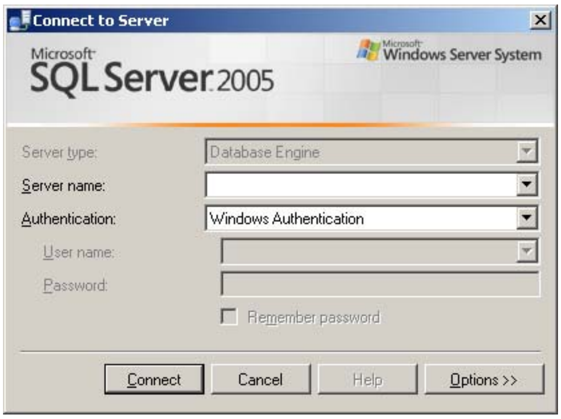
We recommend that the **SQL Server Management Studio Express** tool be installed now, as it is needed for initial setup of the database server. It is a free, easy-to-use graphical management tool for managing SQL Server 2005 Express Edition. Download of this program and installation instructions can be found at:

http://www.microsoft.com/downloads/details.aspx?familyid=C243A5AE-4BD1-4E3D-94B8-5A0F62BF7796&displaylang=en

Enable SQL Server and Windows Authentication Mode

Following installation, enable the SQL Server:

1. Click the Windows **Start** button and click **All Programs**.
2. From the **Microsoft SQL Server 2005** program group, select **SQL Server Management Studio Express**. The Connect to Server window is displayed.



Server type: Database Engine

Server name:

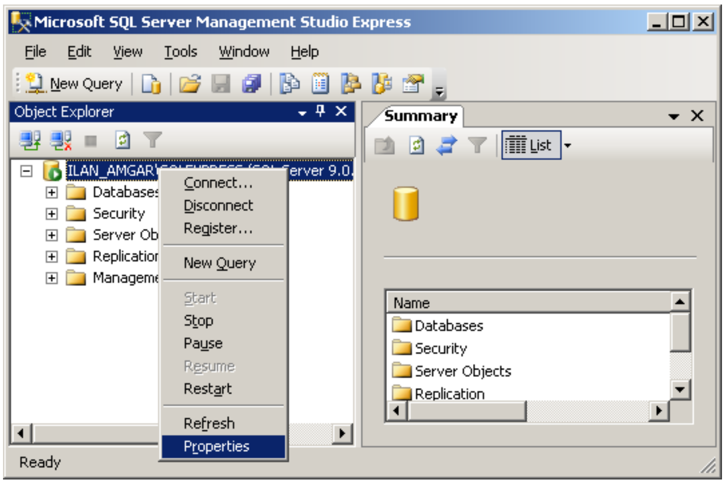
Authentication: Windows Authentication

User name:

Password:

□ Remember password

3. Enter the Server name, select Windows Authentication, and click **Connect**.
4. Right-click on the root node. A popup menu is displayed.



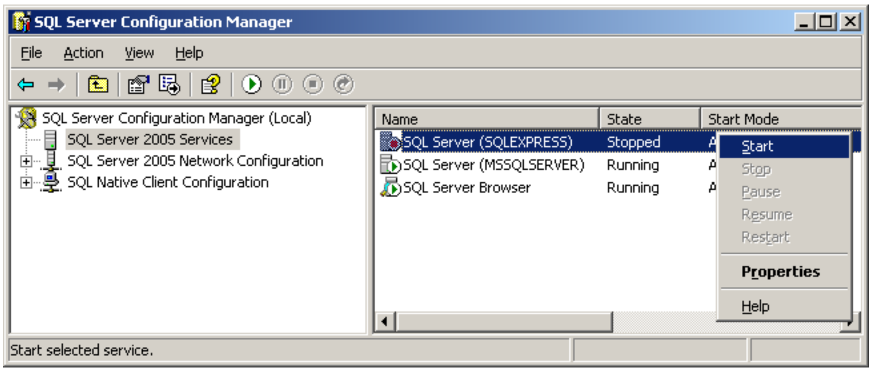
5. Select **Properties**. The Server Properties Window is displayed.
6. Select the **Security** page.
7. In the Server authentication section, select **SQL Server and Windows Authentication mode**.
8. Click **OK**.

SQL Server Verification

To verify that the SQL server is running:

1. On the computer where the SQL Server is installed, click the Windows **Start** button and click **All Programs**.
2. From the **Microsoft SQL Server 2005** program group, select **Configuration Tools > SQL Server Configuration Manager**. The SQL Server Configuration Manager opens.
3. From the left pane, select **SQL Server 2005 Services**.
4. In the right pane, check the State column and ensure that SQL Server and SQL Server Browser are both running.

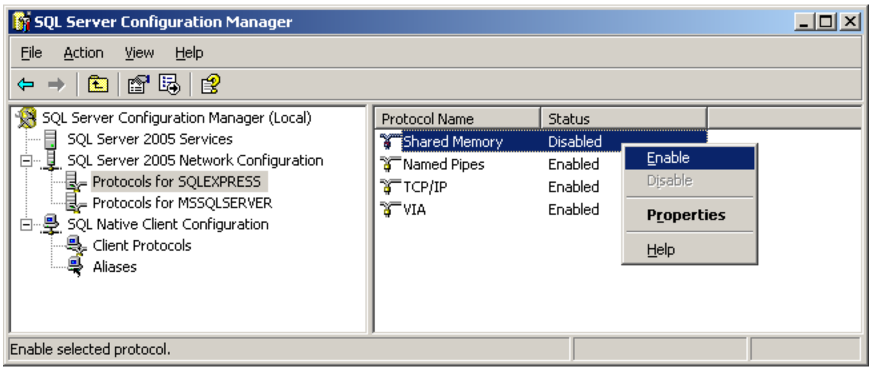
   If they are not, select each, right-click, and from the popup menu, select **Start**. It may be necessary the first time after installation to right-click on the server or server browser entry, select **Properties**, select the **Service** tab and change the **Start Mode** to **Automatic** or **Manual**, and then start the server and/or the browser.


SQL Server Configuration Manager
File
Action
View
Help
SQL Server Configuration Manager (Local)
SQL Server 2005 Services
SQL Server 2005 Network Configuration
SQL Native Client Configuration
Start
Stop
Pause
Resume
Restart
Properties
Help
Start selected service.

Name	State	Start Mode
SQL Server (SQLEXPRESS)	Stopped	A
SQL Server (MSSQLSERVER)	Running	A
SQL Server Browser	Running	A

5. Expand the **SQL Server 2005 Network Configuration** branch.
6. Select the **Protocols for SQLEXPRESS** branch.
7. Ensure that **Shared Memory**, **Named Pipes**, and **TCP/IP** are enabled.

   If they are not, select each, right-click, and from the popup menu, select **Enable**.


SQL Server Configuration Manager
File
Action
View
Help
SQL Server Configuration Manager (Local)
SQL Server 2005 Services
SQL Server 2005 Network Configuration
Protocols for SQLEXPRESS
Protocols for MSSQLSERVER
SQL Native Client Configuration
Client Protocols
Aliases
Enable
Disable
Properties
Help
Enable selected protocol.

Protocol Name	Status
Shared Memory	Disabled
Named Pipes	Enabled
TCP/IP	Enabled
VIA	Enabled

8. To enable secured database communication using the internal SQL Server encryption option, right click on **Protocols for SQLEXPRESS** and select **Properties**. Set **ForceEncryption** to **Yes**.
9. Expand the SQL Native Client Configuration branch.
10. Select the Client Protocols branch.
11. Ensure that Shared Memory, Named Pipes, and TCP/IP are enabled.

    If they are not, select each, right-click, and from the popup menu, select **Enable**.

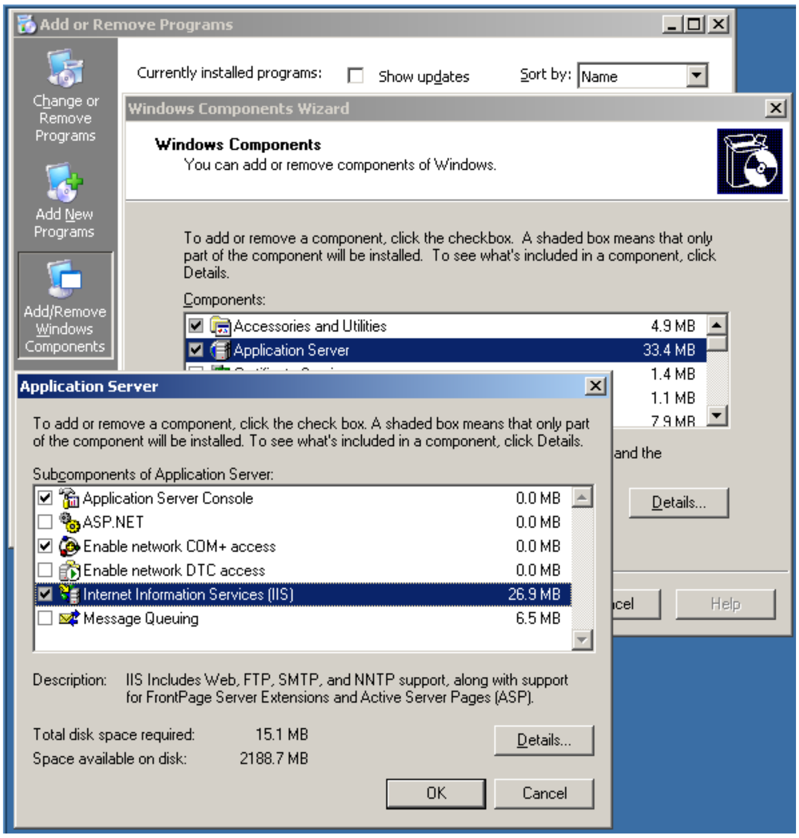
Internet Information Services (IIS) 6.0

Internet Information Services is Microsoft's HTTP server. IIS adds full HTTP capability to the Windows operating system.

Install IIS before installing the Microsoft Certificate Authority on the same server so that Certificate Authority web enrollment can be supported.

To enable IIS:

1. Click the Windows Start button and select **Control Panel**.
2. Double-click **Add or Remove Programs**.
3. From the left panel, click **Add/Remove Windows Components**.


Add or Remove Programs
Change or Remove Programs
Add New Programs
Add/Remove Windows Components
Windows Components Wizard
Windows Components
Application Server
Subcomponents of Application Server:
Details...
OK
Cancel
Help

Currently installed programs: □ Show updates Sort by: Name

You can add or remove components of Windows.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

☑	Accessories and Utilities	4.9 MB
☑	Application Server	33.4 MB

To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Subcomponents of Application Server:

☑	Application Server Console	0.0 MB
□	ASP.NET	0.0 MB
☑	Enable network COM+ access	0.0 MB
□	Enable network DTC access	0.0 MB
☑	Internet Information Services (IIS)	26.9 MB
□	Message Queuing	6.5 MB

Description: IIS Includes Web, FTP, SMTP, and NNTP support, along with support for FrontPage Server Extensions and Active Server Pages (ASP).

Total disk space required: 15.1 MB

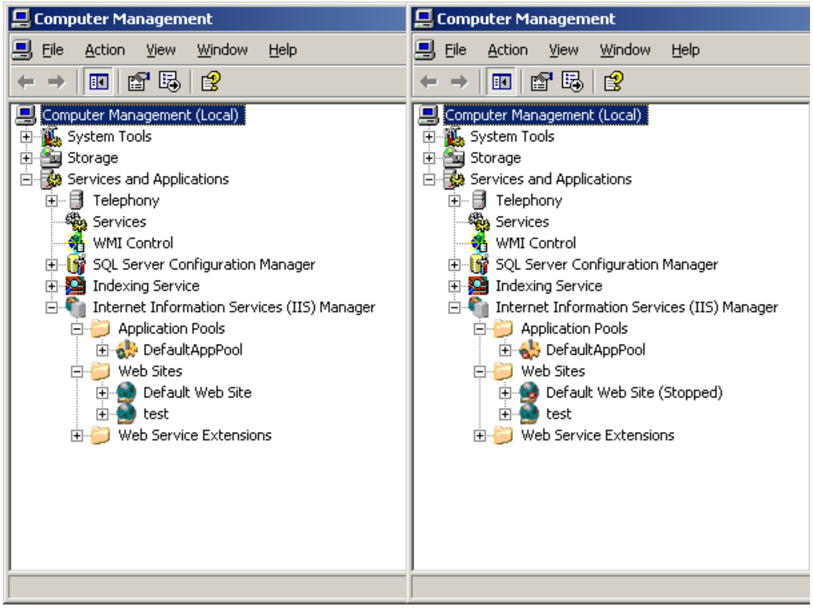
Space available on disk: 2188.7 MB

4. Select the **Application Server** checkbox.
5. Click **Details**.
6. Select the **Internet Information Services** checkbox.
7. Click **OK**. IIS installation process begins.
8. Follow the installation wizard instructions and choose the default options.

IIS Verification

To verify that IIS is running:

1. From the Windows desktop, right-click **My Computer**. A popup menu is displayed.
2. Click **Manage**. The Computer Management Window is displayed.
3. From the right pane, expand the **Services and Applications** branch.
4. Expand the **Internet Information Services** branch.
5. Expand the **Application Pools** branch and ensure that **DefaultAppPool** is in run mode.


Computer Management
File Action View Window Help
Computer Management (Local)
System Tools
Storage
Services and Applications
Telephony
Services
WMI Control
SQL Server Configuration Manager
Indexing Service
Internet Information Services (IIS) Manager
Application Pools
DefaultAppPool
Web Sites
Default Web Site
test
Web Service Extensions
Computer Management
File Action View Window Help
Computer Management (Local)
System Tools
Storage
Services and Applications
Telephony
Services
WMI Control
SQL Server Configuration Manager
Indexing Service
Internet Information Services (IIS) Manager
Application Pools
DefaultAppPool
Web Sites
Default Web Site (Stopped)
test
Web Service Extensions

If it is stopped, right-click **DefaultAppPool** and, from the popup menu, select Start.

6. Expand the **Web Sites** branch. If **Default Web Site** will be used as the SCS Website, then ensure that **Default Web Site** is in run mode.

   If it is stopped, right-click **Default Web Site** and, from the popup menu, select Start.

7. If a website other than Default Web Site will be used, create (right-click on Web Sites) and start that site. If the newly created web site is to use the default port 80, **Default Web Site** must not be started. If the new web site has a dedicated port other than port 80, include the port number with the FQDN when connecting to the web site.

Microsoft Certificate Authority

Intel SCS requires that Microsoft's Certificate Authority (CA) be installed and configured when TLS will be used in communications with Intel AMT devices. The CA can be either a Stand-alone CA or an Enterprise CA.

The CA should be configured to generate certificates automatically so that the SCS can request a certificate each time it performs a setup of an Intel AMT device. Otherwise, an Administrator will have to intervene each time a device is set up.

Microsoft's Enterprise CA requires Microsoft Windows 2003 Enterprise Edition with Service Pack 1.

*To enable web enrollment for certificates, install IIS **before** installing the CA.*

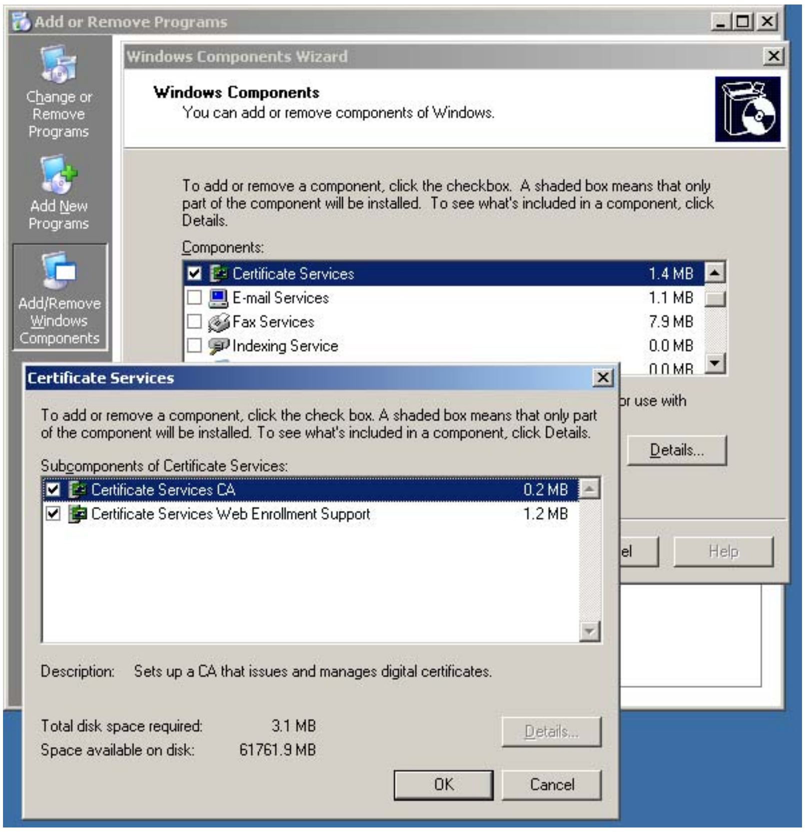
The following prerequisites must be met to install an Enterprise CA:

- The host must be a member of an Active Directory domain. It can be the same host as the domain controller.
- The user performing the installation must be a member of the domain and have sufficient administration privileges (e.g., is a member of the "Domain Admins" group).

Installing the Microsoft CA

To install the Microsoft Certificate Authority as a stand-alone or Enterprise root CA:

1. Click the Windows Start button and select **Control Panel**.
2. Double-click Add or Remove Programs.
3. From the left panel, click Add/Remove Windows Components.



Add or Remove Programs
Change or Remove Programs
Add New Programs
Add/Remove Windows Components
Windows Components Wizard
or use with
Details...
el
Help

Windows Components
You can add or remove components of Windows.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

☑ Certificate Services 1.4 MB
□ E-mail Services 1.1 MB
□ Fax Services 7.9 MB
□ Indexing Service 0.0 MB

Certificate Services

To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

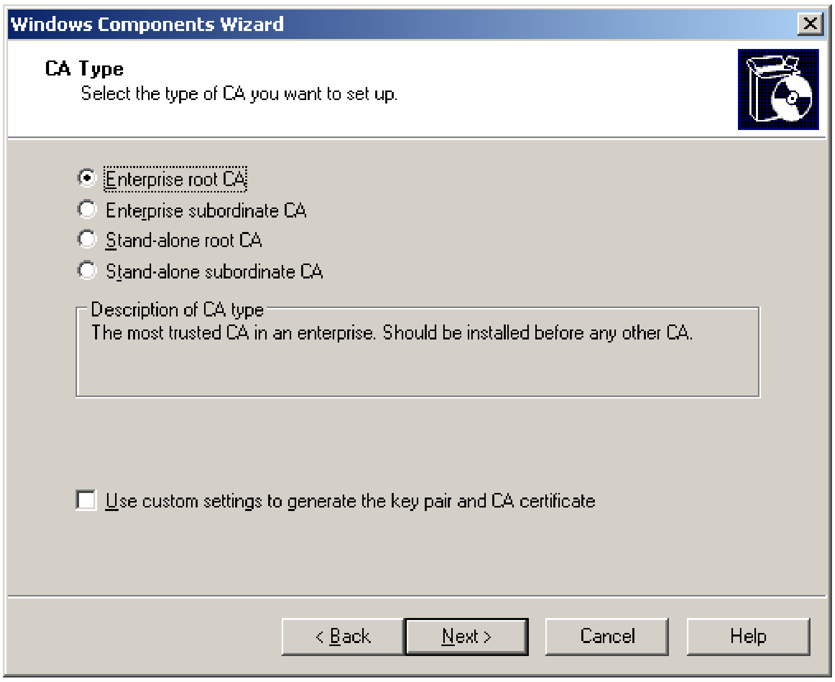
Subcomponents of Certificate Services:

☑ Certificate Services CA 0.2 MB
☑ Certificate Services Web Enrollment Support 1.2 MB

Description: Sets up a CA that issues and manages digital certificates.

Total disk space required: 3.1 MB
Space available on disk: 61761.9 MB

4. Select the **Certificate Services** checkbox. A warning is displayed indicating that the machine name or the domain membership of the machine cannot be changed while it acts as a certificate server. Click **Yes**.
5. Click Details.
6. Select both the Certificate Services CA checkbox and the Certificate Services Web Enrollment Support checkbox and click OK.
7. Click Next. The CA Type screen is displayed.



CA Type

Select the type of CA you want to set up.

● Enterprise root CA

○ Enterprise subordinate CA

○ Stand-alone root CA

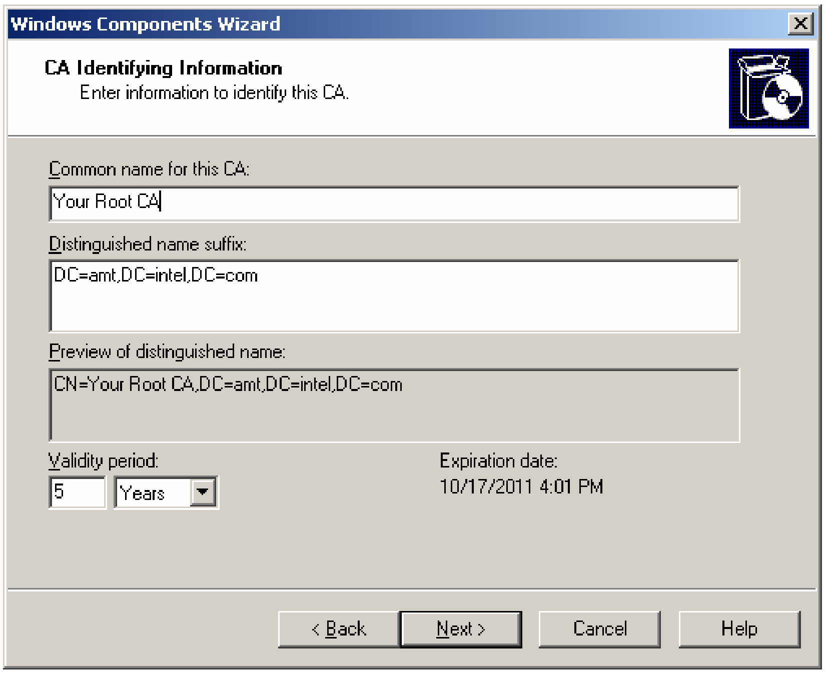
○ Stand-alone subordinate CA

Description of CA type

The most trusted CA in an enterprise. Should be installed before any other CA.

□ Use custom settings to generate the key pair and CA certificate

8. Select either Enterprise root CA or Stand-alone root CA and click Next. The CA Identifying Information screen is displayed.
9. Enter the CA Identifying Information.



CA Identifying Information

Enter information to identify this CA.

Common name for this CA: Your Root CA

Distinguished name suffix: DC=amt,DC=intel,DC=com

Preview of distinguished name: CN=Your Root CA,DC=amt,DC=intel,DC=com

Validity period: 5 Years

Expiration date: 10/17/2011 4:01 PM

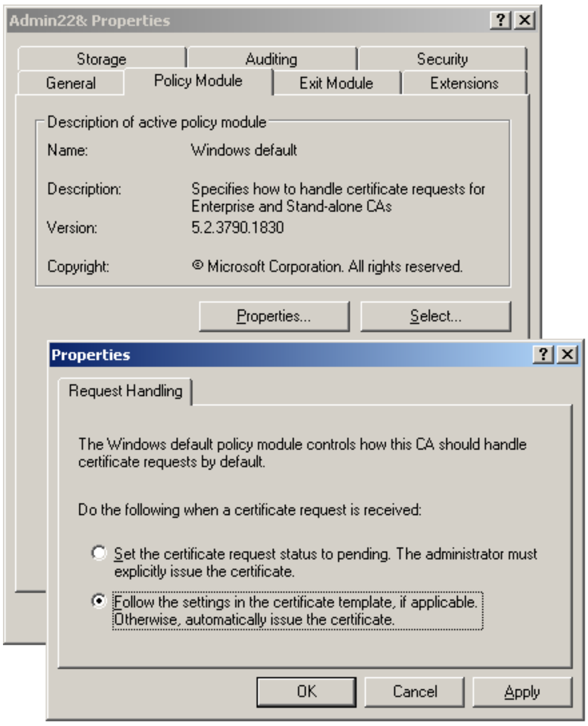
   a. Enter the Common Name: The name by which the CA will be known.
   b. Enter the distinguished name suffix: This is the domain suffix of the host. It will be generated automatically in an AD environment. Click **Next**.

10. Choose the default location for the Certificate Database Settings and click **Next**. There may be a message requesting to stop IIS. Click **Yes**. The installation will run to completion.
11. Configure the CA to automatically issue certificates. This option is recommended as it allows the SCS to process Intel AMT device setups automatically without operator intervention.

a. Click the Windows **Start** button > **Administrative Tools** > **Certificate Authority**. The Certificate Authority Management Console opens.

b. Right-click on the first sub-branch. A popup menu is displayed.

c. Click **Properties** and click the **Policy Module** tab.



Description of active policy module

Name: Windows default

Description: Specifies how to handle certificate requests for Enterprise and Stand-alone CAs

Version: 5.2.3790.1830

Copyright: © Microsoft Corporation. All rights reserved.

The Windows default policy module controls how this CA should handle certificate requests by default.

Do the following when a certificate request is received:

○ Set the certificate request status to pending. The administrator must explicitly issue the certificate.

● Follow the settings in the certificate template, if applicable. Otherwise, automatically issue the certificate.

d. Click **Properties** and select **Follow the settings in the certificate template, if applicable. Otherwise, automatically issue the certificate.**

e. Click **OK**, respond to the message, and click **OK**. The Certificate Authority Management Console returns to focus.

f. Right-click on the root branch and, from the popup menu, select **Start Service**.

Exporting and Installing the CA Certificate

The CA certificate should be stored locally on any platform that authenticates certificates from this CA. This includes:

- Clients of IIS (if IIS used this CA for its certificate), for example, the SCS Console
- Platforms running Management Console applications that authenticate Intel AMT devices that have TLS enabled in their profile, especially the SCS, when it interacts with Intel AMT devices after setup.
- Intel AMT devices need this certificate for authenticating clients when TLS mutual authentication is used, if this CA was used to issue client certificates. The certificate must be included in the Profile for devices supporting mutual authentication. See “Installing an Intel AMT Client Certificate for TLS Mutual Authentication” on page 34.

First save the certificate as a file, and then install it as a trusted root certificate.

1. Export the CA certificate. There are multiple ways to do this. This procedure describes one of them.

a. Click the Windows **Start** button > **Administrative Tools** > **Certificate Authority**.

b. Right-click on the first sub-branch. A popup menu is displayed.

c. Click **Properties** and click the **General** tab.

d. Select the certificate and click **View Certificate**.

e. Click the **Details** tab and click **Copy to file**.

f. Complete the Wizard. A message indicates that the export was successful. Click **OK**. The Details tab returns to focus.

