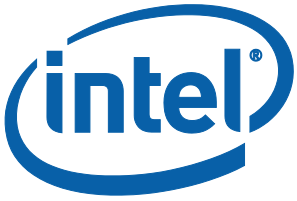


Intel® vPro™ Technology Use Case Reference Design

Out of Box Configuration for KVM Remote Control

Revision 1.3

January, 2011

Document ID: 1053

Revision History

Revision	Revision History	Date
1.0	Initial Release	February, 2010
1.1	Added note that RFB Password must be exactly 8 characters.	February, 2010
1.2	Changed title per Marketing.	June, 2010
1.3	Updates for new KVM Configuration interface.	January, 2011

Contents

Figures

1 Preface

With the release of Intel® Active Management Technology (Intel® AMT) 6, Intel® vPro™ technology adds the capability to do KVM Remote Control out of band. That is, an IT Professional can remotely control the keyboard, video, and mouse (KVM) of a system with Intel vPro Technology in a similar fashion to Remote Desktop or RealVNC's VNC* series, without an OS based server. This Use Case Reference Design will step you through the shortest path from opening the box of your new computer with Intel vPro technology to using KVM Remote Control.

NOTE

Although this document contains setup and configuration steps for PCs with Intel vPro technology, is intended as a tutorial on KVM Remote Control rather than a deployment or activation guide.

1.1 Document Scope

This document describes configuring and using KVM Remote Control on a single system. The steps outlined use tools that are freely downloadable. This document is not meant to describe a large scale production deployment of KVM Remote Control. Rather, it is intended to allow the reader to experience KVM Remote Control and gain insight into its functionality. Finally, the document will conclude with an advance discussion of KVM Remote Control features, security, deployment, and more using a question and answer format.

1.2 Intended Audience

This document is intended for Information Technology (IT) professionals who are interested in experimenting with and learning more about Intel AMT 6 and KVM Remote Control.

2 Introduction

This document will take you through the shortest path from unpacking your new managed client with Intel vPro technology to using KVM Remote Control to access it.

2.1 What You Need

The steps in this document have the following requirements:

Server	DHCP Server. **Note**: static IP addresses are supported but not covered by this document.
Console PC	Any PC with Microsoft* Windows XP or later.
Managed Client with Intel vPro technology	Intel AMT 6.0 or later and supporting the KVM Remote Control feature.

2.2 Process Overview

If you have ever used RealVNC's VNC* viewer or something like it, then you understand the concept of KVM Remote Control. However, in the case of KVM Remote Control, the RFB Compliant server is actually running in the Intel® Manageability Engine (Intel® ME). This means that no server is needed in the operating system (OS). In fact, the system can be in BIOS, DOS, or any ACPI state and you will be able to remotely operate it via KVM Remote Control.

One advantage of KVM Remote Control is that it is based on the RFB standard. Because of this, you can use any Remote Frame Buffer (RFB) compliant viewer, such as RealVNC's VNC viewer series, to remotely operate your Managed Client using KVM Remote Control. The RFB compliant server that normally runs in the OS is now running in the Intel ME.

In the same way that you must first install and configure the RFB compliant server running in the OS, you must also turn on (but not install, since it is pre-installed in the firmware) and configure the RFB compliant server that is hosted in the Intel ME. This is done by sending WS-Man commands from a console PC, over then network, to the Intel ME. Steps are outline below.

Once the RFB compliant server is configured, you can remotely operate the Managed Client via KVM Remote Control.

Security is another important consideration for KVM Remote Control. For instance, having the Intel ME always listening for KVM Remote Control connections leaves it vulnerable to a port scan and brute force attack. Also, RFB compliant traffic is not natively encrypted. As such, for a full security deployment there are specific flows and features enabled by KVM Remote Control that can be used. These are covered in Section 4, Prepare the Console and Section 7, Advanced KVM Remote Control Topics

This document will guide you through configuring KVM Remote Control and then establishing a KVM session to remotely operate a new Managed Client. The document will then provide an advanced discussion of KVM Remote Control features, security, deployment, and more in a question and answer format.

3 Prepare the Managed Client

In order to use Intel AMT you must first set up and configure it. These steps are the quickest path for setting up a single system. This is known as Basic Setup and Configuration.

NOTE

The following detailed steps depict manual configuration of a single client with Intel vPro technology. See the links below for other documented methods to set up and configure a large number of clients.

USB based Local Setup an Configuration

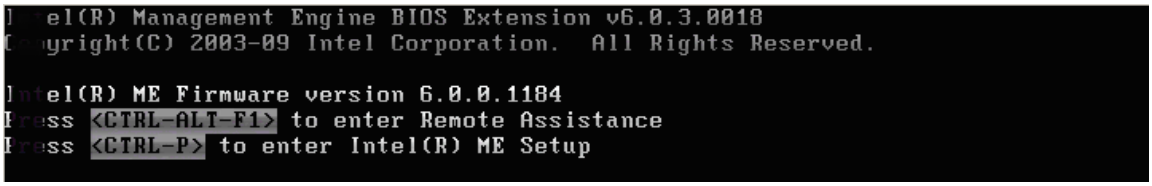
http://communities.intel.com/docs/DOC-4354

Standard Setup and Configuration or Advanced Setup and Configuration

http://communities.intel.com/docs/DOC-3159

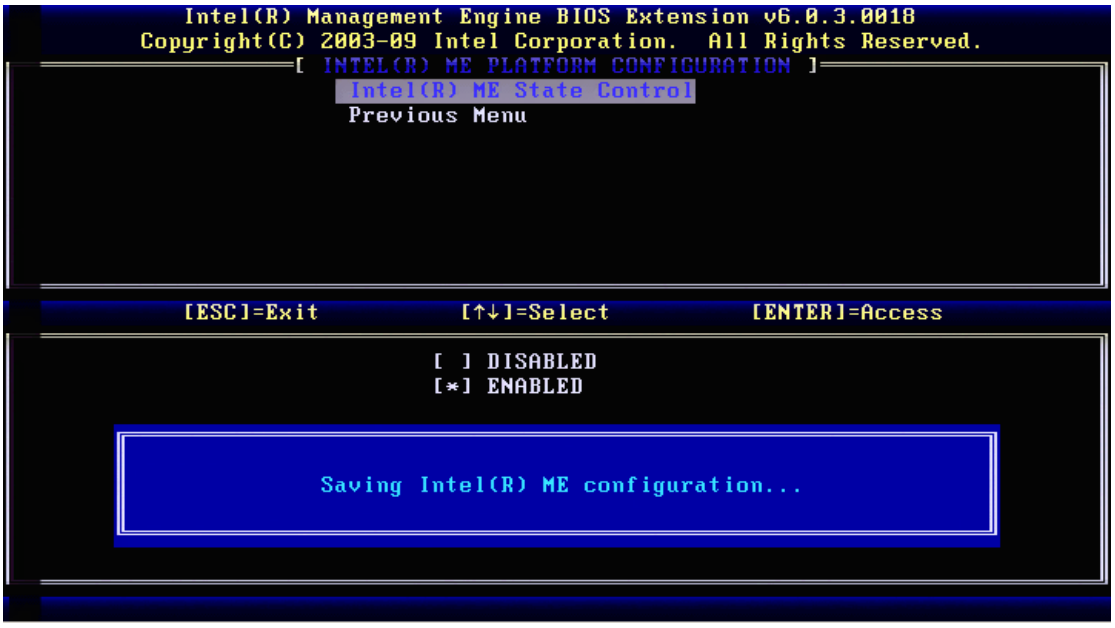
To set up and configure your new Managed Client with Intel vPro technology, perform the following steps:

1. Boot your Managed Client.
2. When prompted, enter the Intel® Management Engine BIOS Extension (Intel® MEBX). On most systems this is be done by pressing Ctrl-P when prompted. However, some systems are different. Check your system documentation.

