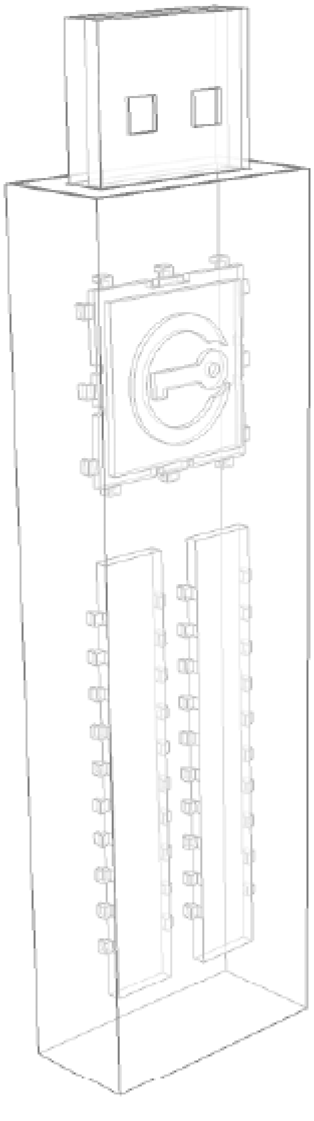
IRONKEY™
by imation

IronKey Enterprise Server 6.0

Setup Guide

Last Updated May 2015



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

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 v6.0.0.0 software – May 2015.. IK-EMS-ADM02-4.0

CONTENTS

About This Guide

This guide is written for IT Administrators and describes how to install and set up IronKey Enterprise Server by Imation. It also describes best practices for deploying and managing IronKey devices in your enterprise environment. This document also lists the commands available to customize and configure the server.

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 Guides (S250/D250, H300, H350, S1000)*
- *IronKey Workspace User Guides (W500, W700, W700-SC)*
- *IronKey Workspace IT Administrator Handbook—This document provides an overview of IronKey Workspace W300, W500, W700, W700-SC products*

About IronKey Enterprise Server

Overview

IronKey Enterprise Server is the world's most secure enterprise solution for managing USB flash drives, hard drives, and portable workspaces. 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 allows you to manage IronKey secure storage drives and IronKey Workspace drives using an on-premise server. Administrators can access the server to manage policies, users, and devices; users access their online accounts to view information about their devices and account settings.

Devices and users are managed by a web-based administrative interface:

- Admin Console—Allows admins to set policies, add users and groups, manage devices and more.
- System Console—Allows Admins to control device updates and automated messages

For more information about managing devices and users, see the *IronKey Enterprise Server Admin Guide*, available in the Admin Console and on the Setup device.

System Requirements

IronKey Enterprise Server uses virtual machine technology and can be installed in one of two different operating environments:

- Running in VMware® vSphere® ESXi Hypervisor environment
- Running in VMware® ACE Player software environment

The following table outlines the minimum requirements needed to install and use IronKey Enterprise Server.

Requirement	Description
Database	Microsoft SQL Server 2005, Microsoft SQL Server 2008, or Microsoft SQL Server 2012, Microsoft SQL Server Express 2005, Microsoft SQL Server Express 2008, Microsoft SQL Server Express 2012 **NOTE:** Only the default database instance is supported. IronKey Enterprise Server does not support named instances.
Host system requirements in ESXi environment	
vSphere ESXi version 5.0 or higher (the ESXi version must support the Guest OS CentOS v6.6—the OS on which IronKey Enterprise Server is installed). See the *VMware Compatibility Guide* for more information.	Host machine must meet the minimum system requirements for this version in addition to minimum ESXi requirements provided by VMware. See VMware product documentation for more details: http://www.vmware.com **NOTE:** You must have VMware vSphere ESXi already installed and set up on your host before you install IronKey Enterprise Server. Information on installing ESXi is outside the scope of this guide, see VMware product documentation.
Ethernet physical network adapter	1GB or faster
Memory	4GB physical RAM
Physical datastore space	70GB available space
Host system requirements in ACE Player environment (cannot be installed on any virtual machines, such as ESXi, Microsoft® Hyper-V®, Oracle VM VirtualBox)	
PC hardware	Two x86/x64 compatible 2+ GHz CPU cores minimum (4 cores recommended)
Operating system	Windows Server 2003, Windows Server 2008, or Windows Server 2012
Memory	4GB minimum (8GB recommended)
Display	16-bit (32-bit display adapter is recommended)
Hard Disk	30GB free disk space required; 60GB recommended.
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 IronKey Enterprise Server
System Admin	The administrator who manages end-users and their IronKey devices once the server is set up and running
Device	Generic term for an IronKey Enterprise Drive
CLI	The Command Line Interface used to configure the system

What's in the Box?

The IronKey Enterprise Server Kit contains six IronKey S250/D250 devices:

- One Setup device (labeled "Carrier/Setup") that contains the necessary software for installing IronKey Enterprise Server
- Four System Admin devices (labeled "Sys. Admin")
- One Standard User device (labeled "User") to be used for testing

IronKey Enterprise Server Support

Imation is committed to providing world-class support to its IronKey Enterprise Server 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 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, and contact information for IronKey Technical Support.

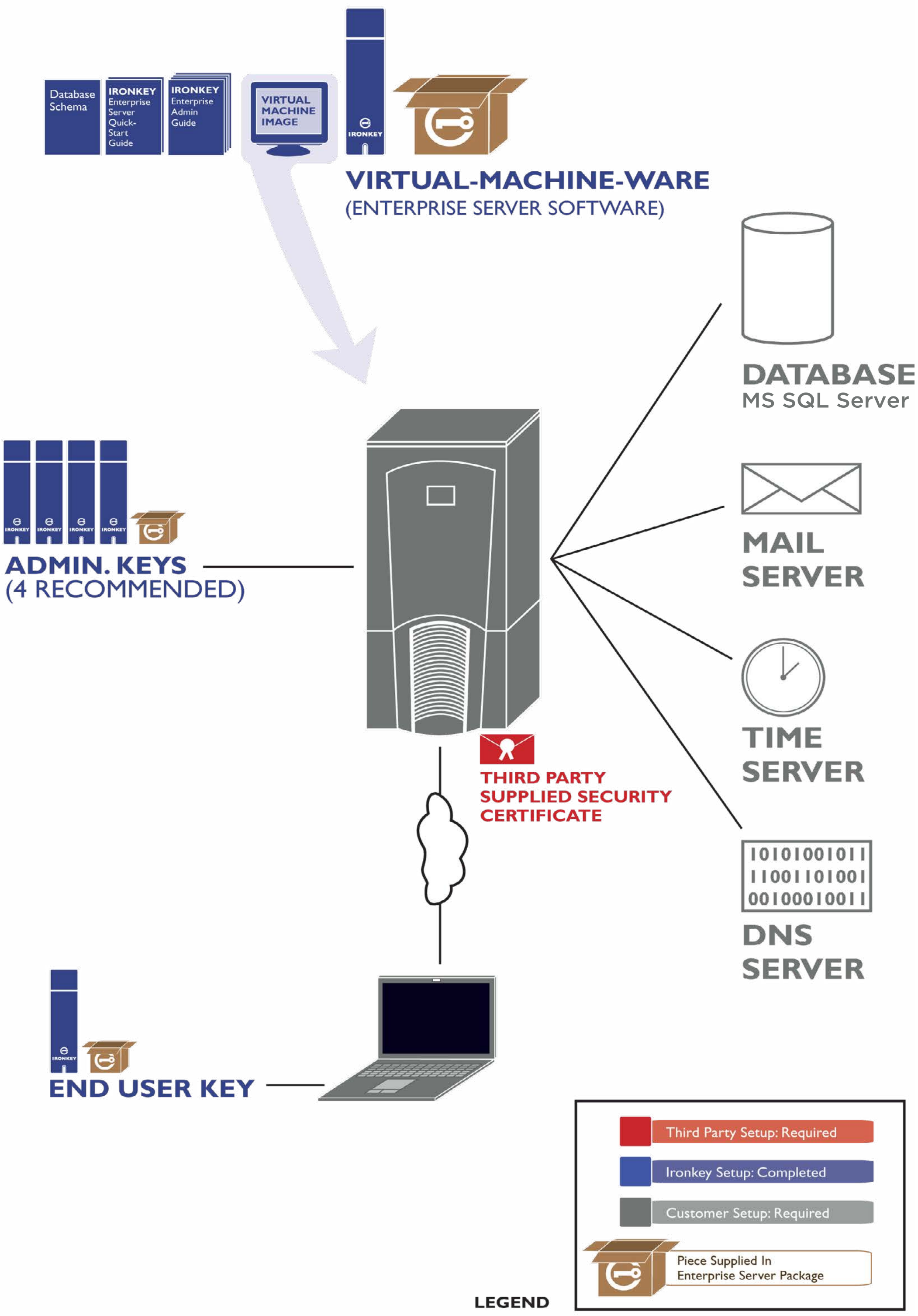
CONTACT INFORMATION

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

Product Architecture

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

ENTERPRISE SERVER ARCHITECTURAL DIAGRAM



Database Schema
IRONKEY Enterprise Server Quick-Start Guide
IRONKEY Enterprise Admin Guide
VIRTUAL MACHINE IMAGE
IRONKEY
VIRTUAL-MACHINE-WARE
(ENTERPRISE SERVER SOFTWARE)
DATABASE
MS SQL Server
MAIL SERVER
TIME SERVER
1010100101 1
1100110100 1
0010001001 1
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

Getting started

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 10 to help you collect and organize this information. The Setup Check List on page 11 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'll need:

- The IronKey Setup Device that contains the Enterprise Server software
- One IronKey System Admin device from the kit, to activate the first 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 environment only) 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 (**NOTE:** Save a backup copy of these files in a secure location.)	
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 Imation.

❑ IronKey Enterprise Server Kit received

❑ *Installation Worksheet* filled out

❑ External ports open (see "External Ports" on page 12)

❑ Third-party SSL Certificate ready (see "Certificate acquisition and renewal" on page 13)

❑ SQL Server database configured (see "Database setup" on page 15)

❑ Setup Device from 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 and 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 activated — can access Admin Console

❑ IronKey Enterprise Server Admin Guide reviewed for deployment

IronKey Enterprise Server Ports

The ports referred to in this section are those that are required to connect to IronKey Enterprise Server. For full functionality of devices (for example, Silver Bullet Service and activation), you must open the 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 and renewal" on page 13 for a list of approved certificate authorities.)

FQDN Example:

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

NOTE: To use the 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 52 for more information.

Application	DNS Name	Configuration	Port(s)
My IronKey	<server>.<full domain name>	HTTP or HTTPS	80, 443/TCP
Services	<server>.<full domain name>	HTTPS and Client Authentication	2000/TCP*
Device Updates Phase1	<server>.<full domain name>	HTTPS and Client Authentication	2001/TCP
Device Update Phase 2	<server>.<full domain name>	HTTP	2002/TCP
Silver Bullet	<server>.<full domain name>	HTTPS	2003/TCP
Device Activation	<server>.<full domain name>	HTTPS and Client Authentication	2004/TCP
* Port 2000/TCP is commonly used for Cisco VoIP phone management and may present a traffic conflict if phone traffic is on the Enterprise Server network. Contact Sales at Imation for an alternate installation of Enterprise Server.			

Certificate acquisition and renewal

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
   ```

   Server 2012
   ```
   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 and Server 2012:
   ```
   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 the 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`. Create a backup of this file and the original certificate file by copying them to a secure location.

NOTE: See "Configuring IronKey Enterprise Server" on page 31 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 44 for more information.
7. Install the certificate using the CLI command:

```
        application certificate install
```

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

```
        service start 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.**

RENEWING AN EXPIRED CERTIFICATE

When your certificate expires, you will need to request a new one from your certificate authority. Once you have the new certificate file, you can create a new `server.crt` file. When you install the new certificate, the old one is automatically replaced.

1. Create the `server.crt` file by opening your private key file (`host.key`) and copying 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`.
2. Use a Secure Copy (SCP) utility (such as command-line PSCP or GUI-based WinSCP) to securely copy your `server.crt` file to the /`upload` directory of the virtual machine.