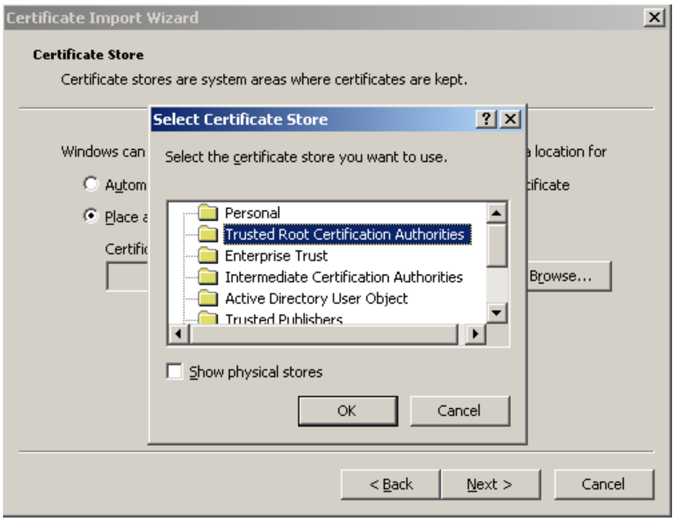
g. Click **OK** > **OK**. The Certificate Authority Management Console returns to focus.

2. Install the CA certificate in the certificate store as a trusted root certificate.

a. Find the certificate. If it was exported directly to another computer, find it on the other computer. If it was exported to a USB key, move it from the USB key to the computer.

b. Right-click on the certificate and, from the popup menu, select **Install Certificate**. The welcome screen of the Certificate Import Wizard is displayed. Click **Next**.

c. Select **Place all certificates in the following store** and click **Browse**. The Select Certificate Store window opens.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Select Certificate Store

Select the certificate store you want to use.

- Personal
- Trusted Root Certification Authorities
- Enterprise Trust
- Intermediate Certification Authorities
- Active Directory User Object
- Trusted Publishers

□ Show physical stores

d. Select **Trusted Root Certification Authorities** and click **OK**.

e. Click **Next** > **Finish**. A message indicates that the import was successful. Click **OK**.

Secure the Connection to IIS Using SSL

Connection to IIS requires a digital certificate. A certificate can be purchased from an outside vendor such as Verisign. If the Microsoft CA was installed because TLS will be used for Intel AMT communications in the enterprise, use that CA as a source for a certificate.

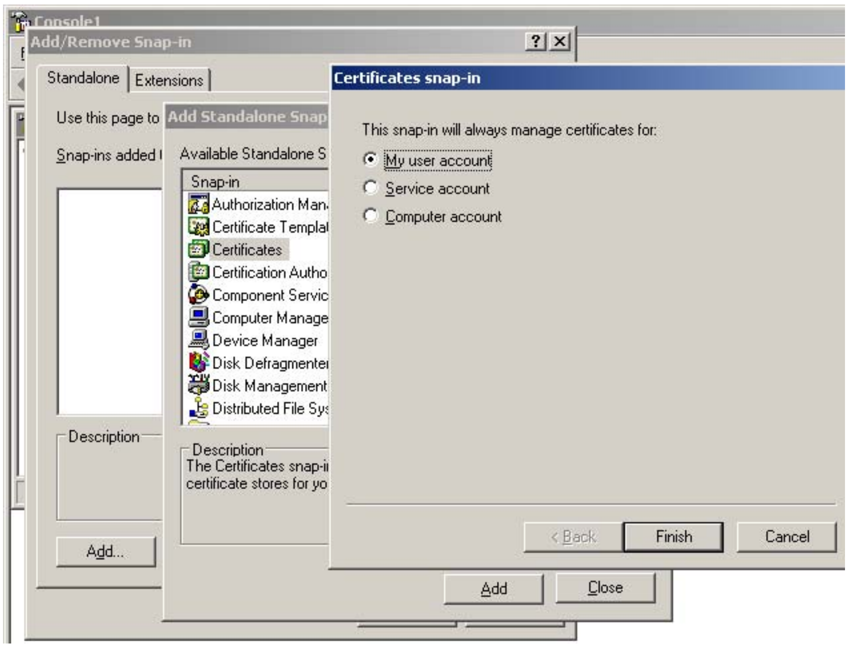
Installing a Certificate on IIS

The following example uses the Microsoft CA as a certificate source. To enable secure communication to IIS, perform the following steps on the platform where IIS is installed:

1. Request a certificate for the IIS machine using the Microsoft CA.
    a. Open a web browser.
    b. Enter the address of the CA Server web interface. In the following example, ca_machine is the host name of the CA Server: http://ca_machine/certsrv
    c. Click **Request a certificate**.
    d. Click **advanced certificate request**.
    e. Click **Create and submit a request to this CA**.
    f. Complete the request form. Ensure that the following critical parameters are completed correctly:
        - On an Enterprise CA, set the **Certificate Template** to **Web Server**.
        - The Name field ***must*** be the **Full computer name** (FQDN) of the computer running IIS. To find this name, from the Windows desktop, right-click My Computer, select Properties, and click the Computer Name tab.

> *Ensure that the "Issue to" field of the certificate is equal to the name of the IIS host machine name as it appears in the domain DNS.*

        - The Type of Certificate Needed field ***must*** be **Server Authentication Certificate**.
        - Select the **Mark keys as exportable** checkbox.
        - Select the Request Format **PKCS10**.
    g. Click **Submit**. A confirmation message is displayed.
    h. Click **Install this Certificate**. A confirmation message is displayed. Click **Yes**.
2. Install the certificate on the platform running IIS.
    a. Click the Windows **Start** button and click **Run**.
    b. Enter **MMC** and click **OK**. The Microsoft Management Console is displayed.
    c. From the File menu, click **Add/Remove snap-in**.
    d. Click **Add**.
    e. Select **Certificates** and click **Add**.
    f. Select **My user account** and click **Finish**.



This snap-in will always manage certificates for:

● My user account

○ Service account

○ Computer account

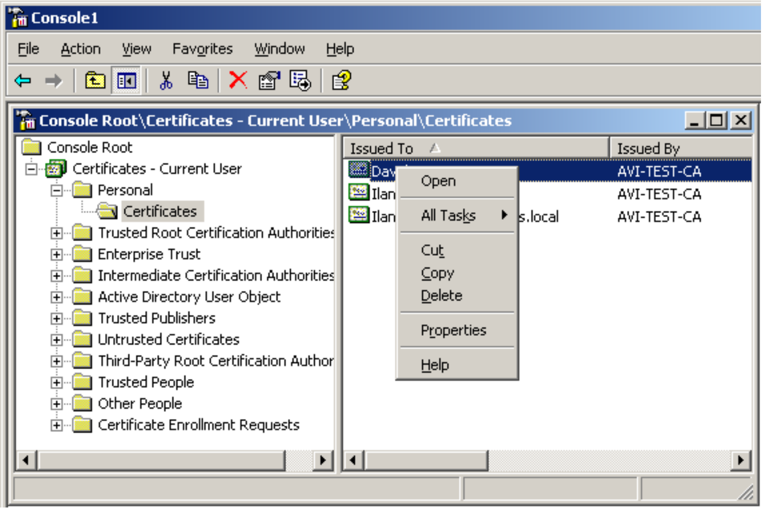
g. Click **Close** > **OK**.

h. From the left panel of the Microsoft Management Console, expand the **Certificates-Current User** branch.

i. Expand the **Personal** branch.

j. Click **Certificates**.

k. In the right panel, right click on the certificate. A popup menu is displayed.



l. Select **Open**. The Certificate Information Window is displayed.

m. Double-click on the certificate and then click the **Details** tab.

n. Click **Copy to File**. The Welcome screen of the Certificate Export Wizard is displayed.

o. Click **Next**. The Export Private Key screen is displayed.

p. Select **Yes, export the private key** and click **Next**. The Export File Format screen is displayed.

q. Select **Enable strong protection** and click **Next**.

r. Enter and confirm the password which protects the private key and click **Next**.

*The password must contain an upper-case letter, a lower-case letter, numbers, and one of the @ # $ % ^ & * symbols at a minimum.*

s. Enter a name for the file and click **Next > Finish**.

t. Click **OK** to close the Certificate Information window.

3. Configure the IIS Manager.

   a. From the Windows desktop, right-click **My Computer** and select **Manage**. The Computer Management console is displayed.

   b. Expand the **Services and Applications** branch.

   c. Expand the **Internet Information Server (IIS) Manager** branch.

   d. Select the **Web Sites** branch.

   e. Right-click either **Default Web Site** or another site, if another will be used for SCS purposes, and click **Properties**.

   f. Click the **Directory Security** tab.

   g. From the Secure communications box, click **Server Certificate**. The Welcome screen of the Web Server Certificate Wizard is displayed. Click **Next**.

   h. Select **Import certificate from .pfx file** and click **Next**.

   i. Locate and select the .pfx file which had been exported and click **Next**.

   j. Enter the password from step “**r**” above and click Next.

   k. Complete the Wizard.

Installing a CA Certificate to Authenticate IIS

A client application requires a certificate of the CA that issued the IIS certificate so that it can authenticate IIS. This applies to the platform running the SCS Console application.

Install the CA issuer certificate in the console’s trusted root certificate store

a. Open a web browser.

b. Enter the address of the CA Server web interface. In the following example, ca_machine is the host name of the CA Server: http://ca_machine/certsrv

c. Click **Download a CA certificate, certificate chain or CRL**.

d. Click **Download a CA certificate**.

e. Click **Save** and save the .cer file in a known location.

f. Right click on the saved certificate and select **Install Certificate**.

g. Select Next on all options on the Certificate Import Wizard.

Installing an Intel AMT Client Certificate for TLS Mutual Authentication

If TLS Mutual Authentication will be used, issue an Intel AMT client certificate and install the certificate in the certificate store of the service user. This includes the SCS application and any Management Console applications. The following procedure applies to a Stand-alone CA. There is a different procedure (not described here) for an Enterprise CA using templates.

This procedure must be performed on the SCS host by the same user as the one that will be identified as the SCS service user (see page 37.)

1. Run Internet Explorer as the SCS user (Start>Programs>right-click Internet Explorer >Run as….
2. In the Run As dialog click **The Following User** and enter the username and password of the SCS user (the name must be in the format domain\username).
3. Press OK
4. Enter the following address: http://ca_machine/certsrv
5. Click **Request a certificate**.
6. Click **advanced certificate request**.
7. Click **Create and submit a request to this CA**.
8. Complete the request form. Ensure that the following critical parameters are completed correctly:
   - The Name field ***must*** be the fully qualified name of the host (FQDN). To find this name, from the Windows desktop, right-click My Computer, select Properties, and click the Computer Name tab.
   - The Type of Certificate Needed field ***must*** be **Other**.
   - In the OID field, enter the client certificate OID and the remote certificate OID. The complete OID value must appear as: `1.3.6.1.5.5.7.3.2,2.16.840.1.113741.1.2.1`
   - Select 1024, 1536, or 2048 as a key size.
   - Select the **Mark keys as exportable** checkbox.

When an Enterprise CA is used, a template must be created that uses the identical OID described above. See Microsoft Certificate Authority documentation for information on creating and using a template.

9. Click Submit. Depending on the selected parameters, one or more confirmation messages are displayed. If the resulting page says “Certificate Pending”, perform step 10. Otherwise, skip to step 11. The behavior depends on how the CA policy module was configured.
10. Issue the certificate.

    A. Click the Windows **Start** button **> Administrative Tools > Certificate Authority**. The Certificate Authority Management Console is displayed.

    B. Expand the first sub-branch and click **Pending Requests**.

    C. Right-click on your request and, from the popup menu, select **All Tasks** > **Issue**.

    D. Return to the CA web enrollment home page and select View the Status of a Pending Certificate Request. Click on the relevant certificate request.

11. Click **Install this certificate**.

Active Directory (AD) and Changes to the AD Schema

AD provides users with a single network logon and a single point of administration and replication. It provides Kerberos Authentication, DNS and X.500 naming standards, as well as Lightweight Directory Access Protocol (LDAP). It also includes several important protocols and various useful APIs.

This manual assumes that AD is installed. For installation instructions, see Microsoft documentation.

Installation of the SCS optionally adds a schema definition and script that are used to extend the Active Directory schema for Intel AMT. When the Administrator runs it, the script creates a new class – Intel-Management-Engine – based on the AD computer object, with the following new attributes:

- Intel-Management-Engine-Version (received in the “Hello” message from the Intel AMT device)
- Intel-Management-Engine-Host-Computer (a link to the platform computer object created when the host joins the domain)
- Intel-Management-Engine-Platform-UUID (received in the “Hello” message)
- Intel-Management-Engine-Host-Computer-BL (added to the computer object class as a back link to an AMT object)
- “Intel-Management-Engine-Host-computer-BL” (added to the top computer object class)

In addition, the SCS installation includes scripts used to create an AD user account for Intel SCS and give it the appropriate privileges.

When the SCS performs setup for an Intel AMT device, the SCS service:

- creates an AMT Object with the first three attributes listed above
- creates a link between the attribute “Intel-Management-Engine-Host-Computer” in the AMT Object and the AMT Host object
- creates a link between the attribute “Intel-Management-Engine-Host-Computer-BL” found on the AMT Host and the AMT Object.

Active Directory will display the AMT Object as the representation of the Intel AMT device itself and show it as having the type Intel-Management-Engine.

Installation of the SCS Server Components

The Intel SCS components can be installed on a single computer or on separate computers. Setup facilitates those options. In either case, required user intervention presumes knowledge of:

- SQL Server administration
- Internet Information Services (IIS) 6.0 administration
- Windows Service installation

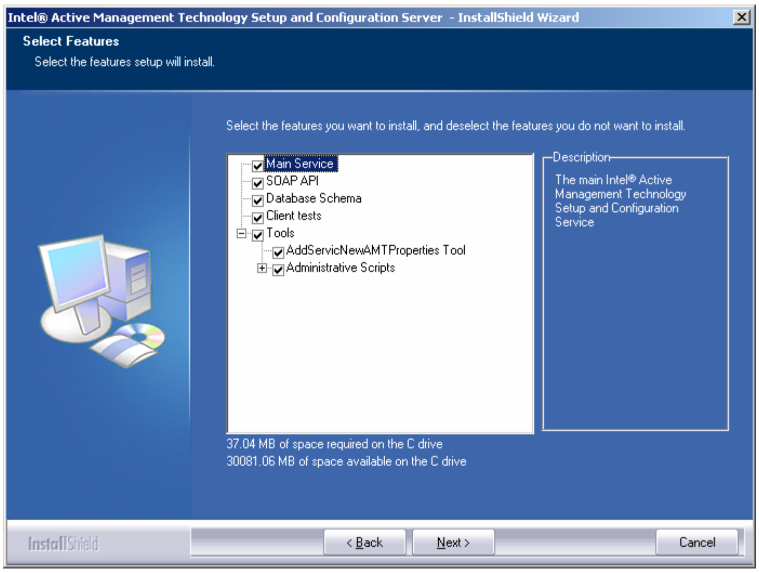
Installing the Intel SCS Server Components

To install the Intel SCS components:

1. Ensure that the computer meets the system requirements listed in “System Requirements” on page 15.
2. Insert the Intel SCS CD-ROM into the computer’s CD-ROM drive, or locate the distribution files as downloaded to the server platform.
3. Locate and double-click the file named `AMTConfServer.exe`. The Welcome screen is displayed. Click **Next**. The License Agreement screen is displayed.
4. Accept the license agreement and click **Next**. The Setup Type screen is displayed.
5. From the Setup Type screen, select Complete.

Intel SCS Setup inspects the computer’s software. Messages are displayed if any of the prerequisites are missing. If any prerequisites are missing, click Cancel and add them.

Use the Custom option only if there are components that are not needed.



Intel® Active Management Technology Setup and Configuration Server - InstallShield Wizard

Select Features

Select the features setup will install.

Select the features you want to install, and deselect the features you do not want to install.

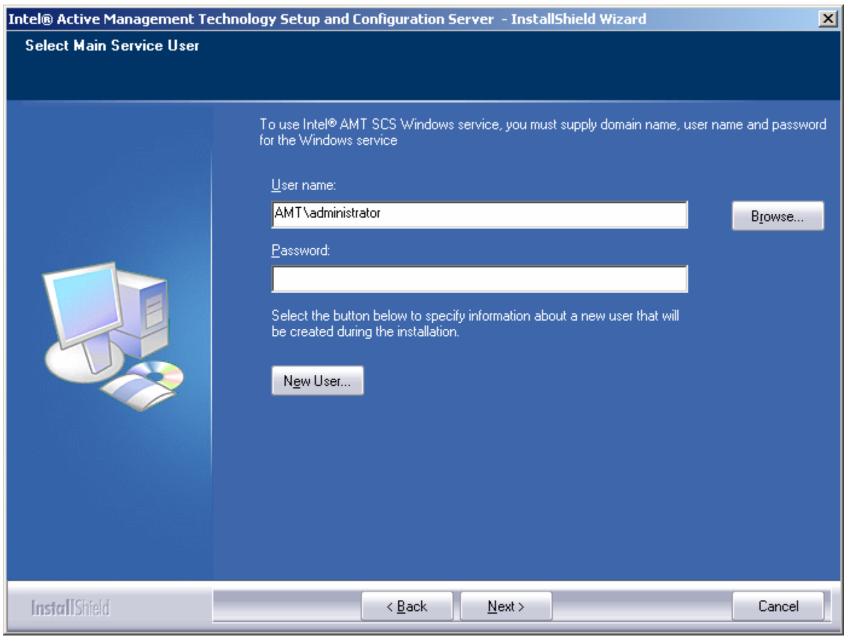
☑ Main Service
☑ SOAP API
☑ Database Schema
☑ Client tests
☑ Tools
  ☑ AddServicNewAMTProperties Tool
  ☑ Administrative Scripts

Description

The main Intel® Active Management Technology Setup and Configuration Service

37.04 MB of space required on the C drive
30081.06 MB of space available on the C drive

6. The Select Main Service User screen is displayed.



Intel® Active Management Technology Setup and Configuration Server - InstallShield Wizard

Select Main Service User

To use Intel® AMT SCS Windows service, you must supply domain name, user name and password for the Windows service

User name: AMT\administrator

Password:

Select the button below to specify information about a new user that will be created during the installation.

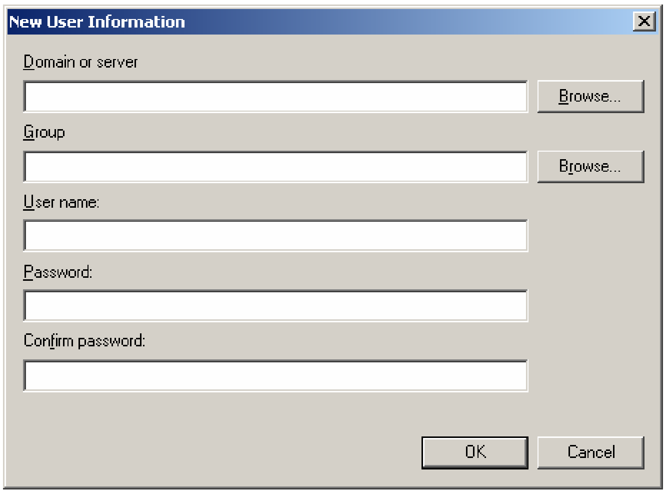
Enter the user name in the format “NetBIOS Name\Username”. In an Active Directory environment, the NetBIOS name will be the domain name. In the absence of Active Directory, this will be the computer name where the installation is taking place.

This user must have the necessary permission to run as a service. The installer prompts to add this permission automatically. The user must have all the permissions described in “SCS and Active Directory Tasks and Permissions” on page 12, including permissions to access the CA.

Enter the User name and Password and click Next.

In a TLS environment, the SCS user must have permissions to issue certificates (Issue and Manage Certificates and Request Certificates permission) on a stand-alone certificate authority (CA). On an Enterprise CA, the user must have Read and Enroll permissions on the template to be used to create certificates.

If a new user will be created later that will be the one associated with the service, select **New User.**



New User Information

Domain or server:

Group:

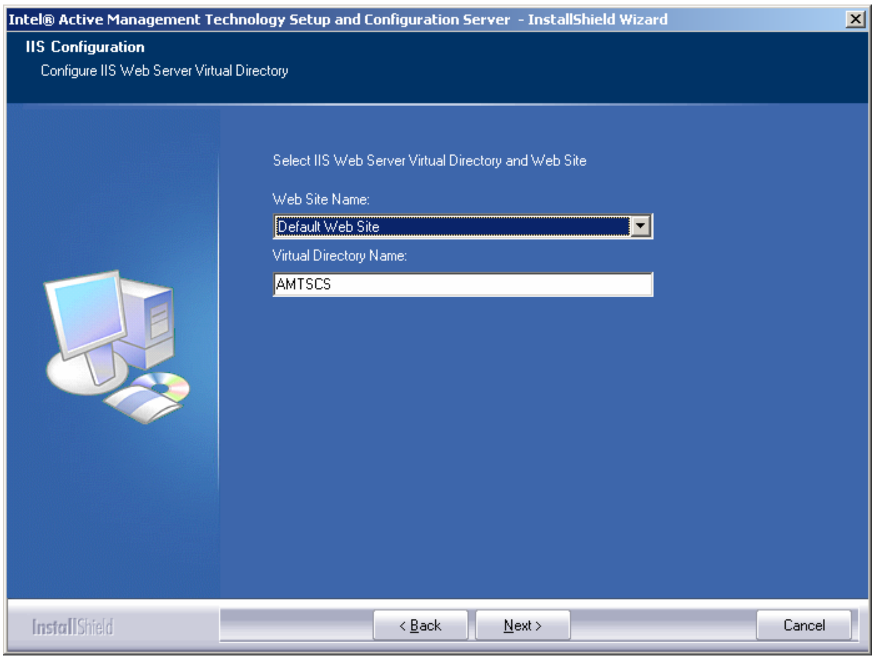
User name:

Password:

Confirm password:

Enter the parameters defining this user and select OK, then click **Next**.

7. The IIS Configuration screen is displayed.



Intel® Active Management Technology Setup and Configuration Server - InstallShield Wizard

IIS Configuration

Configure IIS Web Server Virtual Directory

Select IIS Web Server Virtual Directory and Web Site

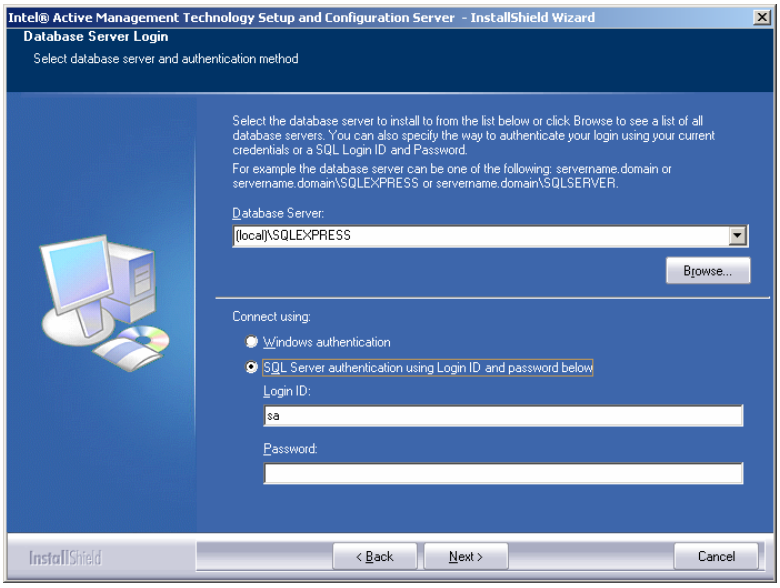
Web Site Name: Default Web Site

Virtual Directory Name: AMTSCS

8. Select a web site from the list of sites defined within IIS.
9. Enter the IIS Web Server Virtual Directory name. The default name is AMTSCS. Click Next.

The Virtual Directory name must be unique. If a Virtual Directory already exists with this name, the existing Virtual Directory will be preserved. As a result, the SOAP Virtual Directory will not be created.

10. The Database Server Login screen is displayed.



Intel® Active Management Technology Setup and Configuration Server - InstallShield Wizard

Database Server Login

Select database server and authentication method

Select the database server to install to from the list below or click Browse to see a list of all database servers. You can also specify the way to authenticate your login using your current credentials or a SQL Login ID and Password.

For example the database server can be one of the following: servername.domain or servername.domain\SQLEXPRESS or servername.domain\SQLSERVER.

Database Server: (local)\SQLEXPRESS

Connect using:

○ Windows authentication

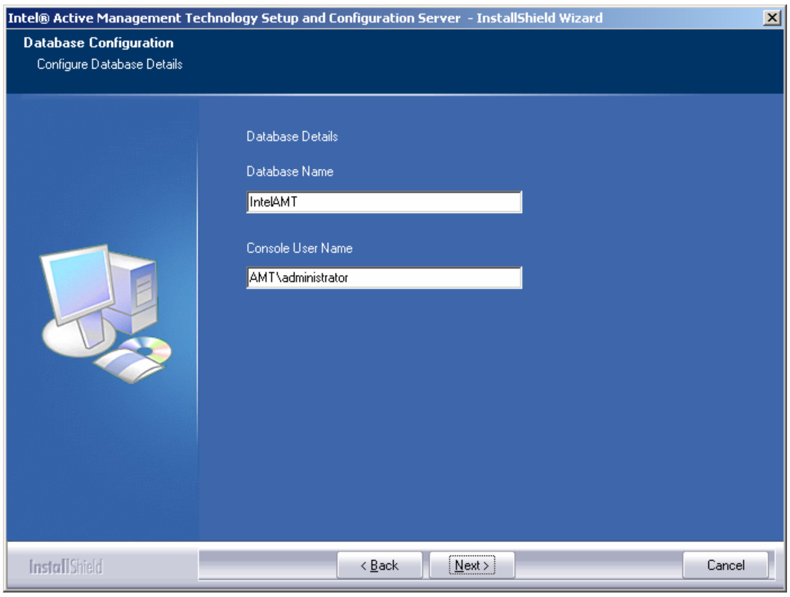
● SQL Server authentication using Login ID and password below

Login ID: sa

Password:

Define the database server—that is, the name of the computer functioning as the database server and the database instance— and the connection type. In the above screenshot, the server is “local” and the instance is SQLEXPRESS. Use the FQDN of the server platform. Click Next. The Database Configuration screen is displayed.

The default Server name is the name of the local computer. In an environment with one shared database and more than one Intel SCS, ensure that the Server name is the name of the computer hosting the database.