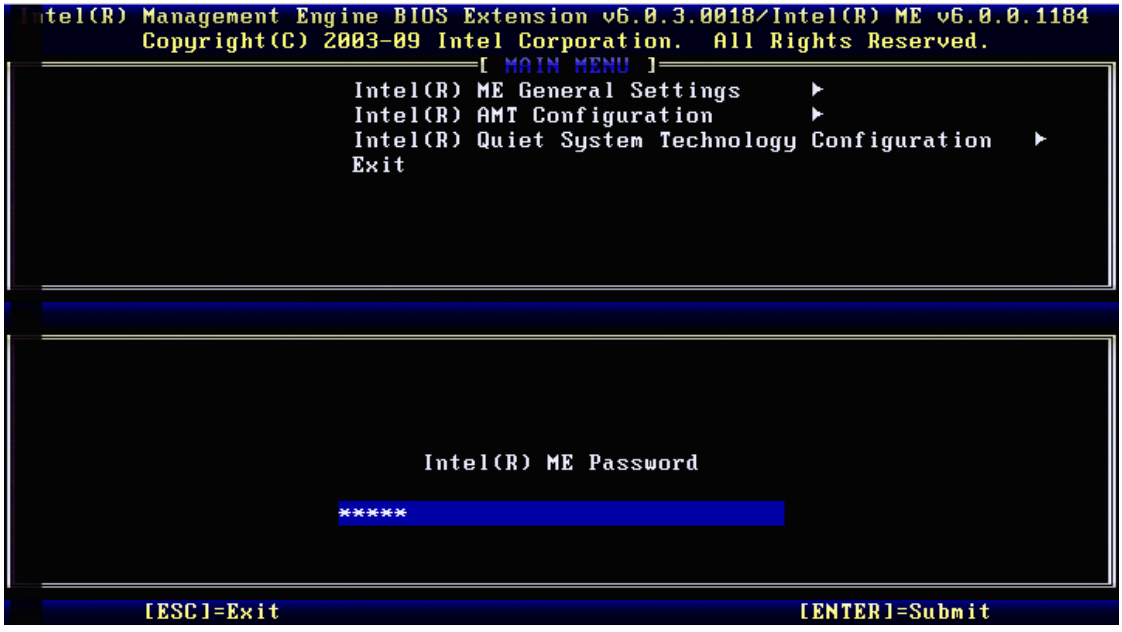


3. Depending on your system, you may be prompted for a password. If so, skip to step 6. Otherwise continue to step 4.

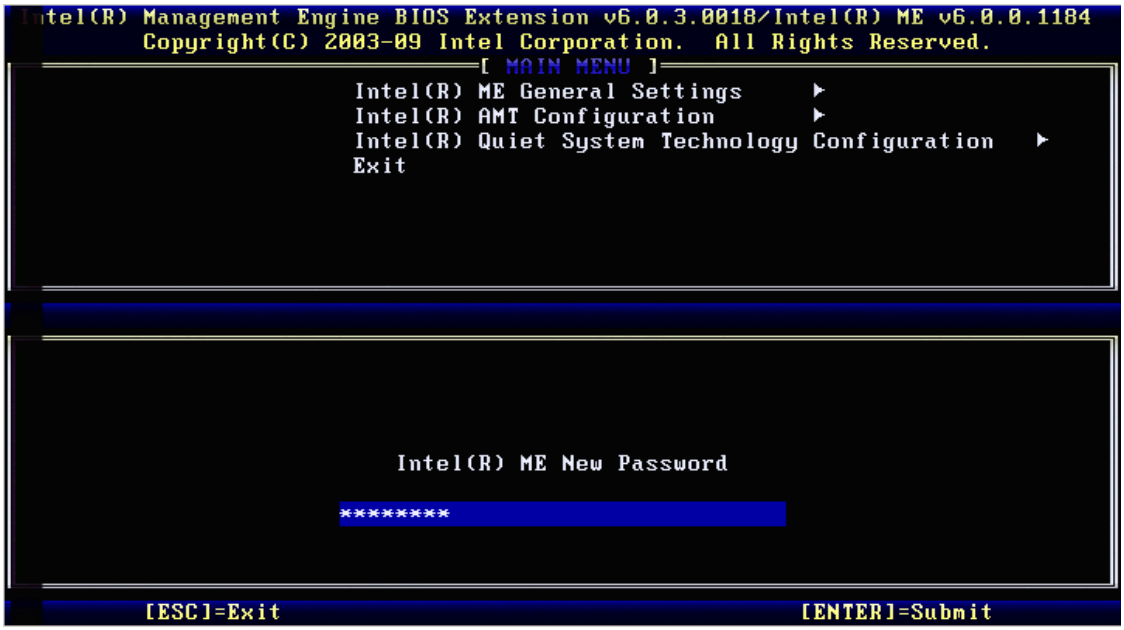
4. Select Intel® ME General Settings -> Intel ME State Control; use the arrow keys to select **Enabled**, then press the Enter key.



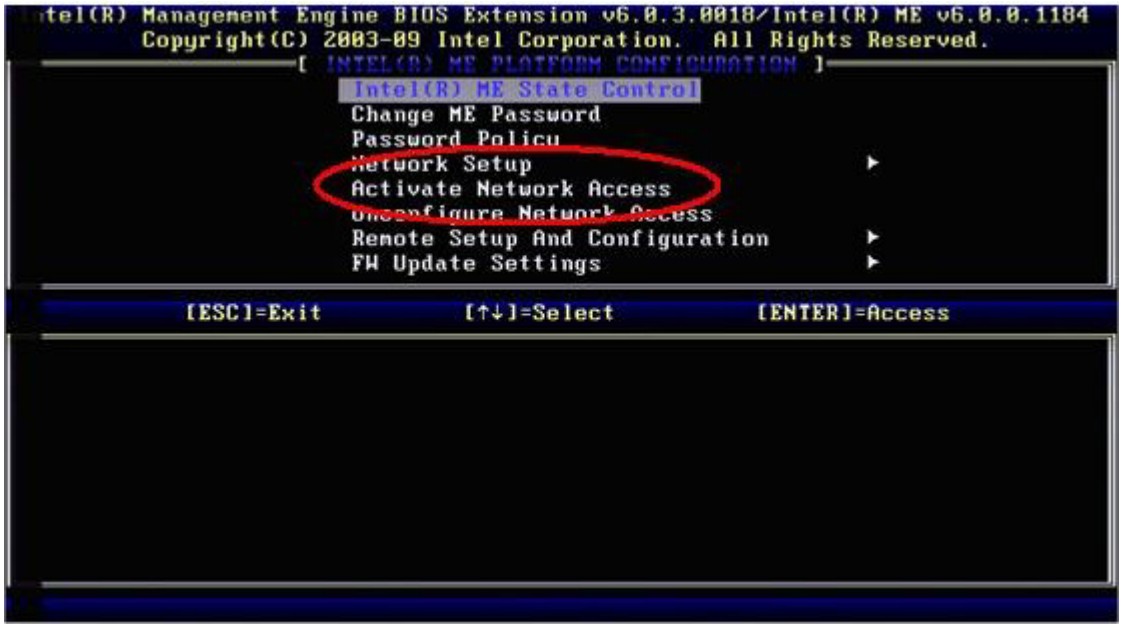
5. Your system will reboot. When prompted, enter the Intel MEBX (press Ctrl-P).
6. You will be prompted for the Intel MEBX password. The default password is **admin**. Enter the password as shown below.



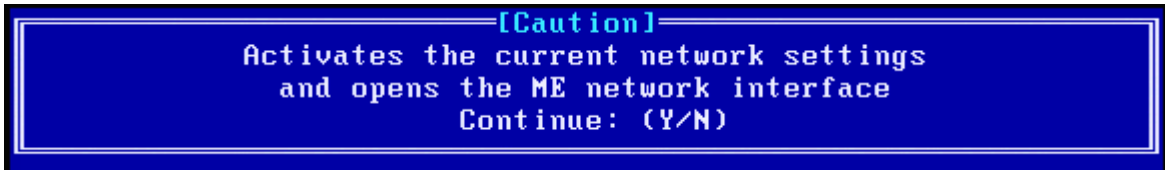
7. Next you are prompted to enter a new password. It must be at least 8 characters, and contain at least one upper and one lower case letter, one number, and one symbol such as @ or $. Choose a new password and enter it twice, as shown below.



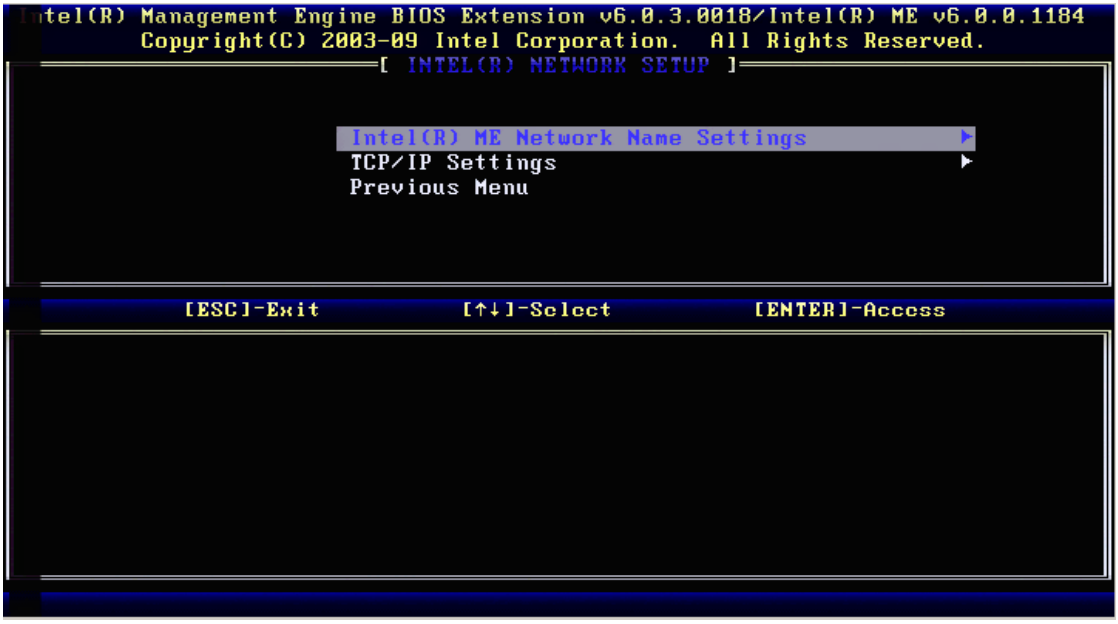
8. Now you must set up the Intel® Management Engine. Enter the Intel® ME General Settings menu and select **Activate Network Access**.



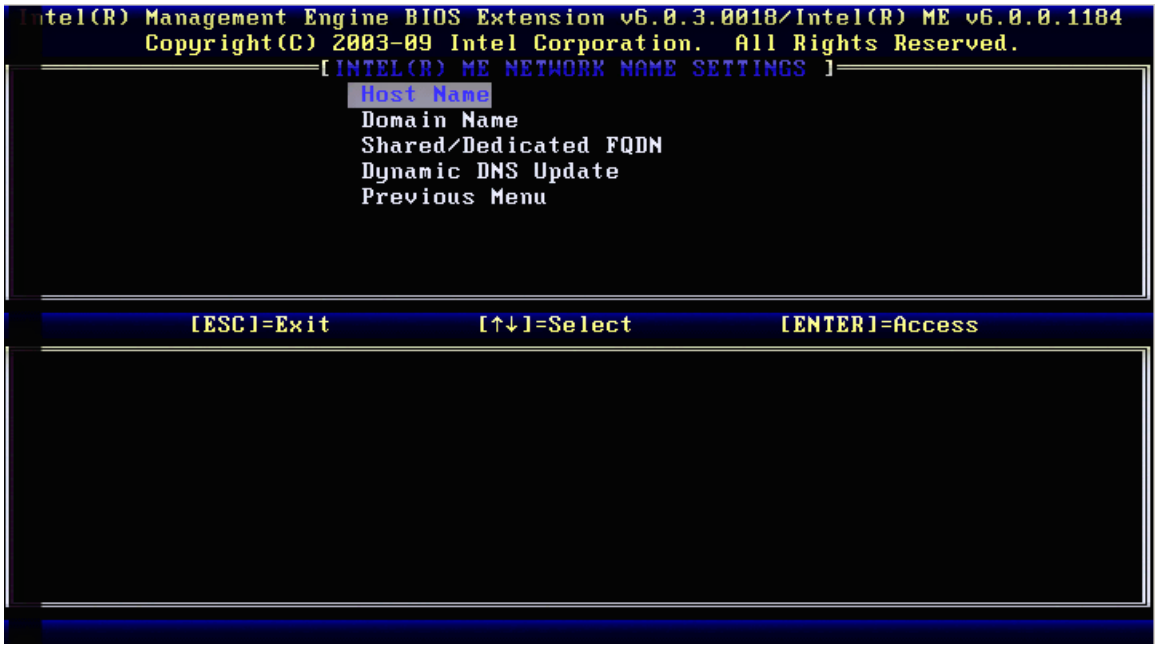
9. Type **Y** to answer "yes" when prompted in the Caution box shown below.