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

3. Stop the application server using the CLI command.

```
        service stop appserver
```

4. Disable HTTPS.

```
        application ssl disable
```

5. Install the certificate.

```
        application certificate install
```

6. After the certificate is installed, enable HTTPS.

```
        application ssl enable
```

7. Restart the Enterprise Server.

```
        sysconf reboot
```

8. Restart the application server.

```
        service start appserver
```

Database setup

Before you install IronKey Enterprise Server, make sure you have 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. Only the default instance of SQL server is supported. Named instances of SQL Server are not currently supported.

IMPORTANT: To ensure that the front-end code base 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/ms144284.aspx* for more information.

DATABASE SETUP: 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*

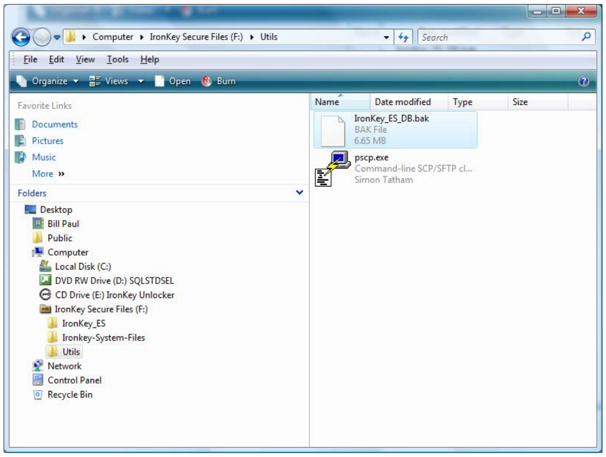
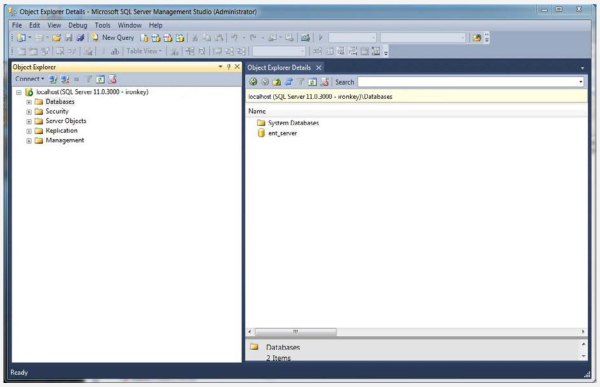
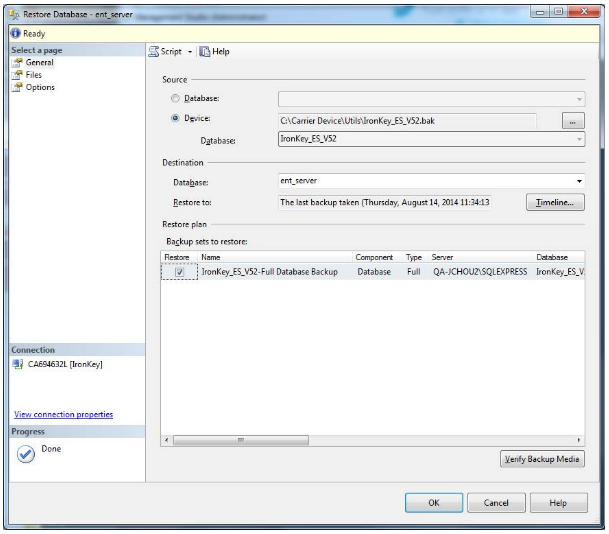
5. **Set the default database for the login (created in Step 1) to the IronKey Enterprise Server database:**

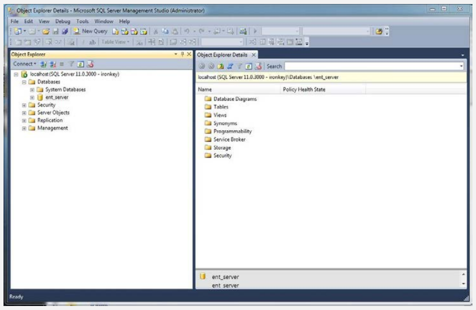
   ```
   alter login <login name> with default_database = <ironkey ES database name>;
   go
   ```

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

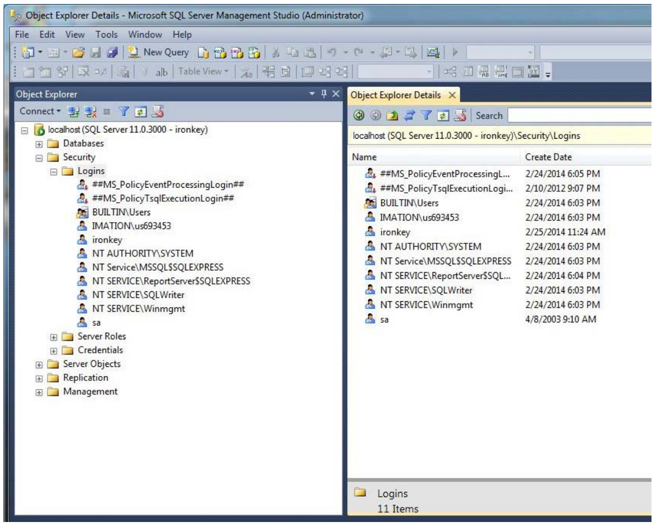
DATABASE SETUP: GUI STEPS

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

Steps		Description
1.1	Browse the secure volume on your Enterprise Server Setup device and click the **Utils** folder to locate the Enterprise Server schema, `IronKey_ES_V6.bak` (a backup of a blank database). **NOTE:** The device password to unlock the Setup device is provided in your Welcome email.	 Computer ▸ IronKey Secure Files (F:) ▸ Utils Search File Edit View Tools Help Organize Views Open Burn Favorite Links Documents Pictures Music More » Folders Desktop Bill Paul Public Computer Local Disk (C:) DVD RW Drive (D:) SQLSTDSEL CD Drive (E:) IronKey Unlocker IronKey Secure Files (F:) IronKey_ES Ironkey-System-Files Utils Network Control Panel Recycle Bin Name Date modified Type Size IronKey_ES_DB.bak BAK File 6.65 MB pscp.exe Command-line SCP/SFTP cl... Simon Tatham
1.2	In SQL Server Management Studio, right-click the **Databases** folder, and then click **Restore Database**.	 Object Explorer Details - Microsoft SQL Server Management Studio (Administrator) File Edit View Debug Tools Window Help New Query Table View Object Explorer Connect localhost (SQL Server 11.0.3000 - ironkey) Databases Security Server Objects Replication Management Object Explorer Details Search localhost (SQL Server 11.0.3000 - ironkey)\Databases Name System Databases ent_server Databases 2 Items Ready
1.3	In the **Restore Database** dialog box, do the following: a. Click **Device** and browse to the `IronKey_ES_V6.bak` file. (In the **Select Backup devices** dialog box, click the **Add** button, browse to the database backup file, and then click **OK**.) b. Enter the name for your new database in the **Database** box. The name cannot contain a dash (-). The location of the backup file is set, and the name of the destination database to restore appears in the **Backup sets to restore** list.	 Restore Database - ent_server Ready Select a page General Files Options Script Help Source Destination Restore plan Connection View connection properties Progress Done Timeline... Verify Backup Media OK Cancel Help ○ Database: ● Device: C:\Carrier Device\Utils\IronKey_ES_V52.bak Database: IronKey_ES_V52 Database: ent_server Restore to: The last backup taken (Thursday, August 14, 2014 11:34:13 Backup sets to restore: Restore | Name | Component | Type | Server | Database ☑ | IronKey_ES_V52-Full Database Backup | Database | Full | QA-JCHOU2\SQLEXPRESS | IronKey_ES_V CA694632L [IronKey]

Steps		Description
1.4	Click **OK** to return to the main window. Your new database appears under the **Database** folder.	

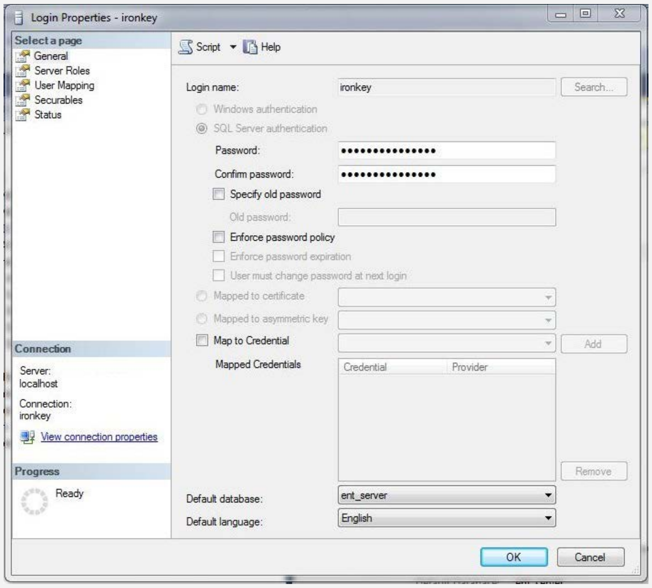
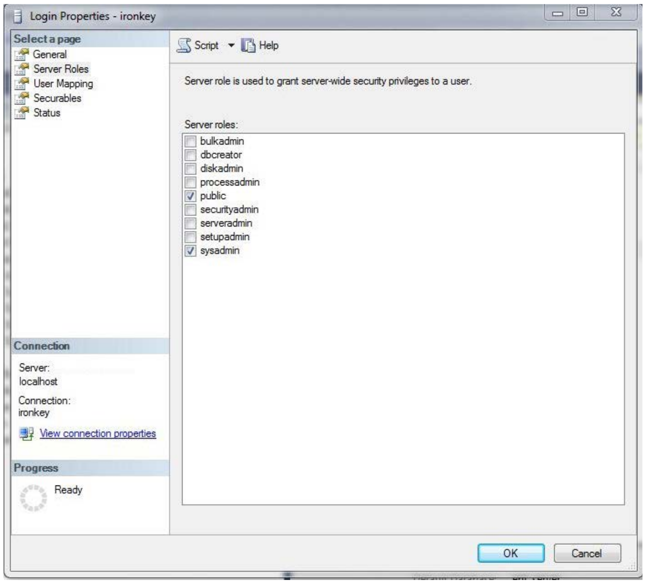
2. **Create a SQL Server login**
3. **Create a Database User (using the Login created in Step 2)**
4. **Grant the Database User (created in Step 3) the "db_owner" Server Role**

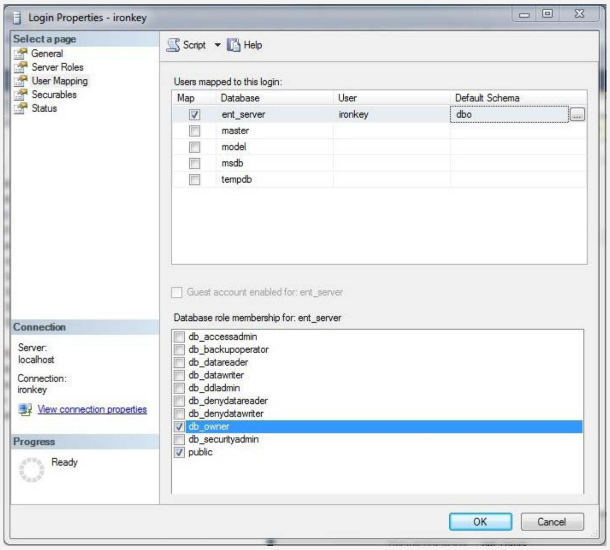
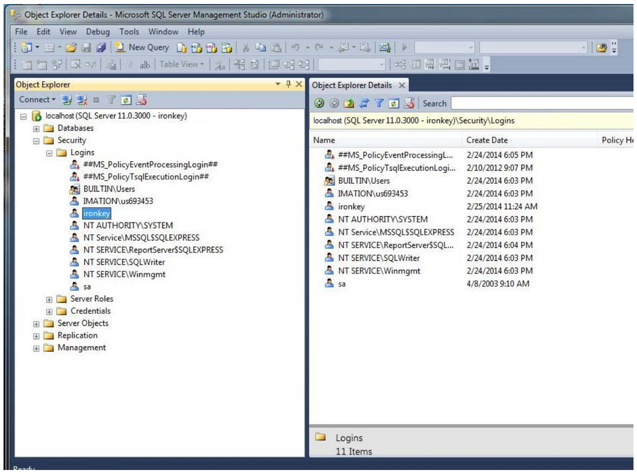
Steps		Description
4.1	In SQL Server Management Studio, expand the **Security** folder, right-click **Logins**, and then click **New login**.	

