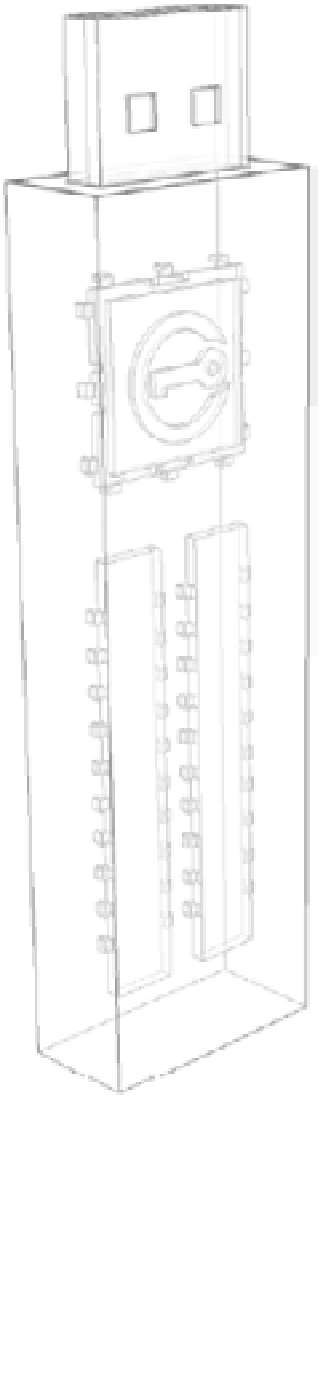
IRONKEY
Setup Guide

IronKey Enterprise Server 5.0

IRONKEY™ by imation

Last Updated September 2013



Thank you for your interest in IronKey™ Enterprise Server by Imation.

Imation's Mobile Security Group is committed to creating and developing the best security technologies and making them simple-to-use, affordable, and available to everyone. Years of research and millions of dollars of development have gone into bringing this technology to you.

We are very open to user feedback and would greatly appreciate hearing about your comments, suggestions, and experiences with this product.

Feedback:
securityfeedback@imation.com

User Forum:
https://forum.ironkey.com

Note: IronKey is not liable for technical or editorial errors and/or omissions contained herein; nor for incidental or consequential damages resulting from the furnishing or use of this material. The information provided herein is subject to change without notice.

The information contained in this document represents the current view of Imation on the issue discussed as of the date of publication. Imation cannot guarantee the accuracy of any information presented after the date of publication. This document is for information purposes only. Imation makes no warranties, expressed or implied, in this document. Imation, the Imation logo, IronKey and the IronKey logo are trademarks of Imation Corp. and its subsidiaries. All other trademarks are the property of their respective owners.

IronKey Enterprise Server v5.0.0.0 software – August 2013. Part Number 05.011.024.04 Rev. A

CONTENTS

About This Guide

This guide describes the steps required to install and get the most out of IronKey Enterprise Server by Imation. It also describes best practices for deploying and managing IronKey devices in your enterprise environment. The second half of this document lists the commands available to customize and configure the server.

This guide contains the following topics:

- *About the IronKey Enterprise Server*: Product overview and specifications, contacting IronKey support
- *Installing the IronKey Enterprise Server*: Instructions for installing the software, activating your Enterprise Account and initializing an IronKey; also includes information about upgrading the Server from a previous version
- *Customization and Configuration Reference*: List of CLI commands

Conventions Used in This Guide

Item	Description
Bold	Button and field names
Italic	Book names, new terms, important items
Italic Bold	URLs
`Monospaced`	Commands, file names, and items typed by the user

Related Documentation

The following documents are also available:

- *IronKey Enterprise Server Quick Start Guide*
- *IronKey Enterprise Server Admin Guide*
- *IronKey Enterprise User Guide*
- *IronKey Workspace W500 On-Premise Server Edition—Deployment and Installation Guide (This document comes with the IronKey Workspace W500 product)*

About IronKey Enterprise Server

Overview

IronKey Enterprise Server is the world's most secure enterprise solution for managing USB flash drives. Installed and managed in your own data center, it gives you control over protecting your organization's portable data and ensures that IronKey security policies are enforced.

IronKey Enterprise Server consists of three interrelated elements:

- The IronKey Enterprise Secure Flash Drive
- Applications bundled on the IronKey (based on policy configuration)
- The IronKey Enterprise Management Console that provides centralized administrative capabilities to your IronKey administrators

System Requirements

IronKey Enterprise Server cannot be installed on any virtual machines (ESXi, Hyper-V, Virtualbox).The minimum requirements for IronKey Enterprise Server include:

PC HARDWARE

- Pentium Core2Duo or higher class system (quad-core recommended)
- 2GHz or faster CPU minimum

OPERATING SYSTEM

Windows Server 2003 or Windows Server 2008

MEMORY

2048MB minimum (4GB is recommended)

DISPLAY

16-bit (32-bit display adapter is recommended)

DATABASE

Microsoft SQL Server 2005 or Microsoft SQL Server 2008

DISK DRIVES

Hard Disk

- IDE and SCSI hard drives supported.
- 7GB free disk space required; 15GB recommended.

Optical CD-ROM/DVD-ROM Drive

- IDE and SCSI optical drives supported.
- CD-ROM and DVD-ROM drives supported.
- ISO disk image files supported.

LOCAL AREA NETWORKING

Any Ethernet controller supported by the host operating system.

Common Terminology

Item	Description
Server Admin	The administrator who manages the host machine and CLI for the IronKey Enterprise Server
System Admin	The administrator who manages end-users and their IronKey devices when the server is set up
Device	Generic term for an IronKey Enterprise Secure Flash Drive
CLI	The Command Line Interface used to configure the system

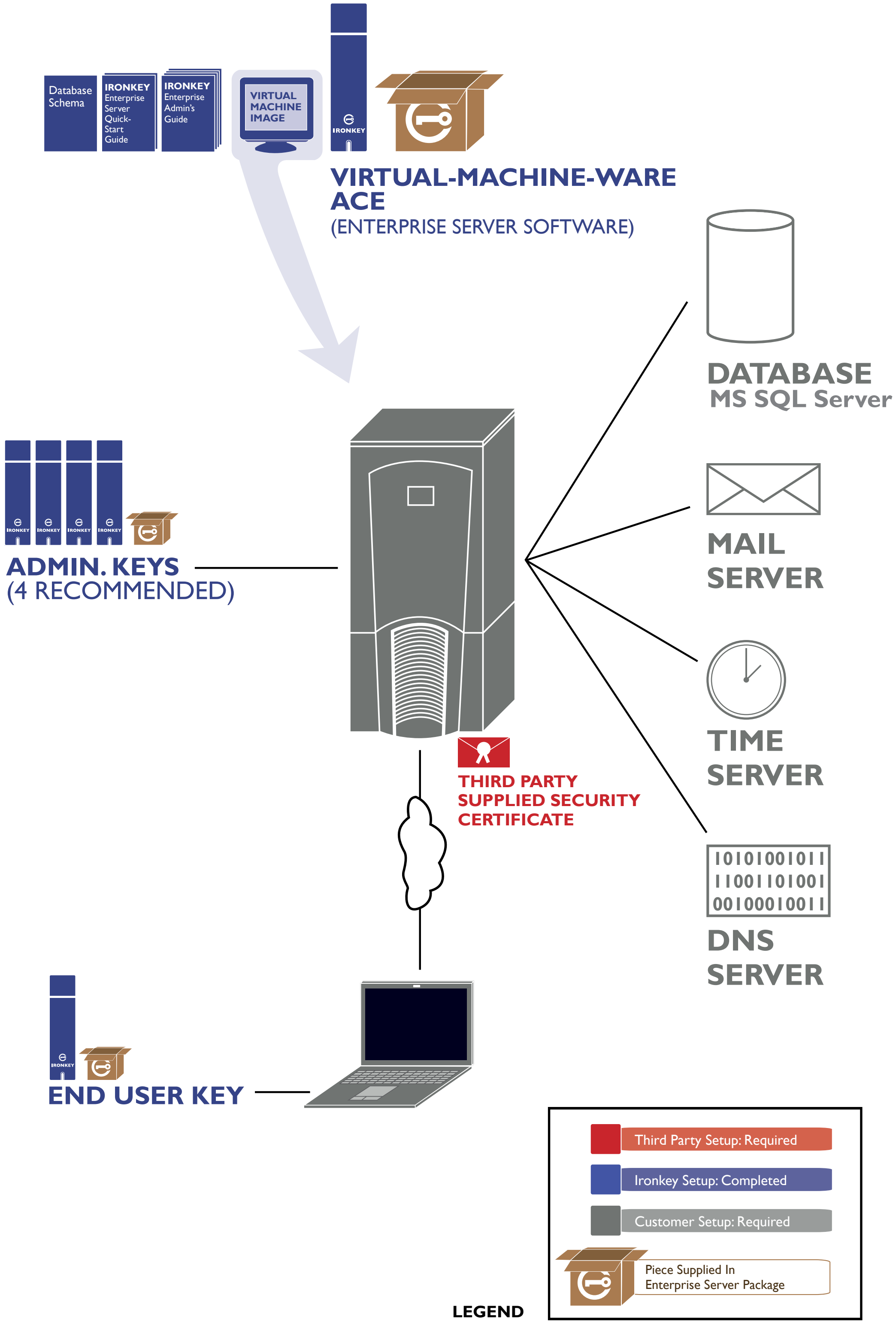
What's in the Box?

The IronKey Enterprise Server Software Kit contains six IronKey x250 devices:

- One Setup device that contains the necessary software for installing the IronKey Enterprise Server.
- Four System Admin devices
- One Standard User device to be used for testing

Product Architecture

This architectural diagram shows a system-level map of the IronKey Enterprise Server.


Database Schema
IRONKEY Enterprise Server Quick-Start Guide
IRONKEY Enterprise Admin's Guide
VIRTUAL MACHINE IMAGE
IRONKEY
VIRTUAL-MACHINE-WARE ACE
(ENTERPRISE SERVER SOFTWARE)
DATABASE
MS SQL Server
MAIL SERVER
TIME SERVER
10101001011
11001101001
00100010011
DNS SERVER
ADMIN. KEYS
(4 RECOMMENDED)
THIRD PARTY SUPPLIED SECURITY CERTIFICATE
END USER KEY
🟥 Third Party Setup: Required
🟦 Ironkey Setup: Completed
⬛ Customer Setup: Required
Piece Supplied In Enterprise Server Package
LEGEND

IronKey Enterprise Server Support

IronKey is committed to providing world-class support to its enterprise customers. IronKey technical support solutions and resources are available through the IronKey Support website, located at *support.ironkey.com* For more information, see “Contact information” on page 7.

Standard Users

Please have Standard Users contact your Help desk or System Administrator for assistance. Due to the customized nature of each IronKey Enterprise Account, technical support for IronKey Enterprise products and services is available for System Administrators only.

System Administrators

Administrators can contact IronKey Support by:

» Filing a support request at https://support.ironkey.com.

» Sending an email to *securityts@imation.com*

IMPORTANT: Always reference your Enterprise Account Number. The Account Number is located on the Enterprise Support page of the Admin Console.

To access resources on the Enterprise Support page

- In the Admin Console, click “Enterprise Support” in the left sidebar.

NOTE Resources available on this page include your Account number, video tutorials and product documentation, contact information for IronKey Technical Support and company holidays.

CONTACT INFORMATION

https://forum.ironkey.com	Online forum with thousands of users and security experts
support.ironkey.com	Support information, knowledge base and video tutorials
securityfeedback@imation.com	Product feedback and feature requests
www.ironkey.com	General information
securitycs@imation.com	All licensing and account questions

910 E. Hamilton Ave. Suite 410
Campbell, CA 95008   UNITED STATES
Monday - Friday, 6am - 5pm PST excluding company holidays (see Enterprise Support page)

Installing IronKey Enterprise Server

Before Starting

To speed up your installation, work with the relevant internal groups and service providers to gather the required information and resources listed below. Use the *Installation Worksheet* on page 9 to help you collect and organize this information. The *Setup Check List* on page 10 can help you track setup tasks as you complete them.