Intel® Active Management Technology Setup and Configuration Server - InstallShield Wizard

Database Configuration

Configure Database Details

Database Details

Database Name

IntelAMT

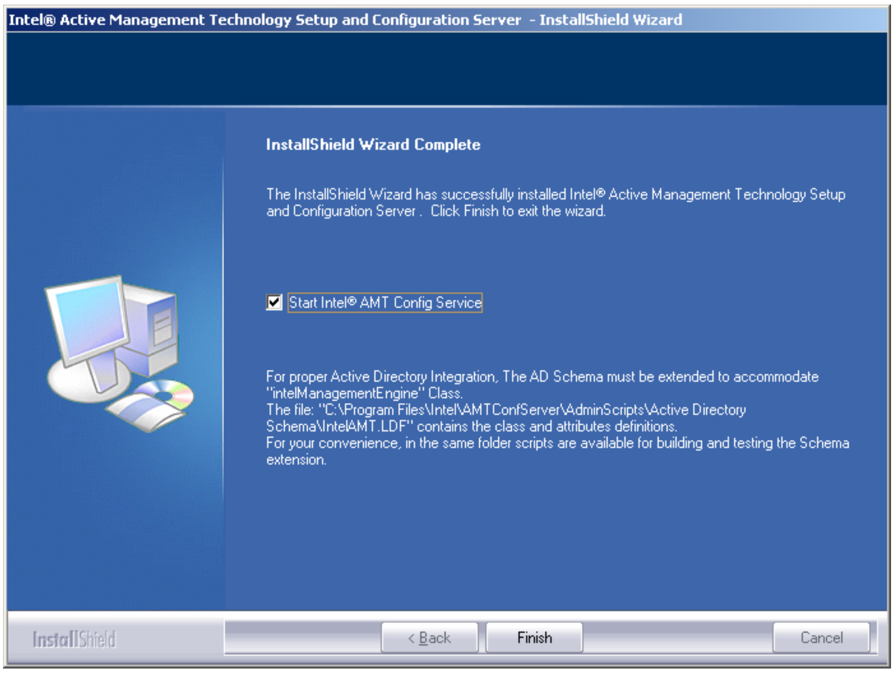
Console User Name

AMT\administrator

11. If Database Schema is being installed, enter both the Database Name—that is, the name assigned to the database; the default name is IntelAMT—and the Console User Name.

If the database was previously installed, the installer displays a notice asking if the database should be replaced. Respond "No" to this request. Install the database only once.

11. From the Ready to Install screen, click **Install**. Installation begins. A progress bar indicates the status of the installation. When the installation is complete, the InstallShield Wizard* Complete screen is displayed.



Intel® Active Management Technology Setup and Configuration Server - InstallShield Wizard

InstallShield Wizard Complete

The InstallShield Wizard has successfully installed Intel® Active Management Technology Setup and Configuration Server . Click Finish to exit the wizard.

☑ Start Intel® AMT Config Service

For proper Active Directory Integration, The AD Schema must be extended to accommodate "intelManagementEngine" Class.
The file: "C:\Program Files\Intel\AMTConfServer\AdminScripts\Active Directory Schema\IntelAMT.LDF" contains the class and attributes definitions.
For your convenience, in the same folder scripts are available for building and testing the Schema extension.

The Installation Complete screen has a reminder to run the scripts required to add the the IntelManagementEngine class to Active Directory. Optionally, select the checkbox to start the SCS immediately.

12. Click **Finish**.

Upgrading the Intel SCS to a New Version

If there is an existing version of the SCS already installed and a new version is to be installed, perform the following steps:

1. Navigate to **Add or Remove Programs** on the **Control Panel**, select the Intel Active Management Technology Setup and Configuration Server and select **Remove**. If the database is to be preserved and migrated to a new version, answer **No** to the question
   Are you sure you want to remove the Database”IntelAMT” on (local)\SQLEXPRESS”?
   All instances of the service should be stopped and removed. Also remove the Intel AMT SCS Console on all platforms where it is installed.
   There may be a delay while IIS is restarted. If requested by the uninstaller (required in certain limited cases), restart the server platform.
2. Using locally available tools, backup the database.
3. Start installation of the new version of the SCS as described above.
4. If the new version has a newer version of the database schema, a message is displayed reminding the user to perform a database backup. Do so now if step 2 was skipped.
5. Continue with the installation. The installer will update the database so that it conforms to the latest version of the schema.

Silent Install

The SCS installation image is an InstallShield* executable. Besides the interactive install described above, the SCS can be installed from a command line using a script file to respond to the installer questions. This capability is called “silent install”.

Another application can invoke the silent install with a properly prepared installation script. This can be used by ISVs that wish to embed the SCS into their application. The usage is:

```
AMTConfServer.exe /s /f1”c:\scsinstall.iss” /f2”c:\scsinstall.log”
```

where `scsinstall.iss` is the install script and `scsinstall.log` is the log file created by the installer.

Note: As with any script-driven application, the parameters included in the script must be verified before activating the script. The silent install assumes that the supplied values are correct.

The following example of an **scsinstall.iss** script provides the necessary parameters to the installer. The highlighted parameters are those that that must be customized per installation.

```
[InstallShield Silent]
Version=v7.00
File=Response File
[File Transfer]
OverwrittenReadOnly=NoToAll
[{DA4F4037-6EB2-4309-86EB-A8902CBC12EC}-DlgOrder]
Dlg0={DA4F4037-6EB2-4309-86EB-A8902CBC12EC}-OnAppSearch-0
Count=15
Dlg1={DA4F4037-6EB2-4309-86EB-A8902CBC12EC}-SdWelcome-0
Dlg2={DA4F4037-6EB2-4309-86EB-A8902CBC12EC}-SdLicense2Rtf-0
Dlg3={DA4F4037-6EB2-4309-86EB-A8902CBC12EC}-SetupType2-0
Dlg4={DA4F4037-6EB2-4309-86EB-A8902CBC12EC}-IntelFlow-0
Dlg5={DA4F4037-6EB2-4309-86EB-A8902CBC12EC}-AskYesNo-0
Dlg6={DA4F4037-6EB2-4309-86EB-A8902CBC12EC}-OnMainServiceInitialize-0
Dlg7={DA4F4037-6EB2-4309-86EB-A8902CBC12EC}-IISDialog-0
Dlg8={DA4F4037-6EB2-4309-86EB-A8902CBC12EC}-SQLServerSelectLogin-0
Dlg9={DA4F4037-6EB2-4309-86EB-A8902CBC12EC}-DBDialog-0
Dlg10={DA4F4037-6EB2-4309-86EB-A8902CBC12EC}-SdStartCopy2-0
Dlg11={DA4F4037-6EB2-4309-86EB-A8902CBC12EC}-MainService_Installed-0
Dlg12={DA4F4037-6EB2-4309-86EB-A8902CBC12EC}-DatabaseSchema_Installed-0
Dlg13={DA4F4037-6EB2-4309-86EB-A8902CBC12EC}-AskYesNo-1
Dlg14={DA4F4037-6EB2-4309-86EB-A8902CBC12EC}-SdFinish-0
[{DA4F4037-6EB2-4309-86EB-A8902CBC12EC}-OnAppSearch-0]
## If the user is not administrator, the installer displays a warning
## message. In silent install, a warning message will terminate the
## installer, so the Admin_logged_On parameter was added:
## 1: Allow installation even if the user is not an administrator
## 0: Don’t allow install without Admin permissions.
Admin_Logged_On=1
## Allow installation if .NET 2.0 is not installed.
NET_2.0_Exists=1
[{DA4F4037-6EB2-4309-86EB-A8902CBC12EC}-SdWelcome-0]
Result=1
[{DA4F4037-6EB2-4309-86EB-A8902CBC12EC}-SdLicense2Rtf-0]
Result=1
[{DA4F4037-6EB2-4309-86EB-A8902CBC12EC}-SetupType2-0]
Result=304
[{DA4F4037-6EB2-4309-86EB-A8902CBC12EC}-IntelFlow-0]
## This warning message is presented in case the user selects to install
SOAP API (on IIS) and IIS6 is not installed.
## Allow installation of SOAP API even if IIS6 is not installed.
IIS6_Warning=1
```

```
[{DA4F4037-6EB2-4309-86EB-A8902CBC12EC}-AskYesNo-0]
## Ignored
Result=1
[{DA4F4037-6EB2-4309-86EB-A8902CBC12EC}-OnMainServiceInitialize-0]
## Domain/User/Password for the main service.
## Note: when running in silent mode the Domain/User/Password is not
validated!
Domain_User=DOMAIN\user
Password=password
[{DA4F4037-6EB2-4309-86EB-A8902CBC12EC}-IISDialog-0]
## The IIS SOAP API virtual directory name and
## web site name. The web site named must exist before installation.
SOAP_Name=AMTSCS
Result=1
SOAP_Web_Site_Name=Default Web Site
[{DA4F4037-6EB2-4309-86EB-A8902CBC12EC}-SQLServerSelectLogin-0]
## User/Password for SQL Server login
## To use Windows authentication simply use blank values, for example:
## szUser=' '.
## Note: The User/Password is not validated in silent mode. If access
## is denied the installation will fail when it tries unsuccessfully
## to access the DB.
szUser=sa
szPass=sa
## Name and Instance of the SQL Server.
szServer=(local)\SQLEXPRESS
Result=1
[{DA4F4037-6EB2-4309-86EB-A8902CBC12EC}-DBDialog-0]
## Database name.
DB_Name=IntelAMT
## Application user to add when installing the Database
App_User=DOMAIN\user
Result=1
[{DA4F4037-6EB2-4309-86EB-A8902CBC12EC}-SdStartCopy2-0]
Result=1
## If there is an existing database, this parameter determines if the
## installer should update to a newer schema. 1=yes; 0=no
## If the installed DB has a newer schema than the version being installed,
## the installation will continue without updating the DB.
## If the installer attempts to update the DB and fails (for example, there
## are other users still active attached to the DB), then the install will
## fail.
Update_DB=1
[Application]
Name=Intel® Active Management Technology Setup and Configuration Server
Version=1.1.0.0.1
Company=Intel
Lang=0009
[{DA4F4037-6EB2-4309-86EB-A8902CBC12EC}-MainService_Installed-0]
## If the user selected to run the service does not have sufficient
## permissions in local security policy to run
## as a service, the installer will add the necessary privileges if
## Set_Privileges is 1 (0 to ignore).
Set_Privileges=1
[{DA4F4037-6EB2-4309-86EB-A8902CBC12EC}-DatabaseSchema_Installed-0]
## When installing, the Database might be already installed. The
## Use_Exist_DB parameter tells the installer what to do.
## 1: The existing DB will be used; 0: delete the DB and recreate it.
Use_Exist_DB=1
```

```
[{DA4F4037-6EB2-4309-86EB-A8902CBC12EC}-AskYesNo-1]
## ignored
Result=1
[{DA4F4037-6EB2-4309-86EB-A8902CBC12EC}-SdFinish-0]
Result=1
# bOpt1 controls whether or not to start the windows service after the
installation.
bOpt1=0
bOpt2=0
[{0027D675-4029-47F6-B217-77C6EB1389CB}-DlgOrder]
Count=0
```

Use the following script to perform a silent uninstall. The highlighted fields must match the corresponding fields in the install script.

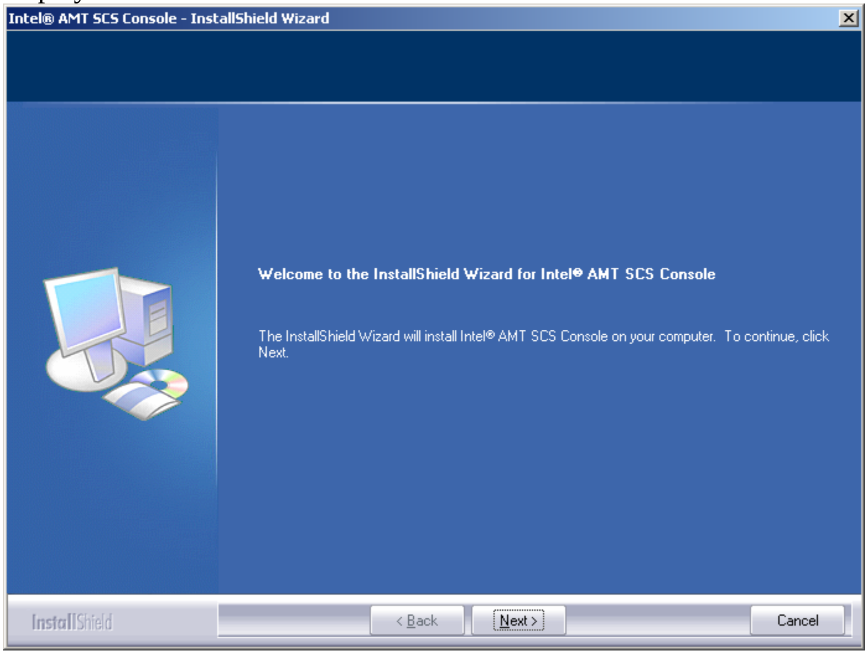
```
[InstallShield Silent]
Version=v7.00
File=Response File
[File Transfer]
OverwrittenReadOnly=NoToAll
[{DA4F4037-6EB2-4309-86EB-A8902CBC12EC}-DlgOrder]
Dlg0={DA4F4037-6EB2-4309-86EB-A8902CBC12EC}-MessageBox-0
Count=6
Dlg1={DA4F4037-6EB2-4309-86EB-A8902CBC12EC}-DatabaseSchema_UnInstalling-0
Dlg2={DA4F4037-6EB2-4309-86EB-A8902CBC12EC}-SQLLogin-0
Dlg3={DA4F4037-6EB2-4309-86EB-A8902CBC12EC}-AskYesNo-0
Dlg4={DA4F4037-6EB2-4309-86EB-A8902CBC12EC}-SdFinish-0
Dlg5={DA4F4037-6EB2-4309-86EB-A8902CBC12EC}-SdFinishReboot-0
 [{DA4F4037-6EB2-4309-86EB-A8902CBC12EC}-MessageBox-0]
Result=6
[Application]
Name=Intel® Active Management Technology Setup and Configuration Server
Version=1.1.0.0.1
Company=Intel
Lang=0009
[{DA4F4037-6EB2-4309-86EB-A8902CBC12EC}-DatabaseSchema_UnInstalling-0]
# Whether or not to remove the DB when uninstalling. 1: Yes; 0: No
Remove_DB=1
[{DA4F4037-6EB2-4309-86EB-A8902CBC12EC}-SQLLogin-0]
## User/Password for SQL Server login
## To use Windows authentication simply use blank values, for example:
## szUser=' '.
## Note: The User/Password is not validated in silent mode. If access
## is denied the uninstall will fail when it tries unsuccessfully
## to access the DB.
szUser=sa
szPass=sa
Result=1
[{DA4F4037-6EB2-4309-86EB-A8902CBC12EC}-AskYesNo-0]
# ignored
Result=0
[{DA4F4037-6EB2-4309-86EB-A8902CBC12EC}-SdFinish-0]
Result=1
bOpt1=0
bOpt2=0
[{DA4F4037-6EB2-4309-86EB-A8902CBC12EC}-SdFinishReboot-0]
## If the SOAP API cannot be removed, the uninstaller may request a reboot.
## BootOption=0 ignores the request; BootOption=1: uninstaller does reboot
## To avoid the reboot request, be sure no clients request access to SOAP
## API after IIS restart.
Result=1
BootOption=0
[{951D2E35-5A48-4ED3-8BA4-78205D908B8C}-DlgOrder]
Count=0
```

Installation of the Intel AMT Management Console

Installation of the Intel SCS Management Console requires no user intervention. The default installation folder is C:\Program Files\Intel\AMTConsole.

To install the Intel SCS Management Console: See “Installation of the Intel AMT Management Console” on page 45.

1. Ensure that the computer meets the system requirements listed in “System Requirements” on page 15.
2. Insert the Intel SCS CD-ROM into the computer’s CD-ROM drive.
3. Locate and double-click the file named `AMTConsole.exe`. The Welcome screen is displayed.



Intel® AMT SCS Console - InstallShield Wizard

Welcome to the InstallShield Wizard for Intel® AMT SCS Console

The InstallShield Wizard will install Intel® AMT SCS Console on your computer. To continue, click Next.

4. Click **Next**. The License Agreement is displayed.
5. Accept the license agreement and click **Next**. The Choose Destination Location screen is displayed.
6. Define the location where the Intel SCS Management Console will be installed and click **Next**. The Ready to Install screen is displayed.
7. Click **Install**. Installation begins. A progress bar indicates the status of the installation. When the installation is complete, the InstallShield Wizard Complete screen is displayed. Click **Finish**.

Post Installation Operations

After the components of the Intel SCS are installed, we recommend completing the following procedures.

Intel AMT Configuration and the DNS

Intel AMT device setup and configuration requires the presence of a Domain Name System (DNS) Server. The DNS must have information for two entities:

The SCS Server must be registered in the DNS.

A configured, operational Intel AMT device must be registered within DNS.

Intel SCS

Any platform running the SCS Service (the Main Service) must be registered in the DNS as “ProvisionServer”. This must be done in each DNS Domain. When it sends its “Hello” message, the Intel AMT device first uses the domain name received from the DHCP server. If there is more than one SCS in the domain, the DNS will alternate between the servers. If there multiple SCS instances or the server platform has a different name, then CNAME records need to be added to the DNS.

Intel AMT Devices

Ensure that the DNS is configured with the Fully Qualified Domain Names (FQDN) of the Intel AMT-enabled machines that are being configured.

Intel AMT devices must be configured to have the same FQDN as the host OS. This stems from the fact the Intel AMT device is not a secure DNS client and it relies on the host OS to maintain the DNS record. For this reason, the Intel AMT device snoops the DHCP requests and responses issued by the host OS. The Intel AMT device then uses the IP provided by the DHCP to the host OS as its own.

When the host OS is down, the Intel AMT device requests DNS registration of its configured FQDN from the DHCP (option 81). This works only if the DNS and DHCP are configured to operate in this way. This is a default feature of Microsoft DNS and DHCP servers.

When an Intel SCS contacts a configured Intel AMT device, it uses the FQDN of the Intel AMT device. When using TLS and/or Kerberos, this is essential, as the platform and the Intel AMT device are identified in certificates and Kerberos tickets with the FQDN. This necessitates that the DNS server contain a Host (A) record for every configured Intel AMT device.

This is the responsibility of the Administrator.

There are several methods to do this:

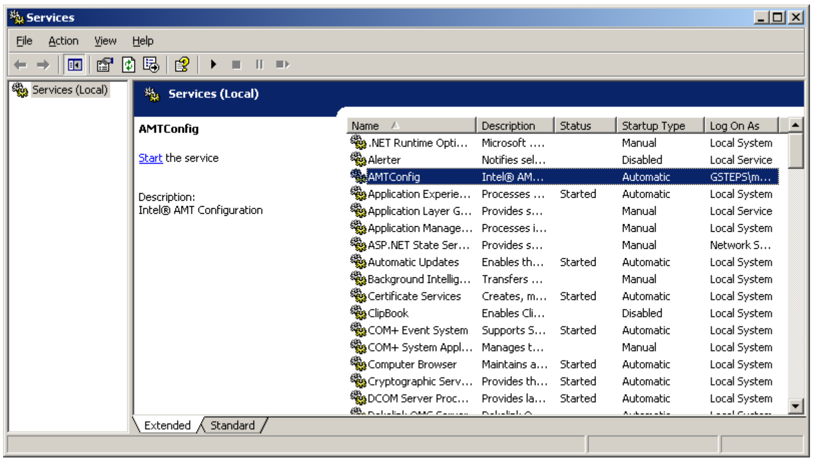
- Manual entry of the Host (A) record
- A successful boot of the host OS that registers a DNS entry with the same name. This method is good as long as the IP lease and DNS entry are maintained.
- Configure DNS and DHCP to enable AMT use of option 81.

AMTConfig Service Verification

To verify that the AMTConfig Windows service is running:

1. Click the Windows **Start** button and click **Run**.
2. In the **Open** field, enter **services.msc** and click **OK**. The Services (Local) Window is displayed.

3. In the Status column, check the status of **AMTConfig**. If there is no listing in the column, the service is not running.
4. Select **AMTConfig**. "Start the service" is displayed.



AMTConfig

Start the service

Description:
Intel® AMT Configuration

Name	Description	Status	Startup Type	Log On As
.NET Runtime Opti…	Microsoft ….		Manual	Local System
Alerter	Notifies sel…		Disabled	Local Service
AMTConfig	Intel® AM…		Automatic	GSTEPS\m…
Application Experie…	Processes …	Started	Automatic	Local System
Application Layer G…	Provides s…		Manual	Local Service
Application Manage…	Processes i…		Manual	Local System
ASP.NET State Ser…	Provides s…		Manual	Network S…
Automatic Updates	Enables th…	Started	Automatic	Local System
Background Intellig…	Transfers …		Manual	Local System
Certificate Services	Creates, m…	Started	Automatic	Local System
ClipBook	Enables Cli…		Disabled	Local System
COM+ Event System	Supports S…	Started	Automatic	Local System
COM+ System Appl…	Manages t…		Manual	Local System
Computer Browser	Maintains a…	Started	Automatic	Local System
Cryptographic Serv…	Provides th…	Started	Automatic	Local System
DCOM Server Proc…	Provides la…	Started	Automatic	Local System

5. Click **Start**. A progress message is displayed. When completed, the word **Started** appears in the Status column.

Quick Start and System Test

This procedure is a summary of the Intel SCS Management Console section which begins on page 59. However, it can also be completed as a test to ensure that the system is configured and running properly.

1. Log-in to the Intel SCS Console. For details, see.
2. Add a new profile. For details, see “Configuring Profiles” on page60.

“Logging In” on page 61.

3. Add a new profile. For details, see “Configuring Profiles” on page 65.

   a. From the navigation panel of the Intel SCS Console, expand the **Configuration Service Settings** branch and select **Profiles**.

   b. Click **Add**. The Profile Configuration dialog box is displayed and the General tab is selected.

   c. Configure the new profile and save it.

4. Add new Intel AMT properties. For details, see “New Intel AMT Systems” on page 79.

   a. From the navigation panel of the Intel SCS Console, select **New** Intel AMT **Systems**. The New Intel AMT Systems table is displayed.

   b. Click **Add**. The New AMT Device Properties dialog box is displayed.

   c. Enter the New Intel AMT device properties and click **OK**.

5. If Intel AMT Release 1.0 devices need to be setup and configured, enable this capability.

   a. From the navigation panel of the Intel SCS Console, expand the **Configuration Service Settings** branch and select **General**. The General screen is displayed.

   b. Select the **Intel AMT 1.0 Provisioning** checkbox.

   c. A confirmation message is displayed. Confirm the selection.

   d. Click **Apply**.

6. If AMT 1.0 devices are installed and need to be setup using the SCS, configure the BIOS administrator password for Intel AMT 1.0.

All Intel AMT Release 1.0 devices must be configured via the MEBx to this administrator password.

   a. From the navigation panel of the Intel SCS Console, expand the **Configuration Service Settings** branch and select **Profiles**.

   b. Select the profile being used and click **Edit**.

   c. Enter the new password in the **AMT 1.0 BIOS password** field.

   d. Click **Apply**.

7. Configure the BIOS administrator password for Intel® AMT 2.0/2.1. For details, see “Configuring Pre-Setup and Configuration Security Keys” on page 74.

   a. From the navigation panel of the Intel SCS Console, expand the **Configuration Service Settings** branch and select **Security Keys**.

   b. Select a TLS-PSK entry. (If there are no entries, click **Create Pre-Provision data** to create entries.)

c. Click **View**.

d. Copy or print the entry’s properties.

e. The Administrator must enter these values in the appropriate place in the Intel AMT device BIOS screen.

8. If using TLS based Authentication, configure the CA parameters.

   a. From the navigation panel of the Intel SCS Console, expand the **Configuration Service Settings** branch and select **Profiles**.

   b. Select the profile being used and click **Edit**.

   c. Click the **Certificates**.

   d. Configure the CA parameters.

   e. Click **Apply**.

Without a proper CA configuration, the SCS service will not be able to work with TLS based Authentication.

9. If using TLS based Authentication, configure the profile’s Mutual Authentication parameters.

   a. From the navigation panel of the Intel SCS Console, expand the **Configuration Service Settings** branch and select **Mutual Authentication**.

   b. Configure the **Trusted Root Certificate** for use with TLS Server Authentication.

   c. Configure the **Service Mutual Authentication Certificate** for use with TLS Server Authentication.

   d. Click **Apply**.

10. Configure the profile’s Network parameters.

    a. From the navigation panel of the Intel SCS Console, expand the **Configuration Service Settings** branch and select **Network**.

    b. Configure the Network parameters:

    - To enable TLS, select the **Use TLS** checkbox and—for both Network Interface and Local Interface—select **TLS Server Authentication**.

Improper Network settings can cause some of the SCS service’s features to malfunction. For example, changing only the Network Interface to TLS Server Authentication causes an API failure.

- To disable the Certificates and Mutual Authentication tabs, clear the **Use TLS** checkbox.

c. Click **Apply**.

11. Test the Intel SCS Main Service.

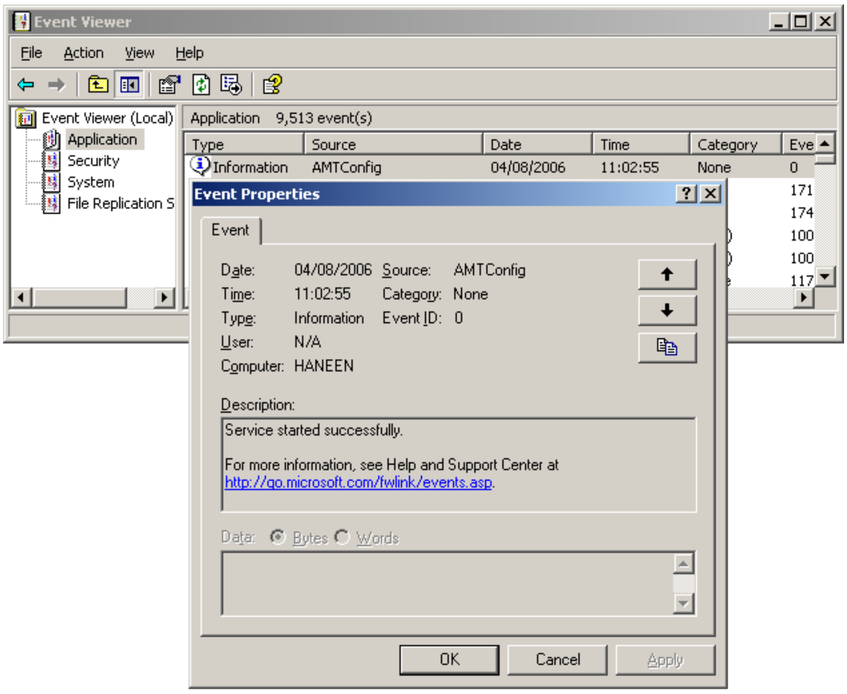
    a. Click the Windows **Start** button > **Administrative Tools** > **Services**.

    b. Right-click on **AMT Config** and, from the popup menu, select **Start**. A progress bar indicates the advancement of the start-up.

    c. Click the Windows **Start** button > **Administrative Tools** > **Event Viewer**.

    d. Click **Application**.

    e. In the Information entries, double-click the AMTConfig message. A popup message should say “Service Started Successfully.”