Object Explorer Details - Microsoft SQL Server Management Studio (Administrator)
File Edit View Tools Window Help
New Query
Table View
Object Explorer
Connect
localhost (SQL Server 11.0.3000 - ironkey)
Databases
Security
Logins
##MS_PolicyEventProcessingLogin##
##MS_PolicyTsqlExecutionLogin##
BUILTIN\Users
IMATION\us693453
ironkey
NT AUTHORITY\SYSTEM
NT Service\MSSQL$SQLEXPRESS
NT SERVICE\ReportServer$SQLEXPRESS
NT SERVICE\SQLWriter
NT SERVICE\Winmgmt
sa
Server Roles
Credentials
Server Objects
Replication
Management
Object Explorer Details
Search
localhost (SQL Server 11.0.3000 - ironkey)\Security\Logins

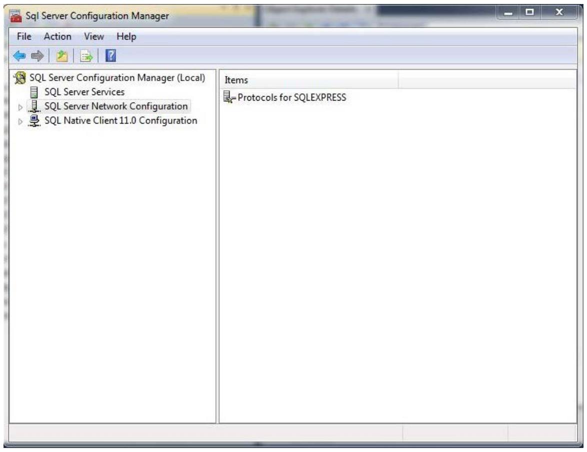
Name	Create Date
##MS_PolicyEventProcessingL...	2/24/2014 6:05 PM
##MS_PolicyTsqlExecutionLogi...	2/10/2012 9:07 PM
BUILTIN\Users	2/24/2014 6:03 PM
IMATION\us693453	2/24/2014 6:03 PM
ironkey	2/25/2014 11:24 AM
NT AUTHORITY\SYSTEM	2/24/2014 6:03 PM
NT Service\MSSQL$SQLEXPRESS	2/24/2014 6:03 PM
NT SERVICE\ReportServer$SQL...	2/24/2014 6:04 PM
NT SERVICE\SQLWriter	2/24/2014 6:03 PM
NT SERVICE\Winmgmt	2/24/2014 6:03 PM
sa	4/8/2003 9:10 AM

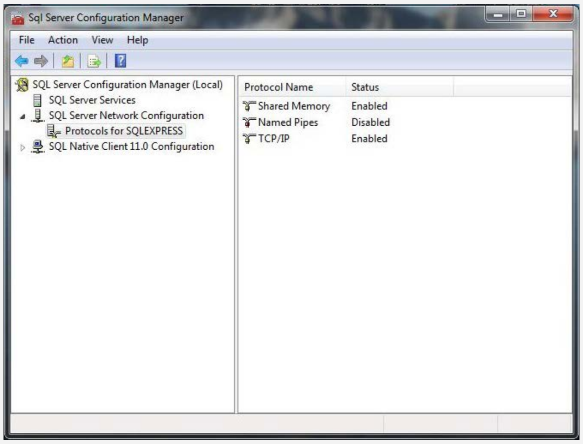
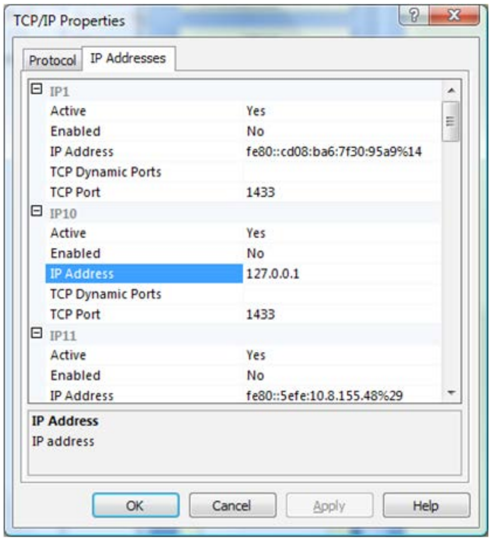
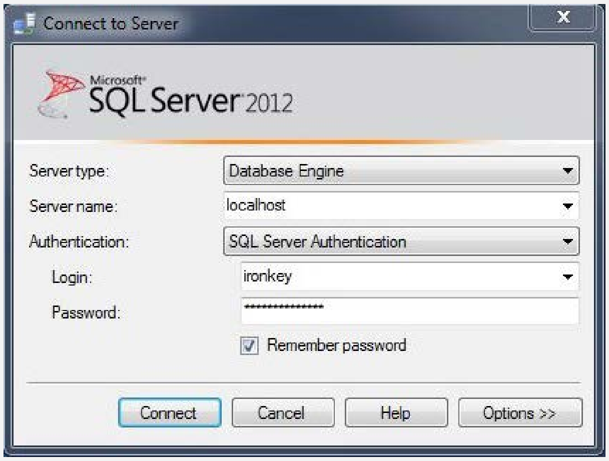
Logins
11 Items

Steps		Description
4.2	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 Properties - ironkey Select a page: General, Server Roles, User Mapping, Securables, Status Script · Help Login name: ironkey ○ Windows authentication ● SQL Server authentication Password: ••••••••••••••• Confirm password: ••••••••••••••• □ Specify old password Old password: □ Enforce password policy □ Enforce password expiration □ User must change password at next login ○ Mapped to certificate ○ Mapped to asymmetric key □ Map to Credential Mapped Credentials: Credential, Provider Default database: ent_server Default language: English Connection — Server: localhost; Connection: ironkey; View connection properties Progress — Ready OK · Cancel
4.3	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.**	 Login Properties - ironkey Select a page: General, Server Roles, User Mapping, Securables, Status Script · Help Server role is used to grant server-wide security privileges to a user. Server roles: □ bulkadmin □ dbcreator □ diskadmin □ processadmin ☑ public □ securityadmin □ serveradmin □ setupadmin ☑ sysadmin Connection — Server: localhost; Connection: ironkey; View connection properties Progress — Ready OK · Cancel

Steps		Description
4.4	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** section, check the boxes for **db_owner** and **public**	 Login Properties - ironkey Select a page: General, Server Roles, User Mapping, Securables, Status Users mapped to this login: Map / Database / User / Default Schema ☑ ent_server / ironkey / dbo ☐ master ☐ model ☐ msdb ☐ tempdb ☐ Guest account enabled for: ent_server Database role membership for: ent_server ☐ db_accessadmin ☐ db_backupoperator ☐ db_datareader ☐ db_datawriter ☐ db_ddladmin ☐ db_denydatareader ☐ db_denydatawriter ☑ db_owner ☐ db_securityadmin ☑ public Connection — Server: localhost; Connection: ironkey Progress: Ready
4.5	Click **OK** to return to the main window. Your new user appears under the **Logins** folder.	 Object Explorer Details - Microsoft SQL Server Management Studio (Administrator) localhost (SQL Server 11.0.3000 - ironkey)\Security\Logins Name / Create Date ##MS_PolicyEventProcessingL... 2/24/2014 6:05 PM ##MS_PolicyTsqlExecutionLogi... 2/10/2012 9:07 PM BUILTIN\Users 2/24/2014 6:03 PM IMATION\us693453 2/24/2014 6:03 PM ironkey 2/25/2014 11:24 AM NT AUTHORITY\SYSTEM 2/24/2014 6:03 PM NT Service\MSSQL$SQLEXPRESS 2/24/2014 6:03 PM NT SERVICE\ReportServer$SQL... 2/24/2014 6:04 PM NT SERVICE\SQLWriter 2/24/2014 6:03 PM NT SERVICE\Winmgmt 2/24/2014 6:03 PM sa 4/8/2003 9:10 AM Logins 11 Items

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

Steps		Description
5.1	Open SQL Server Configuration Manager. (Location: Go to **Start** screen > **Apps** > locate **SQL Server Configuration Manager**	 Sql Server Configuration Manager SQL Server Configuration Manager (Local) SQL Server Services SQL Server Network Configuration SQL Native Client 11.0 Configuration Items Protocols for SQLEXPRESS

Steps		Description
5.2	Expand **SQL Server Network Configuration**, and then click **Protocols for SQLEXPRESS**. **NOTE:** If you are not using SQLEXPRESS, click **Protocols for MSSQLSERVER**. Double-click **TCP/IP** in the right pane.	 SQL Server Configuration Manager (Local) SQL Server Services SQL Server Network Configuration Protocols for SQLEXPRESS SQL Native Client 11.0 Configuration Protocol Name — Status Shared Memory — Enabled Named Pipes — Disabled TCP/IP — Enabled
5.3	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::cd08:ba6:7f30:95a9%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:10.8.155.48%29 **IP Address** IP address
5.4	Open SQL Server Management Studio 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 2012 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 try 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.

Installing IronKey Enterprise Server

Before installing IronKey Enterprise Server, ensure that SQL Server is setup and uses the default installation settings. The Authentication Mode should be set to SQL Server Authentication Mode or Mixed Mode (Windows Authentication or SQL Server Authentication).

Provide the *IronKey_ES_V6.bak* file, located on the secure volume of the IronKey Setup Device in the *Utils* folder, to your DBA to set up the database. In return, the DBA will provide the username, password, database server IP, and port; you will need this information to configure the database settings for IronKey Enterprise Server after installation. See "Database setup" on page 15 for information about setting up the database.

IronKey Enterprise Server software leverages virtual server technology. IronKey Enterprise Server is a virtual server that runs on CentOS 6.6 operating system. There are two methods to install the server. Choose the method that meets your operating environment.

- To deploy the Server in a VMware vSphere ESXi environment, see page 22.
- To install the Server with VMware ACE environment, see page 26.