- Any required network information that you need to setup a new machine in your data center. This information includes DNS, Gateway, IP assignment, SMTP, and NTP information.
- Database administration access for your Microsoft SQL Server that you need to install an instance of the database.
- Access to the network, systems, and ports that the above components will require.
- An SSL website certificate—from an approved Certificate Authority vendor (VeriSign, RSA Security Inc., Thawte, GoDaddy, Comodo, Entrust.net, GeoTrust, Valicert, Visa, BeTrusted, Aba.com, AddTrust, Baltimore, DST, GTE, GlobalSign, Sonera, TC TrustCenter)
- A host computer with network capability and sufficient configuration (disk, memory) required to support the software you will install (see "System Requirements" on page 4)
- The Welcome Email you received from Customer Service at IronKey.

In addition, you need:

- The IronKey Setup Device that contains the Enterprise Server software
- One IronKey device from the kit, which will be for a System Admin

After you have the required information and resources, installation takes about an hour to complete.

Installation Worksheet

Use this worksheet to list the information needed to set up the IronKey Enterprise Server.

Enterprise Account Number (from Welcome Email)	
Password for the Setup Device (from Welcome Email)	
Installation Password (VMware ACE) (from Welcome Email)	
CLI User Name (from Welcome Email)	
CLI Password (from Welcome Email)	
Host Name (to be assigned to the Enterprise Server)	
DNS server IP	
Static IP Address (assigned to Enterprise Server)	
Subnet Mask (for Enterprise Server)	
Default Gateway IP (for Enterprise Server)	
NTP server IP or FQDN (optional)	
SMTP server IP or FQDN (check if your SMTP required a password)	
Database server FQDN or IP	
Database Port	
Database User Name and Password (required: db_owner privileges)	
Database Name (recommended: `es_master`)	
Site Name for SSL certificate (FQDN of server used on certificate)	
SSL certificate file AND a certificate chain file	
IP or FQDN for syslog server (optional)	
Primary Admin: Email and User Name	
Secondary Admin: Email and User Name	

Setup Checklist

Use this list to track each setup task as you complete it.

- ❑ Welcome Email received from IronKey, Inc.
- ❑ IronKey Enterprise Server Software Kit received
- ❑ *Installation Worksheet* filled out
- ❑ External ports open (see "External Ports" on page 11)
- ❑ Third-party SSL Certificate ready (see "Certificate Acquisition" on page 12)
- ❑ SQL Server database configured (see "Database Setup" on page 13)
- ❑ Setup Device from Software Kit unlocked with password from Welcome Email
- ❑ IronKey Enterprise Server VM installed
- ❑ IronKey Enterprise Server configured with required information
- ❑ IronKey Enterprise Account successfully created
    - ❑ Account number entered from Welcome Email
    - ❑ IronKey License Request created & sent to IronKey Customer Service
    - ❑ License Key from IronKey Customer Service entered in Server
    - ❑ Default IronKey Policy created
    - ❑ Contact information for two System Admins entered
- ❑ First System Admin's IronKey device activated — can access Admin Console
- ❑ Second System Admin added and approved — can access Admin Console
- ❑ IronKey Enterprise Server Admin Guide reviewed for deployment

External Ports

For full functionality of devices (for example, Silver Bullet Service and activation), you must open the external ports in the following table. The "DNS Name" must be a Fully Qualified Domain Name (FQDN) for a certificate from an approved certificate authority. (See "Certificate Acquisition" on page 12 for a list of approved certificate authorities.)

FQDN Example:

<server>.<second level domain>.<top level domain>
myhost.domain.com

NOTE: To use Anti-Malware Service, you must allow outbound communication from your server and devices to McAfee at *http://update.nai.com/Products/CommonUpdater*. Alternatively, you can host anti-virus update files on one of your own web servers. See "Hosting McAfee Anti-Malware Updates" on page 41 for more information.

Application Name	DNS Name	SSL Configuration Internal VIP	Component Name	Ports	
				External SSL Port	External Non-SSL Port
My IronKey	<server>.<full domain name>	Normal SSL	Website and Application	443	80
Web Services	<server>.<full domain name>	Client Authentication Required	Web Services	2000	
Device Updates Phase1	<server>.<full domain name>	Client Authentication Required	Web Services	2001	
Device Update Phase 2	<server>.<full domain name>	Non-SSL	Web Services		2002
Silver Bullet	<server>.<full domain name>	Normal SSL	Web Services	2003	
Device Activation	<server>.<full domain name>	Client Authentication Required	Web Services	2004	

Certificate Acquisition

You must have a valid public domain for your public SSL certificate from an approved certificate authority to complete the IronKey Enterprise Server configuration.

APPROVED CERTIFICATE AUTHORITIES

The device is pre-packaged with root certificates from approved certificate authorities:

VeriSign, RSA Security Inc., Thawte, GoDaddy, Comodo, Entrust.net, GeoTrust, Valicert, Visa, BeTrusted, Aba.com, AddTrust, Baltimore, DST, GTE, GlobalSign, Sonera, TC TrustCenter

ACQUIRING AND INSTALLING AN SSL CERTIFICATE

1. Download the OpenSSL binary for Windows at the URL below and install it at the default location on the computer where Enterprise Server will be installed.

   http://downloads.sourceforge.net/gnuwin32/openssl-0.9.8h-1-setup.exe

2. Generate 2048-bit RSA key pair using the CLI command:

   Server 2003:
   ```
   c:\program files\gnuwin32\bin\openssl genrsa -f4 -out host.key 2048
   ```

   Server 2008:
   ```
   c:\program files(x86)\gnuwin32\bin\openssl genrsa -f4 -out host.key 2048
   ```

3. Start generation of the CSR (Certificate Signing Request) using this CLI command:

   Server 2003:
   ```
   c:\program files\gnuwin32\bin\openssl req -config "c:\program files\gnuwin32\
   share\openssl.cnf" -new -nodes -key host.key -out host.csr
   ```

   Server 2008:
   ```
   c:\program files(x86)\gnuwin32\bin\openssl req -config "c:\program files(x86)\
   gnuwin32\share\openssl.cnf" -new -nodes -key host.key -out host.csr
   ```

   Follow the CLI prompts and enter the information as requested.

   IMPORTANT: You must use the Fully Qualified Domain Name (FQDN) of the Enterprise Server as the SSL Certificate's Common Name). You will probably want to enter the Organization Name (your company name). Your Certificate Authority provider might require you to enter information in other fields to process the CSR.

4. Send host.csr file to an approved certificate authority (see above list).

   NOTE: Make sure you ask the Certificate Authority to provide the certificate file in PEM format, which is supported by Apache.

   The approved certificate authority will send a certificate file to you in return.

5. Open your private key file (`host.key`) and copy its contents. Open your certificate file and paste the contents of the private key file to the end of the certificate file. Save this file as `server.crt.`

NOTE: See "Configure the IronKey Enterprise Server" on page 24 for more information about the following installation steps that complete your server configuration.

6. Use a Secure Copy utility (that is, SCP or WinSCP) to copy your `server.crt` file to the virtual machine. See "Useful CLI Commands" on page 35 for more information.
7. Install the certificate using the CLI command:

```
application certificate install
```

8. After the certificate is installed, enable SSL, and restart the application server to test your Enterprise Server configuration.

```
service restart appserver
```

9. If your Certificate Authority requires you to configure web servers with additional certificate chain information to validate their SSL certificates, do the following:
   - Save a copy of the relevant certificate(s) in a separate file called "issuer.crt"
   - Copy the file to the virtual machine as you did in steps 6 - 8 above for the "server.crt" file. **The issuer.crt file must also be in PEM format.**

Database Setup

Before you install IronKey Enterprise Server, make sure you have a SQL Server installed.

To set up your database, you can follow either the CLI steps or the GUI steps in the following sections. Accept the default installation settings.

IMPORTANT: To ensure that the front-end codebase of IronKey Enterprise Server can connect to the database via a username and password, make sure the SQL Server is in either SQL Server Authentication Mode or Mixed Mode (Windows Authentication or SQL Server Authentication). See *http://msdn.microsoft.com/en-us/library/ms143705.aspx* for more information.

DATABASE CLI STEPS

1. **Restore the database backup on an existing SQL Server.**

   Reference: *http://msdn.microsoft.com/en-us/library/ms177429.aspx*

2. **Create a SQL Server login:**

```
CREATE LOGIN <login name> WITH PASSWORD = '<password>' ;
GO
```

   Reference: *http://msdn.microsoft.com/en-us/library/ms189751.aspx*

3. **Create a Database User (use the login created in Step 2)**

```
use <ironkey ES database name>;
go
CREATE USER <user-name-same-as-login-name> FOR LOGIN <login-name>;  GO
```

   Reference: *http://msdn.microsoft.com/en-us/library/aa337545.aspx*

4. **Grant the Database User (created in Step 3) the "db_owner" Server Role:**

```
use <ironkey ES database name>;
go
exec sp_addrolemember N'db_owner', <database user name>;
go
```

Reference: *http://msdn.microsoft.com/en-us/library/aa259605(SQL.80).aspx*

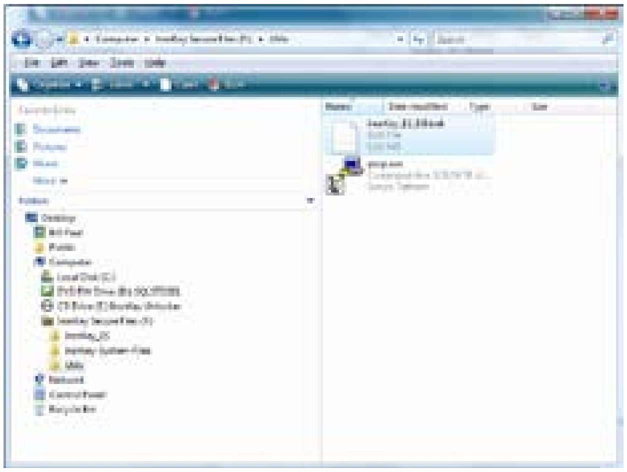
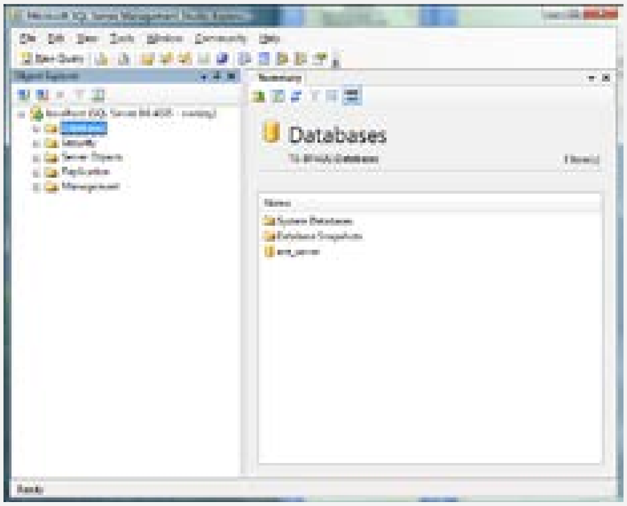
5. **Set the default database for the login (created in Step 1) to the IronKey Enterprise Server database:**