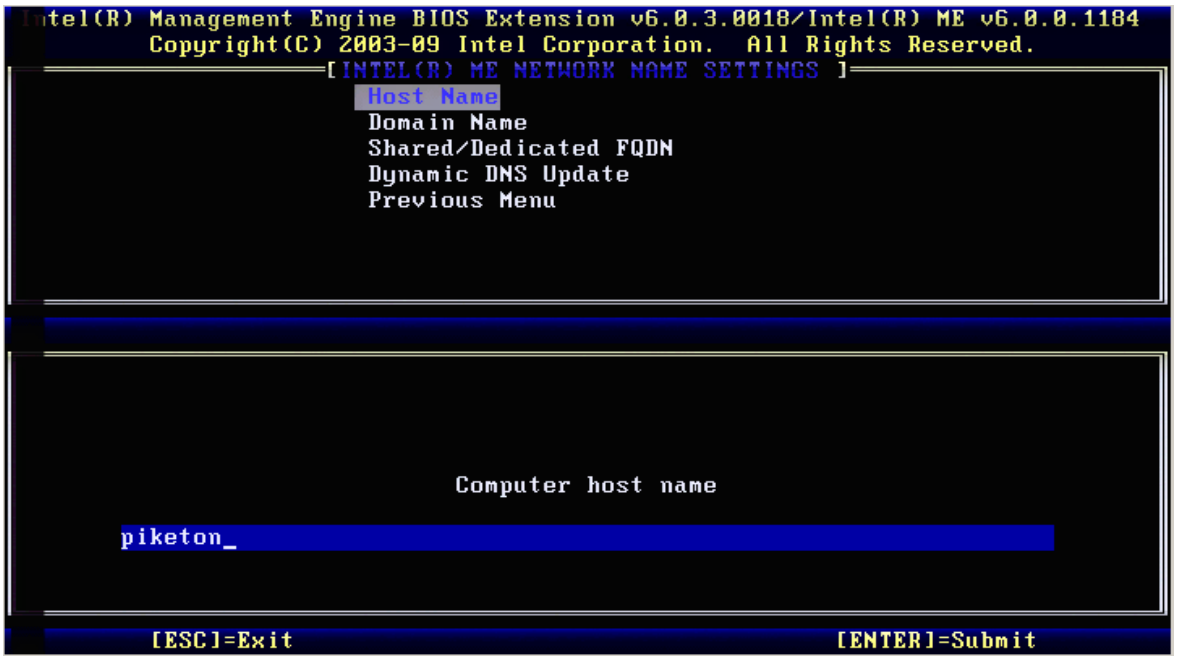
10. Select **Network Setup**. The screen shown below is displayed. Select **Intel® ME Network Name Settings**.



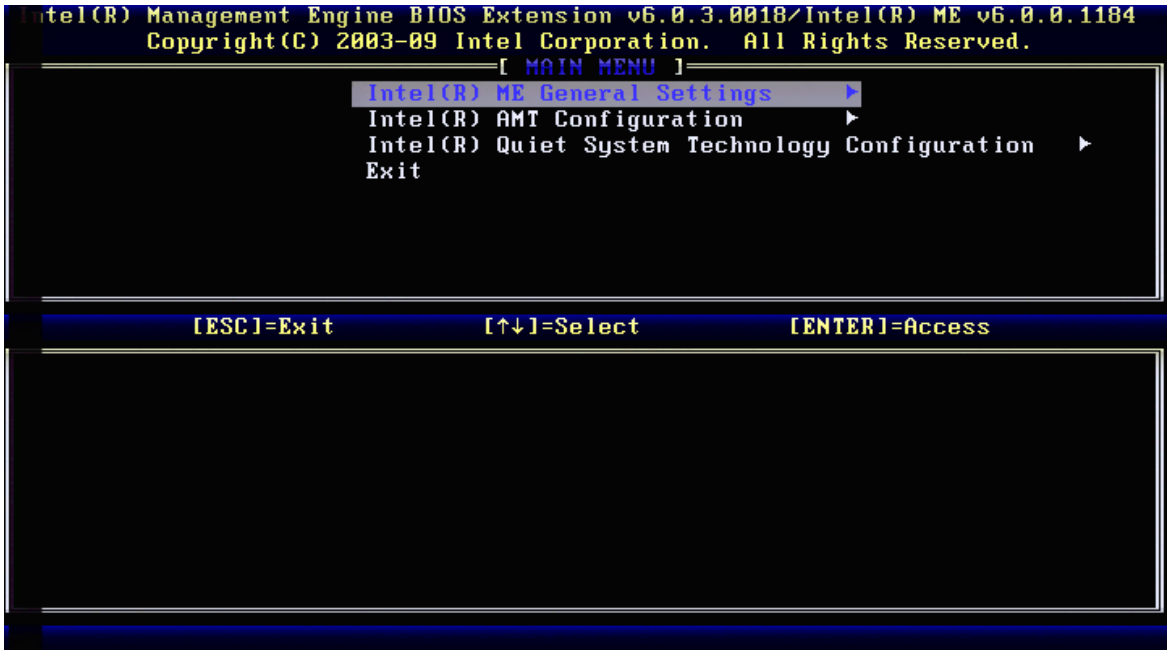
11. Select **Host Name**, as shown below.



12. **Enter the** Computer's name (same as the computer name in the OS) and then press the Enter key.



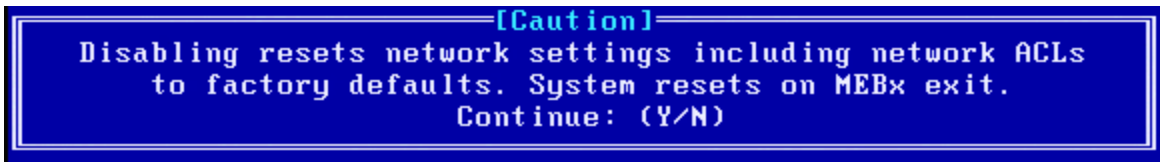
13. Press the Esc key three times to return back to the main menu, shown below.



14. Select **Intel® AMT Configuration**. Press the Enter key to bypass the prompt shown below.

15. Select **Manageability Feature Selection**, as shown below.

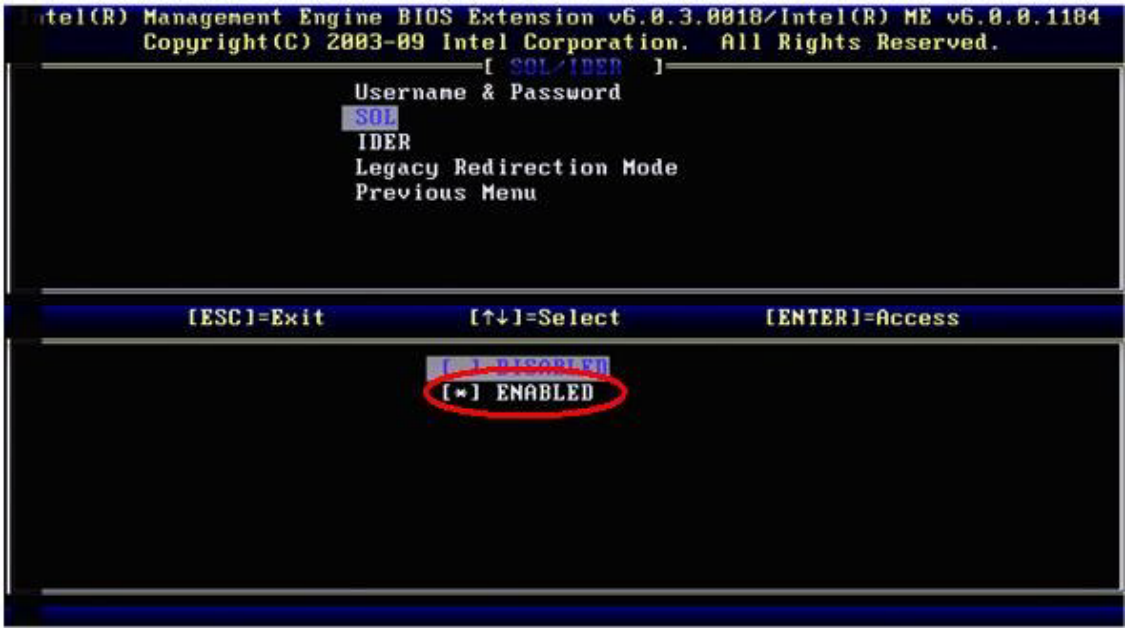
16. In the caution dialog shown below, type **Y** to continue.



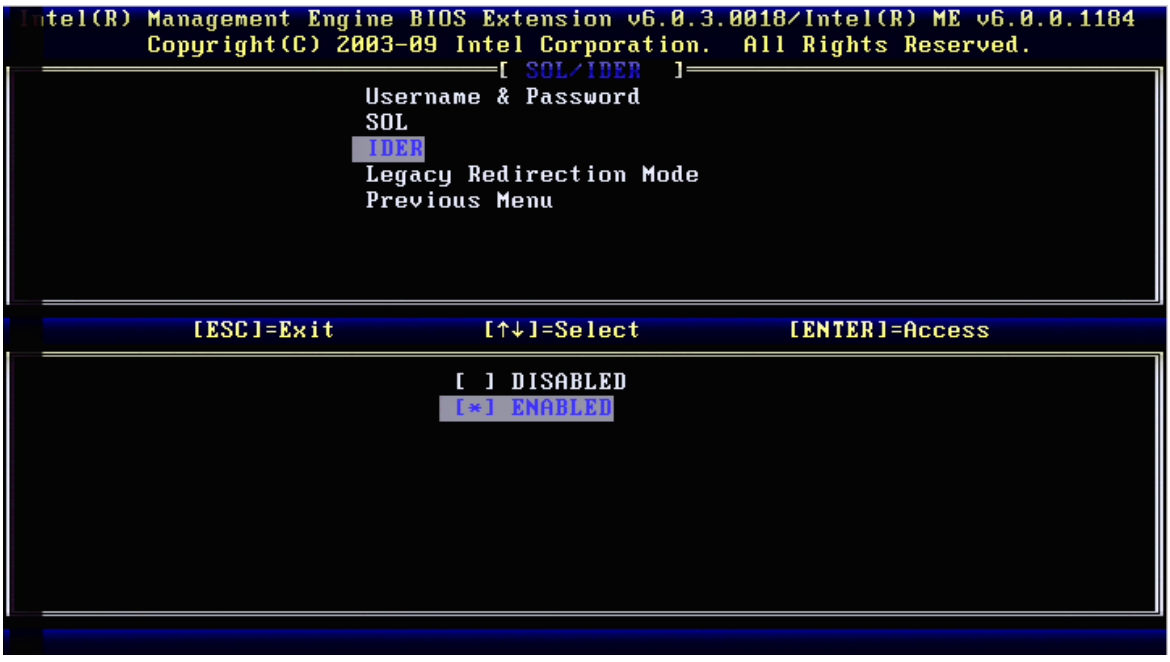
17. Verify the Manageability Feature Selection is set to **Enabled** (as indicated by the asterisk [*]). If not, change the setting.