Date: 04/08/2006 Source: AMTConfig
Time: 11:02:55 Category: None
Type: Information Event ID: 0
User: N/A
Computer: HANEEN

Description:
Service started successfully.

For more information, see Help and Support Center at http://go.microsoft.com/fwlink/events.asp.

Data: ● Bytes ○ Words

f. Click **OK**. The Event Viewer returns to focus.

g. From the File menu, click **Exit**.

Recommended Daily Workflow

After the Intel SCS components are installed and the first Intel AMT devices are configured and operational, we recommend that the following tasks be completed on a regular basis (preferably daily):

- Check for new Intel AMT devices. See "New Intel AMT Systems" on page 79.
- Review the list of "Existing Intel AMT Systems" for anomalies – devices that have not completed setup and configuration, pending addition of information to the device definition (e.g., a missing UUID or FQDN).
- Review the logs. Note anomalies and fix them. See "Intel AMT SCS Console Logs" on page 89.
- Backup the database.

Chapter 3

INTEL AMT PREPARATION

This section contains:

- “Preparation Without a USB Device” on page 53
- “Using a USB Storage Device for Factory Mode Setup” on page 56
- “Preparing Intel AMT for Future Configuration” on page 57

This section describes the steps required to prepare an Intel AMT device to receive its configuration settings from the Intel SCS. An Intel AMT device is considered in Factory Mode until it is ready to send "Hello" messages to the SCS. Once the appropriate preparation is performed, the device transitions to Setup Mode, sending "Hello" messages periodically until it receives a response from an SCS. When setup and configuration is complete, the Intel AMT device is in Operational Mode. There are three possibilities:

- During power up, if the BIOS implementation supports this capability, the Intel AMT device first checks for the presence of a USB storage device. If the device is present, the setup proceeds as described in "Using a USB Storage Device for Factory Mode Setup" on page 56. The PID/PPS pair is installed and, optionally, the Intel Management Engine BIOS extension password may be changed.
- If there is no USB device or USB enablement is not supported, the technician enters the BIOS extension using the method defined by the BIOS vendor. The BIOS implementation may require that the user enable the BIOS extension from the BIOS. The PID/PPS pair is entered manually as described below, based on values generated by the SCS.
- If the device was prepared for configuration with a PID-PPS pair by an OEM or by previous IT actions, then no further preparation is needed: It is already in Setup Mode. The Intel AMT device will send "Hello" messages once it is connected to the network.

Preparation Without a USB Device

If there is no USB device or USB enablement is not supported, the platform displays the BIOS startup screen, and then the BIOS Extensions will be processed.

Intel AMT reference platforms display a screen prompting the user to press <Ctrl+P>. Pressing <Ctrl+P> passes control to the Intel Management Engine BIOS extension (MEBx) Main Menu. This step may vary as a function of an OEM-provided BIOS. Follow the manufacturer's directions for accessing the ME BIOS sub-menu. Steps 1 through 11 or some subset of them may not be required.

Perform the following steps:

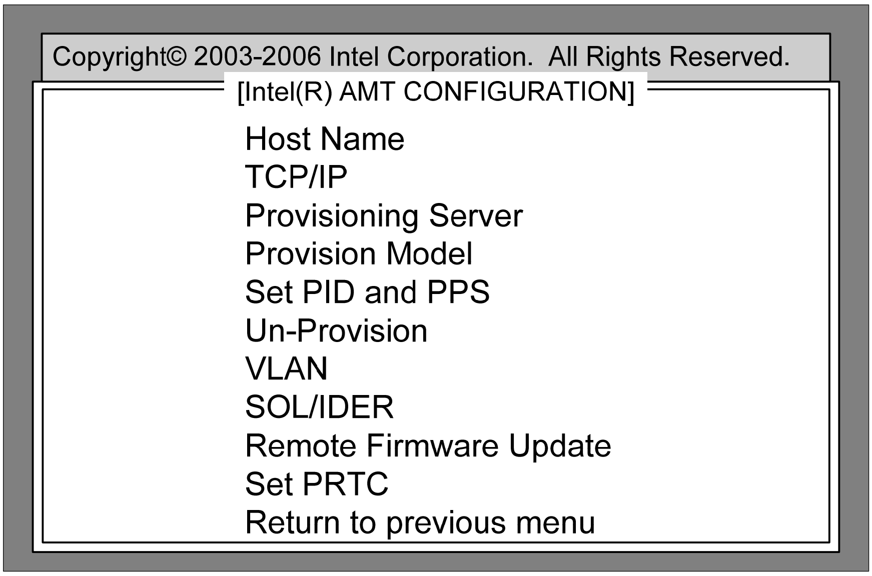
1. Enter the MEBx default password. The default password is **admin**.
2. Change the default password to a new value. This step is required.

*The password must contain an upper-case letter, a lower-case letter, numbers, and one of the @ # $ % ^ & * symbols at a minimum.*

   This password is either generated by the SCS or entered manually in the SCS security keys definition. The Intel AMT device uses this password for authentication during Setup and Configuration. Once Setup mode has begun, a management console application can change the Intel AMT device password without modifying the MEBx password.

3. Select **Intel ME Platform Configuration**. A warning message is displayed saying that a reset will occur after configuration is complete.
4. Enter **Y**.
5. Select **Intel ME Features Control**.
6. Select **Manageability Feature Selection**.
7. Select Intel AMT and return to the previous menu.
8. Select the **Intel ME Power Control** menu.

9. Set the following power control settings:
   - Intel ME State upon Initial Power-On = ON
   - Intel ME ON in Host Sleep States = Always
   - Intel ME Visual LED Indicator = ON
10. Return to the previous menu.
11. Exit all menus. The computer will restart.
12. Press **<Ctrl+P>** and enter the Main Menu.
13. Select **Intel AMT Configuration** and press **Enter**. The Intel AMT Release 2.0/2.1 BIOS extension screen is displayed.



Copyright© 2003-2006 Intel Corporation. All Rights Reserved.

[Intel(R) AMT CONFIGURATION]

14. Configure the parameters as described in the following sections.

Host Name

This parameter is set by the SCS.

TCP/IP Settings

The SCS sets the TCP/IP values

SCS Service IP Address (“Provisioning Server”)

By default, the SCS Service IP address is set to 0.0.0.0. A value of 0.0.0.0 means that the Intel AMT device will attempt to obtain the actual IP address of the SCA by performing a DNS lookup for a host named "ProvisionServer". If the DNS is unable to resolve the host name, the IP address of the SCS must be supplied manually. The name ProvisionServer can be configured by an OEM to a different value, so verify the delivered value of this parameter.

By default, port 9971 is used to establish a connection to the SCS. This default may be changed by an OEM. If the SCS has been configured to listen on a different port, then enter the actual port the SCS is listening on.

Setup Type (“Provision Model”)

The default setup type of Intel AMT is Enterprise. The Small Business Setup option is used in environments where infrastructure required for TLS is not available, and configuration can be completed from the BIOS menu. The SCS service does not support Small Business setups.

The Setup Type menu also allows selection of Legacy Mode. In Legacy Mode, Intel AMT Release 2.0/2.1 has the capabilities of Intel AMT Release 1.0. This allows use of third-party products developed to run with Intel AMT Release 1.0.

Virtual Local Area Network (VLAN) Settings

Set by the SCS

PID-PPS

The Provisioning ID (PID) and the Provisioning Pre-Shared Key (PPS) settings are required for establishing secure communication during the Setup and Configuration of Intel AMT Release 2.0/2.1 platforms. These settings are not available for Intel AMT Release 1.0 platforms and for Intel AMT Release 2.0/2.1 platforms configured in Legacy Mode.

The SCS service generates a file of PID-PPS pairs used either for manual installation or for loading onto a USB storage device. To load a PID/PPS pair manually:

1. At the SCS Console, print the values to be installed manually from the security keys screen, and then mark the selected keys as “used” so they will not be installed on more than one platform.
2. At the platform being prepared for configuration, enter the values as prompted when the “Set PID and PPS” menu item is selected.

The PID-PPS pair may have been preloaded by a platform OEM or loaded using a USB storage device. See “Using a USB Storage Device for Factory Mode Setup” on page 56.

The PID and PPS are 64-bit quantities made up of ASCII codes of some combination of characters – capital alphabet characters (A–Z), and numbers (0–9).

The PID is an eight character entry of the form: XXXX-XXXX and is sent in unencrypted format in the “Hello” message.

The PPS is a thirty-two character quantity of the form:

XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX and is a secret shared between the Intel AMT device and the SCA.

Here is an example pair:

PID: 0000-037M

PPS: NKLD-G5DC-RRNQ-E9YZ-ZIJL-7LFL-VJED-69XJ

The firmware checks for checksum characters embedded in the values. The last character of the PID is expected to be a checksum of the previous seven characters, and the fourth character in each group of four characters in the PPS is expected to be a checksum of the previous three characters. This check is made to reduce the possibility of operator error when entering these values. The SDK contains the source code for a function that generates PID/PPS pairs with checksums embedded in them. The sample values above have the correct checksums.

Intel strongly recommends that Intel AMT Release 1.0 platforms be configured on an isolated network to minimize the opportunities for exposing security information, since Setup and Configuration traffic is sent without encryption for these types of platforms. If the Setup and Configuration Service requires access to both a production network and a private isolated network, then equip the server with more than one network interface. One network interface can be used to establish isolated network connections to Intel AMT devices to be configured, and the second network interface can be used to connect to the production network.

Other Settings

The SOL/IDER, Remote Firmware Update and Set PRTC menu options are not required for setup and configuration. The SOL/IDER option enables the Intel AMT device redirection capabilities. The Remote Firmware Update option enables the ability to perform remote updates to the firmware. The Set PRTC allows an Administrator to set the programmable real-time clock to a correct value if the clock lost its value inadvertently in a situation where it could not be reset remotely.

Exit Intel AMT Configuration

Highlight the Return to Previous Menu option and press Enter. Upon exiting the Intel AMT BIOS extension, the Intel AMT device will enter Setup Mode and begin sending “Hello” messages to the SCS service.

“Hello” Message Retry Frequency

The Intel AMT device sends “Hello” messages according to the following algorithm:

- 5 retries on 1 minute intervals
- 5 retries on 10 minute intervals.
- 5 retries on 1 hour intervals.

The retry algorithm will restart after a firmware reset, which requires disconnecting AC power from the platform containing the Intel AMT device.

Using a USB Storage Device for Factory Mode Setup

The Factory mode setup process can be simplified by using a USB key containing a file of PID/PPS pairs and replacement passwords, when the BIOS supports this method. This method can be used for one-touch configuration if all the defaults listed below are suitable for an enterprise installation. Even if additional parameters need to be changed, the USB key can install the PID and PPS without the problem of operator error. Use this method also for preparing platforms for future Intel AMT configuration.

Requirements

The following items are required to be able to use a USB key for Intel AMT device configuration:

- A dedicated USB key with no data on it.
- The function within the SCS service that generates a file of PID/PPS/password triplets in the proper format.
- Good security procedures for controlling the USB key.

Preparation

All that is required is to execute the SCS function, which will do the following:

1. Create a list of PID/PPS/password triplets. (See “Configuring Pre-Setup and Configuration Security Keys” on page 74).
2. Use the export function to create a file to write to the USB key. The SCS automatically formats the key file format to FAT16 and copies the file to the key.

Initializing a Platform

To install the PID/PPS information on an Intel AMT device an Administrator will:

1. Take the platform out of the box and connect cables, a monitor, and a keyboard.
2. Connect the USB key to a USB port.

3. Turn on the platform.

The BIOS on the platform will detect the presence of the USB key, read the next available entry in the file, authenticate the password, save the PID/PPS values, optionally update with the replacement password, and mark the entry on the USB key as "used". A message displayed on the monitor informs the technician that the process is complete. The Administrator powers down the platform.

Moving to Setup Mode

The platform may now be ready for moving to Setup mode, if the default parameters are appropriate for the specific enterprise. The critical defaults are:

- DHCP mode with no domain defined
- Setup and Configuration Service with the default host name and port
- No DNS IP defined (The DHCP server must be configured to provide a DNS IP, which will be required to discover the IP of the Setup and Configuration Server)

If these defaults are acceptable, the platform can now be connected to the network and powered on. Otherwise, the Administrator can power on the platform, enter the MEBx sub-menu and configure additional parameters.

Preparing Intel AMT for Future Configuration

A user may wish to postpone Intel AMT device setup and configuration until a later date. An OEM may supply platforms with a PID-PPS pair already written to the Intel AMT device Flash memory. In this case, the platform may be already prepared for configuration, as described earlier. The OEM will have to securely deliver a file of the PID-PPS pairs to the customer IT organization for use in the setup and configuration process. The import function on the SCS Console Security Keys screen can import such a file. The platform will start sending "Hello" messages as soon as it is powered on and connected to a network. If no SCS server is present to respond to the messages, the platform will have to be disconnected from AC power and then reconnected to start the "Hello" sequence again, as described on page 56.

It is also possible to prepare the Intel AMT-based platform for configuration without entering Setup Mode. Either use a USB storage device, as described above or follow the Factory Mode Setup steps, but under the TCP/IP menu item, select Y at the "Disable Network Interface?" option. Enter a PID-PPS pair as well. When the time comes to configure and enable the Intel AMT device, re-enter the BIOS sub-menu and change the TCP/IP settings to make the network interface operational by responding Y to "Enable Network Interface" and either changing to DHCP or setting the other TCP/IP parameters to valid values.

Chapter 4

INTEL SCS CONSOLE

This section includes

- “SCS Console Overview” on page 59
- “Logging In” on page 61
- “Defining General Parameters” on page 62
- “Configuring Profiles” on page 65
- “Configuring Pre-Setup and Configuration Security Keys” on page 74
- “Configuring Users” on page 76
- “New Intel AMT Systems” on page 79
- “Configuring Existing Intel AMT Devices” on page 82
- “Maintenance Policies” on page 87
- “Intel AMT SCS Console Logs” on page 89

SCS Console Overview

The SOAP API used to query and manage the SCS service is available for ISVs to create their own interface to the SCS. The Intel SCS also includes an implementation of such an interface, a software component with a graphic user interface. This component, called the SCS Console, supports stand-alone operation of Intel SCS. The SCS distribution includes documentation of the API, the WSDLs that define the interface functions, sample applications, and the full source of the SCS console. ISVs can add value to the console and incorporate it into their Management Console products.

The SCS Console works by communicating with the SOAP API. For example, to change the Power Policy in a Profile, the SCS Console first fetches the data from the database using the SOAP API call getProfilePowerPolicy. After the Administrator has set the new policy, the console performs the SOAP API call `setProfilePowerPolicy` to save the changes in the database.

Using the SCS Console for the First time

To use the SCS Console and the SCS for the first time, perform the following steps, as described in sections of this chapter.

1. Configure the Main (SCS) Service settings. Critical settings on this pane include support for Intel AMT Release 1.0 and integration with Active Directory.
2. Add Users who have the appropriate privileges to use and to administer the SCS.
3. Create one or more Profiles with settings for groups of Intel AMT devices. Profile parameters include the administrative username and password, use of TLS and mutual authentication, the certificates and certificate servers to be used, Digest and Kerberos ACL entries.
4. Create entries in the New Intel AMT Systems list for all platforms to be setup and configured.
5. Create keys (PID/PPS/current password/new password sets) to prepare Intel AMT devices for configuration.

There is now adequate information in the SCS database to respond to “Hello” messages automatically.

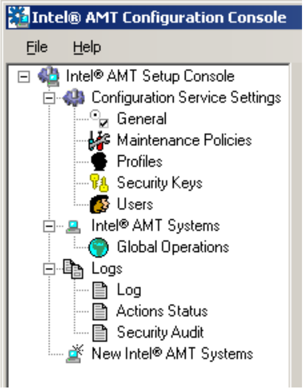
There are two panes on the SCS Console: the Navigation Pane and the Configuration Pane.

Console Navigation Pane

The Navigation pane enables easy access to each of the major subdivisions of the Intel SCS.

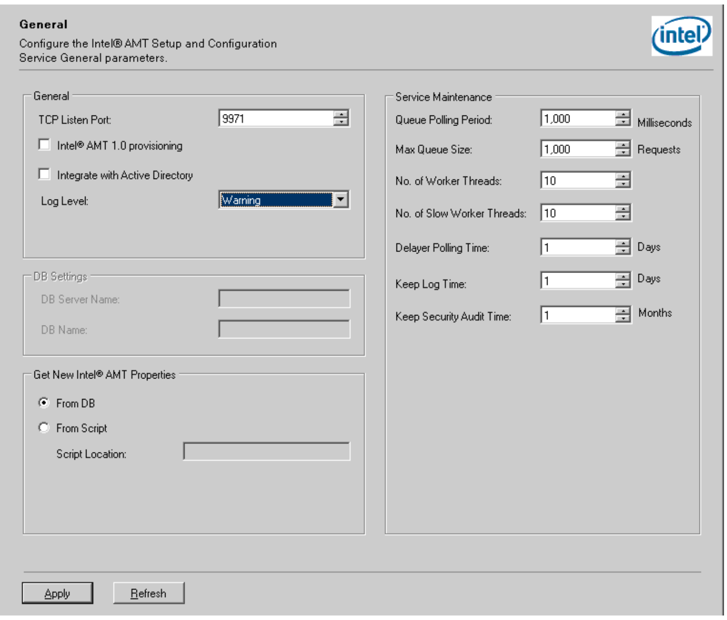
- To view the Configuration Service Settings or the Logs, expand the branch and select a sub-branch.
- To configure new Intel AMT devices, select New Intel AMT Systems.

To review existing Intel AMT devices, select Intel AMT Systems.



Console Configuration Pane

The SCS Console Configuration pane includes standard user interface elements that enable configuration of the Intel SCS. Selecting a sub-branch in the navigation pane opens a configuration pane. For example, selecting Configuration Settings /General opens the General Configuration Pane.



General

Configure the Intel® AMT Setup and Configuration Service General parameters.

General

TCP Listen Port: 9971

□ Intel® AMT 1.0 provisioning

□ Integrate with Active Directory

Log Level: Warning

DB Settings

DB Server Name:

DB Name:

Get New Intel® AMT Properties

● From DB

○ From Script

Script Location:

Service Maintenance

Queue Polling Period: 1,000 Milliseconds

Max Queue Size: 1,000 Requests

No. of Worker Threads: 10

No. of Slow Worker Threads: 10

Delayer Polling Time: 1 Days

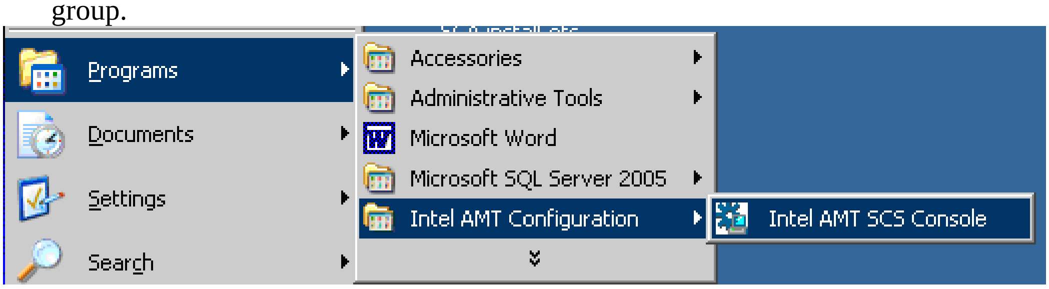
Keep Log Time: 1 Days

Keep Security Audit Time: 1 Months

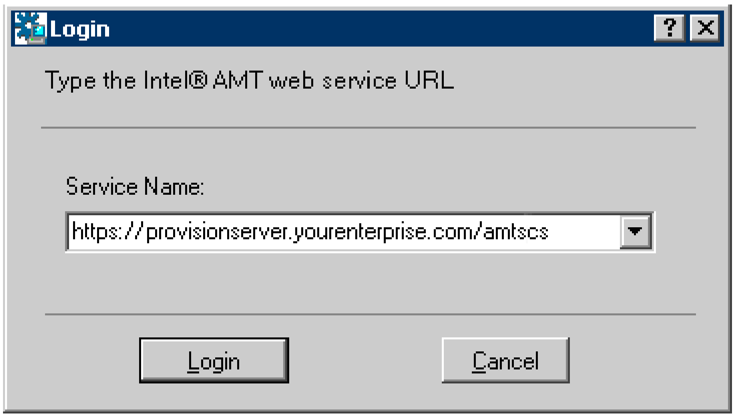
Logging In

To log-in to the Intel SCS Console:

1. Click the Windows Start button to select the Intel AMT **Configuration** program group.



2. Select **Intel AMT SCS Console**. The log-in screen is displayed.



Type the Intel® AMT web service URL

Service Name: https://provisionserver.yourenterprise.com/amtscs

3. Enter the SOAP web service URL path ***including*** the virtual directory. The entry format is:

   `https://FQDN/<Virtual Directory>`

   For example:

   `https://provisionserver.yourenterprise.com/AMTSCS`

   In this example, `provisionserver.yourenterprise.com` is the FQDN of the IIS host of the web service and `AMTSCS` is the virtual directory of soap web service in the IIS host. If the web server expects a port number other than port 80, include the port number after the FQDN. For example,

   `https://provisionserver.yourenterprise.com:123/AMTSCS`

A file named "amtconsole.log" is generated in the console install directory. It contains a log of transactions of the client application.

The Intel SCS Console opens.

If the application does not open, there may be a security problem. See "Secure the Connection to IIS Using SSL" on page 31.

Configuring Main Service Settings

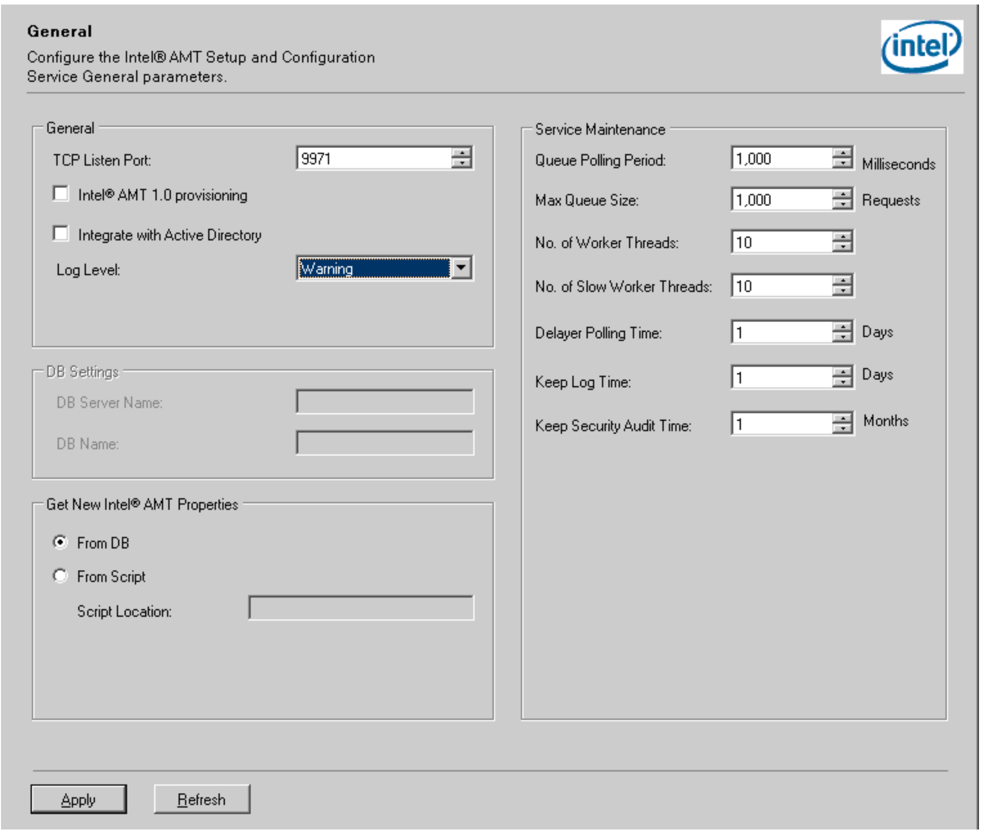
Use the Intel SCS Console to configure, control, and manage the Intel SCS Main Service.

Defining General Parameters

General settings define the configuration of the Intel AMT Main Service. The Intel AMT 1.0 Provisioning and Integrate with Active Directory options can be changed dynamically. All of the other parameters on this pane will not take effect until the SCS service is stopped and restarted.

To configure General settings:

1. Open the AMT Setup and Configuration Console.
2. Expand the **Configuration Service Settings** branch.
3. Select **General**. The General screen is displayed.



General

Configure the Intel® AMT Setup and Configuration Service General parameters.

General

TCP Listen Port: 9971

□ Intel® AMT 1.0 provisioning

□ Integrate with Active Directory

Log Level: Warning

DB Settings

DB Server Name:

DB Name:

Get New Intel® AMT Properties

● From DB

○ From Script

Script Location:

Service Maintenance

Queue Polling Period: 1,000 Milliseconds

Max Queue Size: 1,000 Requests

No. of Worker Threads: 10

No. of Slow Worker Threads: 10

Delayer Polling Time: 1 Days

Keep Log Time: 1 Days

Keep Security Audit Time: 1 Months

4. Define the General parameters:

   ### TCP Listen Port

   Each instance of Intel SCS listens for “Hello” messages from Intel AMT devices on a defined TCP port. Enter the TCP port used for listening. The default port is 9971.

   ### Intel AMT 1.0 Provisioning

   Selecting this checkbox enables the SCS to recognize and configure Intel AMT Release 1.0 devices. Intel AMT Releases 2.0 and 2.1 are backward compatible with Release 1.0. However, Release 1.0 does not support encryption during the initial phases of setup and configuration.

Since the Intel AMT Release 1.0 sends SOAP setup and configuration messages in the clear, setup and configuration of Intel AMT Release 1.0 devices should only be done on an isolated network.

Integrate with Active Directory

Selecting this checkbox will cause the SCS server to add AMT objects to Active Directory. This enables the use of Kerberos authentication and the AD users list.

Log Level

Logs can be recorded at several levels. The more detail recorded, the more system resources and bandwidth must be allocated.