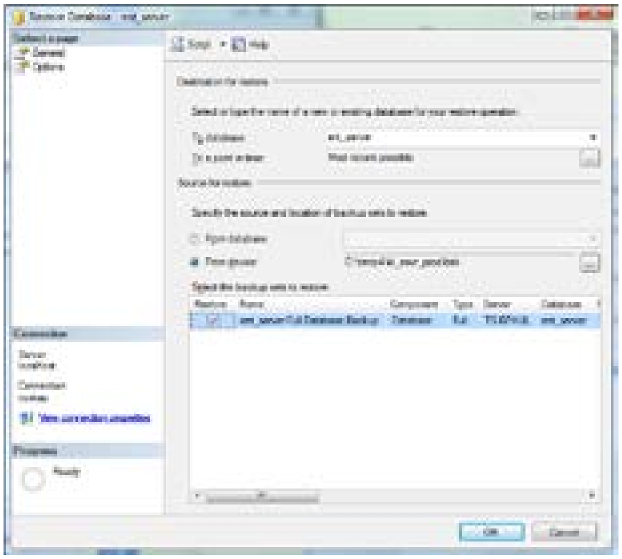
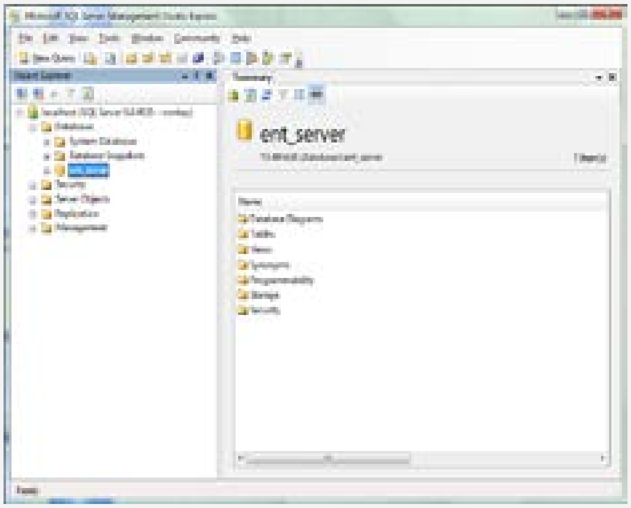
```
alter login <login name> with default_database = <ironkey ES database name>;
go
```

Reference: *http://msdn.microsoft.com/en-us/library/ms189828.aspx*

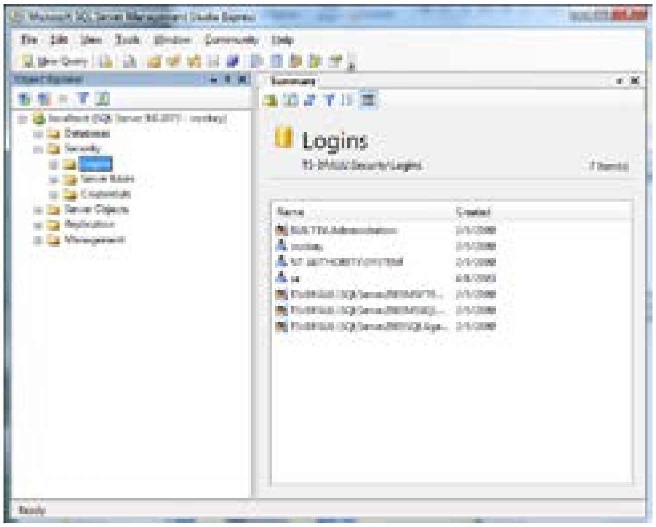
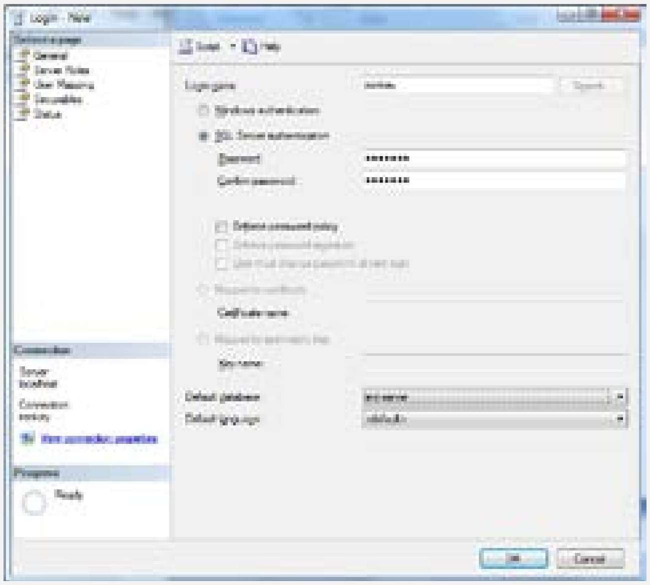
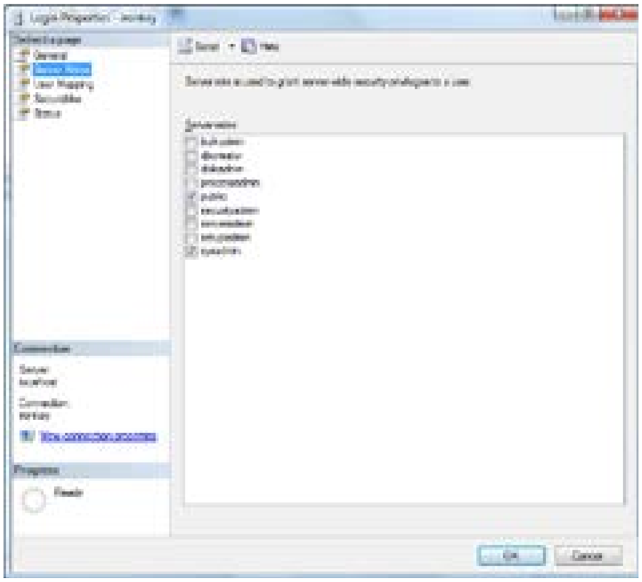
DATABASE SETUP: GUI STEPS

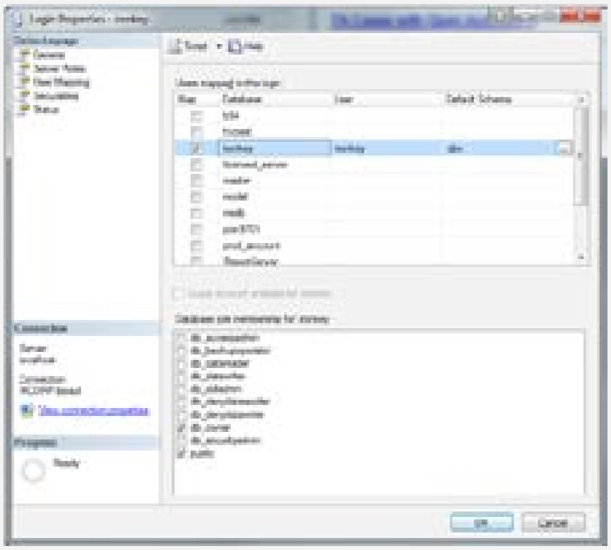
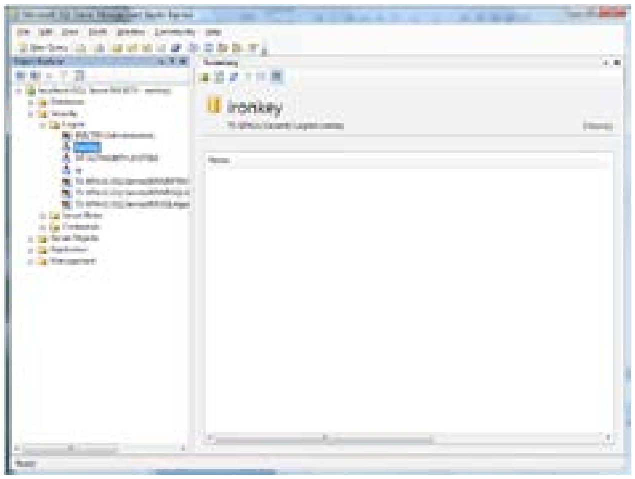
1. **Restore the database backup on an existing SQL Server:**

Step		Description
1	Browse the secure volume on your Enterprise Server Setup Device and click the **Utils** folder to locate the Enterprise Server schema, `IronKey_ES_V5.bak` (a backup of a blank database).	
2	In SQL Server Management Studio Express, right-click the **Databases** folder, and then click **Restore Database**.	

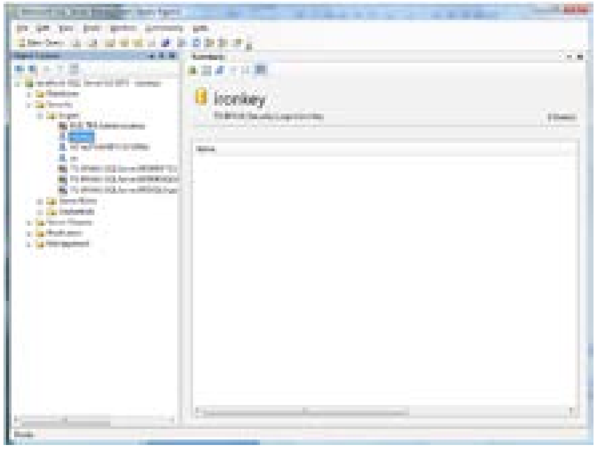
Step		Description
3	In the **Restore Database** dialog box, do the following: a. Enter the name for your new database in the **To database** box. The name cannot contain a dash (-). b. Click **From device**, and browse to the `IronKey_ES_V5.bak` file.(In the **Specify Backup** dialog box, click the **Add** button, browse to the database backup file, then click **OK**.) The location of the backup file is set, and the name of the destination database to restore appears in the **Select the backup sets to restore** list.	
4	Click **OK** to return to the main window. Your new database appears under the **Database** folder.	

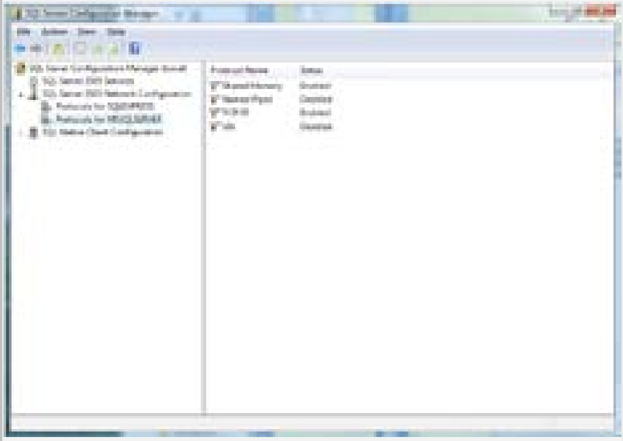
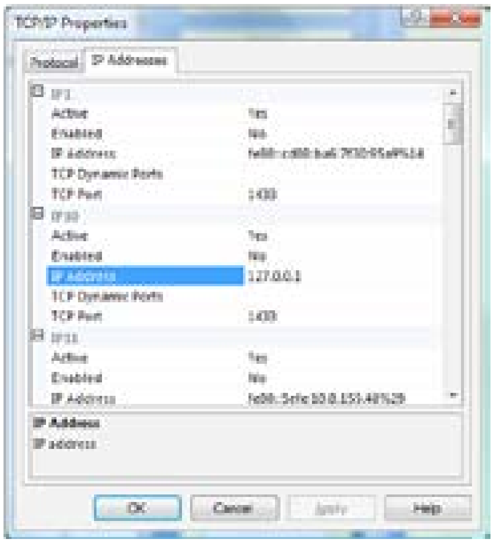
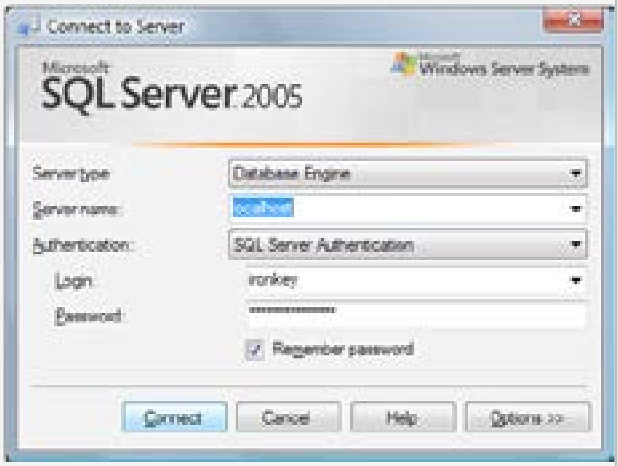
2. **Create a SQL Server login**
3. **Create a Database User (using the Login created in Step 2)**
4. **Grant the Database User (created in Step 3) the "db_owner" Server Role**

Step		Description
1	In SQL Server Management Studio Express, expand the **Security** folder, right-click **Logins**, and then click **New login**.	
2	On the **General** page, do the following: a. Enter a login name for the user. b. Select **SQL Server authentication** and enter a password. c. Select the default database you just created.	 Login - New General Server Roles User Mapping Securables Status Ready OK Cancel
3	On the Server Roles page, select **public** and **sysadmin**. **NOTE:** If you are using another management console, the available options might vary. At a minimum, select **sysadmin.**	 General User Mapping Securables Status Ready OK Cancel

Step		Description
4	Select **User Mapping** in the left panel, and then select the newly created user in the right panel. Make sure **dbo** is entered for the **Default Schema**. In the **Database role membership for:** panel, check the boxes for **db_owner** and **public**	
5	Click **OK** to return to the main window. Your new user appears under the **Logins** folder.	