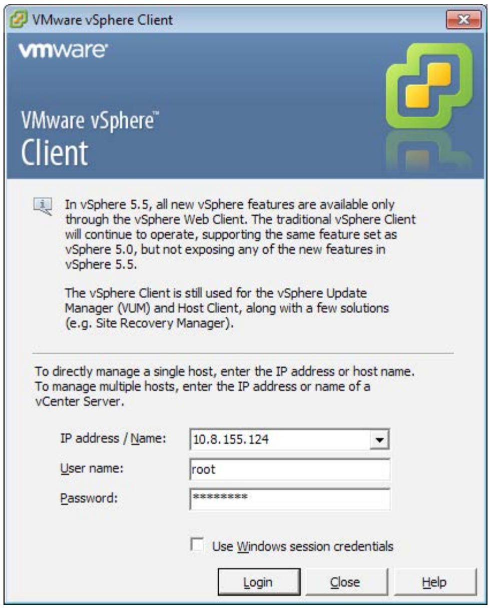
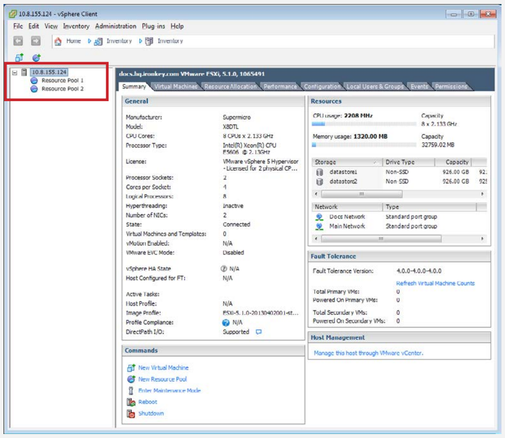
Installation files for both environments are located on the Setup device. Once installed, you must do the following:

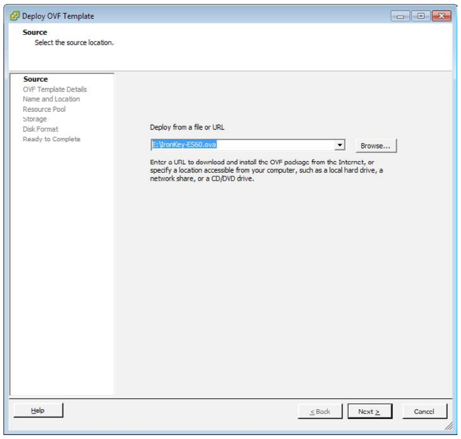
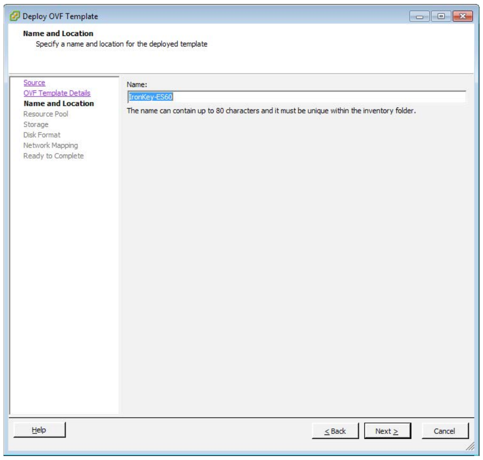
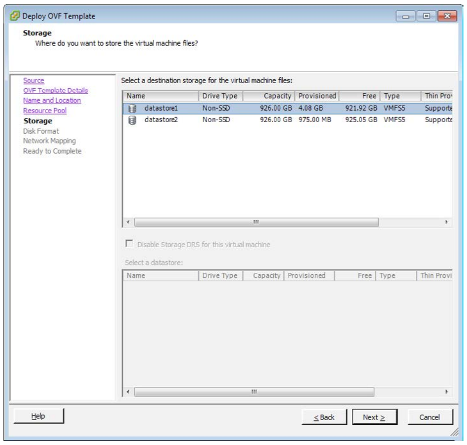
- Configure IronKey Enterprise Server
- Request a license and set up the Enterprise Account
- Initialize the first and second System Admin devices

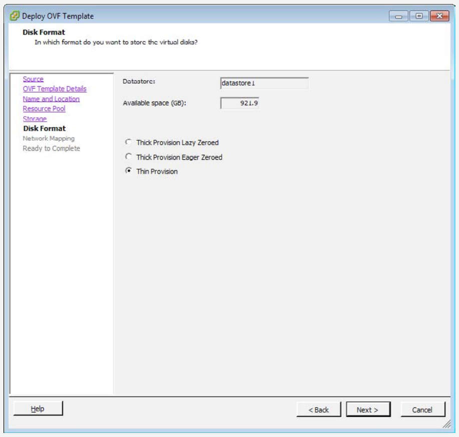
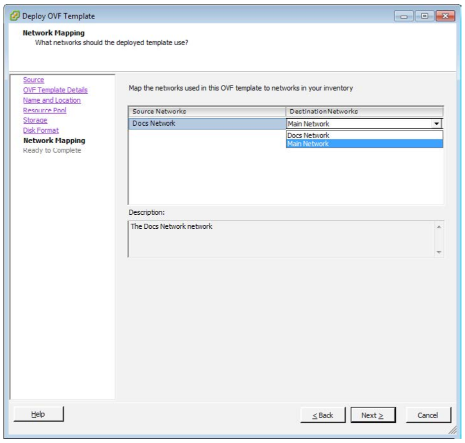
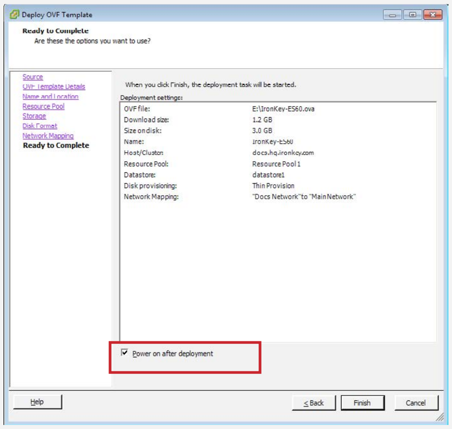
Deploying Enterprise Server in an ESXi environment

The Setup device includes an Open Virtualization Appliance (OVA) file, *IronKey_ES.ova*, to deploy IronKey Enterprise Server on the VMware ESXi host. OVA is an archive file that contains the Open Virtualization File (OVF) and supporting files required to deploy Enterprise Server. This procedure assumes that you already have VMware vSphere ESXi Hypervisor installed and configured. You will also need VMware vSphere Client. The client interface connects to VMware vSphere ESXi and allows you to configure the host and install and control virtual machines, such as IronKey Enterprise Server.

NOTE: IronKey Enterprise Server is supported only on vSphere ESXi version 5.1 Update 1 or later.

Steps		Description
1	Insert 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, and then click the Unlock button.	The password is the same as your account number, which you received in the Enterprise Server kit and in the Welcome Email. The IronKey Control Panel opens.
3	Login to the VMware vSphere ESXi server using VMware vSphere Client. You will be asked for the IP address/name of the host as well as the User name and Password.	 In vSphere 5.5, all new vSphere features are available only through the vSphere Web Client. The traditional vSphere Client will continue to operate, supporting the same feature set as vSphere 5.0, but not exposing any of the new features in vSphere 5.5. The vSphere Client is still used for the vSphere Update Manager (VUM) and Host Client, along with a few solutions (e.g. Site Recovery Manager). To directly manage a single host, enter the IP address or host name. To manage multiple hosts, enter the IP address or name of a vCenter Server. IP address / Name: 10.8.155.124 User name: root Password: ******** ☐ Use Windows session credentials VMware vSphere Client vmware VMware vSphere™ Client Login Close Help
4	In vSphere Client, click **File**, **Deploy OVF Template**. **NOTE:** If you have multiple Resource Pools in your ESXi environment, choose the Resource Pool to which you want to deploy the Server, and then click **File**, **Deploy OVF Template**. If you do not select a Resource Pool, you will be prompted to do so later in the setup.	 10.8.155.124 - vSphere Client 10.8.155.124 Resource Pool 1 Resource Pool 2 docs.hq.ironkey.com VMware ESXi, 5.1.0, 1065491 General Manufacturer: Supermicro Model: X8DTL CPU Cores: 8 CPUs x 2.133 GHz Processor Type: Intel(R) Xeon(R) CPU E5606 @ 2.13GHz License: VMware vSphere 5 Hypervisor - Licensed for 2 physical CP... Processor Sockets: 2 Cores per Socket: 4 Logical Processors: 8 Hyperthreading: Inactive Number of NICs: 2 State: Connected Virtual Machines and Templates: 0 vMotion Enabled: N/A VMware EVC Mode: Disabled vSphere HA State N/A Host Configured for FT: N/A Active Tasks: Host Profile: N/A Image Profile: ESXi-5.1.0-20130402001-st... Profile Compliance: N/A DirectPath I/O: Supported Resources CPU usage: **2208 MHz** Capacity 8 x 2.133 GHz Memory usage: **1320.00 MB** Capacity 32759.02 MB Storage / Drive Type / Capacity datastore1 / Non-SSD / 926.00 GB datastore2 / Non-SSD / 926.00 GB Network / Type Docs Network / Standard port group Main Network / Standard port group Fault Tolerance Fault Tolerance Version: 4.0.0-4.0.0-4.0.0 Total Primary VMs: 0 Powered On Primary VMs: 0 Total Secondary VMs: 0 Powered On Secondary VMs: 0 Host Management Manage this host through VMware vCenter. File Edit View Inventory Administration Plug-ins Help Home Inventory Inventory Summary Virtual Machines Resource Allocation Performance Configuration Local Users & Groups Events Permissions Refresh Virtual Machine Counts Commands New Virtual Machine New Resource Pool Enter Maintenance Mode Reboot Shutdown

Steps		Description
5	On the Deploy OVF Template screen, click **Browse**. Navigate to the **IronKey_ES OVA** folder on the IronKey Setup device and select the **IronKey_ES.ova** file, then click **Next**.	 Deploy OVF Template Source OVF Template Details Name and Location Resource Pool Storage Disk Format Ready to Complete Browse... Help < Back Next > Cancel **Source** Select the source location. Deploy from a file or URL E:\IronKey-ES60.ova Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.
6	Click **Next** after verifying the details of the Enterprise Server virtual machine template.	
7	On the **Name and Location** screen, enter a virtual machine name that is unique to your ESXi inventory and click **Next**.	 Deploy OVF Template Source OVF Template Details Name and Location Resource Pool Storage Disk Format Network Mapping Ready to Complete Help < Back Next > Cancel **Name and Location** Specify a name and location for the deployed template Name: IronKey-ES60 The name can contain up to 80 characters and it must be unique within the inventory folder.
8	If prompted to select a Resource Pool, select it and click **Next**.	
9	Select the destination storage for the virtual machine files. This screen will not display on ESXi servers with a single datastore. Click **Next**.	 Deploy OVF Template Source OVF Template Details Name and Location Resource Pool Storage Disk Format Network Mapping Ready to Complete Help < Back Next > Cancel **Storage** Where do you want to store the virtual machine files? Select a destination storage for the virtual machine files: Name, Drive Type, Capacity, Provisioned, Free, Type, Thin Pro datastore1, Non-SSD, 926.00 GB, 4.08 GB, 921.92 GB, VMFS5, Supporte datastore2, Non-SSD, 926.00 GB, 975.00 MB, 925.05 GB, VMFS5, Supporte □ Disable Storage DRS for this virtual machine Select a datastore: Name, Drive Type, Capacity, Provisioned, Free, Type, Thin Provi

Steps		Description
10	On the **Disk Format** screen, it is recommended that you choose the **Thin Provision** option to reduce the install time and to minimize disk space usage. Click **Next**.	 Deploy OVF Template **Disk Format** In which format do you want to store the virtual disks? Datastore: datastore1 Available space (GB): 921.9 ○ Thick Provision Lazy Zeroed ○ Thick Provision Eager Zeroed ● Thin Provision
11	On the **Network Mapping** screen, select the network that you want Enterprise Server to use from the **Destination Networks** list box. This screen will not display on ESXi servers with only one VM network. Click **Next**.	 Deploy OVF Template **Network Mapping** What networks should the deployed template use? Map the networks used in this OVF template to networks in your inventory Source Networks: Docs Network — Destination Networks: Main Network Docs Network Main Network Description: The Docs Network network
12	Verify the installation options and click to enable the **Power on after deployment** check box. Click **Finish**. **NOTE:** If you do not enable the **Power on after deployment** check box, you must start the VM manually after the deployment is completed.	 Deploy OVF Template **Ready to Complete** Are these the options you want to use? When you click Finish, the deployment task will be started. Deployment settings: OVF file: E:\IronKey-ES60.ova Download size: 1.2 GB Size on disk: 3.0 GB Name: IronKey-ES60 Host/Cluster: docs.hq.ironkey.com Resource Pool: Resource Pool 1 Datastore: datastore1 Disk provisioning: Thin Provision Network Mapping: "Docs Network" to "Main Network" ☑ Power on after deployment
13	An installation status dialog box will display to indicate how much time is left in the install process. Total time will vary depending on the ESXi CPU and the server disk throughput.	
14	When the **Deployment Completed Successfully** dialog box displays, click **Close**.	