5. Select a **Get New AMT Properties** option. This option determines how the SCS acquires the necessary information defining the Intel AMT device properties.
   - **From DB**
     When this option is selected, properties are acquired only from the New AMT Table stored in the SCS database.
   - **From Script**
     When this option is selected, the SCS first searches the New AMT Table for a matching entry, based on the UUID in the Hello message. If there is no matching entry, the SCS determines the properties by invoking a script written by the controlling enterprise and which either refers to an independent database or file or requests the identifying information from the host platform. See “Using a Script to Import New Intel AMT Properties” on page 102.
   - **Script Location**
     Enter the path to the location of the script **on the platform where the SCS executes**. If there is more than one instance of the service running in the domain, the script must be **in the same location on all platforms** running the service.

Warning: If the script is not in the location defined here, the SCS will not complete setup for any Intel AMT devices.

6. Enter the Service Maintenance parameters. These are the parameters used to tune the performance of the SCS, as described in “Intel AMT SCS Functional Flow” on page 5.

Queue Polling Period

This parameter determines how frequently the Intel SCS checks the queue in the database for new tasks.

Max Queue Size

This parameter sets the maximum permitted length of the database queue. If the queue is full when the server or the API tries to add an additional entry, the entry will be lost.

The following three parameters define quantities for several multithreading transactions that are processed by the Intel SCS.

No. of Worker Threads

This parameter limits the number of Worker Threads permitted simultaneously.

No. of Slow Worker Threads

This parameter limits the number of Slow Worker Threads permitted simultaneously.

Delayer Polling Time

When a process fails, it is sent to the Delayer. A process may fail because information is missing. For example, an Intel AMT device sends a “hello” message before the device has an entry in the New Intel AMT devices list, so there is no profile associated with the device and configuration cannot complete. The Delayer is a thread that manages rerunning delayed processes. This parameter determines how frequently the Delayer attempts to rerun a process.

Keep Log Time

This parameter determines how long log entries are saved.

Keep Security Audit Time

This parameter determines how long security status entries are saved.

7. Click **Apply**.

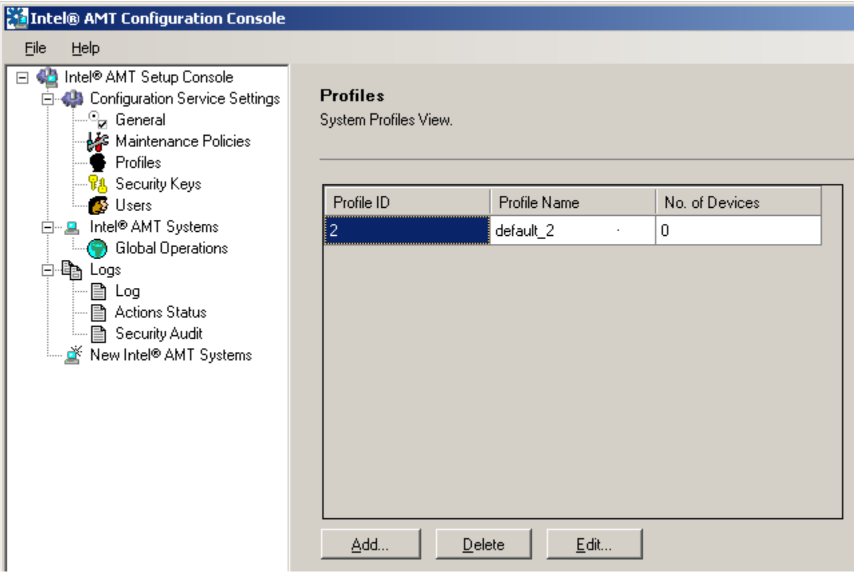
Configuring Profiles

Profiles contain the Intel AMT device configuration parameters. Profiles determine which features are enabled in the device, what authentication mechanism will be used, and which users have access to device features. One or many profiles can be defined. For example, use a different profile for different sites. Each profile can be assigned to one or more Intel AMT devices.

Viewing Existing Profiles

To view existing Profiles:

1. Open the Intel SCS Console.
2. Expand the Configuration Service Settings branch.
3. Select **Profiles**. The Profiles screen is displayed. This screen lists all defined Profiles and the number of devices assigned to each profile.



Profiles

System Profiles View.

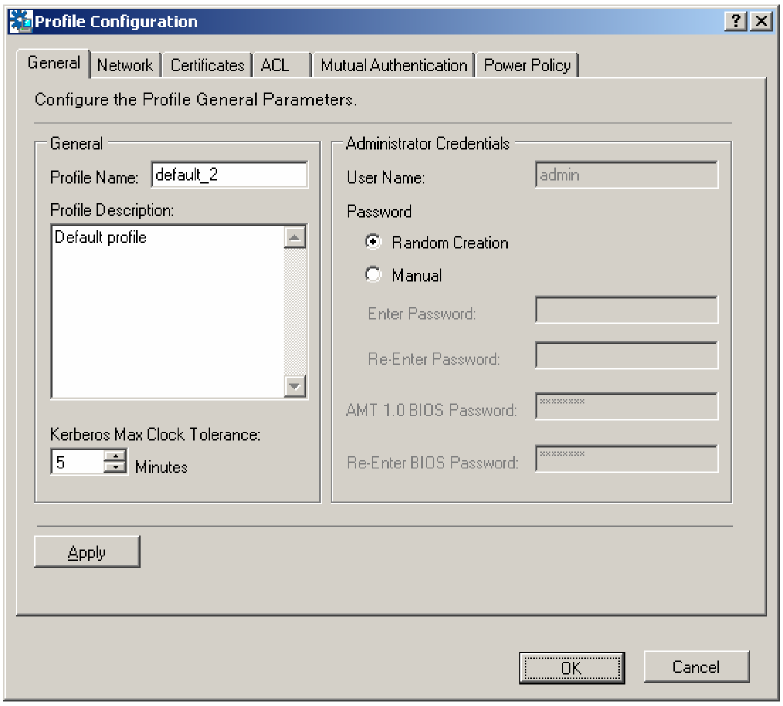
Profile ID	Profile Name	No. of Devices
2	default_2	0

Adding a Profile

1. Open the Intel SCS Console.
2. Expand the **Configuration Service Settings** branch.
3. Select **Profiles**. The Profiles screen is displayed.
4. Click **Add**. The Profile Configuration dialog box is displayed and the General tab is selected.

Each Profile tab is self contained. Changes to a tab require confirmation before moving to another tab. Confirmation is performed by clicking Apply.

The Profile Configuration General Tab



Configure the Profile General Parameters.

General

Profile Name: default_2

Profile Description: Default profile

Kerberos Max Clock Tolerance: 5 Minutes

Administrator Credentials

User Name: admin

Password

● Random Creation

○ Manual

Enter Password:

Re-Enter Password:

AMT 1.0 BIOS Password: ********

Re-Enter BIOS Password: ********

On this tab, enter general information that pertains to this profile.

5. In the General box, enter:

   Profile Name
   Enter a short, descriptive name. This name appears in the Intel AMT devices table.

   Profile Description
   Enter a more complete description of the profile. The description appears in the Profile Details screen.

6. In the Administrator Credentials box, enter:

   User Name
   Enter the Intel AMT administrator user name.

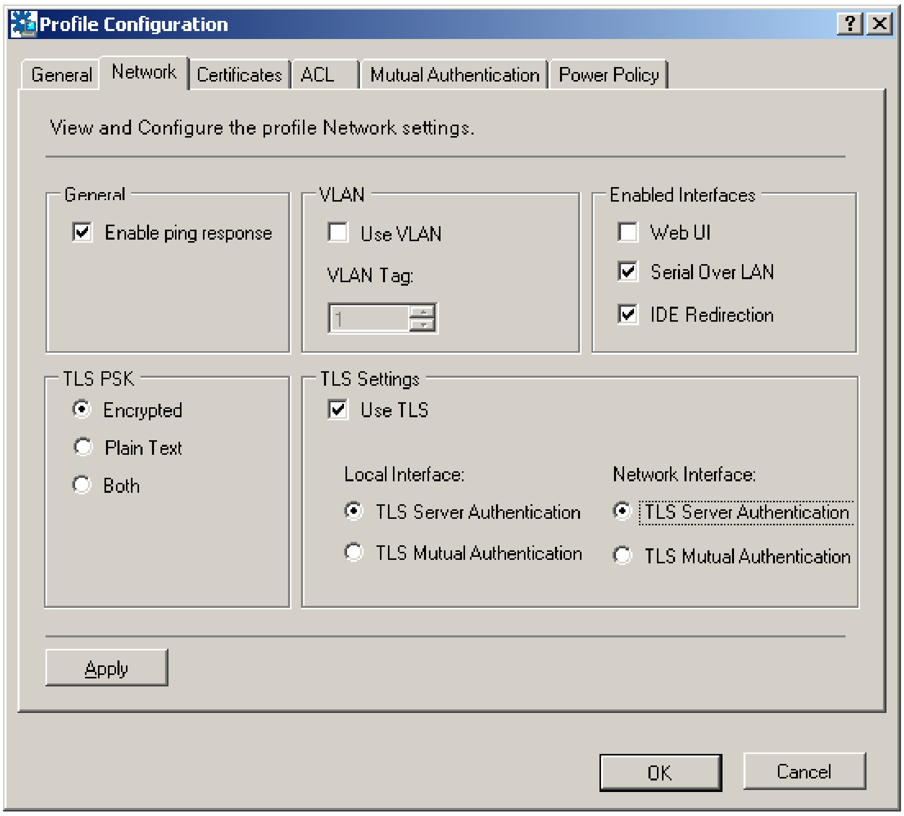
   Password
   Select either Random Creation or Manual. If Manual is selected, enter the password and confirm the entry.
   The above username and password will be the administrative username and password in the Admin ACL entry for all Intel AMT devices configured with this profile. A third-party Management Console application may have a pre-defined username and password for Intel AMT device administration. Those values should be used here. Selecting Random Creation means that only the SCS can use the admin ACL entry for managing the Intel AMT device.

   AMT 1.0 BIOS Password
   If—in the General Settings screen (see page 62)—Intel AMT 1.0 Provisioning is enabled, this password must also be defined. Enter and confirm the entry. The password entered here must be entered via the MEBx on every Intel AMT Release 1.0 platform.

7. Enter Kerberos Max Clock Tolerance—This is the allowable difference between the clock of an Intel AMT device and the timestamp of a received message. This is part of the mechanism used to eliminate “replay” attacks.

8. Click **Apply**.

The Profile Configuration Network Tab



View and Configure the profile Network settings.

General
☑ Enable ping response

VLAN
□ Use VLAN
VLAN Tag: 1

Enabled Interfaces
□ Web UI
☑ Serial Over LAN
☑ IDE Redirection

TLS PSK
● Encrypted
○ Plain Text
○ Both

TLS Settings
☑ Use TLS

Local Interface:
● TLS Server Authentication
○ TLS Mutual Authentication

Network Interface:
● TLS Server Authentication
○ TLS Mutual Authentication

On this tab, define the network settings for this profile.

9. In the **General** box, select or clear the **Enable ping response** checkbox. When enabled, the Intel AMT device will respond to a ping.

10. In the **VLAN** box, select or clear the Use VLAN checkbox. If a VLAN is used, set the **VLAN Tag Integer**, used to distinguish between different VLANs.

Be careful when configuring the VLAN value. If the value is incorrect, the Intel AMT devices will not be accessible.

11. The Intel AMT device includes three special interfaces, or features, that can be enabled or disabled at configuration time. In the **Enabled Interfaces** box, select the checkboxes to activate one or more interface.

    Web UI
    Administrators can use this browser-based interface for management and maintenance of Intel AMT devices.

    Serial Over LAN
    This feature is used to manage an Intel AMT-enabled platform remotely by encapsulating keystrokes and character display data in a TCP/IP stream.

    IDE Redirection
    Use this feature to remotely enable, disable, format or configure individual floppy or IDE CD drives and to reload operating systems and software from remote locations. These actions are independent of and transparent to the host.

12. In the TLS-PSK box, select an option. The **Encrypted** option limits setup and configuration to platforms that support encryption. The **Plain Text** option limits

setup to platforms that do not support encryption. **Both** allows a mix of platforms. Do not select either the **Plain Text** or **Both** options if all platforms containing Intel AMT devices in the enterprise are supposed to support encryption. Use an unencrypted PSK only in cases where Intel® AMT does not support encryption due to import restrictions.

13. In the TLS Settings box, select or clear the **Use TLS** checkbox. When TLS is enabled, the Intel AMT device will require a certificate used to authenticate itself with other applications. If mutual TLS authentication is enabled, then any applications that interact with the device will need to supply certificates that the device will use to authenticate the applications. When Use TLS is selected, configure the interfaces to indicate which will use TLS or mutual TLS or neither. 62

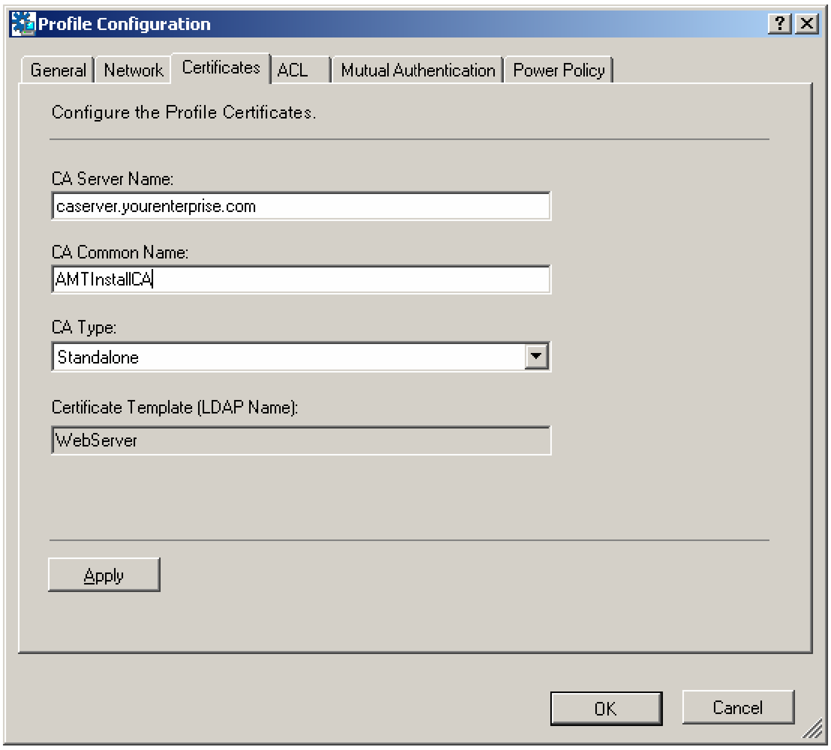
    Local
    When enabled, host communications with the Intel AMT device will require TLS.

    Network
    When enabled, network communications with the Intel AMT device will use TLS.

If the Profile is configured to enable TLS, then the Certificates Tab must also be filled in.

14. Click **Apply**.

The Profile Configuration Certificates Tab



Configure the Profile Certificates.

CA Server Name: caserver.yourenterprise.com

CA Common Name: AMTInstallCA

CA Type: Standalone

Certificate Template (LDAP Name): WebServer

On this tab, enter information pertaining to this profile's Certificates. It provides a path to the Certificate Authority Server and the name used to identify the server.

This tab is grayed out when the Use TLS checkbox (see step 12 on page 62) is cleared.

Applications using the Intel AMT redirection library with TLS require additional steps for authentication with Intel AMT devices to be performed successfully. See "Configuring PEM Files for Redirection Applications" on page 104.

CA Server Name

Enter the FQDN of the computer that handles, stores and issues digital certificates. It is the platform hosting the CA used to generate individual certificates for Intel AMT devices.

CA Common Name

Enter the name of the CA. The name is listed in the CA Administration Manager. Click the Windows **Start** button > **Administrative Tools** > **Certificate Authority**. The name is listed in the first sub-branch in the left pane.

CA Type

Windows Server 2003 Certificate Services supports two types of CAs, Enterprise and Stand-alone. Enterprise CAs are integrated with Active Directory and use information stored in Active Directory. Stand-alone CAs do not require Active Directory but require that all information about the requested certificate type be included in the certificate request.

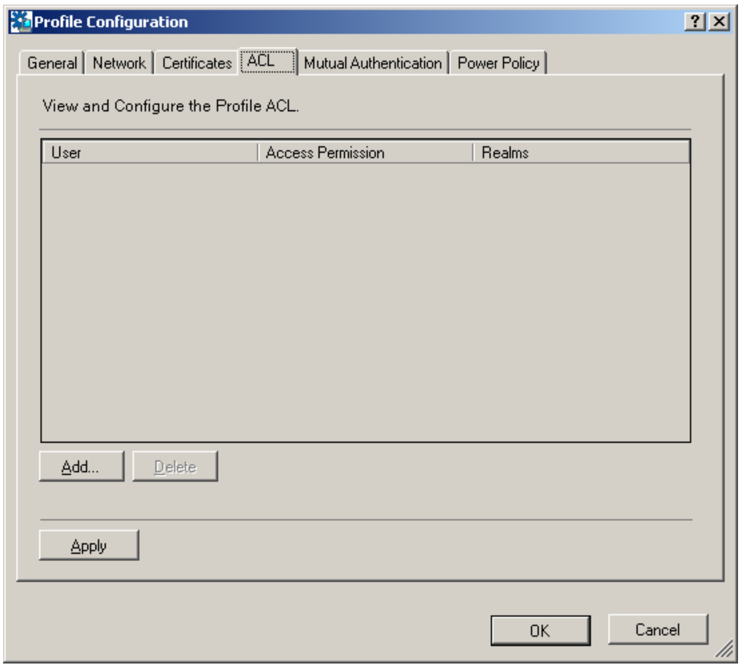
Templates cannot be edited when using a Stand-alone CA. The default template is WebServer.

Certificate Template

When working with an Enterprise CA, enter the name of the Certificate Template to be used. The name must be the LDAP name stored in Active Directory. When the template is displayed using the CA management tools, it is the Template Name and **not** the Template Display Name. A template allows customization of the content of the certificates issued by the Certificate Services. The template defaults to WebServer. If a custom template is defined, the template must support the Server Authentication application policy.

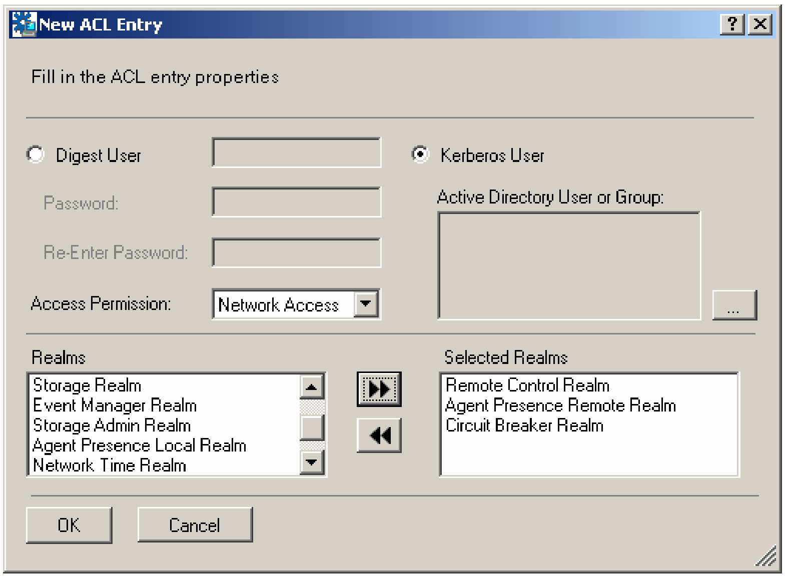
15. Click **Apply**.

The Profile Configuration ACL Tab



Use the ACL (Access Control List) tab to review users already associated with this profile and to add new users and define their access privileges. User identification and realm selection must be coordinated with the requirements and instructions of third-party Management Consoles.

16. Click **Add**. The New ACL Entry dialog box is displayed.



New ACL Entry

Fill in the ACL entry properties

○ Digest User

Password:

Re-Enter Password:

Access Permission: Network Access

● Kerberos User

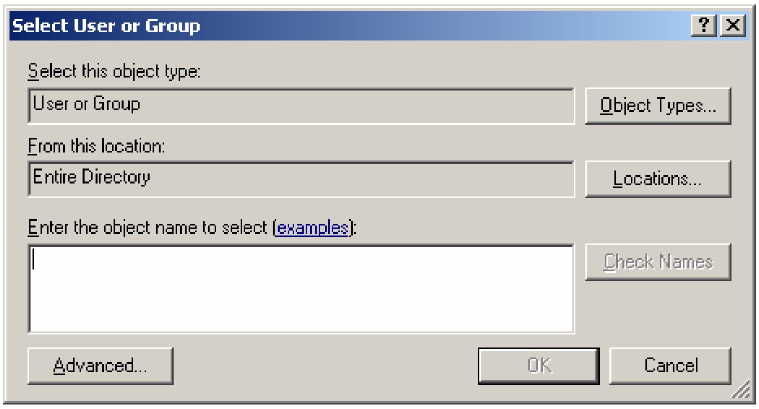
Active Directory User or Group:

Realms:
- Storage Realm
- Event Manager Realm
- Storage Admin Realm
- Agent Presence Local Realm
- Network Time Realm

Selected Realms:
- Remote Control Realm
- Agent Presence Remote Realm
- Circuit Breaker Realm

17. Select one of the following:
    - **Digest User**
      Digest authentication is a password-based authentication. If selected, enter the user name. Then, enter the new password and confirm the entry.
    - **Kerberos User**
      Select this option only if the profile has Active Directory enabled. To complete the entry:

      i. Click the browse button. The Select User dialog box is displayed.



Select User or Group

Select this object type: User or Group

From this location: Entire Directory

Enter the object name to select (examples):

      ii. Enter all or part of a user name. The user must be an individual for Digest ACL entries but can be a Group for a Kerberos ACL entry.

      iii. Click **Check Names**. The Intel SCS searches the AD and completes or confirms the user name.

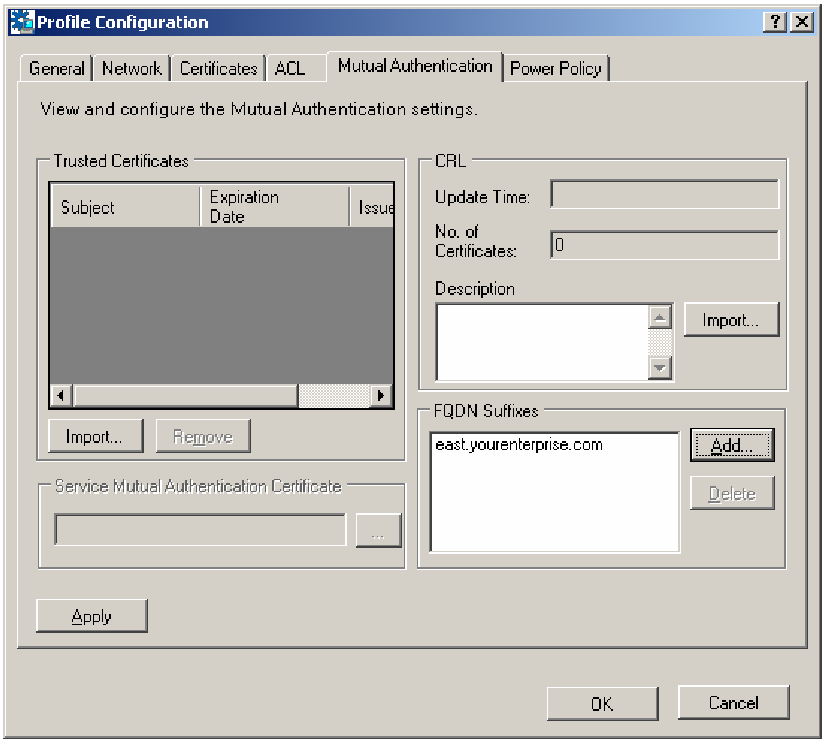
      iv. Click **OK**.

18. Select an **Access Permission**. This parameter defines user access, that is, locations from where the user is allowed to perform an action. A user might be limited to local actions or might also be able to perform actions from the network.
    - **Local Access**
      The user is limited to access to the Intel AMT device via the local host.
    - **Network Access**
      The user can execute an action via the network.

- **Any**
  The user can execute an action both locally or from the network (This option is not recommended).

19. Select the realms—that is, specific functional capabilities such as Redirection or PT Administration—available to this ACL entry.
20. Optionally, add additional ACL entries.
21. Click **OK**.
22. Click **Apply**.

The Profile Configuration Mutual Authentication Tab



View and configure the Mutual Authentication settings.

No. of Certificates: 0

FQDN Suffixes: east.yourenterprise.com

Use the Mutual Authentication tab to configure this profile's two-way authentication settings.

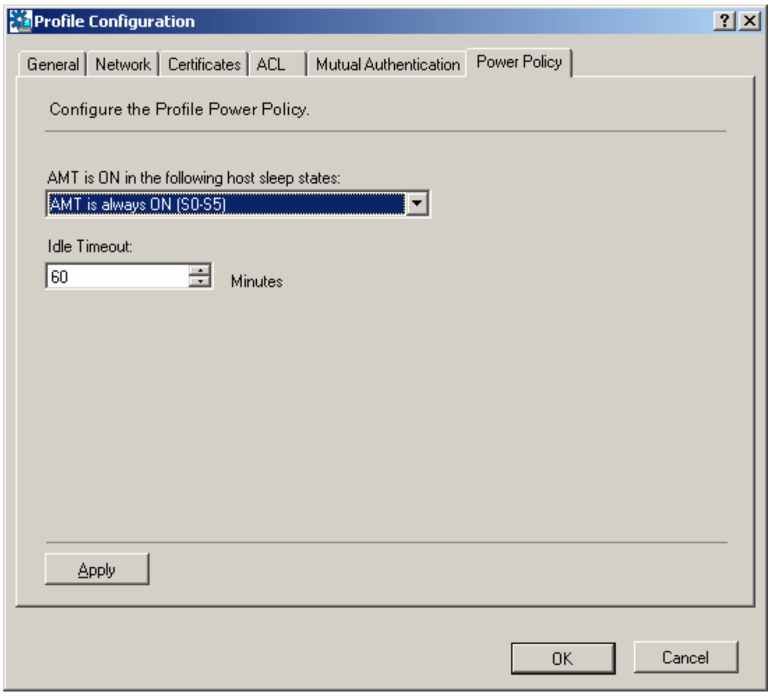
This tab is grayed out when the Use TLS checkbox (see step 12 on page 67) is cleared.

23. In the Trusted Certificates box, click **Import** to add a list of Trusted Root Certificates. These are the issuers of the client certificates that the Intel AMT device will recognize as authentic. These certificates are stored in the database, and then sent to the Intel AMT device during setup and configuration. See "Exporting and Installing the CA Certificate" on page 29.
24. Service Mutual Authentication Certificate This feature is not implemented; the SCS uses the first Intel AMT remote client certificate in the SCS user's personal certificate store (A certificate with the dedicated OID).
25. Import a Certificate Revocation List (CRL). The CRL is a list of entries which indicate which certificates have been revoked. The CRL contains certificate authority URLs and the serial numbers of revoked certificates. See "CRL XML Format" on page 104 for the xml file format.