18. Select **SOL/IDER**. The following screen is displayed.

19. Choose **SOL** and verify/set it to **Enabled** (as indicated by the asterisk [*]).

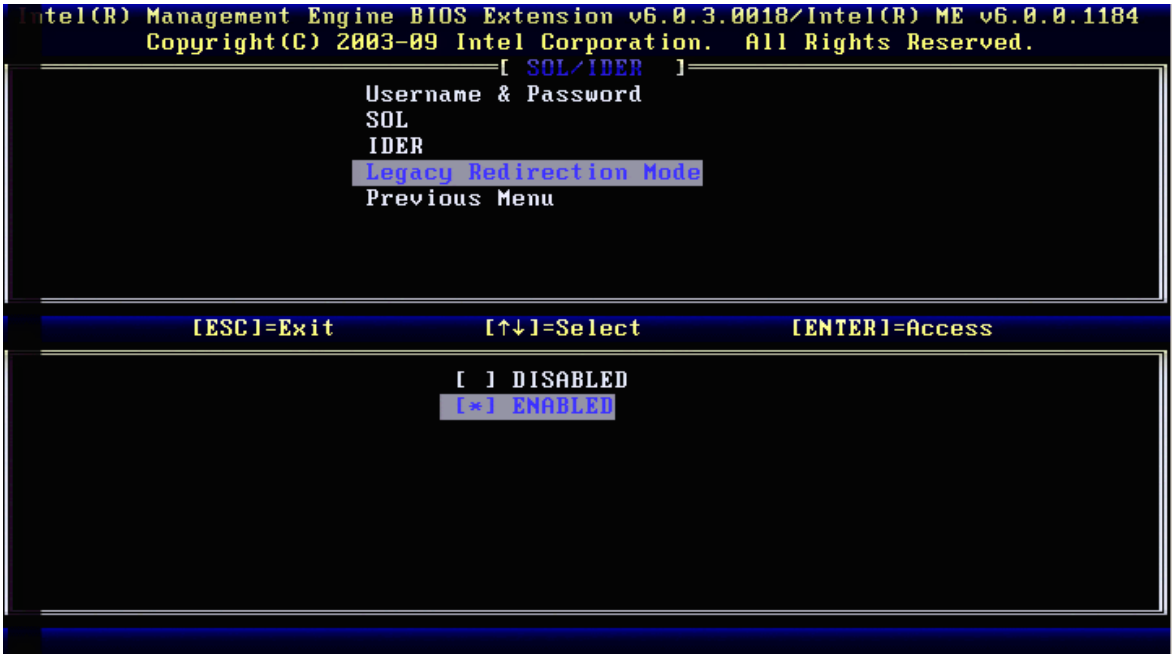


20. Choose **IDER** and verify/set it to **Enabled** (as indicated by the asterisk [*]).



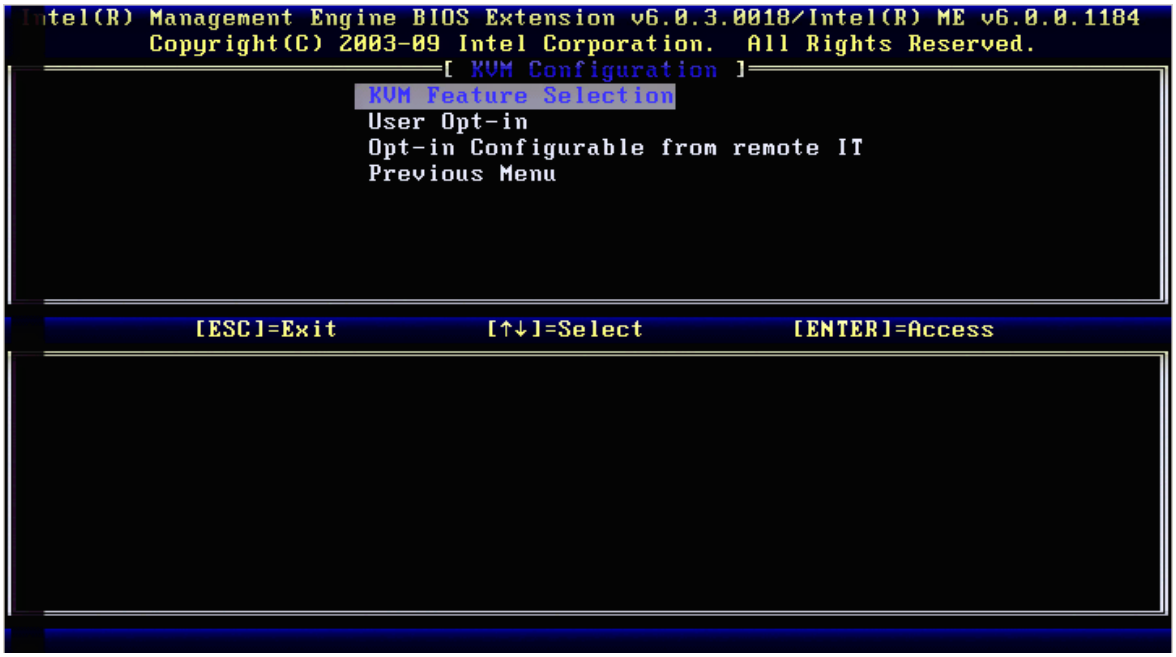
21. Select **Legacy Redirection Mode**. Press the Enter key to bypass the screen shown below.

22. Set **Legacy Redirection Mode** to **Enabled** (as indicated by the asterisk [*]).

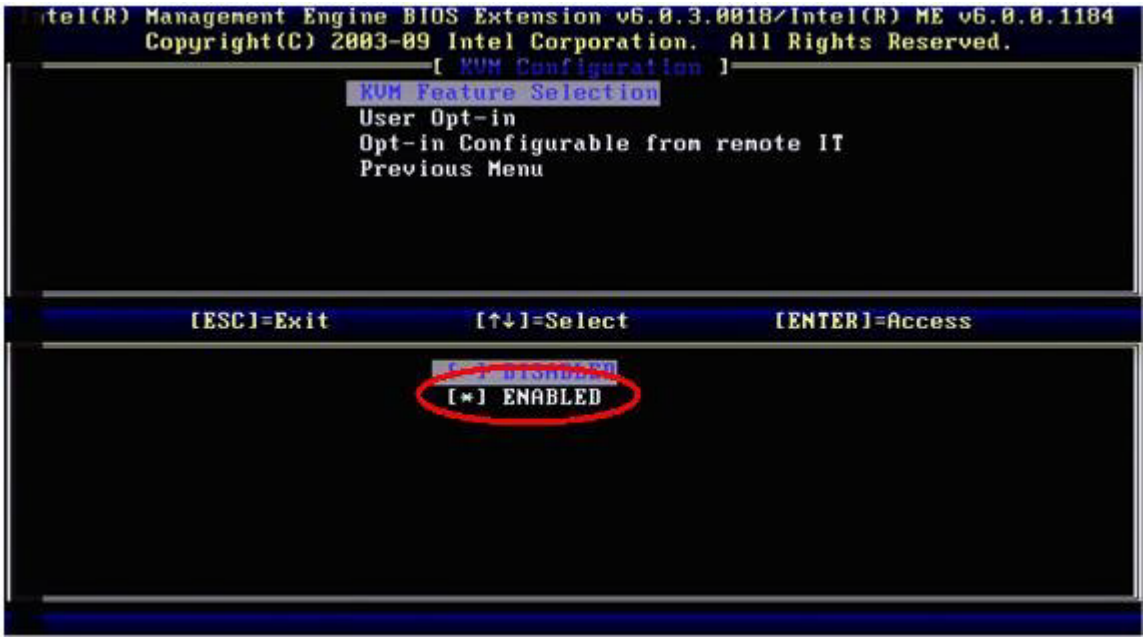


23. Press the Esc key to return to the previous menu.

24. Select **KVM Configuration**. The following screen is displayed.



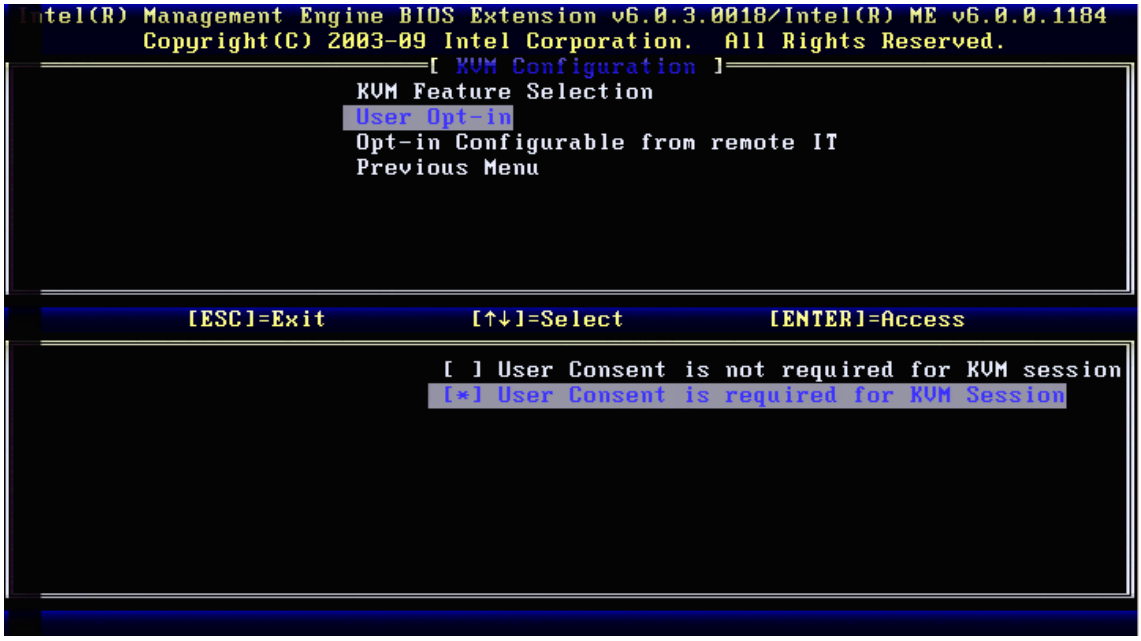
25. Select **KVM Feature Selection** and verify/set it to **Enabled** (***Note****: this is the master switch to turn KVM Remote Control on or off*).