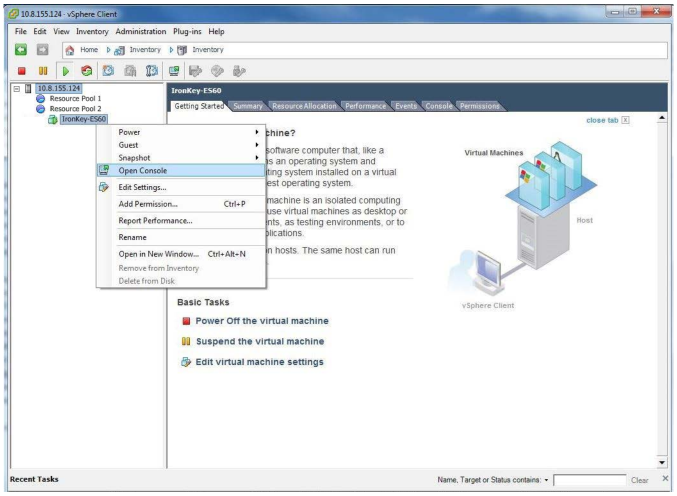
LOGGING IN THE FIRST TIME

<table>
<tr><th colspan="2">Steps</th><th>Description</th></tr>
<tr><td>1</td><td>

In vSphere Client, right-click IronKey Enterprise Server VM and click **Open Console**.

NOTE: If Enterprise Server is not already turned on, right-click the VM and click **Power**, **Power On**.

</td><td>



10.8.155.124 - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home Inventory Inventory
10.8.155.124
Resource Pool 1
Resource Pool 2
IronKey-ES60
Getting Started Summary Resource Allocation Performance Events Console Permissions
Power
Guest
Snapshot
Open Console
Edit Settings...
Add Permission... Ctrl+P
Report Performance...
Rename
Open in New Window... Ctrl+Alt+N
Remove from Inventory
Delete from Disk
close tab
Virtual Machines
Host
vSphere Client
Basic Tasks
Power Off the virtual machine
Suspend the virtual machine
Edit virtual machine settings
Recent Tasks
Name, Target or Status contains:
Clear

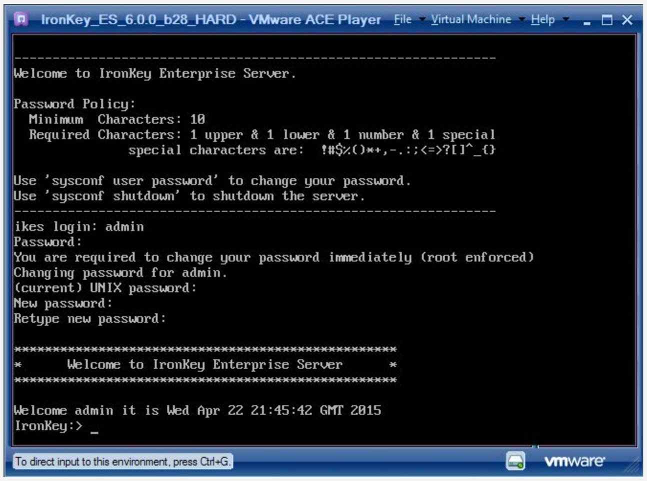
</td></tr>
<tr><td>2</td><td>

When the IronKey Command Line Interface (CLI) appears for IronKey Enterprise Server, log in using the CLI username and password provided in your Welcome Email.

You will be required to change your login password. The password requirements are:

- 10 character minimum
- 1 uppercase letter
- 1 lowercase letter
- 1 digit
- 1 special character

</td><td>



IronKey_ES_6.0.0_b28_HARD - VMware ACE Player File Virtual Machine Help
To direct input to this environment, press Ctrl+G.
vmware

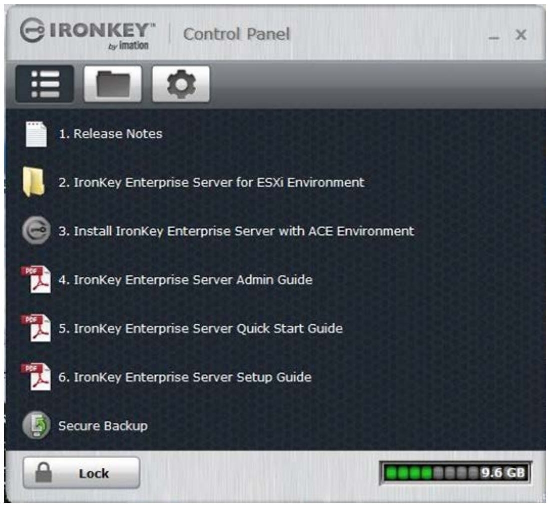
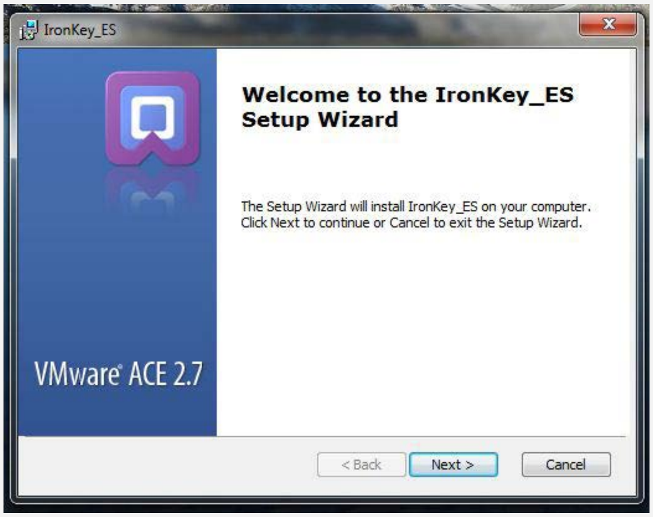
```
------------------------------------------------------------
Welcome to IronKey Enterprise Server.

Password Policy:
  Minimum  Characters: 10
  Required Characters: 1 upper & 1 lower & 1 number & 1 special
               special characters are:  !#$%()*+,-.:;<=>?[]^_{}

Use 'sysconf user password' to change your password.
Use 'sysconf shutdown' to shutdown the server.
------------------------------------------------------------
ikes login: admin
Password:
You are required to change your password immediately (root enforced)
Changing password for admin.
(current) UNIX password:
New password:
Retype new password:

**************************************************
*      Welcome to IronKey Enterprise Server      *
**************************************************

Welcome admin it is Wed Apr 22 21:45:42 GMT 2015
IronKey:> _
```

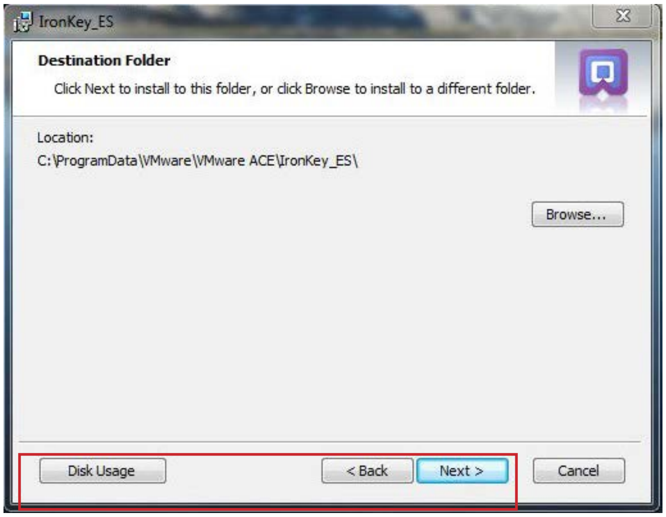
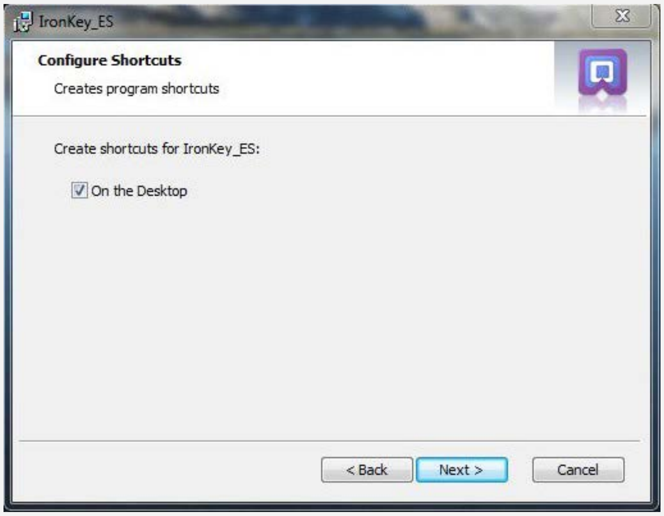
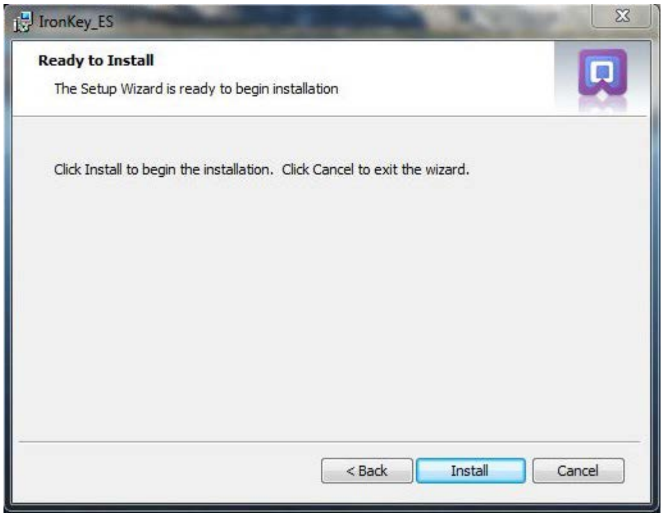
</td></tr>
</table>

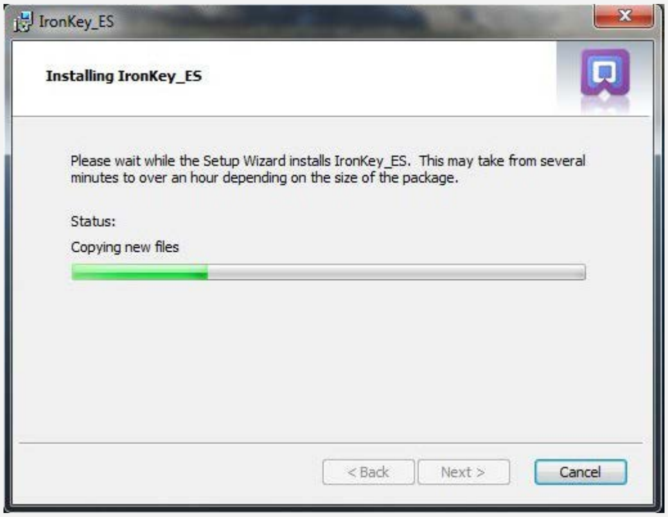
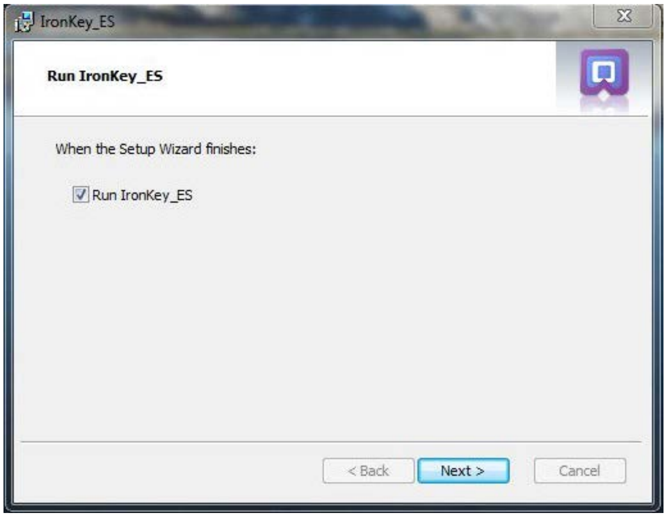
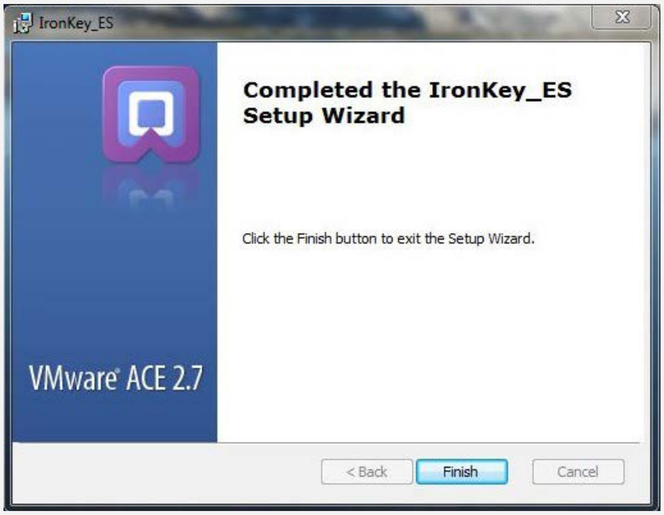
Installing Enterprise Server with ACE environment

When IronKey Enterprise Server is installed in an ACE environment, it runs in a virtual machine using VMware ACE software. This software contains a player that runs the software and the VM itself.