5. **Set the default database for the login (created in Step 1) to the IronKey Enterprise Server database**

Step		Description
1	Open SQL Configuration Manager. (Location: **Start** > **Programs** > **Microsoft SQL Server 2005** > **Configuration Tools** > **SQL Configuration Manager**)	

Step		Description
2	Expand **SQL Server 2005 Network Configuration**, and then click **Protocols for MSSQLSERVER**. Double-click **TCP/IP** in the right pane.	 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 Protocol Name / Status Shared Memory: Enabled Named Pipes: Disabled TCP/IP: Enabled VIA: Disabled
3	In the **TCP/IP Properties**, click the **IP Addresses** tab. Make sure **IP Address** is set to `127.0.0.1` and select a **TCP Port**. You need the port number to configure the database connection from the Enterprise server. The default port is 1433.	 TCP/IP Properties Protocol IP Addresses OK Cancel Apply Help IP1 Active: Yes Enabled: No IP Address: fe80::c80:ba6:7f30:f95a%14 TCP Dynamic Ports: TCP Port: 1433 IP10 Active: Yes Enabled: No IP Address: 127.0.0.1 TCP Dynamic Ports: TCP Port: 1433 IP11 Active: Yes Enabled: No IP Address: fe80::5efe:10.0.155.48%29 **IP Address** IP address
4	Open SQL Server Management Studio Express and do the following: a. Ensure **Server type** is set to **Database Engine** and **Server name** is set to **localhost.** b. Select **SQL Server Authentication** in the **Authentication** list. c. Enter the username and password you created earlier. d. Select **Remember password**. e. Click **Connect**.	 Connect to Server Microsoft SQL Server 2005 Microsoft Windows Server System Connect Cancel Help Options >> Server type: Database Engine Server name: localhost Authentication: SQL Server Authentication Login: ironkey Password: *************** ☑ Remember password

TROUBLESHOOTING TIPS

» When you connect to the application server after entering your account code, if the same screen appears again without the account code entered in the text box, an error has probably occurred while connecting to the database. Check the following, and then retry to connect again:

  - A user account other than the system administrator account is being used.
  - The user account has both system administrator and public privileges.
  - The correct port number is being used by the database server and the application server. The default port for the SQL server is 1433.
  - The firewall on the SQL server is not blocking connectivity.
  - The following ports are open on the firewall: 80, 443, 2000, 2001, 2002, 2003, 2004.
  - The name of the database does not contain a hyphen (-).

» After resetting your SQL Server database using the reset SQL script, run the `service restart appserver` CLI command immediately to avoid initialization problems.

» When you run the `service restart appserver` CLI command, please wait 10 seconds after the command prompt returns control before connecting to the server.

Installation Workflow

1 Unlock the Setup Device

2 Install and Set Up the Server's Virtual Machine

3 Configure the IronKey Enterprise Server

4 Request a License and Set Up Your Enterprise Account

5 Initialize the First System Admin's IronKey Device

1 UNLOCK THE SETUP DEVICE

Step	
1	Plug the IronKey Setup Device into the USB port of the host computer. If you do not see a prompt to unlock the device, go to "My Computer," double-click the **IronKey** icon, and then double-click `IronKey.exe`.
2	Enter the Setup Device password. This is the same as your account number, which you received in the Enterprise Server kit and in the Welcome Email, and then click the **Unlock** button. The IronKey Control Panel opens.
3	In the **Applications** list of the IronKey Control Panel, click the **Install IronKey Enterprise Server** icon to start the installation process.
4	Provide the `IronKey_ES_V5.bak` file to your DBA to set up the database. In return, the DBA will provide the username, password, database server IP, and port that you need to setup the database. You can find this file on the secure volume of your IronKey Setup Device in the **Utils** folder.

Before installing the IronKey Enterprise Server:

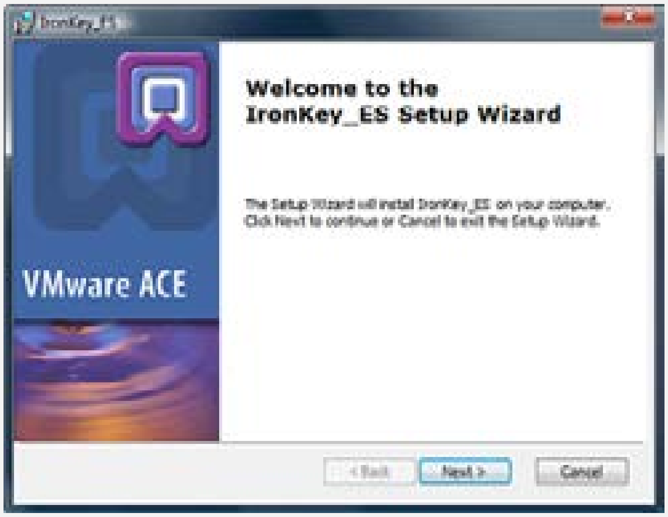
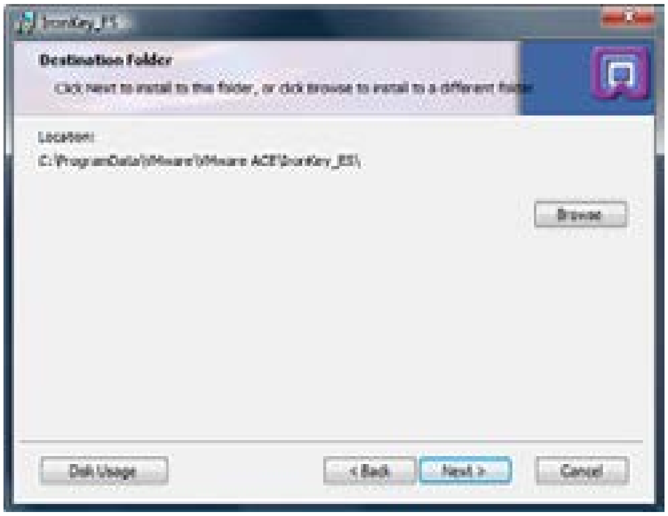
- Ensure that you have a SQL Server installed.
- Accept the default installation settings.
- Ensure the Authentication Mode is set to SQL Server Authentication Mode or Mixed Mode (Windows Authentication or SQL Server Authentication).

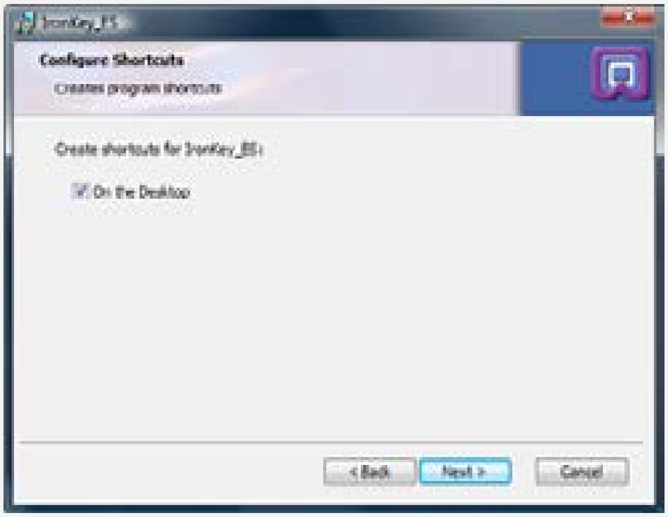
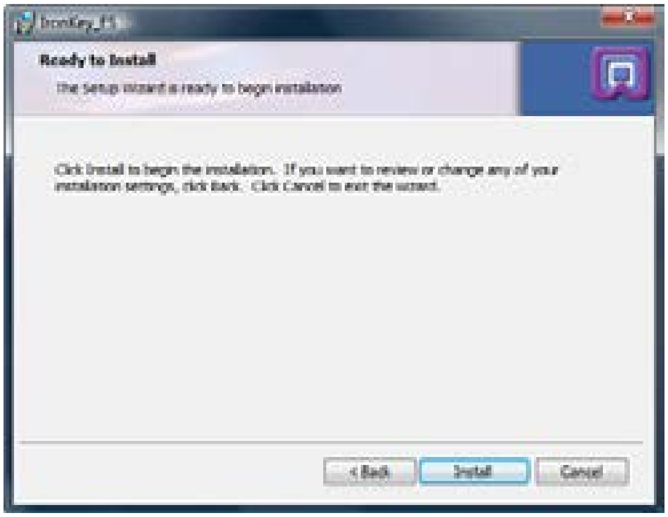
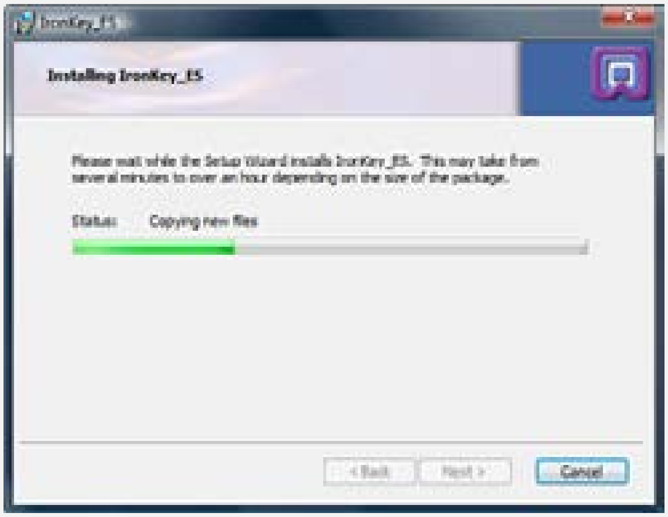
To learn more, see "Database Setup" on page 13 for steps using either the CLI or GUI.

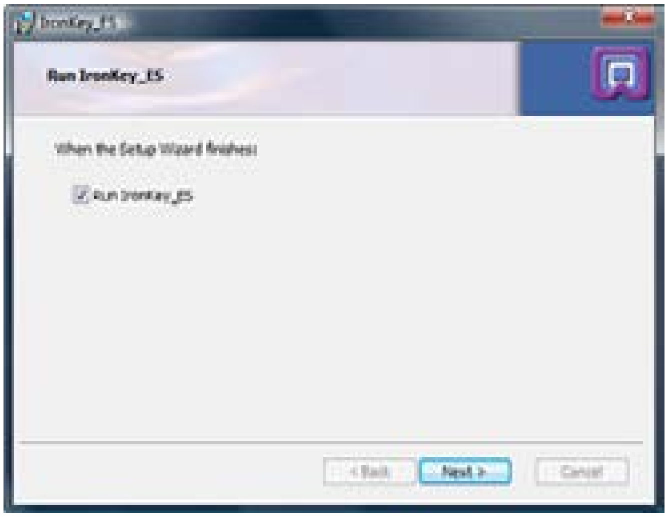
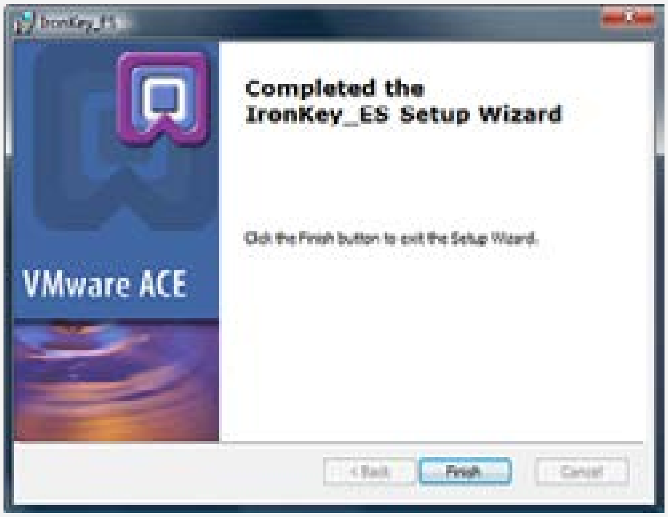
2 INSTALL AND SET UP THE SERVER'S VIRTUAL MACHINE

The software you are installing leverages virtual machine technology for quicker setup and easier maintenance updates. If you are familiar with virtualization and virtual machines, note that this hosted solution is not compatible with a VMware ESX or a Citrix XenSource solution.