Enter information about the list into the Description field.

26. Define the Fully Qualified Domain Name suffixes that will be used by mutual authentication. The certificates used must have one of the listed suffixes in the certificate subject.
27. Click **Apply**.

The Profile Configuration Power Policy Tab



Configure the Profile Power Policy.

AMT is ON in the following host sleep states: AMT is always ON (S0-S5)

Idle Timeout: 60 Minutes

Use the Power Policy settings to determine the highest power state (as defined by the ACPI specification) when the Intel AMT devices assigned this profile will be active or will activate from a sleep state. S0 is the normal working state of a computer platform. S1 to S5 are successively deeper sleep states. A platform in S5 is shut down but still connected to AC power.

AMT is ON in the following host sleep states

This parameter defines the highest power state at which Intel AMT will operate while the device is connected to AC power. Note that this includes operation in higher power states. For example, if the platform is in S3 and this parameter is set to **Host is ON (S0)**, the Intel AMT device will not operate until the platform returns to S0.

Idle Timeout

Once the Intel AMT device wakes up and the host system is not turned on, this parameter determines the minimum time (in minutes) that the Intel AMT device will remain operable when there is no activity. The device will return to a sleep state after the idle timeout period. The timeout timer is restarted whenever the device is serving requests. If the value of the parameter is zero, the device will remain on when there is no activity.
For example, the **AMT is ON** parameter is set to **Host is ON (S0) or in Standby (S3)**. When the platform transitions to S3, the Intel AMT device will remain awake until there is no activity for the number of minutes set in the **Idle Timeout**. At that point the device reduces power. Any network access to the Intel AMT device will cause it to wake up and restart the timeout timer. This parameter should be set to 3 minutes at a minimum.

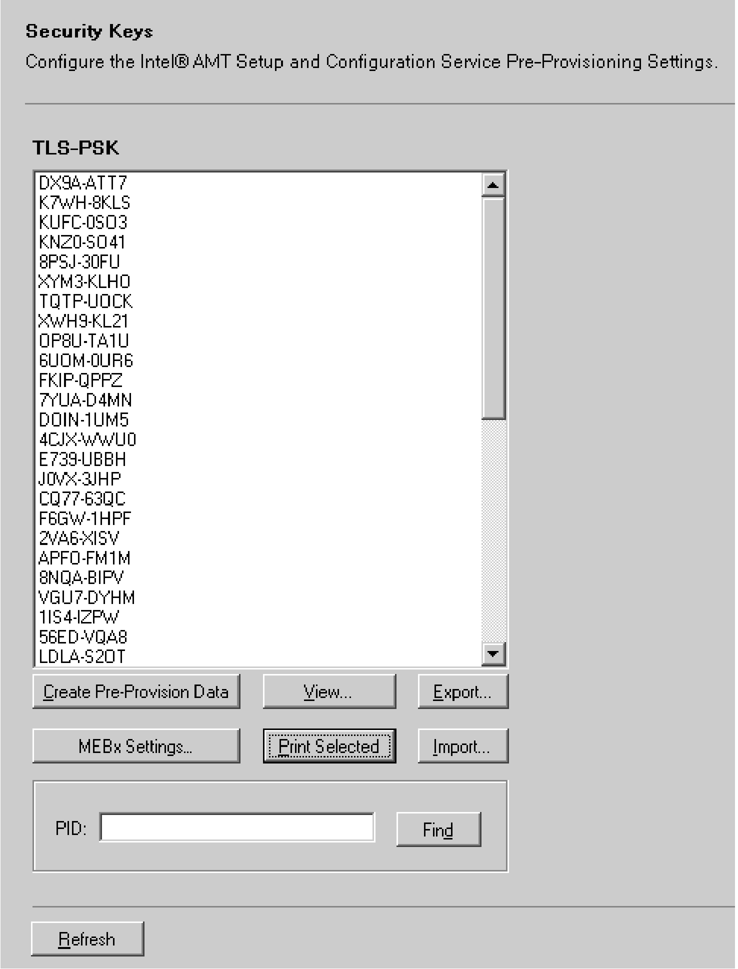
Click **Apply**.

Configuring Pre-Setup and Configuration Security Keys

Setup and configuration of Intel AMT 2.0/2.1 devices is done using the TLS-PSK (Pre-Shared Key) protocol. The protocol requires a security key installed both in the Intel AMT device and in the SCS database. This pane is used to generate the pre-shared keys and associated parameters. Each key has four elements: the key itself (PPS), an identifier sent in the clear by the Intel AMT device in the “Hello” message (called a PID), an initial MEBx password, and a replacement MEBx password. See “PID-PPS” on page 55 for additional information. Sets of these parameters can be exported to a USB key and installed in new Intel AMT devices. Alternately, an OEM may ship platforms with PID/PPS pairs and a default password already installed. In this case, the file from the OEM must be imported into the SCS database. The third option, entering the PID and PPS manually, is also described at the above reference.

To configure the Security Keys:

1. Open the Intel SCS Console.
2. Expand the **Configuration Service Settings** branch.
3. Select **Security Keys**. The Security Keys screen is displayed.
4. Click **Create Pre-Provision data**. Intel SCS creates a list of Security Keys. See the MEBx Settings pane to configure the number of keys generated. Each record consists of an 8 byte PID, a 32 byte PPS and the administrator’s password.



Security Keys

Configure the Intel® AMT Setup and Configuration Service Pre-Provisioning Settings.

TLS-PSK

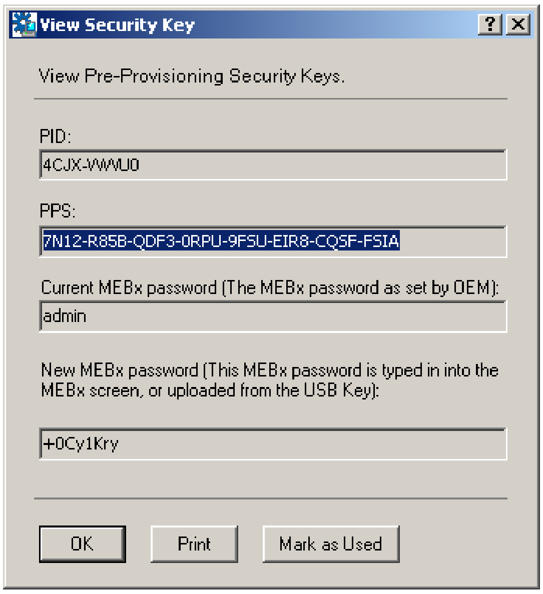
```
DX9A-ATT7
K7WH-8KLS
KUFC-0SO3
KNZ0-SO41
8PSJ-30FU
XYM3-KLHO
TQTP-UOCK
XWH9-KL21
OP8U-TA1U
6UOM-0UR6
FKIP-QPPZ
7YUA-D4MN
DOIN-1UM5
4CJX-WWU0
E739-UBBH
J0VX-3JHP
CQ77-63QC
F6GW-1HPF
2VA6-XISV
APFO-FM1M
8NQA-BIPV
VGU7-DYHM
1IS4-IZPW
56ED-VQA8
LDLA-S2OT
```

5. Select **Export** to write the current list of keys to a file on a USB Key in the format expected by the platform BIOS.
6. Select **Import** to incorporate a file of keys from an OEM into the SCS database.

7. Optionally, to view the details of a particular Security Key, select the Security Key and click **View**.

   This screen is used to print and reserve a single set of security parameters that will be used to configure an Intel AMT device manually:

   First print the parameters using the Print option, then select Mark as Used so that the key will not be used with more than one Intel AMT device.



View Security Key

View Pre-Provisioning Security Keys.

PID:
4CJX-WWU0

PPS:
7N12-R85B-QDF3-0RPU-9FSU-EIR8-CQSF-FSIA

Current MEBx password (The MEBx password as set by OEM):
admin

New MEBx password (This MEBx password is typed in into the MEBx screen, or uploaded from the USB Key):
+0Cy1Kry

The following information is displayed:

PID (Provisioning ID)

The PID is the 8 character identification string sent in the clear in the "Hello" message.

PPS (Provisioning Pre-Shared Key)

The PPS is a 32 character key string that is the secret shared between the Intel AMT device and the SCS service.

Factory Default MEBx Password

The factory default MEBx password is the password assigned when the Intel AMT device is preconfigured, whether by an OEM or from a previous installation. The default value is "admin".

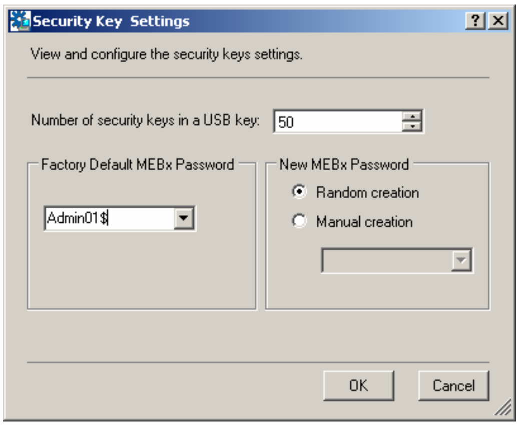
New MEBx Password

The New MEBx password is assigned to the Intel AMT device during setup and configuration.

Print prints the parameters of the single displayed key.

Mark as Used removes the selected key from the visible list. It will remain in the database but will not be exported to a USB Key.

8. To set the passwords, and the maximum number of security keys that can be stored on a single USB key, click **MEBx Settings**.



Security Key Settings

View and configure the security keys settings.

Number of security keys in a USB key: 50

Factory Default MEBx Password: Admin01$

New MEBx Password

● Random creation

○ Manual creation

a. Enter a number in the Number of security keys field.

This number determines the number of keys created by clicking Create Pre-Provision data and how many keys are exported when Export is clicked.

b. Select the factory-assigned OEM password. If it is not in the dropdown list, add it to the list by performing the following steps:

   i. Click within the **Current Password** field. The content is selected.

   ii. Begin typing. The old content disappears but is not deleted.

   iii. Enter the new Current Password.

   iv. Click **OK**. The new OEM MEBx password is added to the list.

c. In the New MEBx Password box, select either Random or Manual. If Manual is selected, enter the new password. This will be the MEBx password after setup and configuration completes.

d. Click **OK**.

Passwords are stored in the Intel AMT table saved in the database.

Configuring Users

The Users list defines identities with access to the Intel SCS Console. Each user is assigned a role which defines the permissions allotted to the user.

When AD is integrated with the SCS and Intel AMT, User identities are imported from Microsoft Active Directory. Otherwise, User identities are added here manually.

A table of users can be added using the AddUser.exe script included in the SCS installation.

Viewing Existing Users

To view a list of existing users:

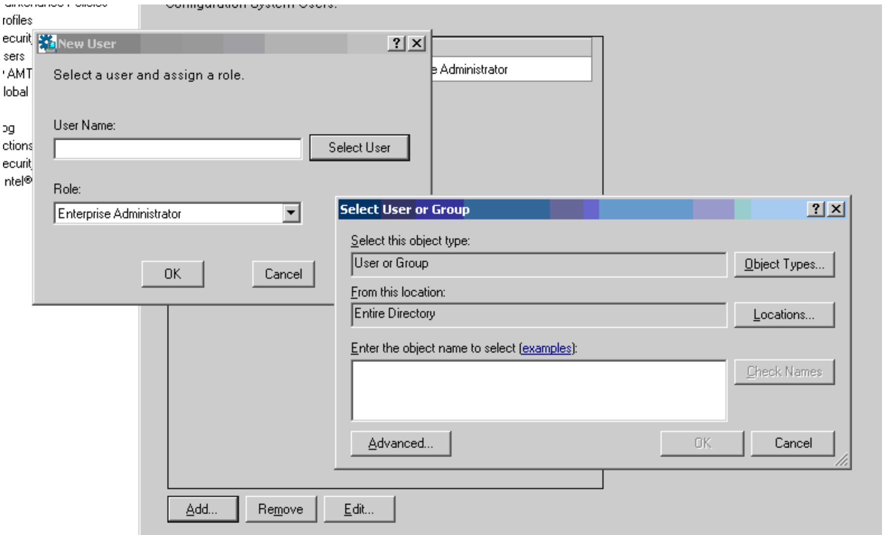
1. Open the Intel SCS Console.
2. Expand the **Configuration Service Settings** branch.

3. Select **Users**. The Users table is displayed.

Adding a User

To add a new user:

1. Open the Intel SCS Console.
2. Expand the **Configuration Service Settings** branch.
3. Select **Users**. The Users table is displayed.
4. Click **Add**. The New User dialog box is displayed.
5. Click **Select User**. The Select dialog box is displayed.

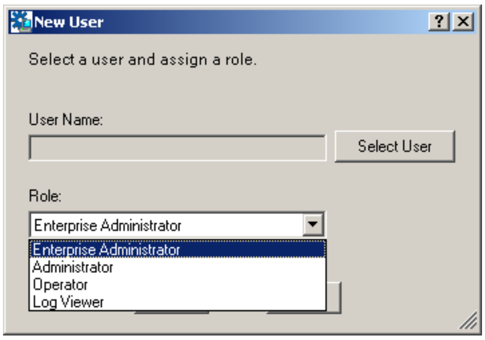


Role: Enterprise Administrator

Select this object type: User or Group

From this location: Entire Directory

6. Enter all or part of a user name.
7. Click **Check Name**. The Intel SCS searches the AD and completes or confirms the user name.
8. Click **OK**.
9. From the Role dropdown menu, select a role:



Role: Enterprise Administrator

Enterprise Administrator

The Enterprise Administrator has access to all Intel SCS Console configuration and management screens, fields, and parameters.

Administrator

The Administrator role has the same permissions as the Enterprise Administer but does not have permission to create or edit Profiles, or access to the Users, General Configuration or Maintenance functions.

Operator

The Operator role has access to the following:

- from the Configuration Service Settings branch, Security Keys:
- from the Intel AMT Systems branch:
    - view the Status table (not implemented in this release)
- the standard Log
- the Security Audit
- the complete New Intel AMT Systems branch

Log Viewer

This role enables a user to view the standard Log and the Security Audit.

10. Click **OK**.

Never remove the user that is used by the SCS service when it is started. Removing this user causes the service to fail.

New Intel AMT Systems

The SCS maintains two lists of Intel AMT devices:

A list of device information entered into the database by the administrator or by external calls to the API. Each entry relates a specific Intel AMT device (defined by its UUID and FQDN) to a Profile and an Active Directory storage location. The SCS Console displays and manages this list with the **New Intel AMT Systems** branch of the tree.

- A list of Intel AMT devices that have sent “Hello” messages to the SCS. These devices may have been configured or not. The administrator can update the configuration of one or all of the already configured devices, among other operations. The console performs these functions and manages the list from the **Intel AMT Systems** branch of the tree.

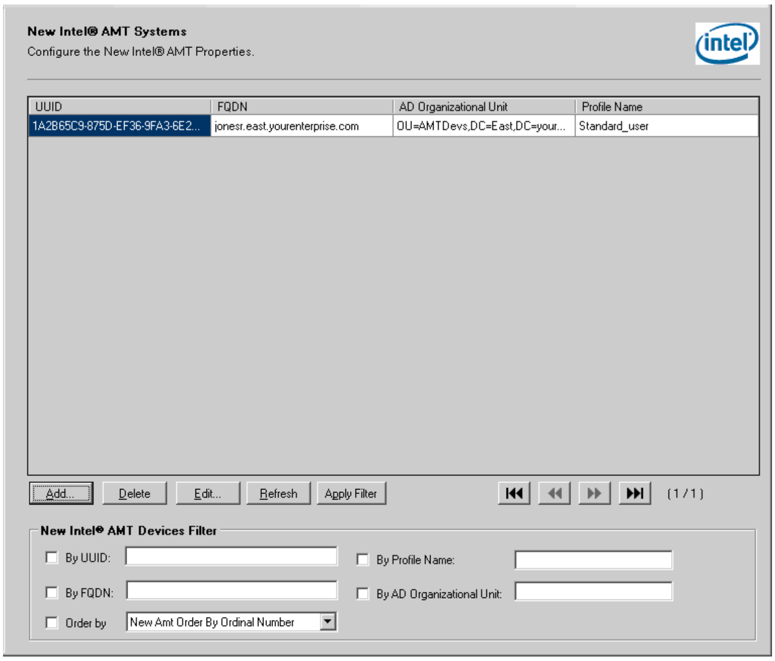
This section describes the New Intel AMT Systems features. The opening screen shows a list of Intel AMT devices that are known to the SCS service. A device must be in the database before it starts sending “Hello” messages, otherwise, the SCS service will not complete device configuration due to the lack of critical setup information.

The SCS may be configured to acquire the necessary Intel AMT device information using a script that executes when the SCS receives a “Hello” message. In this case, entering Intel AMT device parameters using the New Intel AMT Systems is not required.

Viewing Defined Intel AMT Devices

To view a list of Intel AMT Devices already defined in the SCS database:

1. Open the Intel SCS Console.
2. Select **New Intel AMT Systems**. The New Intel AMT Systems table is displayed.



New Intel® AMT Systems

Configure the New Intel® AMT Properties.

UUID	FQDN	AD Organizational Unit	Profile Name
1A2B65C9-875D-EF36-9FA3-6E2...	jonesr.east.yourenterprise.com	OU=AMTDevs,DC=East,DC=your...	Standard_user

New Intel® AMT Devices Filter

□ By UUID:

□ By Profile Name:

□ By FQDN:

□ By AD Organizational Unit:

□ Order by New Amt Order By Ordinal Number

The UUID is a unique value for a specific Intel AMT device. The FQDN (Fully Qualified Domain Name) is the combination of host name and domain that is unique for the platform containing the device. The Active Directory Organizational Unit determines where the AMT object for this device should be placed in the directory system. The profile name is the profile to be used to configure this device.

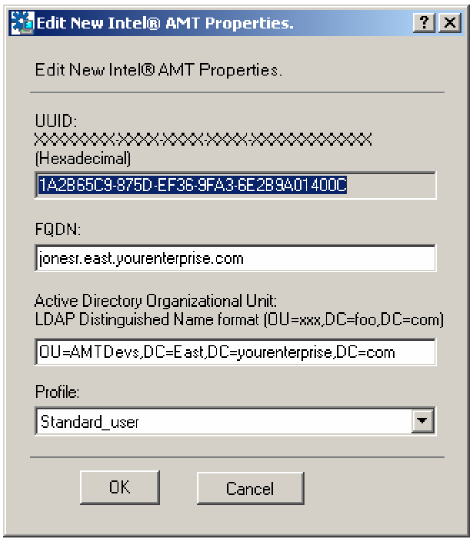
3. To filter the view, select a filter options from the bottom of the screen and click **Apply Filter**.

Defining a New AMT Record

When the AddServicNewAmtProperties.exe program is included in a platform initial configuration script, it can be used to create an entry in the SCS database without additional operator intervention. Use the console to add devices one by one.

To add a new AMT Device:

1. Open the Intel SCS Console.
2. Select **New Intel AMT Systems**. The New Intel AMT Systems table is displayed.
3. Click **Add**. The New AMT Device Properties dialog box is displayed.



Edit New Intel® AMT Properties.

UUID:
XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX
(Hexadecimal)
1A2B65C9-875D-EF36-9FA3-6E2B9A01400C

FQDN:
jonesr.east.yourenterprise.com

Active Directory Organizational Unit:
LDAP Distinguished Name format (OU=xxx,DC=foo,DC=com)
OU=AMTDevs,DC=East,DC=yourenterprise,DC=com

Profile:
Standard_user

4. Enter the parameters.

   UUID
   This is the 128-bit value represented as a hexadecimal string that uniquely identifies an Intel AMT device.

   FQDN (Fully Qualified Domain Name)
   Enter the combined host name and the domain where the platform will be installed.

   Active Directory Organizational Unit
   The AD element where the AMT object will be located after setup and configuration is completed. A value must be entered for this parameter even if Active Directory use is not enabled. If use of Active Directory is possible in the future, select values for this field that will be usable with the AD deployment.

   Profile
   Enter the profile to be used for this device.

5. Click **OK**.

Filtering the Display

The display of potential Intel AMT devices can be filtered. When filtered, only devices that match the specific filtering criteria are displayed.

To filter the display:

1. Select one or more of the checkboxes.
2. As applicable, either select an entry from the dropdown list or complete the entry in the available field.
3. Click **Apply Filter**.

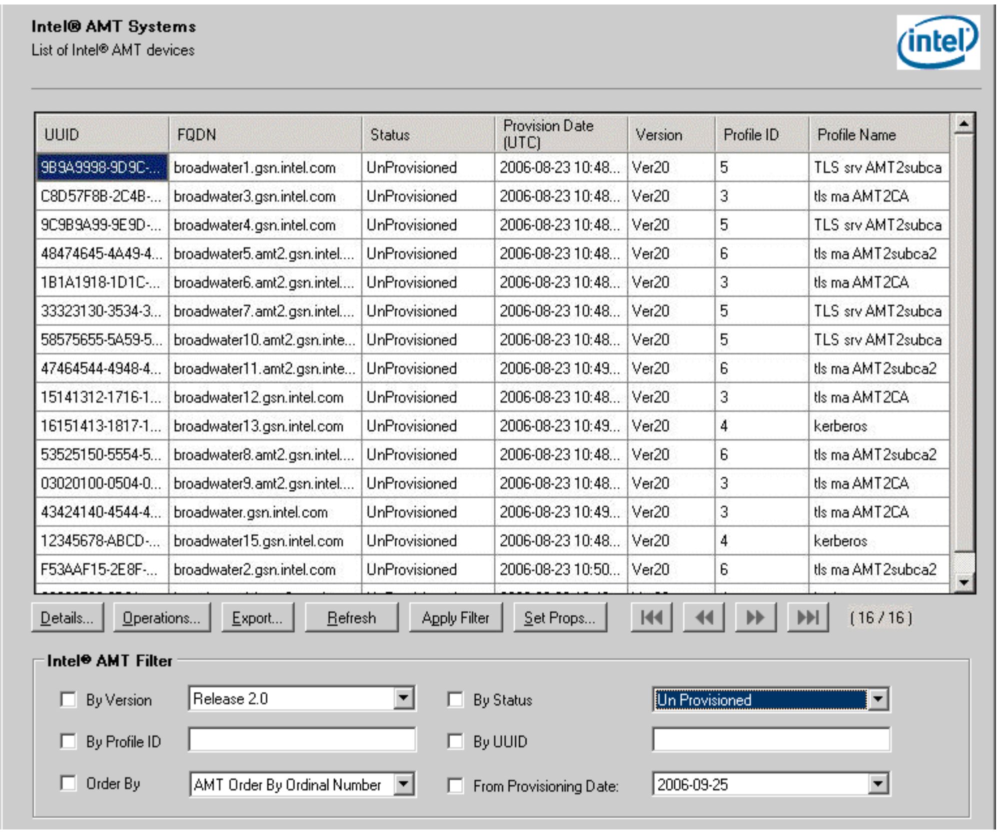
Configuring Existing Intel AMT Devices

Use the Intel AMT Devices screen to view the status of all Intel AMT devices that have sent "Hello" message to the SCS, review details about a single Intel AMT device, and configure an individual Intel AMT device.

Viewing AMT Devices and Reviewing the Details of a Device

To view a list of existing Intel AMT devices:

1. Open the Intel SCS Console.
2. Select **Intel AMT Systems**. The Intel AMT Systems table is displayed.



Intel® AMT Systems

List of Intel® AMT devices

UUID	FQDN	Status	Provision Date (UTC)	Version	Profile ID	Profile Name
9B9A9998-9D9C-...	broadwater1.gsn.intel.com	UnProvisioned	2006-08-23 10:48...	Ver20	5	TLS srv AMT2subca
C8D57F8B-2C4B-...	broadwater3.gsn.intel.com	UnProvisioned	2006-08-23 10:48...	Ver20	3	tls ma AMT2CA
9C9B9A99-9E9D-...	broadwater4.gsn.intel.com	UnProvisioned	2006-08-23 10:48...	Ver20	5	TLS srv AMT2subca
48474645-4A49-4...	broadwater5.amt2.gsn.intel....	UnProvisioned	2006-08-23 10:48...	Ver20	6	tls ma AMT2subca2
1B1A1918-1D1C-...	broadwater6.amt2.gsn.intel....	UnProvisioned	2006-08-23 10:48...	Ver20	3	tls ma AMT2CA
33323130-3534-3...	broadwater7.amt2.gsn.intel....	UnProvisioned	2006-08-23 10:48...	Ver20	5	TLS srv AMT2subca
58575655-5A59-5...	broadwater10.amt2.gsn.inte...	UnProvisioned	2006-08-23 10:48...	Ver20	5	TLS srv AMT2subca
47464544-4948-4...	broadwater11.amt2.gsn.inte...	UnProvisioned	2006-08-23 10:49...	Ver20	6	tls ma AMT2subca2
15141312-1716-1...	broadwater12.gsn.intel.com	UnProvisioned	2006-08-23 10:48...	Ver20	3	tls ma AMT2CA
16151413-1817-1...	broadwater13.gsn.intel.com	UnProvisioned	2006-08-23 10:49...	Ver20	4	kerberos
53525150-5554-5...	broadwater8.amt2.gsn.intel....	UnProvisioned	2006-08-23 10:48...	Ver20	6	tls ma AMT2subca2
03020100-0504-0...	broadwater9.amt2.gsn.intel....	UnProvisioned	2006-08-23 10:48...	Ver20	3	tls ma AMT2CA
43424140-4544-4...	broadwater.gsn.intel.com	UnProvisioned	2006-08-23 10:49...	Ver20	3	tls ma AMT2CA
12345678-ABCD-...	broadwater15.gsn.intel.com	UnProvisioned	2006-08-23 10:48...	Ver20	4	kerberos
F53AAF15-2E8F-...	broadwater2.gsn.intel.com	UnProvisioned	2006-08-23 10:50...	Ver20	6	tls ma AMT2subca2

Intel® AMT Filter

□ By Version: Release 2.0

□ By Status: Un Provisioned

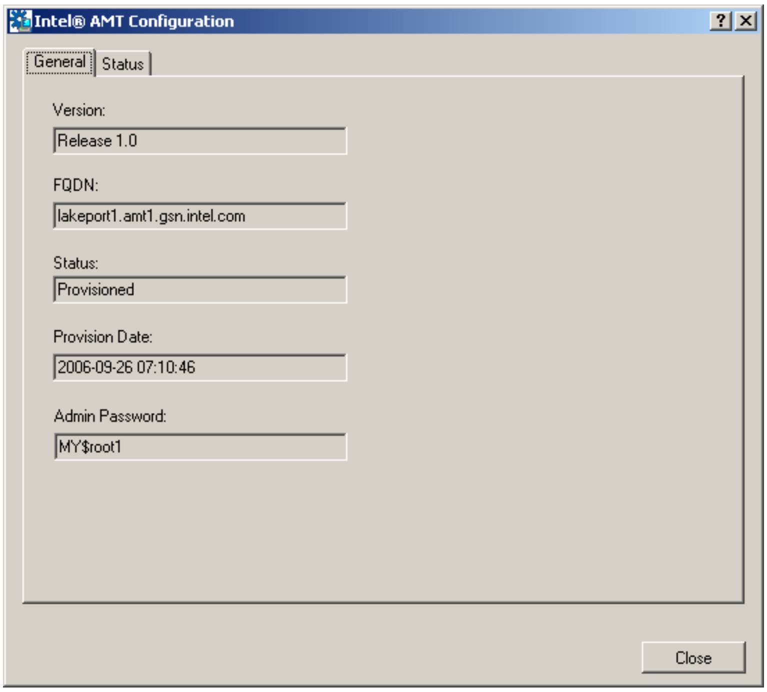
□ By Profile ID:

□ By UUID:

□ Order By: AMT Order By Ordinal Number

□ From Provisioning Date: 2006-09-25

3. Optionally, to review specific details about a devices configuration, select a device and click **Details**. The Details screen has two tabs (see below). The General pane shows basic information for the Intel AMT device, while the Status pane show the last time that certain functions were performed on the device.