If you are familiar with virtualization and virtual machines, the ACE environment is not compatible with Type 1 Hypervisors, such as VMware ESXi or a Citrix XenSource solution. See “Deploying Enterprise Server in an ESXi environment” on page 22 to deploy the Server in ESXi.

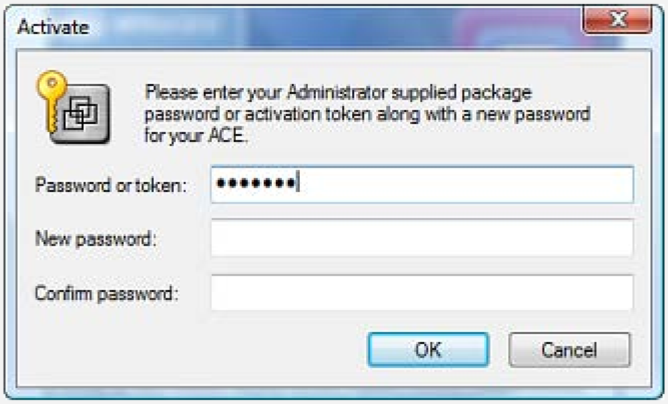
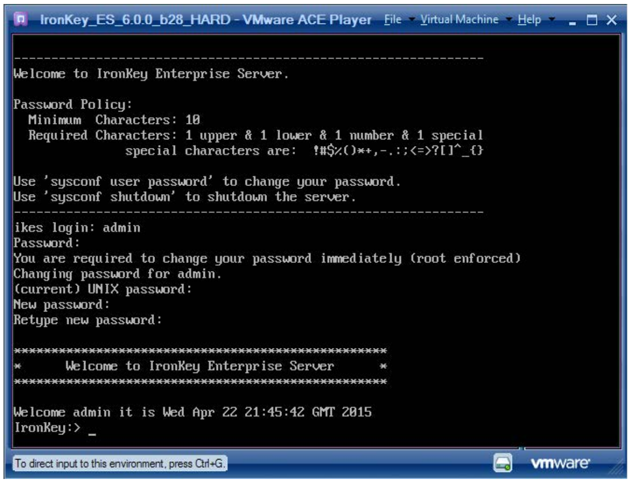
Steps		Description
1	Insert the IronKey Setup device into the USB port of the host computer.	If you do not see a prompt to unlock the device, go to “My Computer,” double-click the **IronKey** icon, and then double-click IronKey.exe.
2	Enter the Setup device password, and then click the **Unlock** button.	The password is the same as your account number, which you received in the Enterprise Server Kit and in the Welcome Email. The IronKey Control Panel opens.
3	In the Applications list of the IronKey Control Panel, click **Install IronKey Enterprise Server with ACE Environment**.	 IRONKEY by imation Control Panel 1. Release Notes 2. IronKey Enterprise Server for ESXi Environment 3. Install IronKey Enterprise Server with ACE Environment 4. IronKey Enterprise Server Admin Guide 5. IronKey Enterprise Server Quick Start Guide 6. IronKey Enterprise Server Setup Guide Secure Backup Lock 9.6 GB
4	When the Setup Wizard opens, click **Next**.	 IronKey_ES **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.

Steps		Description
5	Specify the installation folder where you want to install the VMware software and the VM.	 IronKey_ES **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\
6	• 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
7	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. Click Cancel to exit the wizard.

Steps		Description
8	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
9	- 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
10	When the process completes, click **Finish**.	 IronKey_ES **Completed the IronKey_ES Setup Wizard** Click the Finish button to exit the Setup Wizard.
11	Restart your computer if prompted to do so.	**NOTE:** Some installations require a restart of your computer.

LOGGING IN THE FIRST TIME

Once you've installed IronKey Enterprise Server, you will be required to create a new password for the ACE VM Player as well as for the Server.

Steps		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:
3	At the IronKey Command Line Interface (CLI) IronKey Enterprise Server, log in using the CLI username and password provided in your Welcome Email. You will be required to change your login password. The password requirements are: • 10 character minimum • 1 uppercase letter • 1 lowercase letter • 1 digit • 1 special character	 IronKey_ES_6.0.0_b28_HARD - VMware ACE Player To direct input to this environment, press Ctrl+G.

```
---------------------------------------------------------------
Welcome to IronKey Enterprise Server.

Password Policy:
  Minimum  Characters: 10
  Required Characters: 1 upper & 1 lower & 1 number & 1 special
               special characters are:  !#$%()*+,-.:;<=>?[]^_{}

Use 'sysconf user password' to change your password.
Use 'sysconf shutdown' to shutdown the server.
---------------------------------------------------------------
ikes login: admin
Password:
You are required to change your password immediately (root enforced)
Changing password for admin.
(current) UNIX password:
New password:
Retype new password:

**************************************************
*      Welcome to IronKey Enterprise Server      *
**************************************************

Welcome admin it is Wed Apr 22 21:45:42 GMT 2015
IronKey:> _
```

Configuring IronKey Enterprise Server

Once you have successfully deployed or installed IronKey Enterprise Server, you will use the command line interface (CLI) to configure and customize the 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 the 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 commands, see the "Configuration and command reference" on page 52.

Once you log in to the CLI, enter the commands to configure Enterprise Server. The following procedure outlines the basic steps to complete the configuration and includes 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.

When necessary, use the Shutdown command to safely shut down the Server.

Steps		Description
1	Log in to IronKey Enterprise Server using the command line interface (CLI).	

2	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`

3	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`

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

5	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 (GMT) using the `sysconf` time command. Enterprise Server will show the correct time once you set the date or add the NTP server.
		Example:
		`sysconf time 14:11:00 31 August 2012`

6	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)?`

Steps		Description

7	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`

8	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`

9	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 and renewal" on page 13 and "Useful PSCP.EXE Commands" on page 44 for more information.
10	Install the certificates.	`application certificate install`
11	Enable HTTPS.	`application ssl enable`
12	Start Enterprise 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.`

Shutting down IronKey Enterprise Server

Whether IronKey Enterprise Server is installed in an ESXi or ACE environment, you should use the `sysconf shutdown` command to safely shut down the Server.

- At the command prompt, type `sysconf shutdown`.

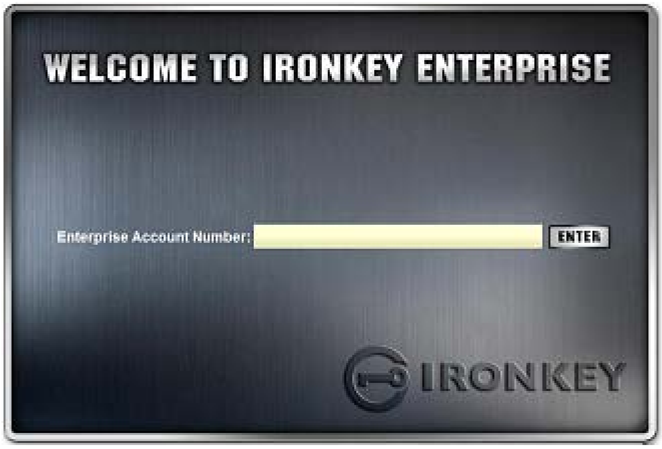
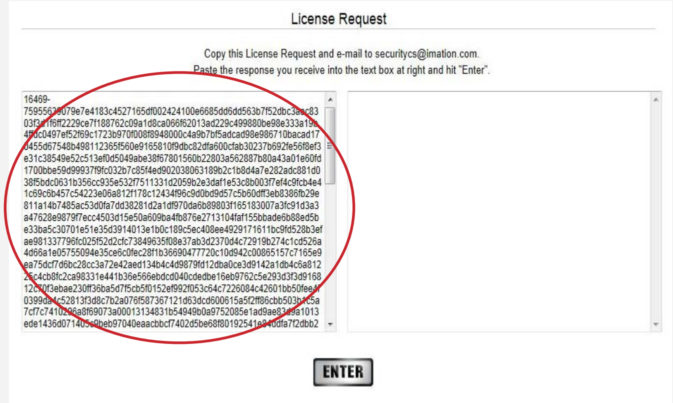
NOTE: In vSphere ESXi Client, closing the console window does not shut down the Server. Also, clicking the **Power Off** button (or right-clicking the Server and choosing **Power**, **Power Off**) is not a recommended method of shutting down the Server.

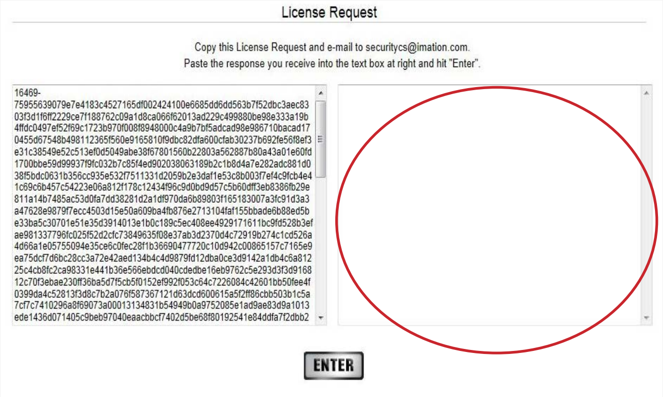
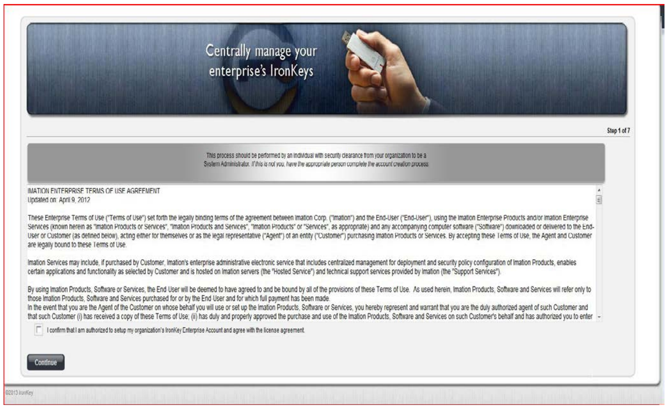
NOTE: In ACE Player, closing the ACE Player application is not a recommended method of shutting down the Server.

Setting up your Enterprise Account

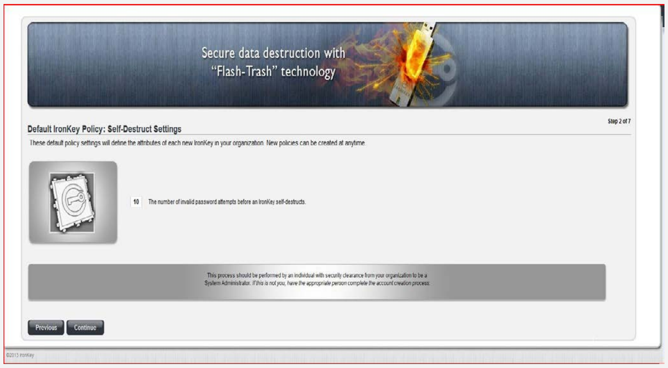
After you have configured IronKey Enterprise Server, you must set up your Enterprise Account. You must have the required license and security information from IronKey Customer Service to set up and activate your Enterprise Account. This ensures that only your organization can use the software provided and protects you against unauthorized use and phishing attacks. During the account setup, you will configure settings for the default device policy.