The IronKey Enterprise Server runs in a virtual machine using VMware ACE software. This software contains a player that runs the software and the VM itself.

Step		Description
1	In the IronKey Control Panel, click **Install IronKey Enterprise Server**.	The Setup Wizard opens.
2	Click **Next** to continue.	 Welcome to the IronKey_ES Setup Wizard The Setup Wizard will install IronKey_ES on your computer. Click Next to continue or Cancel to exit the Setup Wizard.
3	Specify the installation folder where you want to install the VMware software and the VMs.	 Destination Folder Click Next to install to this folder, or click Browse to install to a different folder Location: C:\ProgramData\VMware\VMware ACE\IronKey_ES\ IronKey_ES Browse Disk Usage < Back Next > Cancel

Step		Description
4	• To create a shortcut for the application, leave the default selection as is. • If you do not want a desktop shortcut, click to clear the **On the Desktop** check box. Click **Next**.	 IronKey_ES **Configure Shortcuts** Creates program shortcuts Create shortcuts for IronKey_ES: ☑ On the Desktop
5	Click **Install** to start the process.	 IronKey_ES **Ready to Install** The Setup Wizard is ready to begin installation Click Install to begin the installation. If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
6	A progress screen displays during installation.	 IronKey_ES **Installing IronKey_ES** Please wait while the Setup Wizard installs IronKey_ES. This may take from several minutes to over an hour depending on the size of the package. Status: Copying new files

Step		Description
7	• To have the Setup Wizard run the IronKey software when it is finished, leave the **Run IronKey_ES** check box selected. • If you do not want the IronKey software to start right away, click to clear the **Run IronKey_ES** check box. Click **Next**.	 IronKey_ES **Run IronKey_ES** When the Setup Wizard finishes: ☑ Run IronKey_ES
8	When the process completes, click **Finish**.	 IronKey_ES **Completed the IronKey_ES Setup Wizard** Click the Finish button to exit the Setup Wizard.
9	Restart your computer if prompted to do so.	**NOTE:** Some installations require a restart of your computer.

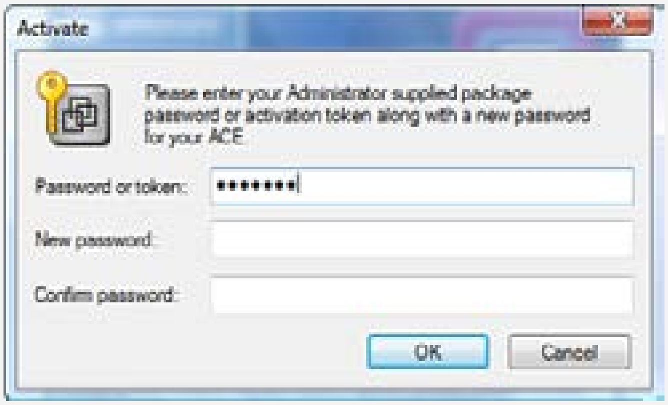
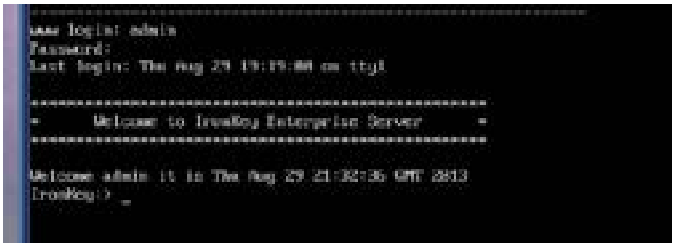
3 CONFIGURE THE IRONKEY ENTERPRISE SERVER

Next, you use the command line interface (CLI) to configure and customize the IronKey Enterprise Server. If you are familiar with CLIs, be aware that this product contains a restricted set of commands rather than a complete command line shell. The restricted command set helps keep the application as secure and simple as possible.

To see a list of commands and related help, type `?` at any CLI prompt. You can also type a command followed by `?` to get information about that command. For example, to get information about the network command, type:

```
network ?
```

A list of network commands appears. For a complete list of the commands you can use, see the "Customization and Configuration Reference" on page 41.

Step		Description
1	Double-click the **IronKey_ES VM** shortcut to start the VM if is not already running.	
2	To activate the IronKey Enterprise Server ACE VM, enter the "Installation Password" provided in your Welcome Email, and then click **OK**. Create and confirm a new activation password that you will use each time you start the IronKey Enterprise Server VM. **NOTE:** IronKey Technical Support does not know your password and cannot recover it if you forget it.	 Activate Please enter your Administrator supplied package password or activation token along with a new password for your ACE Password or token: ••••••• New password: Confirm password: OK Cancel
3	After the installation has finished, the IronKey Command Line Interface (CLI) appears when the IronKey Enterprise Server starts. Log in using the CLI username and password provided in your Welcome Email. You might be required to change your login password. The password requirements for this password are: » 10 character minimum » 1 uppercase letter » 1 lowercase letter » 1 digit » 1 special character	 login: admin Password: Last login: Thu Aug 29 19:19:08 on tty1 *** * Welcome to IronKey Enterprise Server * *** Welcome admin it is Thu Aug 29 21:32:36 GMT 2013 IronKey:> _

Once you log into the CLI, enter the commands to configure your VM. The next procedure shows the basic steps to complete the configuration, plus a list of optional commands. Use the commands that apply to your organization.

Bracketed items, such as <IP address>, represent arguments to be replaced with your own data.

Step		Description

1	Set the host name.	`network hostname <VM hostname>`
		Example:
		`network hostname myhost.domain.com`
		NOTE: Your certificate must have a valid public domain. To use the Silver Bullet Service, you must be able to expose the server on the Internet and allow firewall routing for that URL.
		CRITICAL: When using this command, make sure you enter a Fully Qualified Domain Name (FQDN), not just the hostname of the Enterprise Server. You need to set this same FQDN as the Common Name of your SSL Server Certificate.
		Once you set this value and activate devices, you cannot change the value or you will not be able to manage those devices.
		FQDN Example: (correct)
		`network hostname myhost.domain.com`
		Hostname only Example (incorrect):
		`network hostname myhost`

2	Configure a static IP address	`network interface static <static IP> <IP mask> <Gateway>`
		Example:
		`network interface static 192.168.200.100 255.255.255.0 192.168.200.1`

3	Add the DNS name server.	`network dns add <DNS server IP>`
		Example:
		`network dns add 10.1.1.100`

4	Add the NTP server.	`sysconf ntp addserver <NTP server IP or hostname>`
		Example:
		`sysconf ntp addserver server01.corp.ironkey.com`
		NOTE: You may see a 'FAILED' message during a process shut down. This is a normal part of the initial installation process.
		If no NTP server is available, you must set the time (UTC) using the `sysconf` time command.
		Example:
		`sysconf time 14:11:00 31 August 2012`

Step		Description

5	Configure the SMTP server.
	Answer y or n to the authentication question as appropriate for your relayhost.
		`sysconf smtp set <SMTP server IP or hostname>`
		Example:
		`sysconf smtp set server01.corp.ironkey.com`
		`Does the relayhost <your_SMTP_server> require authentication (y/n)?`

6	Configure the database server.	`application database configure <DB server IP or hostname> <port ID> <database username> <password> mssql <database name>`
		NOTE: You must enable TCP/IP in the database server. The default database Port is 1433. If you use another port, you must configure the enterprise server to use that port.
		The recommended `<database name>` is `es_master`, check with your DB admin to verify the database name.
		Example:
		`application database configure 10.1.1.89 1433 db_usr mypasswd mssql es_master`

7	Set the external name of the server as accessed by devices.	`application siteName set <site name>` **IMPORTANT:** Make sure that your site name uses a Fully Qualified Domain Name (FQDN). The name must match the hostname from step 1 above and the Common Name in the SSL Certificate. *Command Example:* application siteName set myhost.domain.com
8	Name the certificate files and securely copy them to the VM's `/upload` directory.	• Concatenate your private key and your SSL certificate into a single file, and then name the file: `server.crt` • Name the certificate chain file: `issuer.crt` • Use a Secure Copy (SCP) utility (such as command-line PSCP or GUI-based WinSCP) to securely copy the files to `/upload` See "Certificate Acquisition" on page 12 and "Useful PSCP.EXE Commands" on page 35 for more information.
9	Install the certificates.	`application certificate install`
10	Enable SSL.	`application SSL enable`
11	Start the application server.	`service start appserver`

You have successfully configured the server if you can open the following URL in your browser:

https://<siteName>/enterprisesetup

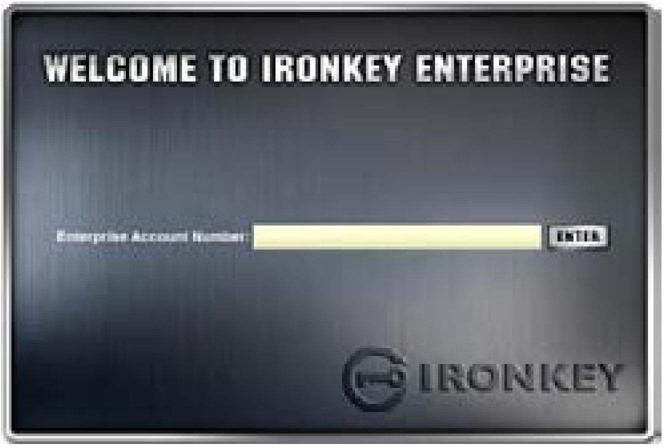
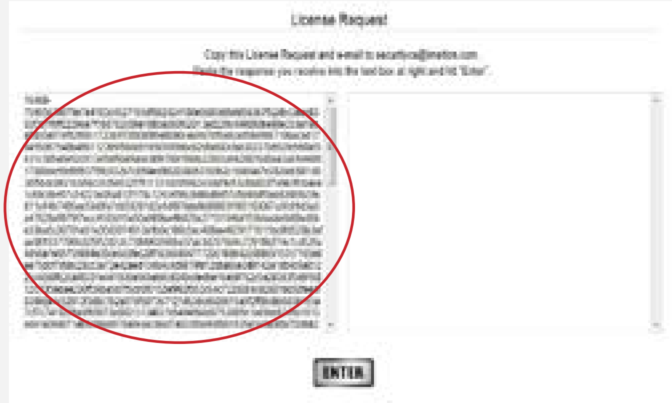
You can also use the following optional commands as needed for your configuration:

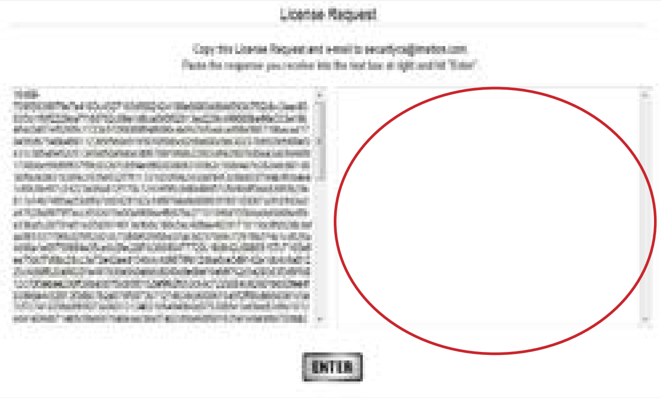
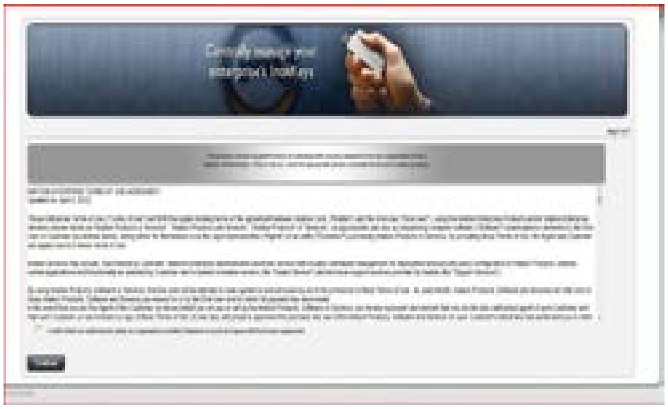
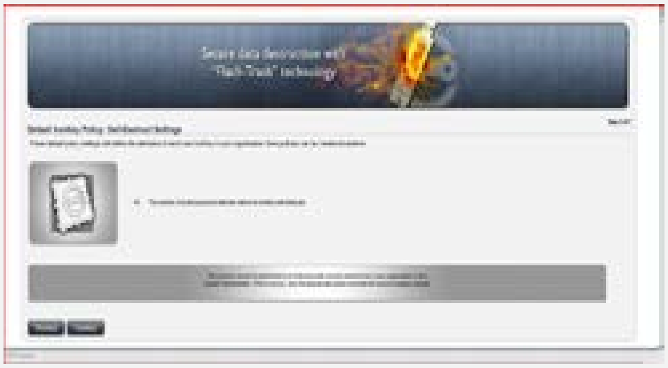
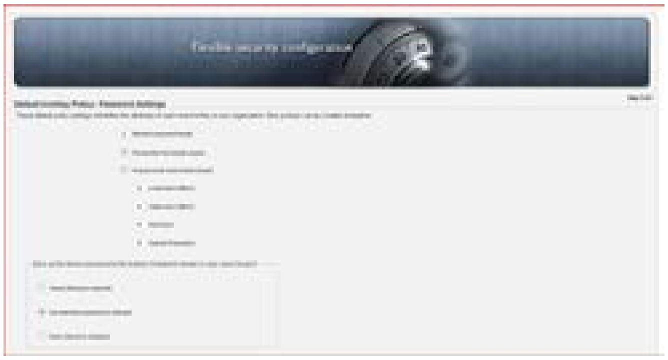
Optional Steps		
a	Configure the remote syslog (store log files on a remote server)	`syslog remote enable <hostname or IP>` Set only if you use a remote syslog server. Default locations of the logs are in `/var/log.`

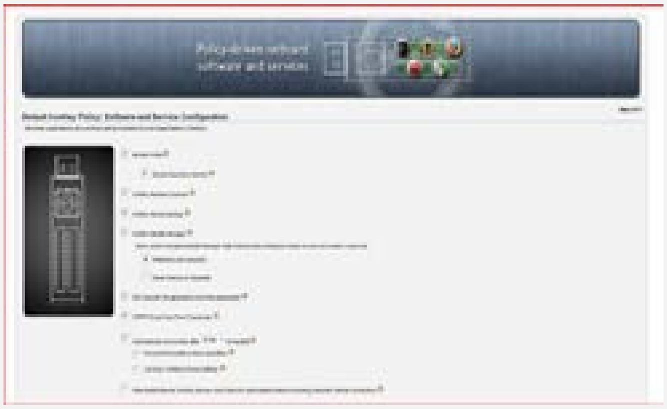
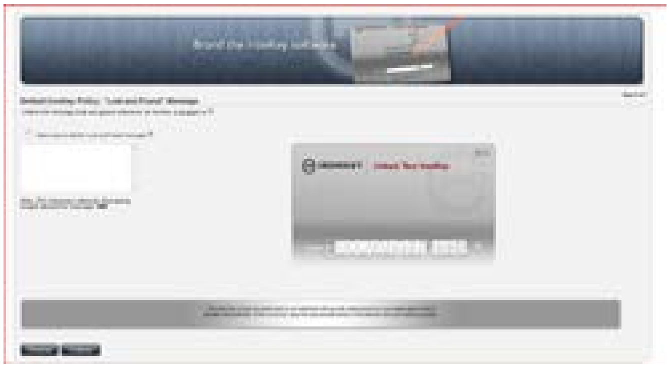
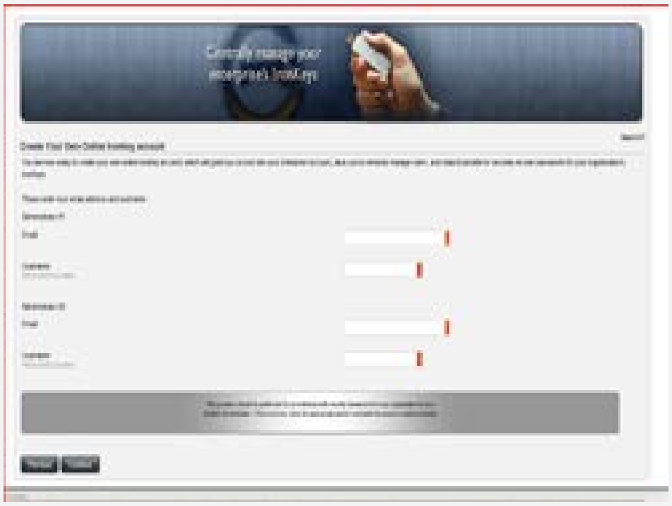
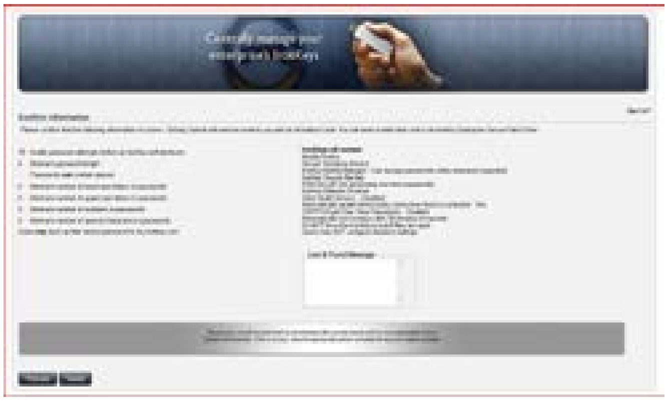
4 REQUEST A LICENSE AND SET UP YOUR ENTERPRISE ACCOUNT

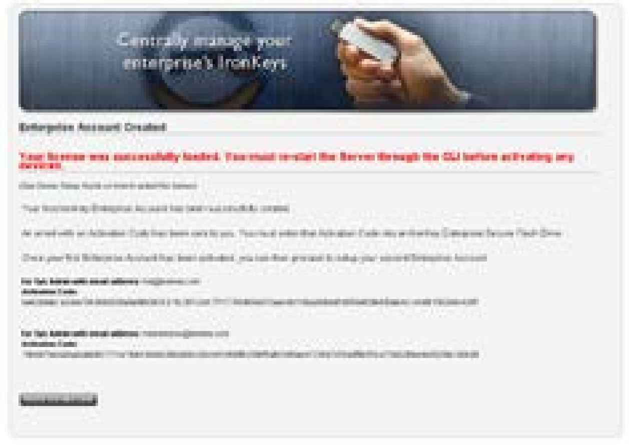
You must have the required license and security information from IronKey Customer Service to finish the installation and activate your Enterprise Account. This ensures that only your organization can use the software provided and protects you against unauthorized use and phishing attacks.

NOTE: You might have to wait to receive your Welcome Email containing your server activation code. You must have the code to start your account setup. You might also have to wait to receive your License Response email containing your server license. You must have the license to complete your account setup.

Step		Description
1	Go to **https://<application siteName>/enterprisesetup** (where **<application siteName>** is the value you entered in step 7 of the previous procedure (section 3). From your Welcome email, copy the 10-digit account code (in the format XXXXX-XXXXX) and paste it into the **Enterprise Account Number** box. Click **Enter**.	 WELCOME TO IRONKEY ENTERPRISE Enterprise Account Number: ENTER IRONKEY
2	On the **License Request** page, copy the string from the text box on the left and email it to *securitycs@imation.com*	 License Request Copy this License Request and email to securitycs@imation.com Paste the response you receive into the text box at right and hit "Enter".
3	Check your email for a message from Customer Service.	You need the license key contained in this email to complete the installation.

Step		Description
4	On the License Request page, copy the license key that you received from Customer Service and paste it into the text box on the right. Click **Enter**.	 License Request Copy this License Request and e-mail to securityca@imation.com. Paste the response you receive into the text box at right and hit "Enter".
5	Read the license agreement, and then select the check box to confirm that you are authorized to set up your organization's IronKey Enterprise account. Click **Continue**.	
6	Select the number of failed password attempts that a user can enter before the IronKey self-destructs. **NOTE:** When an IronKey self-destructs, all data is permanently lost and the drive is destroyed. Click **Continue**.	
7	Select the password policy options that will be applied to each device. Click **Continue**.	

Step		Description
8	Select the set of software applications and services that you want users to have on their devices. You can also configure a time-out policy to automatically lock devices after a specified period of user inactivity. Click **Continue**.	
9	Define a message for the Lost and Found screen of a device (the first screen that appears when a device is plugged in). For example, you can include contact information in case a lost device is found, or department information for easily distinguishing devices. You can also leave this blank or allow users to define their own message. Click **Continue**.	
10	For each Administrator, enter an email address and assign a user name. User names can contain letters and/or numbers. Click **Continue**. **NOTE*:*** You must complete the **Email** and **Username** fields for both Admins before you can complete the installation.	
11	Review your Enterprise account information. If everything is correct, click **Submit**.	

Step		Description
12	A confirmation message appears when your Enterprise account has been created. IronKey emails an Activation Code to the email addresses provided for the System Admins. However, it's a good idea to keep this confirmation page open until you receive the confirmation email. If you do not receive the codes, you can resend them from this page.	 Enterprise Account Created Your license was successfully loaded. You must re-start the Server through the CLI before activating any devices. [illegible]
13	Reboot the Enterprise server.	Enter this CLI command: `sysconf reboot`

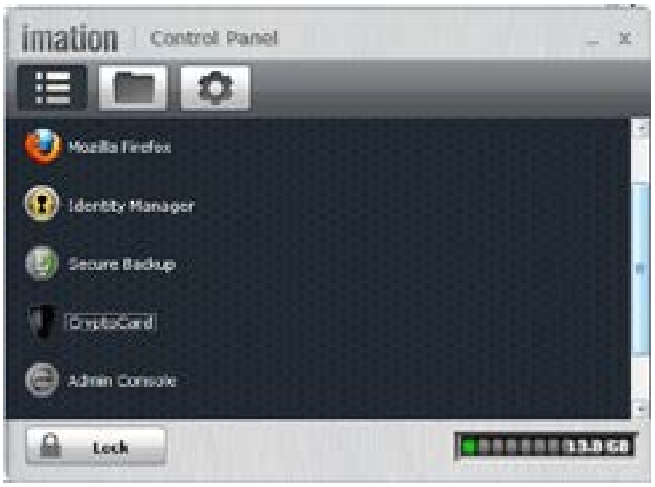
5 INITIALIZE THE FIRST SYSTEM ADMIN'S IRONKEY DEVICE

After you confirm your information, you will receive an email containing the Activation Code for the IronKey Enterprise Secure Flash Drive that belongs to the first System Admin. Make sure that this email is available before continuing.

IMPORTANT: Always maintain multiple active System Admins for your Enterprise Account as a precaution against loss. Keep all System Admin devices in safe places. They are essential components for maintaining your IronKey Enterprise Account.

You must activate your device on a Windows or Mac computer. To use the full speed of the IronKey, plug it into a USB 2.0 port. Note that you can have only one IronKey unlocked on a computer at a time (except during device recovery).