26. Select **User Opt-in**. In the bottom pane, select **User Consent is required for KVM Session**, as shown below.

NOTE

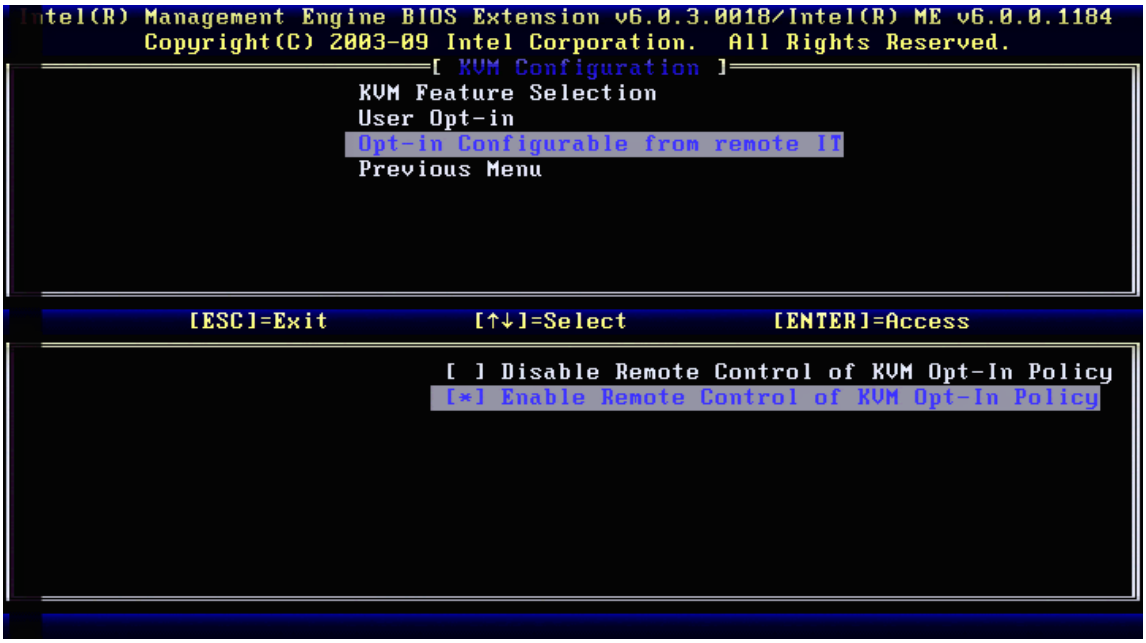
This is the default Opt-in setting. Opt-in means the local user has the ability to allow or deny a KVM connection. This will be demonstrated later in the document.



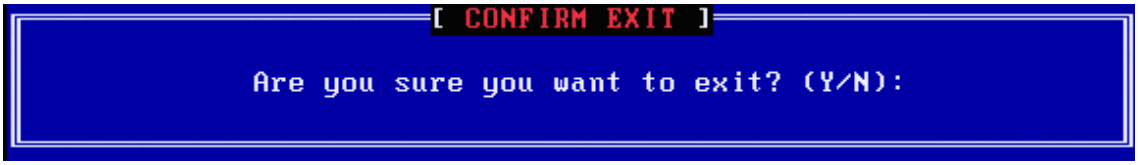
27. Select **Opt-In Configurable from remote IT**. In the bottom pane select **Enable Remote Control of KVM Opt-In Policy**.

NOTE

*Setting this field to **Enabled** allows an administrator to later turn **User Opt-In** on or off remotely, which allows the administrator to establish a KVM Remote Control session without requiring the client's user to consent to the session.*



28. Press the Esc key three times to exit the Intel MEBX. In the following dialog, enter **Y** to confirm exiting the Intel MEBX.



Intel AMT is now set up and (mostly) configured. The Intel ME has a new password, it is on the network, and Intel AMT's SOL, IDER, and KVM services have been enabled.

4 Prepare the Console

Before you can access your new Managed Client with Intel vPro technology via KVM Remote Control, you must prepare a management console by installing an RFB compliant viewer and configuring Windows Remote Management (WinRM) on the management console system.

4.1 Install an RFB Compliant Viewer

Your management console needs Windows Remote Management (WinRM) and an RFB compliant viewer such as RealVNC's VNC* Free Edition 4.1. A set of batch files is included in this Use Case Reference Design download package, along with this document, to make the process easier.

Start by copying those batch files to your console system in the folder c:\kvm. Next, you will need to set up an RFB compliant viewer. The document example uses RealVNC's VNC Free Edition 4.1. If you prefer to use a different RFB compliant viewer, you will need to set that up on your own.

NOTE

Any RFB compliant viewer will work. However, all steps in this document refer to RealVNC's VNC Free Edition 4.1.

1. Download the latest version (4.1 as of this writing) of RealVNC's VNC Free Edition viewer from the link below.

   http://www.realvnc.com/vnc/features.html

   As of this writing the resulting download file was vnc-4_1_3-x86_win32.exe.

2. Install the software. When you get to the Select Components screen change the setting to **VNC Viewer** only (i.e., deselect the server component, as shown below).

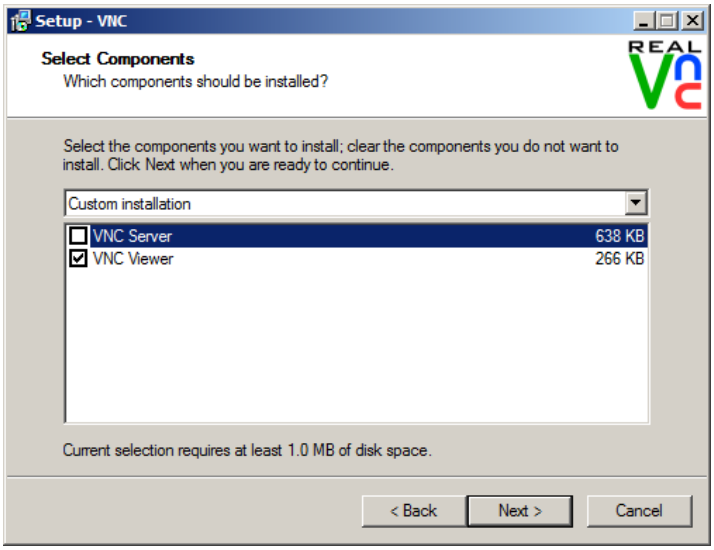


Figure 1: Setup - VNC Select Components Screen

3. Click **Next**.
4. Finish the installation using the default options (you can change them if you want. However, all you need is the viewer).

4.2 Configure WinRM

At this point you are ready to configure Windows Remote Management (WinRM). WinRM is needed to send WS-Man commands to Intel AMT. These commands allow the remote configuration of KVM Remote Control.

NOTE

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

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

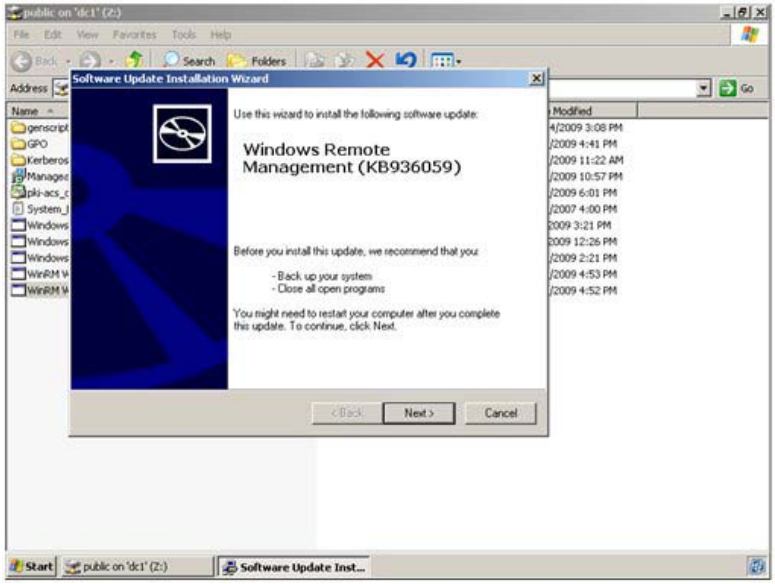


Figure 2: Installing WinRM in Windows XP

Once WinRM is on your console system, it must be configured. The procedure in this section makes use of a KVM Remote Control configuration application, kvm.hta.

The kvm.hta application is a simple HTML application that runs the batch files included in this Use Case Reference Design download package. These batch files make use of WinRM to change KVM Remote Control settings in the managed client's Intel AMT firmware. Note that these batch files can also be run standalone from the command line or by double clicking them, bypassing the need to open the rkvm.hta application.

NOTE

The steps below are specific to the example system being configured. However, depending on your console or viewer capability, some or all of this process may be automated.

1. Double Click c:\KVM\KVM.hta. If you have User Account Control enabled, right-click **KVM.hta** and select **Run as Administrator**.
2. In the KVM Remote Control Configuration dialog, click **Configure WinRM**, as shown below.

At this point you are finished preparing the console.

If interested, see Section 4.2.1 below for detailed information about the scripts that are run when you click **Configure WinRM**. If not, proceed to Section 5, Turn On and Configure KVM Remote Control, on page 27.

4.2.1 Detailed Information on Configuring WinRM

This section provides more technical details on the scripts used to configure WinRM. If you are not interested in this level of detail, proceed to Section 5, Turn On and Configure KVM Remote Control, on page 27.

Clicking **Configure WinRM** in the kvm.hta GUI causes the WinRMcfg.bat file to execute. WinRMcfg.bat contains the following three commands:

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

If desired, all included batch files may be run from a command line instead of using KVM.hta. The following steps illustrate the use of these batch files from the command line.

NOTE

*These steps are included for informational purposes only. They are not necessary if you have already configured WinRM using the **Configure WinRM** button in the KVM Remote Control Configuration dialog (kvm.hta).*

1. Open a command prompt (**Start -> Run** and enter **cmd**). If you have User Account Control enabled, right-click **cmd** and select **Run as Administrator**.