NOTE: After you receive the Welcome Email containing your server activation code, you are ready to start the Enterprise Account setup. During the setup, you will send a license request to Imation. In return, Imation Customer Service will send a License Response email that contains your server license. Once you receive the email, you can complete your account setup.

Steps		Description
1	Go to **https://<application siteName>/enterprisesetup** (where **<application siteName>** is the value you entered in step 7 of the Configuring IronKey Enterprise Server procedure). From the 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 e-mail to securitycs@imation.com. Paste the response you receive into the text box at right and hit "Enter". 16469- 75955639079e7e4183c4527165df002424100e6685dd6dd563b7f52dbc3aec83 03f3d1f6ff2229ce7f188762c09a1d8ca066f62013ad229c499880be98e333a19b 4ffdc0497ef52f69c1723b970f008f8948000c4a9b7bf5adcad98e986710bacad17 0455d67548b498112365f560e9165810f9dbc82dfa600cfab30237b692fe56f8ef3 e31c38549e52c513ef0d5049abe38f67801560b22803a562887b80a43a01e60fd 1700bbe59d99937f9fc032b7c85f4ed902038063189b2c1b8d4a7e282adc881d0 38f5bdc0631b356cc935e532f7511331d2059b2e3daf1e53c8b003f7ef4c9fcb4e4 1c69c6b457c54223e06a812f178c12434f96c9d0bd9d57c5b60dff3eb8386fb29e 811a14b7485ac53d0fa7dd38281d2a1df970da6b89803f165183007a3fc91d3a3 a47628e9879f7ecc4503d15e50a609ba4fb876e2713104faf155bbade6b88ed5b e33ba5c30701e51e35d3914013e1b0c189c5ec408ee4929171611bc9fd528b3ef ae981337796fc025f52d2cfc73849635f08e37ab3d2370d4c72919b274c1cd526a 4d66a1e05755094e35ce6c0fec28f1b36690477720c10d942c00865157c7165e9 ea75dcf7d6bc28cc3a72e42aed134b4c4d9879fd12dba0ce3d9142a1db4c6a812 25c4cb8fc2ca98331e441b36e566ebdcd040cdedbe16eb9762c5e293d3f3d9168 12c70f3ebae230ff36ba5d7f5cb5f0152ef992f053c64c7226084c42601bb50fee4f 0399da4c52813f3d8c7b2a076f587367121d63dcd600615a5f2ff86cbb503b1c5a 7cf7c7410296a8f69073a00013134831b54949b0a9752085e1ad9ae83d9a1013 ede1436d071405c9beb97040eaacbbcf7402d5be68f80192541e84ddfa7f2dbb2

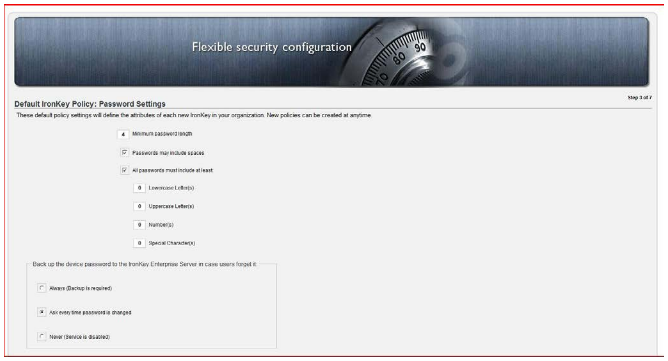
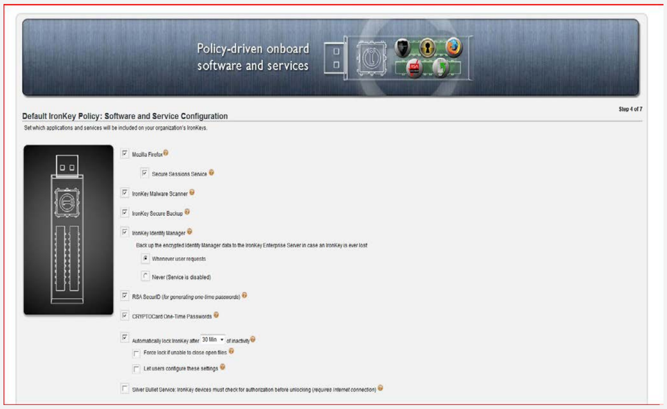
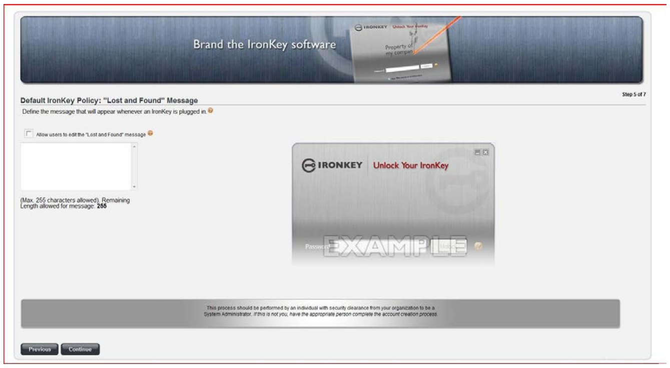
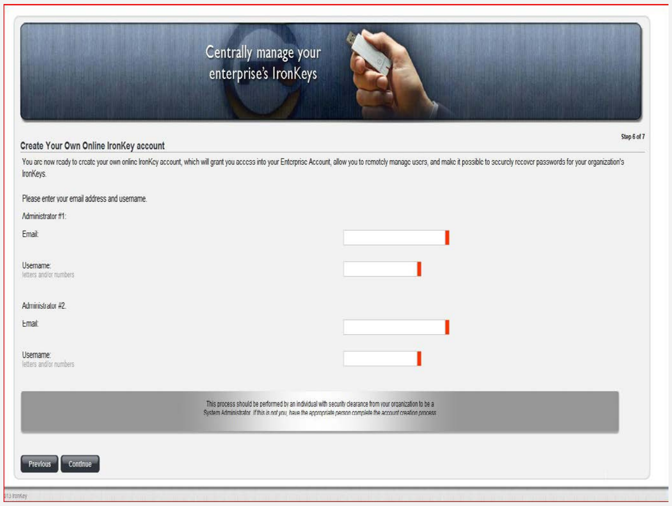
<table>
<tr><th colspan="2">Steps</th><th>Description</th></tr>
<tr><td><b>3</b></td><td>Check your email for a message from Customer Service. This may take 24-48 hours to complete.</td><td>You need the license key contained in this email to complete the installation.</td></tr>
<tr><td><b>4</b></td><td>On the <b>License Request</b> page, copy the license key that you received from Customer Service and paste it into the text box on the right.
Click <b>Enter</b>.</td><td>
License Request
Copy this License Request and e-mail to securitycs@imation.com.
Paste the response you receive into the text box at right and hit "Enter".
16469-
75955639079e7e4183c4527165df002424100e6685dd6dd563b7f52dbc3aec83
03f3d1f6ff2229ce7f188762c09a1d8ca066f62013ad229c499880be98e333a19b
4ffdc0497ef52f69c1723b970f008f8948000c4a9b7bf5adcad98e986710bacad17
0455d67548b498112365f560e9165810f9dbc82dfa600cfab30237b692fe56f8ef3
e31c38549e52c513ef0d5049abe38f67801560b22803a562887b80a43a01e60fd
1700bbe59d99937f9fc032b7c85f4ed902038063189b2c1b8d4a7e282adc881d0
38f5bdc0631b356cc935e532f7511331d2059b2e3daf1e53c8b003f7ef4c9fcb4e4
1c69c6b457c54223e06a812f178c12434f96c9d0bd9d57c5b60dff3eb8386fb29e
811a14b7485ac53d0fa7dd38281d2a1df970da6b89803f165183007a3fc91d3a3
a47628e9879f7ecc4503d15e50a609ba4fb876e2713104faf155bbade6b88ed5b
e33ba5c30701e51e35d3914013e1b0c189c5ec408ee4929171611bc9fd528b3ef
ae981337796fc025f52d2cfc73849635f08e37ab3d2370d4c72919b274c1cd526a
4d66a1e05755094e35ce6c0fec28f1b36690477720c10d942c00865157c7165e9
ea75dcf7d6bc28cc3a72e42aed134b4c4d9879fd12dba0ce3d9142a1db4c6a812
25c4cb8fc2ca98331e441b36e566ebdcd040cdedbe16eb9762c5e293d3f3d9168
12c70f3ebae230ff36ba5d7f5cb5f0152ef992f053c64c7226084c42601bb50fee4f
0399da4c52813f3d8c7b2a076f587367121d63dcd600615a5f2ff86cbb503b1c5a
7cf7c7410296a8f69073a00013134831b54949b0a9752085e1ad9ae83d9a1013
ede1436d071405c9beb97040eaacbbcf7402d5be68f80192541e84ddfa7f2dbb2
</td></tr>
<tr><td><b>5</b></td><td>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 <b>Continue</b>.</td><td>

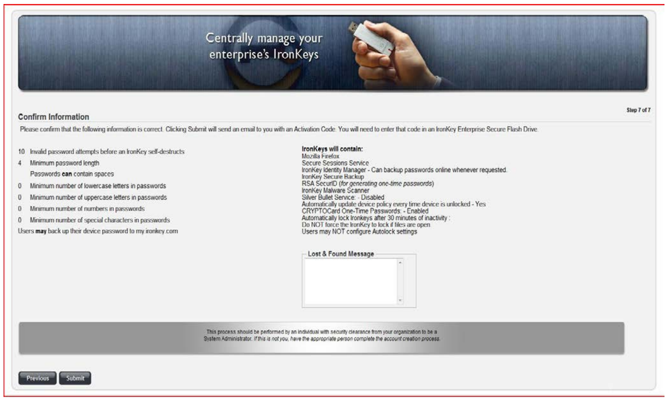
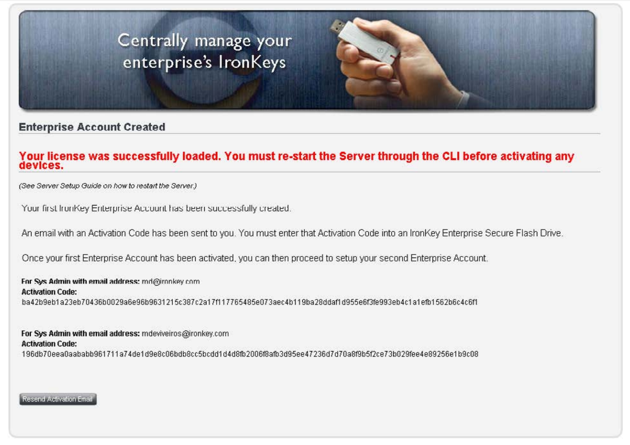
Step 1 of 7
This process should be performed by an individual with security clearance from your organization to be a System Administrator. <i>If this is not you, have the appropriate person complete the account creation process.</i>
IMATION ENTERPRISE TERMS OF USE AGREEMENT
Updated on: April 9, 2012
These Enterprise Terms of Use ("Terms of Use") set forth the legally binding terms of the agreement between Imation Corp. ("Imation") and the End-User ("End-User"), using the Imation Enterprise Products and/or Imation Enterprise Services (known herein as "Imation Products or Services", "Imation Products and Services", "Imation Products" or "Services", as appropriate) and any accompanying computer software ("Software") downloaded or delivered to the End-User or Customer (as defined below), acting either for themselves or as the legal representative ("Agent") of an entity ("Customer") purchasing Imation Products or Services. By accepting these Terms of Use, the Agent and Customer are legally bound to these Terms of Use.
Imation Services may include, if purchased by Customer, Imation's enterprise administrative electronic service that includes centralized management for deployment and security policy configuration of Imation Products, enables certain applications and functionality as selected by Customer and is hosted on Imation servers (the "Hosted Service") and technical support services provided by Imation (the "Support Services").
By using Imation Products, Software or Services, the End User will be deemed to have agreed to and be bound by all of the provisions of these Terms of Use. As used herein, Imation Products, Software and Services will refer only to those Imation Products, Software and Services purchased for or by the End User and for which full payment has been made.
In the event that you are the Agent of the Customer on whose behalf you will use or set up the Imation Products, Software or Services, you hereby represent and warrant that you are the duly authorized agent of such Customer and that such Customer (i) has received a copy of these Terms of Use; (ii) has duly and properly approved the purchase and use of the Imation Products, Software and Services on such Customer's behalf and has authorized you to enter
□ I confirm that I am authorized to setup my organization's IronKey Enterprise Account and agree with the license agreement.