Steps	
1	Plug in an unactivated IronKey device from your kit into the host computer. You can label this drive as the administrator drive, or leave it unmarked, depending on your security preferences.
2	The "Device Setup" screen appears. The IronKey autoruns as a virtual CD-ROM. The setup software runs automatically from a virtual DVD. This screen may not appear if your computer does not allow devices to autorun. You can start it manually by: • WINDOWS: Double-clicking the "IronKey Unlocker" drive in "My Computer" and launching "IronKey.exe". • MAC: Opening the IronKey Unlocker drive in Finder and opening the IronKey application in the Mac folder.
3	Do the following: • Type the Activation Code. • Select a default language preference and agree to the end-user license agreement. Click the "Activate" button. By default, IronKey software uses the same language as your computer's operating system. NOTE: You should have received the code in an Activation email message sent from IronKey. If you did not receive an email, check your spam or bulkmail folder.
4	Type a device password and confirm it, and then click the "Continue" button. Your password is case-sensitive and must comply with the password policy you set when you created the Enterprise Account.
	A message prompt will appear indicating that an email has been sent to you. Follow the instructions in the email to set up your online account; this includes creating a "secret question". Your online account is required for some security features, such as resetting a password, browsing the web using secure sessions, updating your device software and more. Once you set up your online account, click OK in the message prompt to proceed with the device setup.
5	The IronKey initializes. This process generates the AES encryption keys, creates the file system for the secure volume, and copies secure applications and files to the secure volume based on your policy settings. Depending on your configuration, this might take several minutes.

Steps	
	When the initialization is complete, the IronKey Control Panel appears. Your device is now ready to protect your data and can be used on a Windows, Mac or Linux computer. Log in to the Admin Console by clicking the Admin Console button on the Applications page of the IronKey Control Panel. A "Welcome Screen" will appear to guide you through finalizing the default policy for your account and configuring some new x250 policy features.  imation Control Panel Mozilla Firefox Identity Manager Secure Backup CryptoCard Admin Console Lock 13.8 GB
6	**IMPORTANT:** We strongly recommend that you back up your database now to save critical data associated with all devices. Loss of critical data will result in the inability to use activated devices.

You are now ready to activate and initialize the 2nd System Admin, add additional users, define policies, and perform other account maintenance. See the *IronKey Enterprise Server Admin Guide* for instructions on how to use the Admin Console to perform these tasks.

Activating and Initializing the 2nd System Admin Device

It is very important to set up a 2nd System Admin device as quickly as possible; without a second System Admin device, it will be impossible to manage the IronKey Enterprise Server account if anything happens to the 1st System Admin device.

When the 1st System Admin configures the IronKey Enterprise Server account, both the 1st and 2nd System Admins automatically receive emails containing activation codes.

NOTE: The following steps are performed by the 2nd System Admin.

Step	Description
1	You (2nd System Admin) receive an Activation Email.
2	Complete all of the steps in the previous procedure, "Initialize the First System Admin's IronKey Device" on page 31.

NOTE: If you need to manage x200, x250, and W500 devices, the Admin should use an x200 device. When you add a new Admin user or promote a Standard user to an Admin, another Admin must approve the change before the user can receive Admin privileges. Admin approval is not required for Administrators using x250 devices. For more information about managing x200 devices, see the "Managing Devices" chapter of the *IronKey Enterprise Server Admin Guide*.

Best Practices

DEPLOYMENT CONFIGURATION

While the Enterprise Server can be deployed anywhere on your network, the end-user devices will need to connect to the IronKey Enterprise Server based on configuration policies you have set up. For example, if you choose to always require authentication (as part of Silver Bullet), those devices must access your IronKey Enterprise Server each time they must be unlocked.

IronKey recommends that you place and protect your IronKey Enterprise Server just as you would any other system that resides in your data center. You can use a proxy server to provide Internet access to your server. Always use firewalls, IDS, and other standard defense-in-depth tools and technologies.

Also, prepare your IronKey Policies ahead of time (see the *IronKey Enterprise Server Admin Guide* for more details), and prepare a list of all users and (optionally) their email addresses.

ADMINISTRATOR DEVICES

While only one System Admin device is required to set up and operate the IronKey Enterprise Server, we strongly recommend having two or more devices (your original Administrator's Kit came with four devices for this purpose). If you lose all of your System Admin devices, you cannot manage your users' devices. It is critical that you set up at least two System Admins and keep at least one as part of your normal business continuity/offsite backup process.

USE X200 DEVICES TO MANAGE A MIXED DEVICE ENVIRONMENT

If you will be managing x200, x250, and W500 devices, Admins should use x200 devices. An x200 device can manage both x200 and x250 Standard User devices, while an Admin using an x250 device can manage only x250 devices. For more information, see about managing x200 devices, see the "Managing Devices" chapter of the *IronKey Enterprise Server Admin Guide*.

BACKUP/RESTORE

While user-specific data is stored in your database, system-level data (such as network configuration information) is stored in a configuration file in the IronKey Enterprise Server. We recommend that you periodically back up this file and store it securely (ideally on an IronKey) as part of standard business continuity processes.

To back up the config file, type the following into the CLI: `sysconf backup`
and then use a Secure Copy (SCP) utility (such as command-line PSCP) to securely copy the files it generates from the `/download` directory.

If a loss happens, or if you otherwise want to update your VM, simply install a new IronKey Enterprise Server VM and restore the backed-up items from the config file for immediate setup. You can restore by using the following command: `sysconf restore`
and then use a Secure Copy (SCP) utility (such as command-line PSCP or GUI-based WinSCP) to securely copy the files from the previous backup to the `/upload` directory.

DATABASE ADMINISTRATION

While you might have a dedicated DBA that maintains your database, it is important to note:

1. If the database is unavailable, the IronKey Enterprise Server will not work; plan database downtime with this in mind.
2. If the username/password used to access the database is changed by the DBA, you must change the username/password in the IronKey Enterprise Server CLI.

SECURITY LAYERS

As part of a defense-in-depth strategy, you have been provided with several layers of protection, including several security passwords. It is important that you review and change those passwords on a timely basis. Also, immediately disable (or detonate) devices when a device is suspected of being lost or stolen.

USEFUL CLI COMMANDS

Occasionally, you must perform certain tasks using the CLI. See "Customization and Configuration Reference" on page 41 for a full CLI command reference.

1. *Version Check.* To check the IronKey Enterprise Server version, enter this command:

   ```
   application version
   ```

2. *Generate Information for a Support call.* It is helpful to have all of your vital system configuration data in advance of a support call. Running the following command in the CLI will provide data that IronKey Support can use to help you:

   ```
   supportInfo
   ```

3. *Monitoring System Health*: IronKey includes an overall monitoring command for determining the status of the system and for troubleshooting.

   ```
   application healthCheck
   ```

   If all systems come back with "[OK]" then everything is working as it should be. If you see an error, note the component and then contact IronKey Support.

USEFUL PSCP.EXE COMMANDS

The following are example commands using the PSCP command-line utility.

Certificate Download

```
      pscp.exe -scp admin@x.x.x.x:/download/server.crt  c:\server.crt
```

Certificate Upload

```
      pscp.exe -scp server.crt admin@x.x.x.x:/upload
```

Backup Download

```
      pscp.exe -scp admin@x.x.x.x:/download/ikbackup_<###>.tar.gz c:\ikbackup_<###>.
tar.gz
```

Backup Upload

```
      pscp.exe -scp ikbackup_<###>.tar.gz admin@x.x.x.x:/upload
```

Support File Download

```
      pscp.exe -scp admin@x.x.x.x:/download/iksupport_<ES hostname>_<####>.tar.gz
c:\ikbackup_<###>.tar.gz
```

Downloading All Files from the Download Folder

```
pscp -scp -r admin@x.x.x.x:/download <destination directory on host machine>
```

Downloading All Files from the Upload Folder

```
pscp -scp -r admin@x.x.x.x:/upload <destination directory on host machine>
```

x.x.x.x is the IronKey Enterprise Server IP address
### is the timestamp

Upgrade the Enterprise Server

You can upgrade your Enterprise Server from a previous version. Before you begin, back up your existing Server configuration and your database. You must also unlock your new Setup Device using the same password as the one used to unlock your original Setup Device.

Step		Description
1	Stop the application server on Enterprise Server's ACE VM.	Enter this CLI command: `service stop appserver`
2	Create a backup of your Server configuration. This backs up your network settings, SSL server certificate, SSL Service certificate private key, database, and other server information.	Enter this CLI command: `sysconf backup`
3	Download the backup file from the Enterprise Server VM to the host computer. **IMPORTANT**: All server configuration information, including your SSL certificate, is deleted from the Server VM during a server upgrade.	Enter this CLI command: `pscp.exe -scp admin@x.x.x.x:/download/ikbackup_<###>.tar.gz c:\ikbackup_<###>.tar.gz` x.x.x.x is the IronKey Enterprise Server IP address ### is the timestamp
4	Shut down VM Ware ACE.	Quit / Exit the VMware ACE application.
5	Back up your database.	**IMPORTANT:** We strongly recommend that you back up your database to save critical data that is associated with all devices. You cannot use activated devices if you lose that data.

Step		Description
6	Upgrade the database. Use the SQL Server Management Studio to run the script named “db_upgrade_from_v4_to_v5.sql” (located in the \Utils folder).	1. Click the database you want to update. 2. Click the **New query** button. 3. Copy and paste the text in the **db_upgrade_from_4_to_v5.sql** file to the query window. 4. Click the **Execute** button next to the drop-down database selection list. 5. The length of time this takes to complete varies with the size of the database. Any errors returned are displayed.
7	Uninstall Enterprise Server v4.	
8	On the Admin Setup device, run the Installer to install the new version of Enterprise Server.	In the IronKey Control Panel, click **Install IronKey Enterprise Server**. **NOTE**: You may be required to uninstall VMWare ACE and/or the VMWare Player. If you are prompted to do this, use the Windows Control Panel.
9	Double-click the **IronKey_ES VM** shortcut to start the VM.	
10	Enter your VMWare ACE Password.	
11	Log into the CLI.	

12	Configure the server’s static IP address.	Enter this CLI command:
		`network interface static <static IP> <IP mask> <Gateway>`
		Example:
		`network interface static 192.168.200.100 255.255.255.0 192.168.200.1`

Step		Description
13	Upload your Server Configuration Backup file.	Enter this CLI command: `pscp.exe -scp ikbackup_<###>.tar.gz admin@x.x.x.x:/upload` x.x.x.x is the IronKey Enterprise Server IP address ### is the timestamp **NOTE**: If there is a network connection timeout during the upload, all the VM's services may not have started—wait a few minutes then perform the upload again.
14	Restore your Server configuration.	Enter this CLI command: `sysconf restore`
15	Enable SSL.	Enter this CLI command: `application SSL enable`
16	**Update your license.** **IMPORTANT:** You must add a new license to your server to be able to initialize new devices. See the *Enterprise Server Admin Guide*, "Licensing" section for details.	1. Click the "Admin Console" button in the IronKey Control Panel. 2. Click "Enterprise Support" on the Admin Console, and then click the "Manage IronKey Licenses" button to view your IronKey Services list. 3. Email the License Request text from Box 1 to Customer Service, paste the new license information from the reply email in Box 2, and then click the "Enter" button.
17	Restart the application server.	Enter this CLI command: `sysconf reboot`

IMPORTANT: You must add a new license to your server to be able to initialize new devices. See the Enterprise Server Admin Guide, "Managing Licenses" section for details.

NOTE: When you upgrade the server, you can also add software updates for devices if you have not done so already. If you already uploaded a device software update package in Enterprise Server v4.0, you will need to re-upload this file as it is removed when the V4.0 was uninstalled during the server upgrade process. For more information, see "Provide software updates for devices" on page 38.

Provide software updates for devices

The software update process involves adding alerts, versions, and release notes to the database so that they will be available in the Admin Console. It also requires you to upload and install the update package on the VM. The software *update* process is independent of the process for *upgrading* the server.

Both the software update package and the database script are available on the Setup device in the *Device Updates* folder. There are two files:

- **Update package file**—upload and install this file on your VM
- **Update script file**—run this file in the database to add update alerts, versions, and release notes to the Admin Console.

The list below shows filenames and paths for the update package and database script that comes on the device:

- Update package: `\\Device Updates\ikupdate_022513.tgz`
- Update script: `\\Device Updates\secure_storage_2.5.2.0_3.4.0.0_update.sql`

NOTE: When you upgrade Enterprise Server from v4.0 to v5.0, any software update package that was added to the server is removed when the v4.0 server is uninstalled. You must re-upload the software update package and install it to the new v5.0 server. However, you do not need re-run the script to update the database.