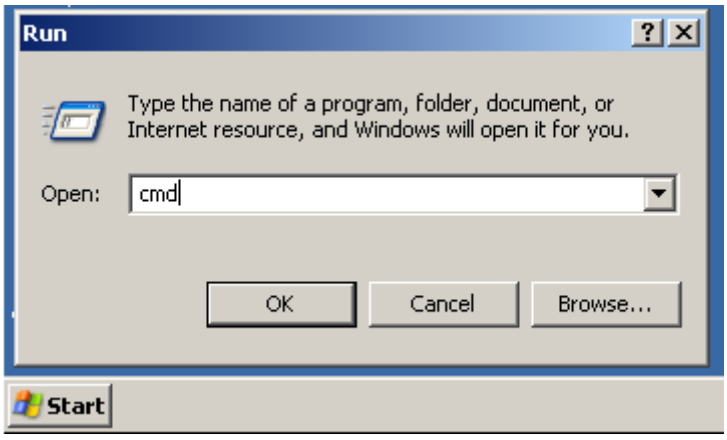


Figure 3: Open a Command Prompt Window

2. At the command prompt, type **cd /d c:\kvm**.

3. Type **WinRMcfg.bat**. The output is shown in Figure 4 below.

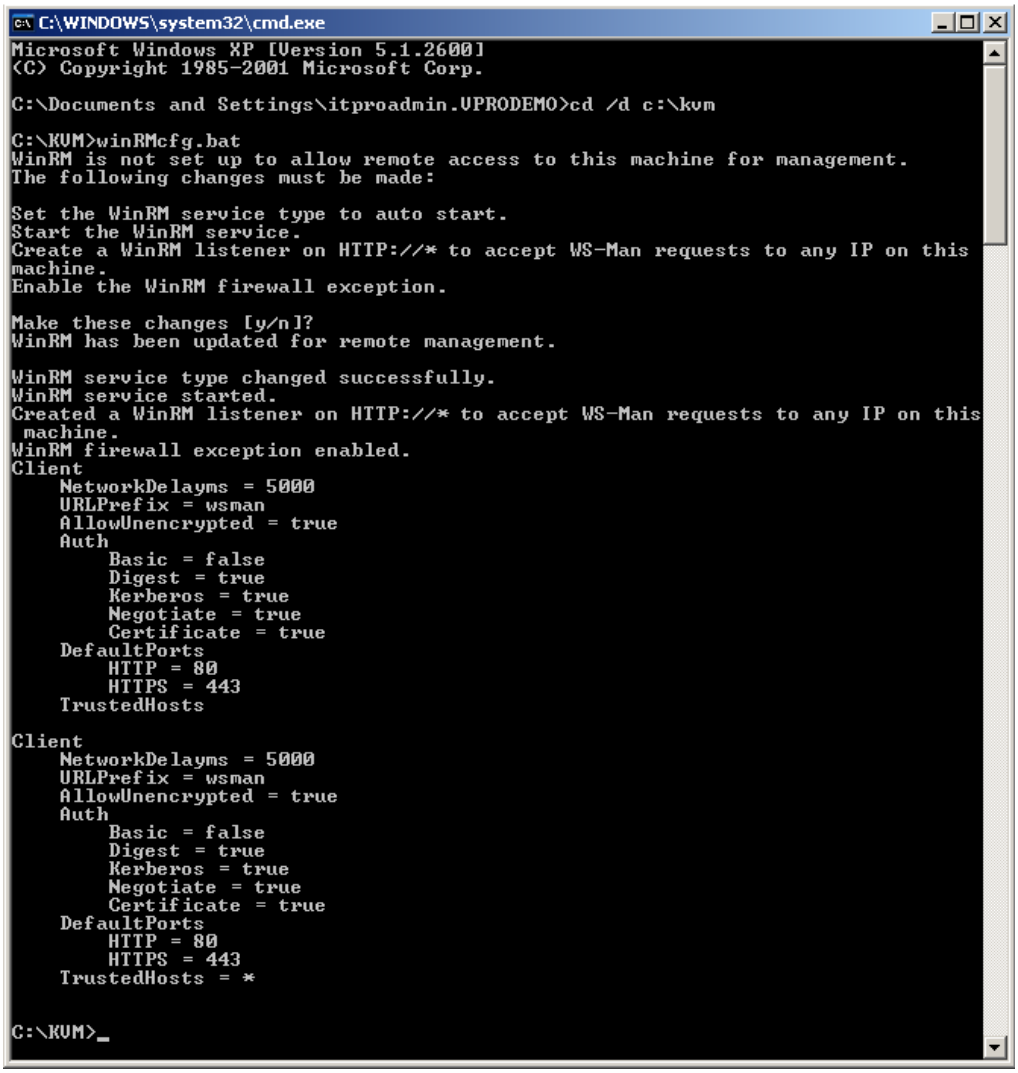


Figure 4: Command Prompt Window Output

4. Exit the command prompt by typing **exit** and pressing the Enter key.

5 Turn On and Configure KVM Remote Control

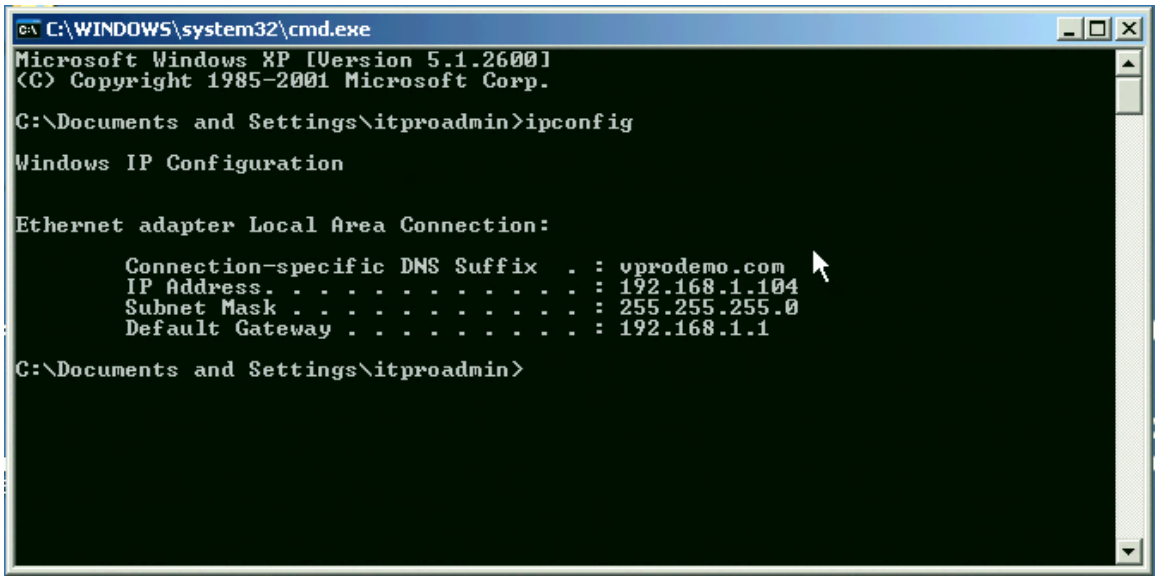
Before you can use KVM Remote Control, specific settings to enable KVM Remote Control must be set in the managed client's Intel AMT firmware. The document example shows this task being performed over a network, using WinRM to make the appropriate WS-MAN calls. The procedure in this section also makes use of a KVM Remote Control configuration application, kvm.hta.

NOTE

The steps below are specific to the example system being configured. However, depending on your console or viewer capability, some or all of this process may be automated.

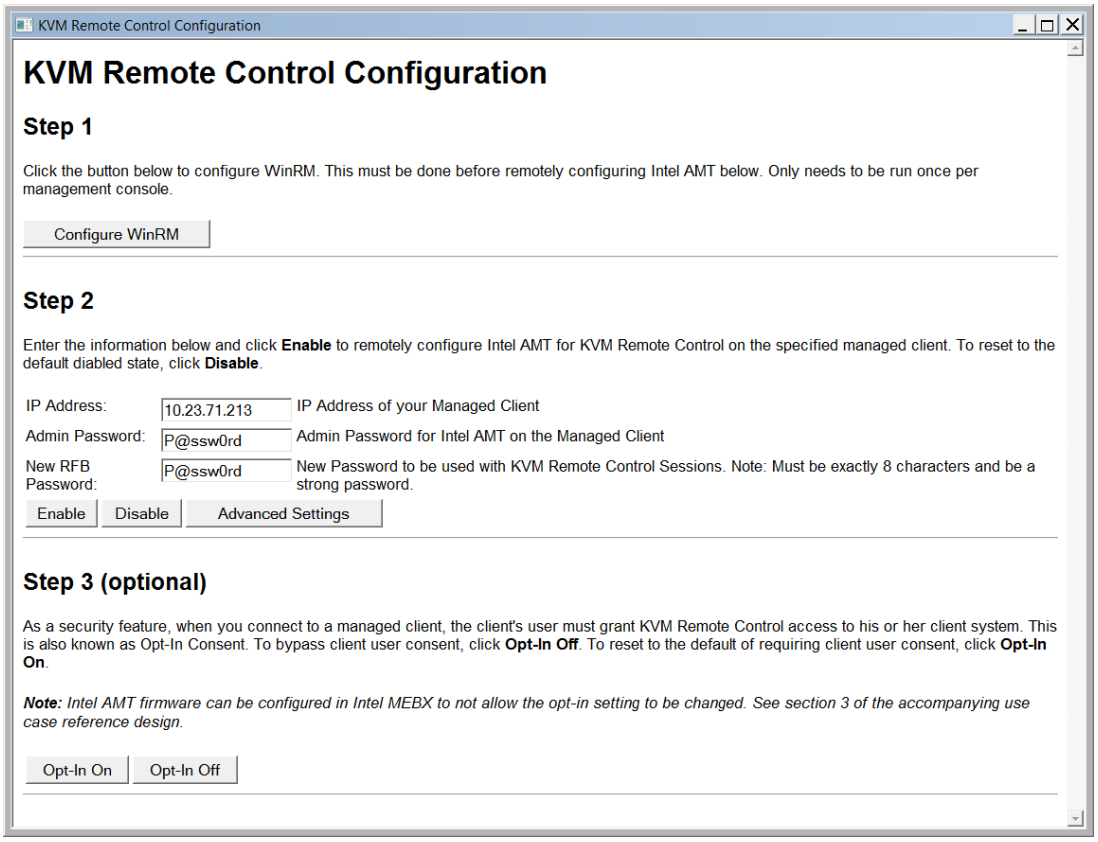
Follow the steps below to turn on and configure KVM Remote Control.

1. Obtain the client's IP address.
   a) Boot the client to Windows.
   b) Open a command prompt window (**Start -> Run**, then enter **cmd**).
   c) Type **ipconfig** and press the Enter key, as shown below.



2. On the console, log in with full administrator permissions.

3. Double-click c:\kvm**kvm.hta**. If you have User Account Control enabled, be sure to run this application as Administrator. The following screen is displayed.