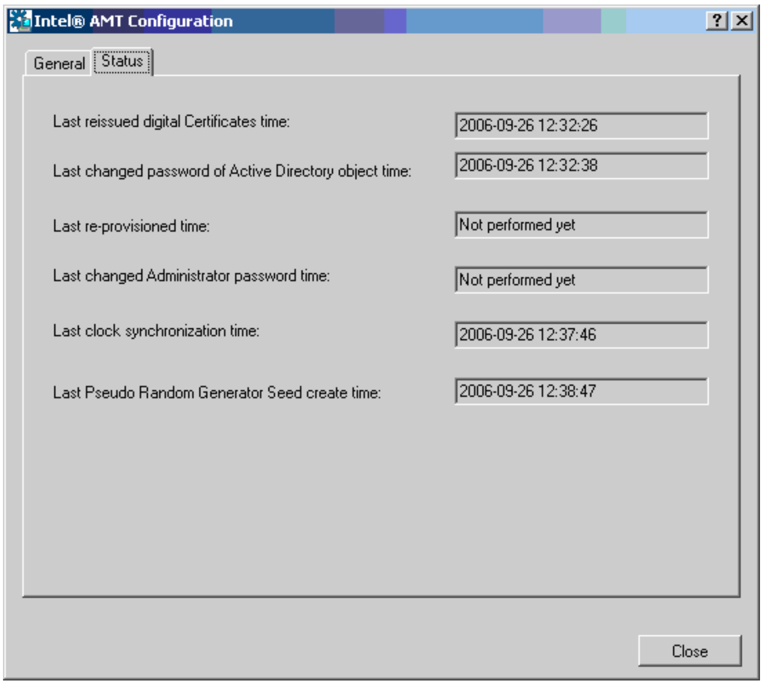
Version:
Release 1.0

FQDN:
lakeport1.amt1.gsn.intel.com

Status:
Provisioned

Provision Date:
2006-09-26 07:10:46

Admin Password:
MY$root1



Last reissued digital Certificates time: 2006-09-26 12:32:26

Last changed password of Active Directory object time: 2006-09-26 12:32:38

Last re-provisioned time: Not performed yet

Last changed Administrator password time: Not performed yet

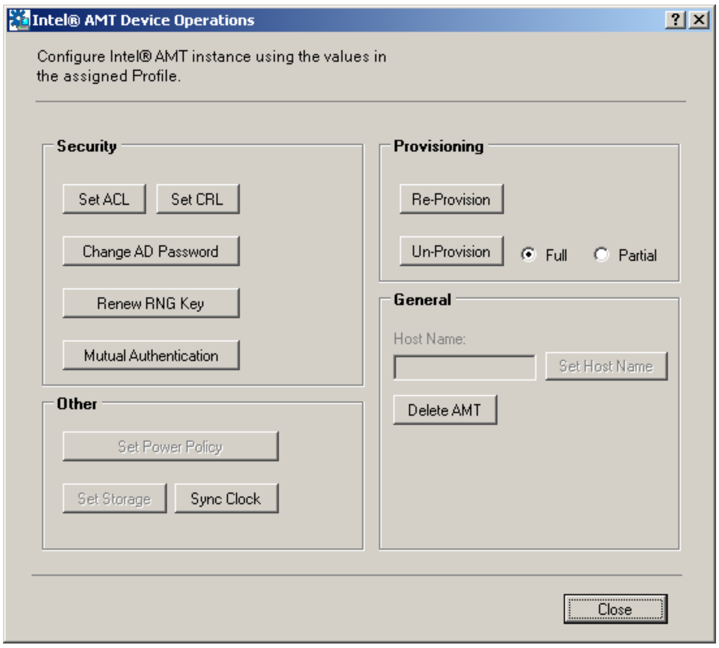
Last clock synchronization time: 2006-09-26 12:37:46

Last Pseudo Random Generator Seed create time: 2006-09-26 12:38:47

Ad Hoc Operations on an Individual Intel AMT Device

To configure a single, existing Intel AMT device:

1. Open the Intel SCS Console.
2. Select Intel AMT **Systems**. The Intel AMT Systems table is displayed.
3. Select a device and click **Operations**. The Operations screen is displayed.



Configure Intel® AMT instance using the values in the assigned Profile.

● Full ○ Partial

4. To perform an operation, click a button.

Re-Provision

This operation applies all the current settings in the profile associated with the Intel AMT device.

Un-Provision

This operation disables the Intel AMT device and leaves it without any Setup and Configuration parameters. There are two modes:

- Full unprovisioning:
  Deletes all data from the Intel AMT device. The Intel AMT device is not functional.
- Partial unprovisioning:
  Deletes all data on every Intel AMT device except for the PID, PPS, admin ACL settings, host name, domain name, and provisioning server IP and port number. The device will immediately start sending “Hello” messages. The SCS will setup and configure the device according to the profile associated with it.

Set ACL

This operation updates the list of Intel AMT users—according to the ACL entries in the profile—and their access privileges. See also “The Profile Configuration ACL Tab” on page 70.

Set CRL

This operation updates the list of revoked certificates.

Change AD Password

Normally, AD includes a policy requiring that AD objects change their password after a configured number of days. If the Administrator does not change the AD password, AD will ignore the AMT object.

Renew RNG Key

This operation replaces the random number generator seed.

Mutual Authentication

This operation sets the mutual authentication parameters in an Intel AMT device. See also “The Profile Configuration Mutual Authentication Tab” on page 72.

Set Power Policy

This operation updates the power policy according to the parameters defined in the profile. See also “The Profile Configuration Power Policy Tab” on page 73.

Sync Clock

This operation synchronizes the clocks between the Intel AMT device and the SCS service.

Delete AMT

This operation deletes the selected Intel AMT device from the database. A warning message is displayed which requires confirmation of intent to delete.

Filtering the Display

The display of existing Intel AMT devices can be filtered. When filtered, only Intel AMT devices that match the specific filtering criteria are displayed.

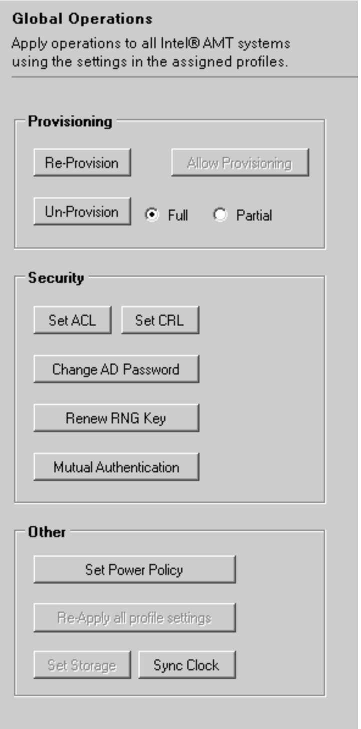
To filter the display:

1. Select one or more of the checkboxes.
2. As applicable, either select an entry from the dropdown list or complete the entry in the available field.
3. Click **Apply Filter**.

Global Operations

To apply new settings to all existing Intel AMT devices:

1. Open the Intel SCS Console.
2. Expand the Intel AMT **Systems** branch.
3. Select **Global Operations**. The Global Operations page is displayed.



Global Operations

Apply operations to all Intel® AMT systems using the settings in the assigned profiles.

Un-Provision: ● Full ○ Partial

4. To perform an operation, click a button.

Re-Provision

This operation applies all the current settings in the profile associated with each Intel AMT device.

Un-Provision

This operation disables each Intel AMT device and leaves it without any Setup and Configuration parameters. There are two modes:

- Full unprovisioning:
  Deletes all data from each Intel AMT device. The Intel AMT devices are not functional.
- Partial unprovisioning:
  Deletes all data on every Intel AMT device except for the PID, PPS, admin ACL settings, host name, domain name, and provisioning server IP and port number. The devices will immediately start sending “Hello” messages. The SCS will setup and configure the devices according to the profiles associated with them.

Set ACL

This operation updates the list of Intel AMT users—according to the ACL entries in the profile associated with each device—and their access privileges. See also “The Profile Configuration ACL Tab” on page 70.

Set CRL

This operation updates the list of revoked certificates.

Change AD Password

This operation will update the password on all AMT objects in Active Directory. Normally, AD includes a policy requiring that AD objects change their password after a configured number of days. If the Administrator does not change the AD password, AD will ignore the AMT object.

Renew RNG Key

This operation resets the random number generator key for each device.

Mutual Authentication

This operation updates the mutual authentication parameters for all devices. See also “The Profile Configuration Mutual Authentication Tab” on page 72.

Set Power Policy

This operation updates the power policy for all devices according to the parameters defined in the profiles. See also “The Profile Configuration Power Policy Tab” on page 73.

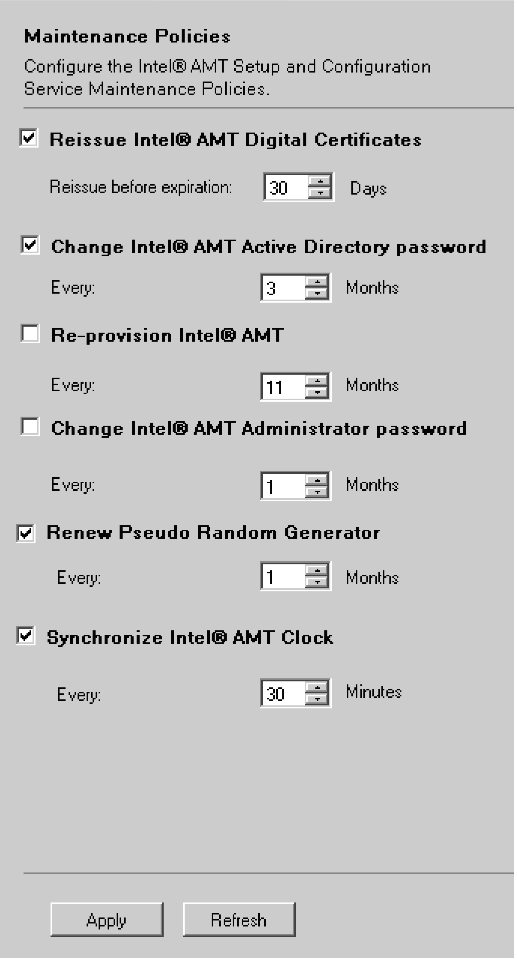
Sync Clock

This operation synchronizes the clocks of the Intel AMT devices with the SCS service.

Maintenance Policies

The Maintenance Policies pane defines actions that the SCS will perform periodically on all configured Intel AMT devices. The items enabled with a checkbox can be used to implement a specific site security policy.

If TLS is not enabled, maintenance messages to the Intel AMT devices are sent in the clear, without encryption. It is recommended that in non-TLS environments, passwords for the AMT objects in Active Directory should be configured as "Password Never Expires". The maintenance function should be used only to synchronize the Intel AMT clock.



Maintenance Policies

Configure the Intel® AMT Setup and Configuration Service Maintenance Policies.

☑ **Reissue Intel® AMT Digital Certificates**

Reissue before expiration: 30 Days

☑ **Change Intel® AMT Active Directory password**

Every: 3 Months

□ **Re-provision Intel® AMT**

Every: 11 Months

□ **Change Intel® AMT Administrator password**

Every: 1 Months

☑ **Renew Pseudo Random Generator**

Every: 1 Months

☑ **Synchronize Intel® AMT Clock**

Every: 30 Minutes

Reissue Intel AMT Digital Certificates

If this item is checked, a new certificate will be requested from the Certificate Authority and updated on each Intel AMT device before the current certificate expires.

Change Intel AMT Active Directory Password

This option automatically changes the password of each AMT object in Active Directory. The SCS then updates the associated Intel AMT device with the new value.

Re-provision Intel AMT

When this option is selected, the SCS will apply all the current settings in the profile associated with each Intel AMT device according to the defined interval.

Change Intel AMT Administrator Password

The administrative user has access to all functions of the Intel AMT device. Only the SCS has access to this ACL entry. When this option is selected, the administrative password is changed periodically to either a randomly-generated password or to a fixed password. The option used is defined on the Profiles Configuration General Tab for the profile associated with each Intel AMT device. Normally, this maintenance function is used only with the random password option.

Renew Pseudo Random Generator

When this option is selected, the SCS generates and sends a new random number generator seed to each Intel AMT device.

Synchronize Intel AMT Clock

This option synchronizes the clock in each Intel AMT device to the clock on the SCS platform. This operation is critical when using Kerberos authentication. It ensures that the clocks do not differ by more than the Kerberos Max Clock Tolerance defined in the Profiles.

Intel AMT SCS Console Logs

The Intel AMT Console logs activity into the database. There are three log categories:

System Log

This log displays system wide actions. This includes actions that succeeded and actions that failed. In particular, this log highlights failed actions. It also displays security entries.

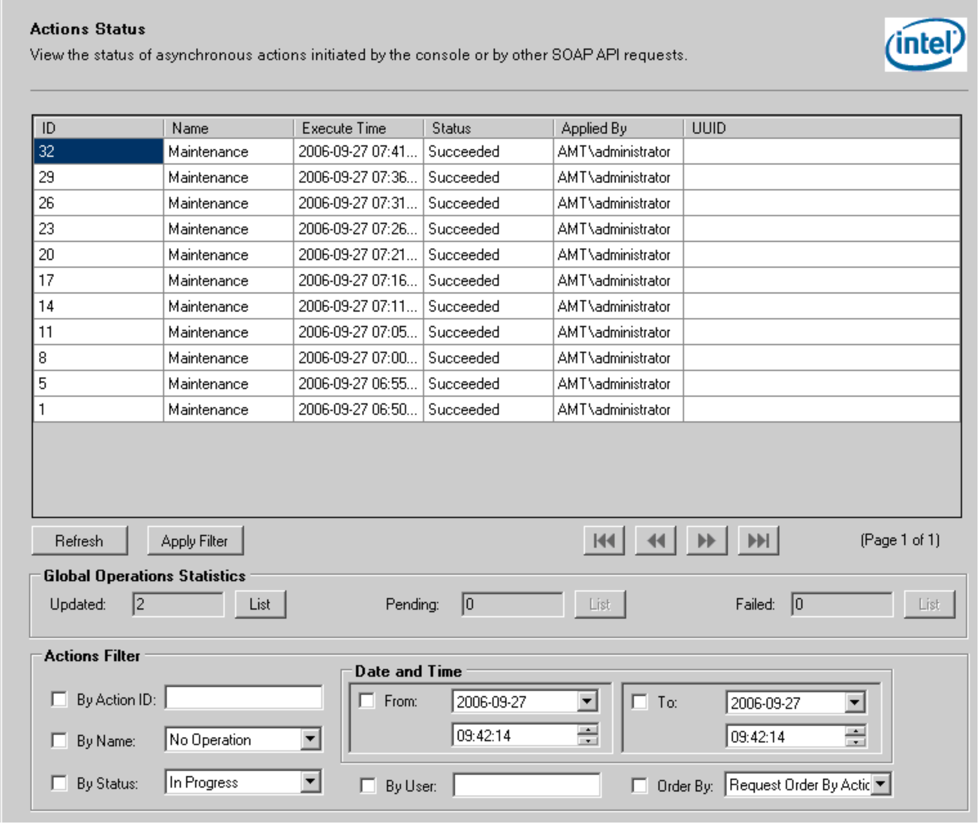
Action Status

This log displays asynchronous actions—such as global operations or operations per Intel AMT device—that are entered into the queue. Their status in the queue is also displayed. The Name field shows the attempted action, the Status field shows success or failure or whether an action is queued, delayed or in progress.

Security Audit

This log displays potential breaches in security, such as unauthorized attempts to log-in and unauthorized attempts to perform the re-provision function on all Intel AMT devices.

The following is an example of the Action Status log display:



Actions Status

View the status of asynchronous actions initiated by the console or by other SOAP API requests.

ID	Name	Execute Time	Status	Applied By	UUID
32	Maintenance	2006-09-27 07:41...	Succeeded	AMT\administrator	
29	Maintenance	2006-09-27 07:36...	Succeeded	AMT\administrator	
26	Maintenance	2006-09-27 07:31...	Succeeded	AMT\administrator	
23	Maintenance	2006-09-27 07:26...	Succeeded	AMT\administrator	
20	Maintenance	2006-09-27 07:21...	Succeeded	AMT\administrator	
17	Maintenance	2006-09-27 07:16...	Succeeded	AMT\administrator	
14	Maintenance	2006-09-27 07:11...	Succeeded	AMT\administrator	
11	Maintenance	2006-09-27 07:05...	Succeeded	AMT\administrator	
8	Maintenance	2006-09-27 07:00...	Succeeded	AMT\administrator	
5	Maintenance	2006-09-27 06:55...	Succeeded	AMT\administrator	
1	Maintenance	2006-09-27 06:50...	Succeeded	AMT\administrator	

(Page 1 of 1)

Global Operations Statistics

Updated: 2   Pending: 0   Failed: 0

Actions Filter

☐ By Action ID:

☐ By Name: No Operation

☐ By Status: In Progress

Date and Time

☐ From: 2006-09-27 09:42:14

☐ To: 2006-09-27 09:42:14

☐ By User:

☐ Order By: Request Order By Actic

Filtering a Log Display

The Log Displays can be filtered. When filtered, only log entries that match the specific filtering criteria are displayed.

To filter the display:

1. Select one or more of the checkboxes.
2. As applicable, either select an entry from the dropdown list or complete the entry in the available field.
3. Click **Apply Filter**.

The filtering capability is especially useful with the Action Status log. The administrator can view recently configured Intel AMT devices, or which ones are queued to be configured or which ones failed configuration and require manual action.

Chapter 5

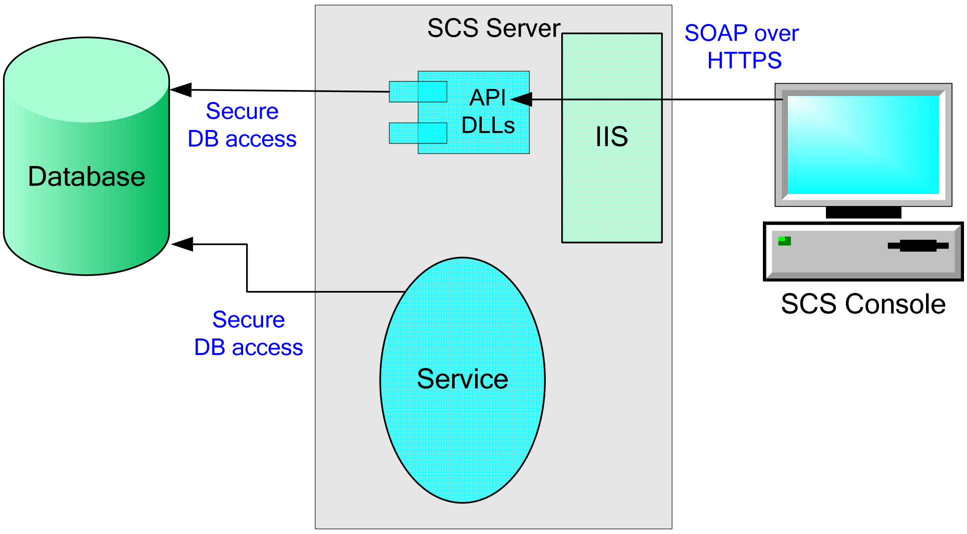
SOAP API

This section includes

- “Client Samples” on page 93
- “SOAP Faults” on page 96

Overview of the SOAP API

The SCS service receives a stimulus from Intel AMT devices sending “Hello” messages requesting that they be configured. The SCS service polls and updates the database and Active Directory. An external application such as the SCS Console configures the service indirectly by sending SOAP requests via the SOAP API to modify or query the database. The SOAP API does not interact with the SCS service directly.



An ISV-developed Management Console can also use the SOAP API for platform discovery: It can query the SCS database for a list of configured Intel AMT devices or a list of those devices configured recently.

The API is implemented with three .dll files that are installed on the same platform as the SCS service. An application addresses the API with SOAP requests addressed to the IIS web server virtual directory, in this case AMTSCS, requests are directed to the appropriate API dll.

The API functions are segmented into four groups, and each group has a WSDL that defines the parameters of each function within the group.

The groups are:

- **Authentication Interface**: Used to log in, define users, and set database parameters
- **Profile Interface**: Manages Profile objects in the database
- **AMT Interface**: Manages AMT System objects in the database
- **Service Interface**: manages all other SCS service functions

The SCS distribution includes the four WSDLs, the SOAP API description document *Configuration Service SOAP API.doc* and the Console source code, contained in AMTConsoleSln.zip.

The distribution also includes the Sample Clients. These are simple applications that demonstrate the functions in each group, with the source and binary of an application for each group. There is also a gSoap implementation of the WSDL for each group.

Client Samples

The directory of Client Samples, located at [InstallDrive]:\Program Files\Intel\AMTConfServer\SOAP Client Tests, contains sample sources for the all of the APIs defined in the Intel AMT Setup and Configuration Service.

Each sample is a command line program that executes a single API.

The sources are written in C++ using SOAP to connect to and communicate with the server.

Usage

The main files have the same usage, with the following parameters:

Table 5: Client Samples Parameters

-url server-url	The url of the server where the API server is located, for example https://my_server.com/amtscs
-in params-file	The name of an XML file with the invocation of the services data (more explanations below)
-out response-file	The name of an XML file that will be created to store the responses from the server. This is an optional argument and, if it is omitted, the output is displayed to the standard output device.

Input File

The samples are designed to run in batch mode (not interactively) and they read the input from XML files. The XML files use a different schema for each service, depending on the service parameters.

Since some services have very complex input data, the input folder contains sample XML files for all the services. The XML files contain sample data that should be modified when testing the service.

Select which services are tested by removing or commenting-out those services which are not to be tested. The same service can be tested a number of times in the file.

For example, the following file uses the “profile” name-space. This sample invokes two commands: SetProfilePowerPolicy and GetProfilePowerPolicy. The second command is invoked twice.

```
<requests>
    <!-- Request for service SetProfilePowerPolicy -->
    <request name='SetProfilePowerPolicy'>
        <ProfileID>2</ProfileID>
        <Entry>
            <ActiveStateAC>1</ActiveStateAC>

<WakeOnNetAccessThresholdAC>1</WakeOnNetAccessThresholdAC>
            <WakeOnNetAccessSleepTimer>1</WakeOnNetAccessSleepTimer>
        </Entry>
    </request>

        <!-- Request for service GetProfilePowerPolicy -->
        <request name='GetProfilePowerPolicy'>
```

```
            <ProfileID>2</ProfileID>
        </request>

        <!-- Request for service GetProfilePowerPolicy -->
        <request name='GetProfilePowerPolicy'>
            <ProfileID>2</ProfileID>
        </request>
</requests>
```

The following is an actual capture of a call with this data:

```
ProfileClient -url https://avi_t/amtscs -in req.xml
<results>
    <response name="SetProfilePowerPolicy" soapResult="0">
        <status>
            0
        </status>
    </response>
    <response name="GetProfilePowerPolicy" soapResult="0">
        <Response>
            <PowerPolicy>
                <ActiveStateAC>
                    0
                </ActiveStateAC>
                <WakeOnNetAccessThresholdAC>
                    0
                </WakeOnNetAccessThresholdAC>
                <WakeOnNetAccessSleepTimer>
                    1
                </WakeOnNetAccessSleepTimer>
            </PowerPolicy>
        </Response>
    </response>
    <response name="GetProfilePowerPolicy" soapResult="0">
        <Response>
            <PowerPolicy>
                <ActiveStateAC>
                    0
                </ActiveStateAC>
                <WakeOnNetAccessThresholdAC>
                    0
                </WakeOnNetAccessThresholdAC>
                <WakeOnNetAccessSleepTimer>
                    1
                </WakeOnNetAccessSleepTimer>
            </PowerPolicy>
        </Response>
    </response>
</results>
```

Input Binary Data

To send binary data, a file name containing the data must be specified instead of the data itself. For example, the AddTrustedRootCertificate requires binary data such as the certificate or the serial number.

To invoke it, the following must be written in the XML file. The references to the files appear in bold.

```

<!-- Request for service AddTrustedRootCertificate -->
<request name='AddTrustedRootCertificate'>
    <ProfileID>1</ProfileID>
    <TrustedRootCertificate>
        <Certificate>c:\trusted.der</Certificate>
        <CertLength>1</CertLength>
        <Issuer>X</Issuer>
        <SerialNumber>c:\serial.ser</SerialNumber>
        <SerialNumberLength>1</SerialNumberLength>
        <Subject>X</Subject>
        <ExpirationTime>X</ExpirationTime>
        <ChainLength>1</ChainLength>
        <certificateType>1</certificateType>
    </TrustedRootCertificate>
</request>
```

Output Binary Data

When receiving binary data, the data is encoded as base64 text in the resulting XML file.

Default Values

The samples assume the following default values if a parameter is not specified:

Data Type	Default
Numeric values	0
Boolean	false
Strings	""
Binary	Null

SOAP Faults

Each API may throw a standard SOAP Fault Response.

SOAP Fault version 1.1

```
<SOAP-ENV:Fault>
		<faultcode>301</faultcode>
		<faultstring xsi:type="xsd:string">User is not authorized</faultstring>
		<detail>Profile get error 301: Action not allowed for the user</detail>
</SOAP-ENV:Fault>
```

Chapter 6

SCS SUPPORT CONTENT

This section includes:

- “SCS Tools” on page 98
- “Using a Script to Import New Intel AMT Properties” on page 102
- “Configuring PEM Files for Redirection Applications” on page 104
- “CRL XML Format” on page 106
- “Troubleshooting” on page 107
- “Windows Service Error Codes” on page 109
- “Log Mapping” on page 110
- “Glossary” on page 111

SCS Tools

This section describes the command line and administrative tools installed with the SCS.