TO UPDATE THE DATABASE

1. IMPORTANT: We strongly recommend that you back up your database to save critical data that is associated with all devices. You cannot use activated devices if you lose that data.
2. To execute the SQL script file against the existing database, click the database you want to update.
3. Click the New query button.
4. Copy and paste the text in the update script (`secure_storage_2.5.2.0_3.4.0.0_update.sql`) from the Device Updates folder on the Setup device to the query window.
5. Click the Execute button next to the database selection list.
6. The length of time this takes to complete varies with the size of the database. Any errors returned are displayed.

TO UPLOAD AND INSTALL THE UPDATE PACKAGE

1. On the Virtual Server, stop the appserver on the VM by running the following command:

   ```
   service stop appserver
   ```

2. Upload the update package from the Device Updates folder on the Setup devcie (for example, `ikupdate_022513.tgz`) to the upload directory on the server.
   a. Type the following command from a command prompt on the local machine: `pscp.exe -scp  c:\Device Updates\<ikupdate_022513.tgz> admin@x.x.x.x:/upload` (for additional information about the PSCP utility commands, see "Useful PSCP.EXE Commands" on page 35).
   b. Enter the Admin password when prompted and the file will upload to the VM.
3. Type the following command and verify that the file was successfully uploaded to the Server: `device availableUpdates` (uploaded update package `ikupdate_022513.tgz` should be listed).
4. Type the following command to install the updates to the server: `device installUpdate`

5. Type the name of the file that you uploaded in Step 2 when prompted: `ikupdate_022513.tgz`

6. When you are prompted by the VM User Interface to restart the appserver, type the following command: `service restart appserver`

7. Once the VM appserver restarts, type the following commands to verify that the system status is ok:

    a. `application HealthCheck` – the command checks the database connection and the signing service. Both should return the value `OK`.

8. To verify that the update package was installed, type the following CLI:

    `device deployedUpdates` The newly installed update package will be listed.

TO VIEW THE ALERTS, VERSIONS, AND RELEASE NOTES

1. Unlock your System Admin device.

2. Access the Admin Console

    a. New update alerts will be displayed.

    b. Device versions and Release notes are added to the System Console on the **Update Management** page.

3. Perform your test to update devices. (See the "Updating devices" section of the *IronKey Server Admin Guide* on pages 40 and 41 for information about testing and updating device firmware/software settings.)

Customization and Configuration Reference

This section describes the commands you can use to customize and configure the IronKey Enterprise Server using a command line interface. Also see "Useful PSCP.EXE Commands" on page 35.

Background

Some CLI commands require write access on the Virtual Machine that hosts the Enterprise Server before you can run the commands. For example, `sysconf restore` requires configuration files to be copied to the Enterprise Server before it starts. Similarly, some CLI commands require data to be copied out of the Enterprise Server after running them. For example, `sysconf backup` creates a backup configuration file and places it in the /download directory. To restore the file, the Server Admin needs to run the `scp` command to copy the backup file to /upload and then run the restore command to extract the file from the IronKey Enterprise Server.

Required Components

The installation of the IronKey Enterprise Server requires several commands/steps. These include the ability to set configuration for: NTP, SMTP, Network settings (DNS, Gateway, and so on), Activation URL (that is, where *my.ironkey.com* points), and so on.

Hosting McAfee Anti-Malware Updates

The McAfee anti-malware client software on IronKey Enterprise devices downloads virus definition file updates directly from update.nai.com servers at McAfee.

If you are using the IronKey Enterprise Server to manage IronKey Enterprise devices, you can configure devices to download the virus update (.DAT) files from a location you specify, such as a locally hosted server, to reduce your internet bandwith usage.

To configure an alternative download server for McAfee virus definition updates do the following:

1. Set up a web server to host the anti malware definition files.

2. Copy the contents of *http://update.nai.com/products/commonupdater/* (including the directory structure) to a location on the web server.

3. Make sure the computers on which IronKey devices are used can access the files over the network.

4. Set up a script to regularly download updates from the McAfee to your web server.

For example, you can schedule the following sample command to run

```
wget -r http://download.nai.com/products/commonupdater/
```

This will download files to a "download.nai.com" directory in the directory from which the command is run. You may need to alter this to suit your particular needs. Documentation can be found at: http://www.gnu.org/software/wget/manual/wget.html

5. Run the following two commands from the Command Line Interface (CLI) on the Enterprise Server:

```
application malwareScanner set defintionURL [http://<url-to-update-
  files>.com]
```

(Use the appropriate URL for your environment)

```
application malwareScanner set iniURL [http://<url-to-update-files.
  com>/oem.ini]
```

(Use the appropriate URL for the oem.ini file)

6. Enter the following CLI commands to restart the Enterprise Server service and enable the changes:

```
sysconf reboot
```

Enterprise devices should now download their antivirus updates from your locally hosted web server.

Commands Summary

Application Configuration Commands

```
application
```

Description:

Get all available application configuration commands.

```
application ssl
```

Description:

Get all available SSL configuration commands.

```
application ssl enable
```

Description:

Enable SSL.

```
application ssl disable
```

Description:

Disable SSL.

```
application ssl show
```

Description:

Display SSL configuration.

```
application certificate
```

Description:

Get all certificate management commands.

```
application certificate install
```

Description:

Install server certificate. The Server Admin has to import a VeriSign (or other supported public CA) Key and Certificate in PEM format using an SCP utility.

```
application certificate show
```

Description:

Display certificate details.

```
application database
```

Description:

Get all database commands.

```
application database configure <hostname or ip> <port> <username>
   <password> <type> <db name>
```

Description:

Configure database server information.

Arguments:

`hostnameorip`	hostname or ip address of database server.
`username`	Database user name
`password`	Database user password
`port`	Database server listener port
`type`	Type of Database (mssql,...)
`db name`	Database name (example: es_master)

`application database show`

Description:

Display database configuration.

`application healthCheck`

Description:

Verify connections between components of the product.

`application siteName`

Description:

Get all site name commands.

`application siteName set <siteName>`

Description:

Set the URL of the server as it will be accessed by devices.

`application siteName show`

Description:

Display the current site name.

`application version`

Description:

Get application version.

Logout Commands

`exit`

Description:

Exit from CLI.

`logout`

Description:

Log out of the current CLI session.

Help Command

`help`

Description:

Display an overview of the CLI syntax.

History Command

```
history <limit>
```

Description:

Display the current session's command line history.

Argument:

`limit`	Set the size of the history; zero means unbounded

Network Commands

```
network
```

Description:

Get all available network commands.

```
network dns
```

Description:

Get all available DNS commands.

```
network dns show
```

Description:

Display the DNS settings.

```
network dns add <ipaddress>
```

Description:

Add the DNS name server.

```
network dns del <ipaddress>
```

Description:

Delete the DNS name server.

```
network hostname <hostname>
```

Description:

Set the host name.

```
network interface
```

Description:

Get network interface configuration commands.

```
network interface dhcp
```

Description:

Enable DHCP.

```
network interface static <ip> <netmask> <gateway>
```

Description:

Configure static IP address.

```
network ping <dest>
```

Description:

Ping host or IP address.

```
network route
```

Description:

Get route configuration commands.

```
network route add <dest ip> <netmask> <gateway>
```

Description:

Add route.

Arguments:

`destip`	Network or host IP address
`netmask`	Subnet NetMask associated with this entry
`gateway`	Gateway ip address to use when forwarding

```
network route clear
```

Description:

Clear routes.

```
network route delete <dest ip> <netmask> <gateway>
```

Description:

Delete route.

Arguments:

`destip`	Network or host IP address
`netmask`	Subnet NetMask associated with this entry
`gateway`	Gateway ip address to use when forwarding

```
network route show
```

Description:

Display routing table.

```
network show
```

Description:

Display network configuration.

```
network traceroute <dest ip>
```

Description:

Remote system to trace.

Service Commands

```
service
```

Description:

Get service configuration commands.

```
service restart <name>
```

Description:

Restart service.

```
service start <name>
```

Description:

Start service.

```
service stop <name>
```

Description:

Stop service.

```
service status <name>
```

Description:

Get service status.

Status Commands

```
status
```

Description:

Get all system status commands.

```
status cpu
```

Description:

Get CPU status.

```
status disk
```

Description:

Get disk status.

```
status interface
```

Description:

Get network interface status.

```
status mem
```

Description:

Get memory status.

```
status netstat
```

Description:

Get network status.

```
status ps
```

Description:

Get processes status.

```
status time
```

Description:

Get the system time.

```
status top
```

Description:

Get the top information.

```
status vmstat
```

Description:

Get virtual memory status.

Sysconf Configuration Commands

```
sysconf
```

Description:

Get all available system configuration commands.

```
sysconf backup
```

Description:

Backup system configuration.

```
sysconf cleanup
```

Description:

Deletes temporary files from upload and download directories.

```
sysconf ntp
```

Description:

Get all available NTP configuration commands.

```
sysconf ntp addserver <hostname or ip>
```

Description:

Add NTP server name or IP.

```
sysconf ntp delserver <hostname or ip>
```

Description:

Delete NTP name or IP.

`sysconf ntp disable`

Description:

Enable NTP server.

`sysconf ntp enable`

Description:

Disable NTP server.

`sysconf ntp listservers`

Description:

Show the NTP servers from which to fetch `ntpupdate`.

`sysconf reboot`

Description:

Reboot system.

`sysconf restore`

Description:

Restore system configuration.

`sysconf time <time> <day> <month> <year>`

Description:

Set system time. Use this command if not using NTP.

Arguments:

`time`	Current time (`HH:MM:SS`)
`day`	Day of the month (`1..31`)
`month`	Month of year (`January`/`February`/`March`/`April`/`May`/`June`/`July`/`August`/`September`/`October`/`November`/`December`)
`year`	Four-digit year (`2008..2035`)

`sysconf timezone`

Description:

Get timezone commands.

`sysconf timezone show`

Description:

Get timezone information.

NOTE: To change the default Enterprise Server time zone from GMT, go to the Admin Console on *my.ironkey.com*, and click the "My Accounts" tab, and then click "Account Settings" in the left sidebar.

```
sysconf smtp
```

Description:

Get all available SMTP commands.

```
sysconf smtp show
```

Description:

Display SMTP RelayHost, if set.

```
sysconf smtp restart
```

Description:

Restart SMTP service.

```
sysconf smtp set <hostname or ip>
```

Description:

Configure SMTP RelayHost.

Arguments:

`hostnameorip` hostname or IP address of SMTP server.

```
sysconf smtp delete <hostname or ip>
```

Description:

Delete SMTP RelayHost.

Arguments:

`hostnameorip` hostname or IP address of SMTP server.

```
sysconf smtp test <email>
```

Description:

Test the SMTP RelayHost.

Arguments:

`email` Email address for test email to SMTP server.

```
sysconf user
```

Description:

Get all available user commands.

```
sysconf user password
```

Description:

Change user password.

```
sysconf user adduser <username>
```

Description:

Add a user.

```
sysconf user deluser <username>
```

Description:

Delete a user.

```
sysconf user listusers
```

Description:

List all users.

Syslog Configuration Commands

```
syslog
```

Description:

Get all available syslog commands.

```
syslog remote
```

Description:

Get all available syslog remote commands.

```
syslog remote disable
```

Description:

Disable remote logging.

```
syslog remote enable <hostname or ip>
```

Description:

Configure remote syslog.

Arguments:

`hostnameorip`	Remote syslog server hostname or ip address.

```
syslog tail <entries>
```

Description:

Tail particular syslog file.

Arguments:

`entries`	Number of entries to display.

```
syslog restart
```

Description:

Restart the syslog service.

Support Information

```
supportInfo
```

Description:

Generate support ticket. This generates an archive containing system information, application logs and configuration. It does not include customer keys and data.

Device Update Commands

```
device availableUpdates
```

Description:

Get all available device update packages (format: ikupdate_*.*) in the /upload folder.

```
device deleteUpdate
```

Description:

Delete the device update package already installed on the server.

```
device deployedUpdates
```

Description:

Get the current installed device update package

```
device installUpdate
```

Description:

Install device update package to the server. This prompts the user for the name of the package.