4. In the section labeled **Step 2**, enter the IP Address and Intel AMT admin password for the managed client.

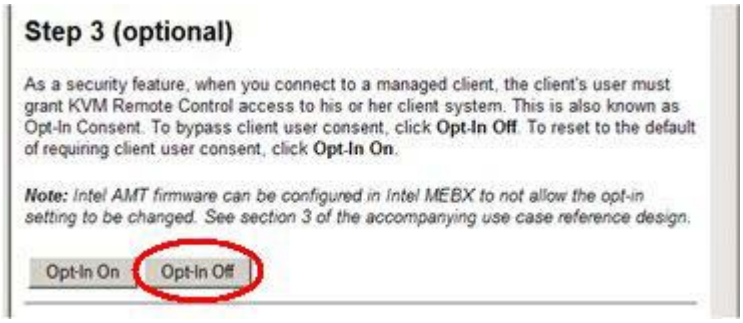
5. Enter a new RFB password (the password that will be used with KVM Remote Control sessions). Be sure to use a strong password, and note that the RFB password must be EXACTLY eight (8) characters long.

NOTE

The RFB Password is the password you will provide in your RFB compliant viewer when you connect to KVM Remote Control. This can be different than your Intel AMT password.

6. Click **Enable** to configure the managed client's Intel AMT firmware for KVM Remote Control using the settings you have entered. The output of this action is displayed in the lower pane, shown below.

7. (Optional) As a security feature, when you connect to a managed client, the client's user must grant KVM Remote Control access to his or her client system by providing a Client Consent Code. This is known as Opt-In Consent. If you want to bypass the Opt-In Consent feature (so that you are not prompted to enter a Client Consent Code when you connect to the client via KVM Remote Control), click **Opt-In Off** in the section labeled **Step 3 (optional)**, as shown below.



NOTES

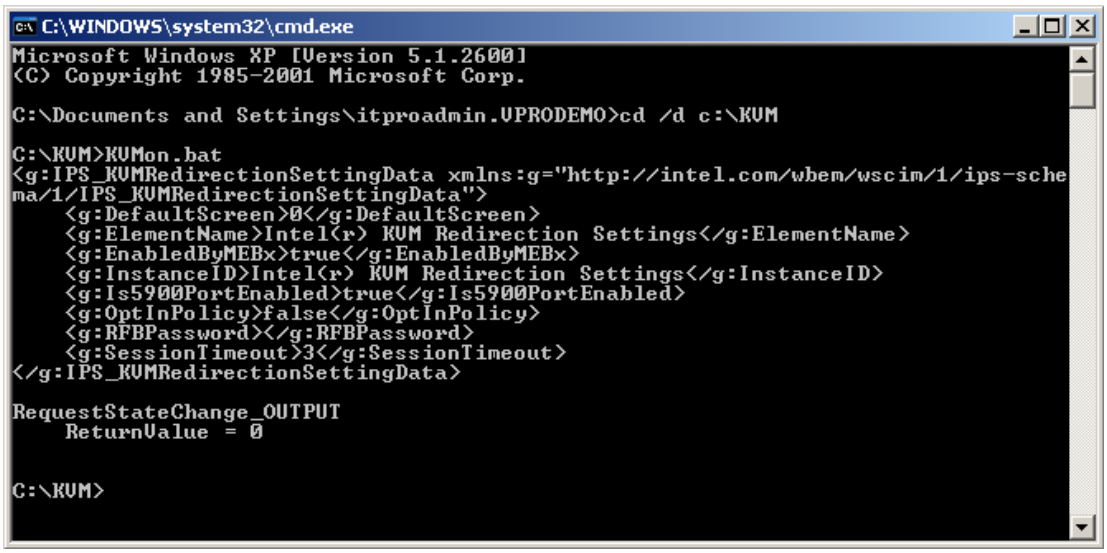
- *The instructions in Section 3 of this document configure Intel AMT to allow Opt-In Consent to be bypassed using the **Opt-In Off** button above. However, if the managed client's Intel AMT firmware has been configured to not allow Opt-In Consent to be bypassed, then setting the **Opt-In Off** button will not work, and you will still be prompted to enter a Client Consent Code when you connect to the managed client through KVM Remote Control. See Section 3, Prepare the Managed Client, step 27, page 20 for details.*
- *To turn Opt-In Consent back on, click **Opt-In On**.*

KVM Remote Control is now ready for use.

5.1 Configuration Details

This subsection contains more technical detail of what is taking place when the configuration batch files are run (i.e., when you click **Enable**). If you are not interested in this level of detail, skip ahead to Section 6.

The **Enable** button runs the batch file KVMon.bat. If you were to run KVMon.bat at the command prompt, the output would appear as shown in the figure below.



KVMon.bat contains the following two commands. If you choose to run these commands by entering them at the command prompt, be sure to substitute your specific values for the items in bold/underline (the rkvm.hta application does this for you when you enter the values in the GUI).

```
winrm put http://intel.com/wbem/wscim/1/ips-
schema/1/IPS_KVMRedirectionSettingData
@{Is5900PortEnabled="true";RFBPassword="P@ssw0rd"} -
remote:192.168.1.104:16992/wsman -u:admin -p:P@ssw0rd -a:Digest -encoding:utf-8 -
format:#pretty
winrm invoke RequestStateChange http://schemas.dmtf.org/wbem/wscim/1/cim-
schema/2/CIM_KVMRedirectionSAP @{RequestedState="2"} -
remote:192.168.1.104:16992/wsman -u:admin -p:P@ssw0rd -a:Digest -encoding:utf-8
```

NOTE

The RFBPassword value must be EXACTLY eight (8) characters long, and should be a strong password.

The first command instructs Intel AMT to enable the KVM Remote Control server to listen on port 5900 (Is5900PortEnabled), which is the default port an RFB compliant server listens on. This command also sets the RFB compliant viewer password to **P@ssw0rd** or whatever you changed it to when you edited the batch file (RFBPassword="P@ssw0rd"). The RFB password is specific to the RFB compliant server. That is, it can be different from the Intel AMT admin password. When you establish a session with a standard RFB compliant viewer, this is the password you will use.

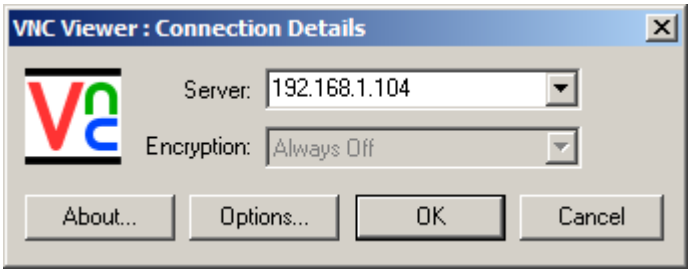
The second command starts the KVM Remote Control server. To turn it off, change the value of RequestedState from **2** to **3** ({RequestedState="2"} to {RequestedState="3"}). For added security, it is a good idea to turn off the server when it is not in use.

6 Using KVM Remote Control

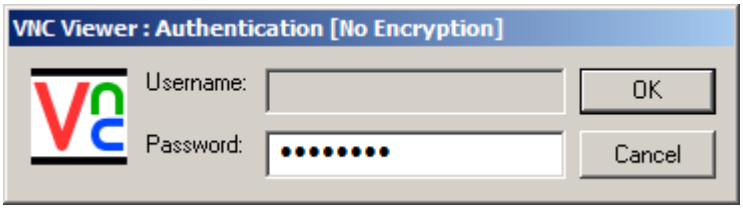
Now that KVM Remote Control is enabled in the Managed Client's Intel AMT firmware, this section describes how to use it to connect to the Managed Client.

The following steps would be followed in a scenario in which the user of a Managed Client calls his or her IT help desk, and the IT help desk staffer uses KVM Remote Control to establish contact with the user's system. The user then reads the User Consent Code over the phone to the IT Help Desk staffer, and the staffer enters it. Once in the User Consent Code is entered correctly, the IT Help Desk staffer has access to the user's Managed Client via KVM Remote Control.

1. On the Console open VNC Viewer (**Start –> Programs -> RealVNC -> Run VNC Viewer**).
2. Enter your Managed Client's IP address in the Server field, then click **OK**.



3. Enter your RFB Password (which you created in step 5 on page 29) and click **OK**.



4. A VNC Viewer session window is displayed and a prompt is displayed for you to enter a User Consent Code.

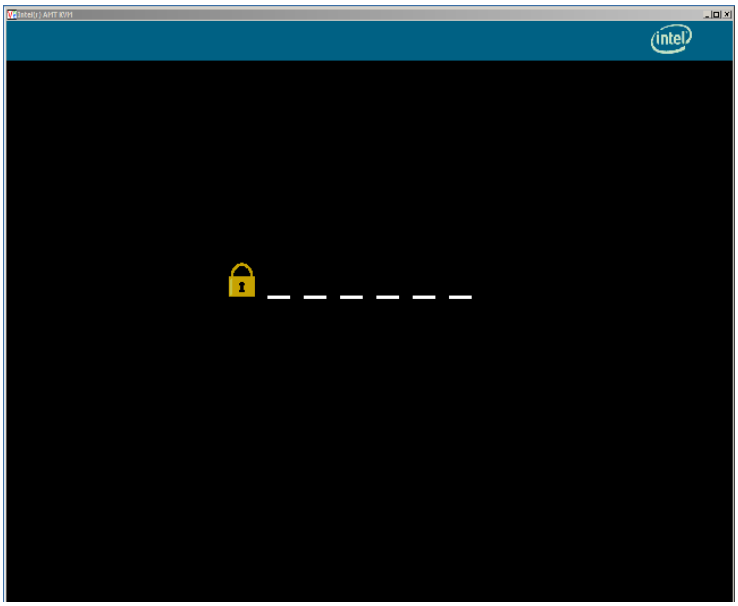


Figure 5: The VNC Viewer Console

At the same time, a User Consent Code is displayed on the Managed Client's screen, as shown below. In the example scenario, the Managed Client's user would read the User Consent Code over the phone to the IT Help Desk staffer.

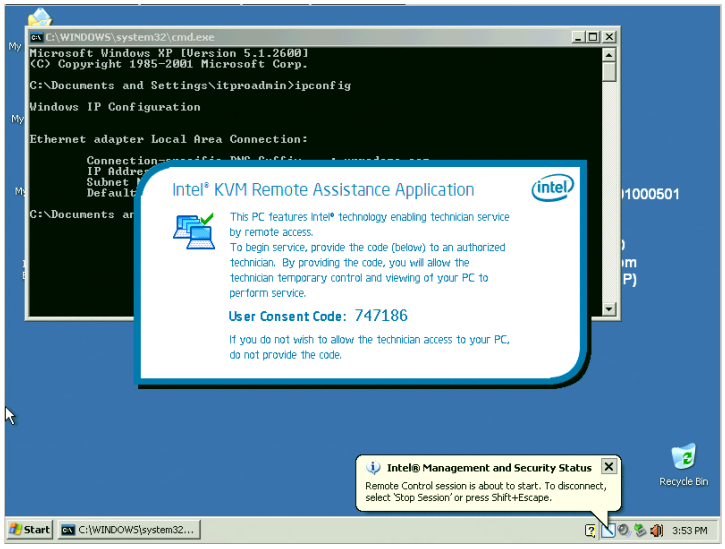


Figure 6: The Managed Client Displays a User Consent Code

5. On the Management Console, enter the consent code (**Note**: if your connection timed out, start again at step 1). You are now connected to the Managed Client via KVM Remote Control.