Command Line Tools

Add new AMT Properties

The Administrator can use this command line tool to add a new record to the NewAMTs table in the SCS database. The tool runs on the platform host and retrieves the UUID and the platform FQDN. It takes as input the URL of the IIS virtual directory so it can send a request to the SOAP API to add the entry to the database. It also takes as input the Profile name and the AD OU where the entry should be stored.
The trusted root certificate for the IIS instance on the SCS service platform must be installed on the host to enable the tool to send the entry to the database.

1. Navigate to the directory named:
   [InstallDrive]:\Program Files\Intel\AMTConfServer\Tools
2. From the command line, run: **AddServicNewAMTProperties.exe** The function displays a usage message.

Database Dump

The Administrator uses this tool to dump the contents of the setup and configuration database. The tool uses ADO.NET and Window authentication to access the database.

1. Navigate to the directory named:
   [InstallDrive]:\Program Files\Intel\AMTConfServer\Tools
2. From the command line, run: **DumpDB.exe** A usage message will be printed. The parameters are: DB Server name/Server Instance, and DB name. Optionally provide a DB User and password for SQL Server authentication.

The program dumps the DB contents to a file in the same directory as the command.

Administrative Tools

Administrative Tools are vbs scripts that extend and test the Active Directory schema. They are located in folders under
[InstallDrive]:\Program Files\Intel\AMTConfServer\AdminScripts

We recommend running the scripts from the command line prompt using cscript, for example: "cscript myscript.vbs". This ensures that, instead of opening separate messages, all messages are printed on the command line.

Active Directory Schema

This folder contains three scripts.

BuildSchema.VBS

Extends the Active Directory Schema to support the Intel-Management-Engine class. This script is run only once per domain.

The file `IntelAMT.LDF` must be in the same folder.

Parameters: None.

CheckSchemaExists.VBS

Checks that the Schema is properly extended.

Parameters: None.

ExportSchema.VBS

Exports the portion of the Intel-Management-Engine Schema to `IntelAMTExport.LDF`.

Parameters: None.

Group, User, and ACL Management Scripts

The Group, User and ACL scripts provide a means to create users and groups with the appropriate privileges needed to manage AMT objects and the SCS service instances in an enterprise. The scripts are used to:

1. Create global and local security groups
2. Create users within the groups.
3. Add specific access privileges to all users within the groups.

Active Directory User and Groups

This folder contains two scripts.

CreateGroups.vbs

This script creates a global security group and one or more local security groups in Active Directory. These groups are given the necessary privileges to manage instances of the SCS across the enterprise. Then users who will perform manual management tasks are made members of these groups.

Table 6: CreateGroups.vbs Command Line Parameters

Parameter	Description	Default
Server Name	This is the name of any computer within a domain in which the global group is added. It does not have to be the name of the domain controller.	localhost
OU (Organizational Unit)	CN of the organizational unit within AD where groups should be created.	CN=Users
These parameters are optional but the Server Name must be entered if the OU will be changed before setting the second. For example: `cscript creategroups.vbs localhost AMTUsers`		

The script performs the following steps:

a. It binds to the “RootDSE” of the Server Name. This determines the AD instance where the changes will be made.

b. It creates a global security group with the name “Enterprise IntelME Setup and Configuration Servers” under the OU

c. It enumerates all the domains visible in the AD instance.

e. For each domain the script adds a local security group with the name “IntelAMT SCServers”

f. Adds the global security group to each local security group

CreateUsers.vbs

This script adds users to Active Directory. The constants in the following table are embedded in the script.

Table 7: CreateUsers.vbs Constants

Constant Name	Description	Default
GLOBAL_GROUP_ NAME	The user is made a member of this group after the user is created.	Enterprise IntelME Setup and Configuration Servers
PASSWORD	The initial password defined for the user.	PASSWORD

Table 8: CreateUsers.vbs Command Line Parameters

Parameter	Description	Default
User Name	Name of the user to be created	SCS User
OU (Organizational Unit)	CN of the organizational unit within AD	CN=Users
Server Name	Name of the computer in the domain where the user will be added.	localhost
Group OU	This parameter defines the path to the group where the user will be added.	Value of the second parameter
These parameters are optional but previous parameters must be entered if a subsequent parameter is required.		

The script performs the following steps:

a. It binds to the “RootDSE” of the Server Name.

b. It creates a user in the OU with the “User Name”.

c. sets the password to “PASSWORD”

d. Adds the user to the Enterprise IntelME Setup and Configuration Servers group.

Active Directory ACL

The ACL scripts create the privileges required for users who will be managing AMT objects. This directory contains three scripts.

CreateACL.vbs

This script creates the required ACLs for a group.

Table 9: CreateACL.vbs Command Line Parameters

Parameter	Default
Server Name	localhost
OU (Organizational Unit)	AMTOU
Group name (or user name)	IntelAMT SCServers
These parameters are optional but previous parameters must be entered if a subsequent parameter is required.	

The script performs the following steps:

a. It binds to the “RootDSE” of the Server Name.

b. It creates all the required ACL’s for the OU related to group name.

c. The ACLs

- Set read/write permissions for all Intel AMT attributes
- Set create/delete permissions for Intel AMT objects
- Set reset password permissions
- Set read/write permissions to the Intel BL (back link) attribute on computer objects

RemoveACL.vbs

This script deletes the ACLs in a group.

Command line parameters for this script are the same as for CreateACL.vbs.

The script performs the following steps:

a. It binds to the “RootDSE” of the Server Name.

b. Itextracts and deletes all the ACLs for the OU related to group name.

PrintACL.vbs

This script prints the ACLs in a group.

Command line parameters for this script are the same as for CreateACL.vbs.

The script performs the following steps:

a. It binds to the “RootDSE” of the Server Name.

b. It extracts and prints all the ACLs for the OU related to group name.

Using a Script to Import New Intel AMT Properties

When the SCS is configured to use a script to obtain information about an Intel AMT device that sent a setup request, the following occurs:

- The Intel AMT device sends a “Hello” message.
- When the SCS receives the “Hello” message, it first searches the New AMT table for a matching UUID entry.
- If there is no matching entry, the SCS sets environment variables based on values in the message.
- The SCS activates the script.
- The script locates the necessary parameters and creates a file consisting of an XML fragment.
- When the script completes, the SCS reads the file and adds an entry to the New AMT table using the values returned by the script in the file.
- The SCS performs setup and configuration using the information in the file.

Environment Variables

The SCS sets the following environment variables to pass values to a script:

- CS_AMT_UUID: The UUID from the Hello message
- CS_AMT_STATUS: status of the device to be setup— “U” (Unprovisioned), “I” (In provisioning), or “P” (Already provisioned)
- CS_AMT_ADDR: The value depends on the value of the previous parameter.
  - If CS_AMT_STATUS = “U” or “I”, CS_AMT_ADDR = the source IP address from the Hello message.
  - If CS_AMT_STATUS = “P”, CS_AMT_ADDR = the FQDN of the Intel AMT device to be set up.
- CS_OUT_FILE_NAME: A file name generated by the SCS. The script return the Intel AMT properties in a file with this name in the same directory as the script in the format described below.

Output File Format

The output file generated by a script must be an XML fragment interpretable by the SCS. The fragment has the tag **amtConfiguration** and contains the following attributes:

- **fqdn**: The FQDN of the platform containing the Intel AMT device
- **addn**: The Active Directory OU to be used for this device or “NA” when the SCS is not integrated with Active Directory.
- **profile** or **profile_id**: Either the SCS Profile name or the index of the profile to be used when setting up this device (only one of these can be used).

The file will have the structure shown in the following examples:

```
<amtConfiguration fqdn=“jonesr.west.yourenterprise.com”
addn=”OU=AMTDevs,DC=west,DC=yourenterprise,DC=com”
profile=”Standard_user”/>
```

or

```
<amtConfiguration fqdn=“jonesr.west.yourenterprise.com”
addn=”OU=AMTDevs,DC=west,DC=yourenterprise,DC=com”
profile_id=”2”/>
```

Script Functionality

Script functionality is the responsibility of the ISV or the IT organization. The script may retrieve the information from an external source or from the platform containing the Intel AMT device, or some combination of the two methods. For example, the script may request the FQDN from the platform using the IP address, then determine the Active Directory OU and SCS Profile based on the FQDN.

Sample Script

The SCS distribution includes a sample script called AMT_lookup.vbs. The script sends a WMI query to the host platform that sent the Hello message, and therefore requires that the host is operational and running a version of Microsoft Windows.

The SCS user requires appropriate permissions to invoke WMI remotely. To use this script, the SCS user must be an administrator on the local host (a member of the local Administrators group). A user who is a member of the Domain Admins group is automatically a member of the local Administrators group. A user who is a member of Enterprise Admins is automatically a member of Domain Admins.

The script has a 30 second timeout in case WMI freezes on the host; however, the script may require 10 to 20 seconds to execute normally, due to WMI timing on the host.

The script:

1. Validates the environment variables.
2. Using the WMI protocol, requests the Win32_ComputerSystemProduct object to recover the platform UUID from the host platform.
3. Using the WMI protocol, requests the Win32_ComputerSystem object to recover the platform name and domain from the host platform.
4. Creates the fqdn by concatenating the name and domain.
5. Validates that the returned UUID is the same as the UUID environment variable.
6. Creates an amtConfiguration XML fragment using the fqdn and a hard-coded OU and profile name.
7. Writes the fragment to an output file.

The script is run by executing runvbs.bat, which invokes cScript.exe, the command-line version of the Windows script host. The script writes output files to the same directory as the one containing the script and runvbs.bat.

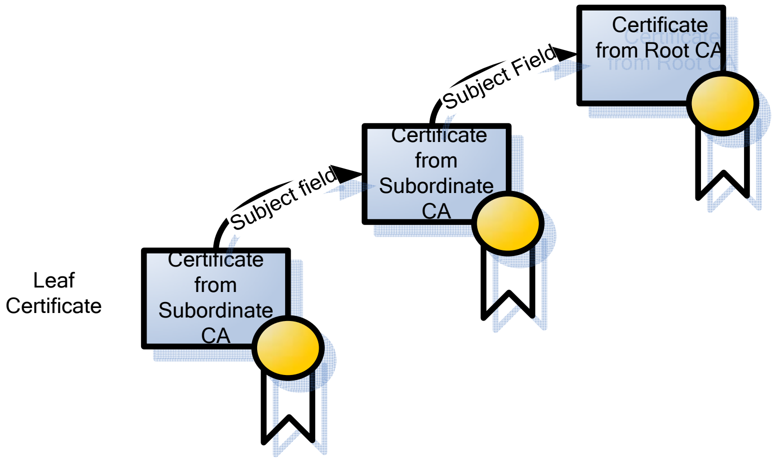
On the General Properties pane of the SCS Console, select **Get New Intel AMT Properties/From Script** and enter the path name to the batch file on each platform running the SCS, for example:

```
C:\program files\intel\scs\scripts\runvbs.bat
```

See Step 5 on page 63.

Configuring PEM Files for Redirection Applications

A certificate generated by a subordinate CA is linked to a sequence of certificates that eventually link to a certificate from the root certificate authority.



The Issuer Field of a certificate equals the Subject Field of the certificate of the issuing CA. In this way, each certificate points to the next certificate in the chain, until the path reaches a certificate created by the root CA.

When the Intel AMT Setup and Configuration Server enrolls a certificate (installs it in an Intel AMT device) it only sends the leaf certificate and does not include any subordinate certificates. When a client initiates a TLS session with an Intel AMT device, the device only sends the leaf certificate to the client application (an ISV Management console application).The client needs to know the full chain and must acquire the intermediate subordinate CA certificates. In a correctly configured Microsoft environment, the client dynamically retrieves the intermediate CA certificates based on the information in the issued leaf certificate. This can succeed if the IT administrator has set up the environment correctly by ensuring that the application has the necessary privileges to obtain the subordinate certificate information.

If a TLS stack other than the Microsoft stack is used (for example, if the application uses the Intel AMT redirection library that depends on OpenSSL), then the certificate chain must be provided explicitly.

The user must create a .PEM file that contains all of the certificates in the chain to the certificate from the root CA, not including the leaf certificate itself.

The way to do this is to convert each certificate in the chain to a .PEM file, then concatenate the PEM files.

When the subordinate CA was installed, certificates for all the CAs in the chain were also installed in the Trusted Certificate Store on the server where the subordinate CA was installed. Go to the web interface for the CA, (for example, open a web browser and navigate to http://<CA hostname>/certcrv) and download the certificates for each subordinate CA. Downloading in Base 64 format results in a .cer file that is in PEM format.

The file starts with the string
-----BEGIN CERTIFICATE----- and ends with the string
-----END CERTIFICATE-----.

Concatenate the files by combining the files using copy and paste in a text editor including the opening and ending strings. Rename the file as a PEM file.

The resultant file is used as an input to the redirection library function IMR_SetCertificateInfo (see the *Redirection Library User Guide*).

CRL XML Format

The Intel AMT SCS Console can import a Certificate Revocation List (CRL) into a Profile. The following file is an example of the XML format.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<!--
This file maps the untrusted certificates serial number to the URI of the issuer.
The URI value represents the a valid CRL distribution point of a Certificate Authority.
 -->
<crl>
    <uri name="http://crl.myenterprise.com/pki/mscorp/crl/mswww(2).crl">
        <cert serialnumber="15 27 82 20 00 00 00 00 00 01"/>
        <cert serialnumber="15-27-82-20-00-00-00-00-00-02"/>
        <cert serialnumber="15278220000000000003"/>
    </uri>
    <uri name="http://corppki/crl/mswww(2).crl">
        <cert serialnumber="15 27 82 20 00 00 00 00 00 04"/>
        <cert serialnumber="15 27 82 20 00 00 00 00 00 05"/>
    </uri>
</crl>
```

The *serialnumber* attribute must contain the following format:

1. Use exactly two hexadecimal characters for each byte (a byte with a single character will be ignored).
2. The serial number can be represented as a single hexadecimal number. If the bytes are separated from each other, use any **non-hexadecimal** character separator between each pair.

The file format is defined with following XSL style sheet:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified">
    <xs:element name="cert">
        <xs:complexType>
            <xs:attribute name="serialnumber" type="xs:base64Binary" use="required"/>
        </xs:complexType>
    </xs:element>
    <xs:element name="crl">
        <xs:complexType>
            <xs:sequence>
                <xs:element ref="uri" maxOccurs="unbounded"/>
            </xs:sequence>
        </xs:complexType>
    </xs:element>
    <xs:element name="uri">
        <xs:complexType>
            <xs:sequence>
                <xs:element ref="cert" maxOccurs="unbounded"/>
            </xs:sequence>
            <xs:attribute name="name" type="xs:string" use="required"/>
        </xs:complexType>
    </xs:element>
</xs:schema>
```

Troubleshooting

This section includes miscellaneous tables for troubleshooting and maintenance.

Table 13: Troubleshooting

Symptom	Solution
Received “Cannot contact CA” error in SCS Service log during provisioning and re-provisioning process.	On the SCS Console, select Profile > Certificate tab. Verify that the “CA Server Name” field has no leading spaces. Do this for each profile in the system.
I’m having an authentication problem when running the AMTConfig (Windows Service).	The installer inserts the password for the windows service correctly, but there is a local security policy that needs to be added. Once the security policy is added, the service can run. To overcome this problem, the user needs to open the service in the Service Manager and re-enter the password. Windows then automatically opens the security policy.
I'm trying to uninstall the “SOAP API” and I'm getting an error: “Failed to extract SOAP directory from the registry” or “Failed to extract SOAP virtual directory name from the registry”	The installer failed to locate the SOAP Directory/Virtual Directory in the registry. This failure will prevent the installer from disabling web extensions added earlier during installation and from deleting the Virtual Directory.
I'm trying to uninstall the “Database schema” and I'm getting an error: “Build Database script failed! Error code:X”	The installer successfully ran the build Database Schema script, but the script returned error code X.
I'm getting an error: “RegDBCreateKeyEx failed.” Or “RegDBSetKeyValueEx failed.”	The installer failed to create or set registry values. Make sure you are logged-in as an Administrator user.
I can't install/remove the Database. “xxxxx”	This problem might occur during installation or removing of the Database Schema, The “Microsoft SQL Server Management Studio Express” does not present the Database in the list of Databases but the Database files exist. To resolve this problem delete the Database files (LDF and MDF extension) manually from: “Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Data” Restart and reinstall.
I've checked “Start AMT Config Service” at the end of the installation, but got an error that the service can't be started.	Open the Windows Management Console and select the Services tab. Locate the “AMTConfig” service. Open it. Go to “Log on” and re-type the password. Then, restart the service.

Symptom	Solution
IIS application pool has a protection from rapid failures in a given time (default 5 failures in 5 minutes). If that condition occurs the application pool shuts down.	1. Restart the default application pool. 2. If that does not help, restart the IIS.
The server seems to be stuck: The symptoms are 100% CPU usage for more than 10 minutes and the service does not respond to setup requests from Intel AMT devices.	1. On the Console Configuration Service Settings / General pane, decrease the number of threads. 2. Restart the service.

Windows Service Error Codes

Table 14: Windows Service Error Codes

Error Code	Causing Scenario/Symptom	Possible Resolutions
21	SOAP_TCP_ERROR 1. Configure Intel AMT device 2. SCS service tries to reconnect to AMT using its FQDN 3. Error code 21 appears in SCS service log.	1. The AMT’s FQDN might not been configured in the DNS. 2. To verify this, try to ping the AMT using its FQDN.
22	SOAP_HTTP_ERROR 1. Perform any action upon AMT 2. Error code 22 appears in SCS service log	1. No available web service on the AMT. 2. The service use invalid HTTP protocol (unencrypted). 3. Check that the AMT’s status is synchronized with its status as it appears in the AMT’s table view in the Console.
23	SOAP_SSL_ERROR 1. Perform any action upon AMT 2. Error code 23 appears in SCS service log	1. AMT’s certificate is not valid. 2. Manually repeat setup and configure the device (to force generation of a new certificate).
4099/2057	Invalid Parameter/Data missing 1. Perform setup and configuration of an Intel AMT device 2. Error code 4099/2057 appears in SCS service log	1. Invalid data or data missing in AMT’s profile configuration. 2. Open the problematic profile configuration dialog in the Console and re-configure the missing/inappropriate parameters.

Log Mapping

Table 15: Log Mapping

Component Name	Log File
Windows Service + Web Service + DB + Client Sample Installation	[InstallDrive]:\Program Files\InstallShield Installation Information\DA4F4037-6EB2-4309-86EB-A8902CBC12EC\setup.ilg
GUI Console Installation	[InstallDrive]:\Program Files\InstallShield Installation Information\66469B6E-D328-4416-BD1E-C4692C4A1A96\setup.ilg
GUI Console	[InstallDrive]:\Program Files\Intel\AMTConsole\amtconsole.log

Glossary

Term	Definition
Access Control List (ACL)	A set of data associated with a file, directory or other network resource that defines the permissions that users, groups, processes or devices have for accessing it. In Intel AMT, a list of users and their access privileges.
Active Directory (AD)	Active Directory is an advanced, hierarchical directory service that comes with Windows 2000 servers. It is LDAP (Lightweight Directory Access Protocol—a protocol used to access a directory listing) compliant and built on the Internet's Domain Naming System (DNS). Workgroups are given domain names, just like Web sites, and any LDAP-compliant client (Windows, Mac, Unix, etc.) can gain access to it.
AD OU Active Directory Organizational Unit	Organizational Units (OU's) within an Active Directory are a way to delegate control over part of the directory to a user or group of users. That is, unlike Windows NT 4.0 domains, subsets of users, groups and/or computers can be delegated to different groups, allowing a greater degree of control and granularity without the need to run dedicated domain controllers for that group.
Intel AMT	Intel Active Management Technology is a technology developed by Intel that enables Administrators to remotely manage and repair networked computers even when they are powered down. Three primary features of Intel AMT are better asset management, reduced downtime and minimized desk-side visits, also called by Intel the "discover, heal and protect process." See: http://www.intel.com/technology/manage/iamt/benefits.htm
API	Application Programming Interface: A language and message format used by an application program to communicate with the operating system or some other control program such as a database management system (DBMS) or communications protocol. APIs are implemented by writing function calls in the program, which provide the linkage to the required subroutine for execution. Thus, an API implies that some program module is available in the computer to perform the operation or that it must be linked into the existing program to perform the tasks.
Authentication	A security measure designed to establish the validity of a transmission, message, or originator.

Term	Definition
Authentication Server (AS)	A Kerberos element in a KDS that recognizes a client at log-on time based on information in its trusted database.
Authenticator	An authentication protocol string created each time authentication occurs and sent with the ticket to the server. It contains a time-stamp encrypted in the session key that can reliably show that the authentication request actually came from the client identified in the ticket.
Authorization	The process of determining what types of activities are permitted. Usually, authorization is in the context of authentication: once you have authenticated a user, the user may be authorized for different types of access or activity.
CRL	Certificate Revocation Lists. The CRL is a list of time stamped entries which indicate which lists have been revoked.
Domain	Part of the DNS (domain naming system) name that specifies details about a host. A domain is the main subdivision of Internet addresses, the last three letters after the final dot, and it tells you what kind of organization you are dealing with. In the context of Active Directory, every host is a member of a domain. A user logs in to the domain of which he is a member.
DNS	A system for converting host names and domain names into IP addresses on the Internet or on local networks that use the TCP/IP protocol. For example, when a Web site address is given to the DNS, DNS servers return the IP address of the server associated with that name.
EACL	Enterprise Access Control List
FPACL	Factory Partners Access Control List
FQDN	Fully qualified domain name: the human-readable name corresponding to the IP address of a network interface, as found on a computer, router or other networked device. It includes both its host name and its domain name.
Group	In Active Directory, a collection of users and objects that share properties and permissions. A group may have another group as a member. The second group is then a sub-group of the first group.
GSS-API	Generic Security Services Application Programming Interface. The generic API for performing client-server authentication.

Term	Definition
ISV	Independent Software Vendors that develop applications that use Intel AMT capabilities.
Kerberos	An Access Control System that was developed at MIT in the 1980s. The Kerberos concept uses a “master ticket” obtained at logon, which is used to obtain additional “service tickets” when a particular resource is required. It is named after a mythological creature.
Key	A key is a piece of information that controls the operation of a cryptography algorithm. In encryption, a key specifies the particular transformation of plaintext into ciphertext, or vice versa during decryption. Keys are also used in other cryptographic algorithms, such as digital signature schemes and keyed-hash functions (also known as MACs), often used for authentication.
Key Distribution Center (KDC)	In the Kerberos protocol, a trusted third party that has secret information (passwords) for all clients and services under its supervision.
Mutual Authentication	Mutual authentication, also known as two-way authentication, is a process whereby two parties, typically a client and a server, authenticate each other in such a way that both parties are assured of the others' identity. In mutual authentication, the server also requests a certificate from the client.
Provisioning	Provisioning deals with planning, setting up and configuring the hardware, software and networks that deliver access to data and network resources for the users.
Proxy	A firewall mechanism that replaces the IP address of a host on the internal (protected) network with its own IP address for all traffic passing through it. A software agent that acts on behalf of a user, typical proxies accept a connection from a user, make a decision as to whether or not the user or client IP address is permitted to use the proxy, perhaps does additional authentication, and then completes a connection on behalf of the user to a remote destination.
PSK Pre-Shared Key	The use of secret passwords or encryption keys that are entered into both sides of the message exchange ahead of time. Pre-shared keys are typed into the clients and servers (authentication servers, access points, etc.) or entered via floppy, CD-ROM or smart card. Contrast with “server-based keys,” in which one side generates a key and sends it to the other side during the authentication session.

Term	Definition
RC4-HMAC	An encryption type based on the RC4 encryption algorithm that uses an MD5 HMAC for checksum. It is included in the Windows implementation of Kerberos.
Realm	In Kerberos, a realm is the same as an Active Directory domain. Kerberos V5 expects realms to have all capital letters. Intel AMT functionality is divided among different realms, for example, the Storage Realm and the Storage Administration Realm. ACLs associate a user or an SID with one or more realms.
RNG Random Number Generator	A computer Random Number Generator is a software routine that implements an algorithm to generate random numbers. Modern cryptography rests on the assumption that ciphers can be constructed whose output is indistinguishable from random noise without knowledge of a secret key used in the algorithm. See “Key”.
Schema	A conceptual model of the structure of a database that defines the data contents and relationships. The Microsoft Active Directory schema contains formal definitions of every object class that can be created. One of these objects is the computer object. The Intel - Management-Engine-Class, based on the computer object, is added to the Active Directory schema and used to define AMT objects. The SCS database schema defines the data tables maintained in the database and the relationships of the tables.
Security Identifier (SID)	A numeric value that identifies a logged-on user who has been authenticated by Active Directory or a user group.
SOAP Simple Object Access Protocol	A message-based protocol based on XML for accessing services on the Web. SOAP employs XML syntax to send text commands across the Internet using HTTP.
SOL/IDER Serial-over-LAN/IDE-Redirection	The proprietary protocols defined for Intel AMT for redirecting keyboard/text or floppy disk/CD transfers from a local host to a remote workstation.
SPEGNO Simple and Protected GSS-API Negotiation Mechanism	SPNEGO is a standard GSS-API pseudo-mechanism for peers to determine which GSS-API mechanisms are shared, select one and then establish a security context with it.
SPN	A service principal name - the name by which a client uniquely identifies an instance of a service.
Ticket Granting Server (TGS)	A Kerberos element in a KDC that creates tickets used to by clients to access servers.

Term	Definition
TLS Transport Layer Security	A protocol intended to secure and authenticate communications across a public network by using data encryption. TLS uses digital certificates to authenticate the user as well as authenticate the network (in a wireless network, the user could be logging on to a rogue access point). The TLS client uses the public key from the server to encrypt a random number and send it back to the server. The random number, combined with additional random numbers previously sent to each other, is used to generate a secret session key to encrypt the subsequent message exchange.
Token	In Kerberos, a fixed length element that contains a user's SID and includes the user's rights and group memberships.
UUID Universally Unique Identifier	A UUID is an identifier standard used in software construction. The intent of UUIDs is to enable distributed systems to uniquely identify information without central coordination. Thus, anyone can create a UUID and use it to identify something. Information labelled with UUIDs can therefore be combined into a single database without need to resolve name conflicts. A UUID is essentially a 16-byte number and in its canonical form a UUID may look like this: 550E8400-E29B-11D4-A716-446655440000
VLAN Virtual LAN	A VLAN is a logical subgroup within a local area network that is created via software rather than manually moving cables in the wiring closet. It combines user stations and network devices into a single unit regardless of the physical LAN segment they are attached to and thereby allows traffic to flow more efficiently within populations of mutual interest.