Congratulations, you have successfully accessed your new Managed Client using KVM Remote Control. At this point you can do anything as if you were working at the Managed Client's physical keyboard and monitor. From the console, try rebooting the client and then enter BIOS.

7 Advanced KVM Remote Control Topics

Now that you have a general understanding of KVM Remote Control, read on to gain further insight into deployment, security, and other features.

1. Can KVM Remote Control listen on a port other than 5900?

   Answer: You cannot choose which port KVM Remote Control listens on. However, KVM Remote Control has another mode in which it listens through a tunnel on port 16994/5. This is called the Redirection Listener.

2. What happens to a service in the OS running on port 5900?
   Answer: KVM Remote Control will accept and respond to the traffic before it reaches the OS. Move your OS service to another port, or, use the Redirection Listener.

3. What if I want more than one username/password or want to use Kerberos authentication for KVM Remote Control?

   Answer: Intel AMT does not support multiple user accounts or Kerberos when using port 5900. To enable take advantage of this support, use the Redirection Listener.

4. Can I use a viewer besides RealVNC's VNC Viewer Free Edition?

   Answer: Yes, any RFB compliant viewer will work when configured in the fashion outlined above. There are also enhanced viewers that support extended features such as encrypted communication, improved security models, automatic KVM Remote Control setup and configuration, and integration of other Intel vPro technology features such as Remote Power Control and SOL/IDER. One important feature that requires an enhanced viewer is the Redirection Listener.

5. What versions of RFB are supported by KVM Remote Control?
   Answer: 3.3, 3.8, and 4.0

6. What are some of the Security Risks of KVM Remote Control?

   Answer: Using a standard RFB compliant viewer in this way provides no encryption of the KVM Remote Control session. To gain encryption the Redirection Listener must be used.

   Leaving the KVM Remote Control server running poses a potential security risk in that someone may maliciously attempt to scan and/or connect to it. As such it is recommended that the KVM Remote Control server be disabled after use. This can be done with the following command:

   ```
   KVMoff.bat
   ```

   or

   ```
   winrm invoke RequestStateChange http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/CIM_KVMRedirectionSAP @{RequestedState="3"} -remote:192.168.1.104:16992/wsman -u:admin -p:P@ssw0rd -a:Digest -encoding:utf-8
   ```

   An enhanced viewer may also provide the ability to disable KVM Remote Control automatically when the session ends.

7. What is the Redirection Listener?

   Answer: Since Intel AMT does not support multiple logins, Kerberos logins, or encrypted sessions on port 5900, the Redirection Listener adds these capabilities. It works by creating an encrypted network tunnel through Intel AMT's redirection (aka SOL/IDER) service. The tunnel provides all the encryption and authentication you need. Once the tunnel is up, a standard RFB compliant session can take place inside the tunnel. To use the Redirection Listener, you need either an enhanced viewer with redirection support or a proxy capable of creating and managing a bridge between the viewer and the redirection tunnel.

8. What else can I do with WinRM?

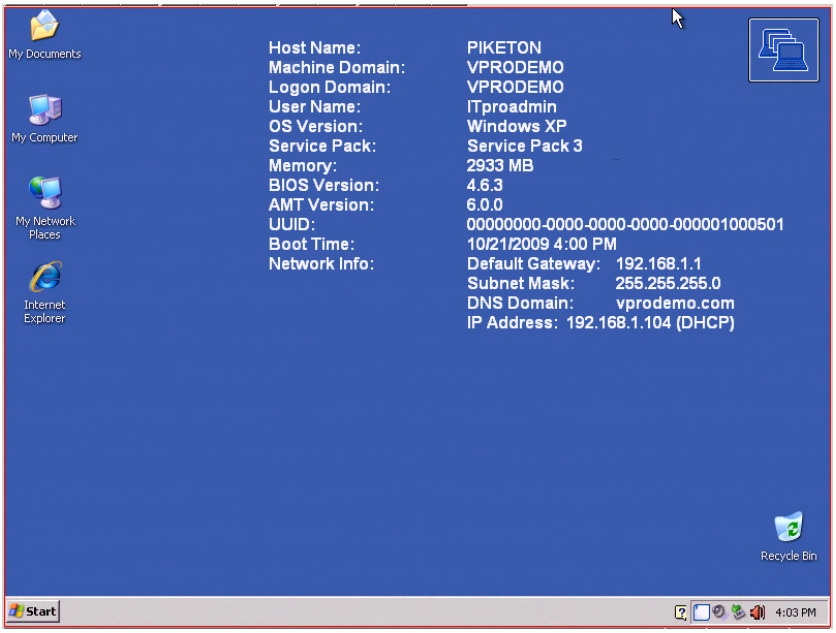
   Answer: Additional WinRM features are beyond the scope of this document. See the Intel AMT SDK for more information, and post your questions to the Intel® vPro Expert Center or Intel Software Communities.

   http://communities.intel.com/community/openportit/vproexpert

   http://software.intel.com/en-us/

9. Can the user determine if their system is being controlled?

   Answer: When a user's system is being controlled, a red border appears around the edge of their screen and a blinking sprite appears in the upper right corner, as shown below.



10. What happens to the User Consent dialog, red border, and sprite if the OS is not running?

    Answer: The User Consent dialog, red border, and Sprite are all driven by the Intel ME. As such they will appear regardless of the OS state. In fact, the OS is not even aware of them.

11. Can the user disconnect the KVM Remote Control session?

    Answer: If the OS is up and the Intel® Management and Security Status tool is installed (part of the Intel ME driver set), the user can use Intel Management and Security Status to disconnect the KVM Remote Control session. However, without Intel Management and Security Status the user cannot disconnect the session, except by unplugging the network. By default, <Shift> + <Esc> will disconnect the session via Intel Management and Security Status.

12. What if I don't want use User Opt-In?

    Answer: If User Opt-In was configured in the Intel MEBX as outlined in Section 3, Prepare the Managed Client, it can be turned on and off remotely by using KVM.hra or by running the following commands on the console. If it is off, once you enter the RFB Password you will take immediate remote control. Another option is to set your desired setting in the Intel MEBX.

User Opt-In On

OptinOn.bat or

winrm put http://intel.com/wbem/wscim/1/ips-schema/1/IPS_KVMRedirectionSettingData @{OptInPolicy="true"} -remote:**192.168.1.104**:16992/wsman -u:admin -p:**P@ssw0rd** -a:Digest -encoding:utf-8 -format:#pretty

User Opt-In Off

OptinOff.bat

or

winrm put http://intel.com/wbem/wscim/1/ips-schema/1/IPS_KVMRedirectionSettingData @{OptInPolicy="false"} -remote:**192.168.1.104**:16992/wsman -u:admin -p:**P@ssw0rd** -a:Digest -encoding:utf-8 -format:#pretty

13. Can I use KVM Remote Control over a Fast Call for Help link?

    Answer: KVM Remote Control works over a Fast Call for Help link. Your viewer will need to support use of a Socks Proxy. For information on Fast Call for Help: http://communities.intel.com/community/openportit/vproexpert/blog/2009/09/20/webinar-now-available-for-on-demand-viewing-fast-call-for-help

14. Where can I buy an enhanced viewer?

    Answer: Contact a preferred console vendor about adding support. Many are already working to add this support.

15. What level of Intel AMT firmware user permissions are required to access KVM Remote Control?

    Answer: For enabling KVM Remote Control and setting the User Opt-In policy, the user must have Intel AMT administrative level permissions. For all other functions, including setting the RFB Password, enabling the default or redirection listener, and connecting and using KVM Remote Control, only redirection permissions are required. Generally, it is a recommended minimum to give a help desk user redirection and remote control permissions. Note that this can create a challenge when using an enhanced viewer that configures KVM Remote Control at the time the session is established. The challenge is that the help desk user will not have access to enable KVM Remote Control. For more information on help desk permissions framework see: http://communities.intel.com/docs/DOC-4404

16. I'm ready to deploy this into my production environment. What do I do?

    Answer: You must choose a viewer (standard or enhanced) and a method of setting up and configuring KVM Remote Control. See below.

Standard Viewer

Pros:

- Common in many production environments
- Widely used

Cons:

- Single password for KVM Remote Control server
- No Kerberos Support
- Unable to set up and configure KVM Remote Control
- KVM Remote Control session is not encrypted

Enhanced Viewer (check with the vendor as actual feature lists will vary)

Pros:

- Multiple User Accounts including Kerberos support
- Support for Encrypted RFB sessions
- Setup and/or configuration of KVM Remote options on the fly.
- Integration of other vPro features such as SOL/IDER or Fast Call for Help

Cons:

- May be a new application to support in your environment.

For setup and configuration you have two options. First, you could use an enhanced viewer or management console that can configure KVM Remote Control for you. Alternatively, you could create your own script or application to perform the setup and configuration of KVM Remote Control, thereby building on the example here and in the Intel AMT 6 SDK. In either case, there are generally two methods to choose from: "pre-configure" or "when needed".

Pre-Configure:

1. Set up and configure Intel AMT (locally or remotely)
2. Set up and configure KVM Remote Control (remotely) one time.
3. When KVM Remote Control is needed, just access the system via KVM Remote Control.

Pros:

- Standard or Enhanced RFB compliant viewer
- KVM Remote Control server is available on demand
- Supports Help Desk level permissions.

Cons:

- For a standard viewer KVM Remote Control is always listening.

  Note – an enhanced viewer can still enable the listener when needed with helpdesk level AMT permissions.
- One time setup can cause a scaling issue for a single server configuring a large number of clients.

- May require upgrading an existing Intel AMT setup and configuration server to gain this support.

When Needed:

1. Set up and configure Intel AMT (local or remote)
2. When KVM Remote Control is needed:
   - Set up and configure KVM Remote Control
   - Access the system via KVM Remote Control
   - Disable KVM Remote Control

Pros:

- KVM Remote Control is only listening when needed for enhanced security.
- No scaling concern since KVM Remote Control is configured by the console when needed.
- KVM Remote Control server is available on demand.
- Works with existing Intel AMT setup and configuration server deployments.

Cons:

- Enhanced RFB compliant viewer only (or some creative scripting)
- User needs Intel AMT Admin level permissions

Check with your viewer and Intel AMT setup and configuration server for a list of supported options. This will help in determining the method you choose.