©2013 IronKey</td></tr>
<tr><td><b>6</b></td><td>Select the number of failed password attempts that a user can enter before the IronKey device self-destructs.
<b>NOTE:</b> When an IronKey device self-destructs, all data is permanently lost and the drive can no longer be used.
Click <b>Continue</b>.</td><td>

Step 2 of 7
Default IronKey Policy: Self-Destruct Settings
These default policy settings will define the attributes of each new IronKey in your organization. New policies can be created at anytime.
10 The number of invalid password attempts before an IronKey self-destructs.
This process should be performed by an individual with security clearance from your organization to be a System Administrator. <i>If this is not you, have the appropriate person complete the account creation process.</i>

©2013 IronKey</td></tr>
</table>

Steps		Description
7	Select the password policy options that will be applied to each device. Click **Continue**.	 Flexible security configuration Step 3 of 7 **Default IronKey Policy: Password Settings** These default policy settings will define the attributes of each new IronKey in your organization. New policies can be created at anytime. 4 Minimum password length ☑ Passwords may include spaces ☑ All passwords must include at least: 0 Lowercase Letter(s) 0 Uppercase Letter(s) 0 Number(s) 0 Special Character(s) Back up the device password to the IronKey Enterprise Server in case users forget it: ○ Always (Backup is required) ● Ask every time password is changed ○ Never (Service is disabled)
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**.	 Policy-driven onboard software and services Step 4 of 7 **Default IronKey Policy: Software and Service Configuration** Set which applications and services will be included on your organization's IronKeys. ☑ Mozilla Firefox ☑ Secure Sessions Service ☑ IronKey Malware Scanner ☑ IronKey Secure Backup ☑ IronKey Identity Manager Back up the encrypted Identity Manager data to the IronKey Enterprise Server in case an IronKey is ever lost: ● Whenever user requests ○ Never (Service is disabled) ☑ RSA SecurID (*for generating one-time passwords*) ☑ CRYPTOCard One-Time Passwords ☑ Automatically lock IronKey after 30 Min ▾ of inactivity ☐ Force lock if unable to close open files ☐ Let users configure these settings ☐ Silver Bullet Service: IronKey devices must check for authorization before unlocking (*requires Internet connection*)
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**.	 Brand the IronKey software Step 5 of 7 **Default IronKey Policy: "Lost and Found" Message** Define the message that will appear whenever an IronKey is plugged in. ☐ Allow users to edit the "Lost and Found" message (Max. 255 characters allowed). Remaining Length allowed for message: **255** IRONKEY Unlock Your IronKey EXAMPLE This process should be performed by an individual with security clearance from your organization to be a System Administrator. *If this is not you, have the appropriate person complete the account creation process.* Previous Continue
10	Enter an email address and assign a user name for the first and second System Administrator. 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.	 Centrally manage your enterprise's IronKeys Step 6 of 7 **Create Your Own Online IronKey account** You are now ready to create your own online IronKey account, which will grant you access into your Enterprise Account, allow you to remotely manage users, and make it possible to securely recover passwords for your organization's IronKeys. Please enter your email address and username. Administrator #1: Email: Username: letters and/or numbers Administrator #2: Email: Username: letters and/or numbers This process should be performed by an individual with security clearance from your organization to be a System Administrator. *If this is not you, have the appropriate person complete the account creation process.* Previous Continue 013 IronKey

Steps		Description
11	Review your Enterprise account information. If everything is correct, click **Submit**.	 Centrally manage your enterprise's IronKeys **Confirm Information** Step 7 of 7 Please confirm that the following information is correct. Clicking Submit will send an email to you with an Activation Code. You will need to enter that code in an IronKey Enterprise Secure Flash Drive. 10 Invalid password attempts before an IronKey self-destructs 4 Minimum password length Passwords **can** contain spaces 0 Minimum number of lowercase letters in passwords 0 Minimum number of uppercase letters in passwords 0 Minimum number of numbers in passwords 0 Minimum number of special characters in passwords Users **may** back up their device password to my.ironkey.com **IronKeys will contain:** Mozilla Firefox Secure Sessions Service IronKey Identity Manager - Can backup passwords online whenever requested. IronKey Secure Backup RSA SecurID (*for generating one-time passwords*) IronKey Malware Scanner Silver Bullet Service: - Disabled Automatically update device policy every time device is unlocked - Yes CRYPTOCard One-Time Passwords: - Enabled Automatically lock Ironkeys after 30 minutes of inactivity : Do NOT force the IronKey to lock if files are open Users may NOT configure Autolock settings Lost & Found Message This process should be performed by an individual with security clearance from your organization to be a System Administrator. *If this is not you, have the appropriate person complete the account creation process.*
12	A confirmation message appears when your Enterprise account has been created. Each System Admin will receive an email message with an Activation Code, sent to the address provided in step 10. It is recommended that you 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.	 Centrally manage your enterprise's IronKeys **Enterprise Account Created** **Your license was successfully loaded. You must re-start the Server through the CLI before activating any devices.** *(See Server Setup Guide on how to restart the Server.)* Your first IronKey Enterprise Account has been successfully created. An email with an Activation Code has been sent to you. You must enter that Activation Code into an IronKey Enterprise Secure Flash Drive. Once your first Enterprise Account has been activated, you can then proceed to setup your second Enterprise Account. **For Sys Admin with email address:** md@ironkey.com **Activation Code:** ba42b9eb1a23eb70436b0029a6e96b9631215c387c2a17f117765485e073aec4b119ba28ddaf1d955e6f3fe993eb4c1a1efb1562b6c4c6f1 **For Sys Admin with email address:** mdeviveiros@ironkey.com **Activation Code:** 196db70eea0aababb961711a74de1d9e8c06bdb8cc5bcdd1d4d8fb2006f8afb3d95ee47236d7d70a8f9b5f2ce73b029fee4e89256e1b9c08
13	Reboot Enterprise Server.	Enter this CLI command: `sysconf reboot`

IMPORTANT – If you do not reboot the Server prior to activating your devices then the activation process will fail. Be sure to perform this step before activating any devices.

Activating the 1st and 2nd System Admin devices

After you set up the Enterprise Account, the first and second System Admin users will receive an email containing the Activation Code that is used to activate the first and second System Admin devices. The username and email address for the first and second System Admin users was added during the Account Setup. Make sure that the users have received the email message before continuing.

Your Server package comes with four IronKey Enterprise devices (250 Series) for use by a System Admin. However, you can also use any inactivated IronKey Enterprise H300, H350 or S1000 device if these devices are part of the set purchased. IronKey Basic devices (H300, H350 or S1000) must be upgraded to an IronKey Enterprise device before you can activate them as a System Admin device. See *IronKey Enterprise Server Admin Guide* for information about upgrading a Basic device.

NOTE: W500, W700, or W700-SC devices cannot be used as the 1st or 2nd System Admin device.

IMPORTANT: Always maintain multiple active System Admin devices 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 device, plug it into a USB 2.0 port (USB 3.0 is recommended for H300, H350 or S1000 devices).

Activating the 1st System Admin device

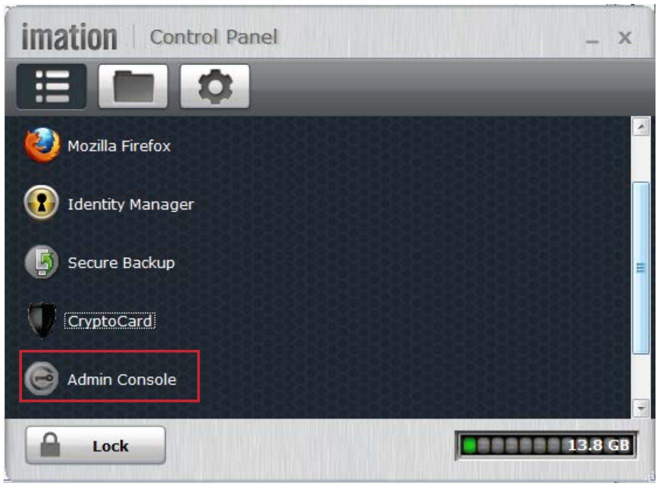
Steps	
1	Plug in an IronKey Enterprise System Admin (labeled Sys. Admin) device from your kit into the host computer. The device must be new and not previously activated.

Steps	
2	The "Device Setup" screen appears. The setup software runs automatically from a virtual DVD (250 Series). This screen may not appear if your computer does not allow devices to autorun or if you are using an H300, H350, or S1000 device, which mounts as a drive. 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: • Copy and paste 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 Imation. If you did not receive an email, check your spam or bulk mail folder.
4	Type a device password and confirm it, and then click **Continue**. Your password is case-sensitive and must comply with the password policy you set when you created the Enterprise Account.
5	If using an S250/D250, H300/H350, or S1000 device, 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 setting up a "secret question" and "answer". Your online account is required for accessing the Admin Console. S250/D250 devices also require the account for browsing the web using Secure Sessions and backing up Identity Manager. Once you set up your online account, click **OK** in the message prompt to proceed with the device activation.
6	The IronKey device 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.

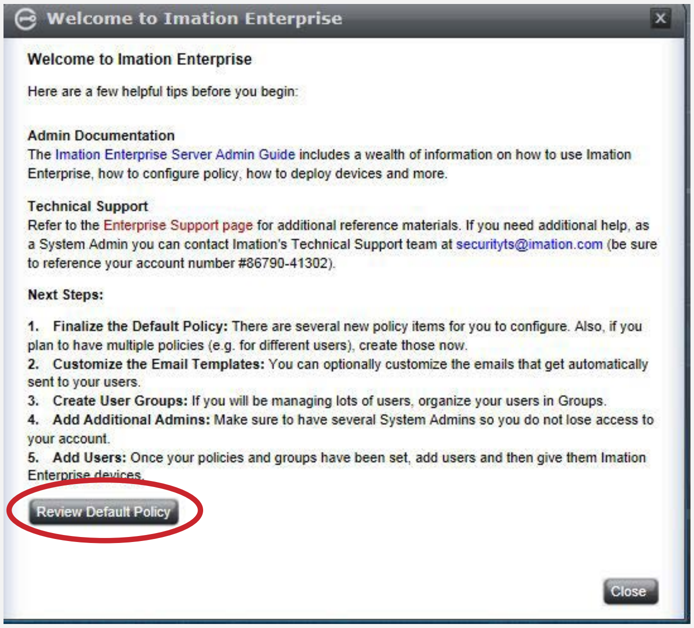
Steps

7 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 in IronKey Control Panel.



8 A "Welcome Screen" will appear to guide you through finalizing the default policy for your account and configuring some new some policy features that were *not* set during the Account Setup.



Welcome to Imation Enterprise

Welcome to Imation Enterprise

Here are a few helpful tips before you begin:

Admin Documentation
The Imation Enterprise Server Admin Guide includes a wealth of information on how to use Imation Enterprise, how to configure policy, how to deploy devices and more.

Technical Support
Refer to the Enterprise Support page for additional reference materials. If you need additional help, as a System Admin you can contact Imation's Technical Support team at securityts@imation.com (be sure to reference your account number #86790-41302).

Next Steps:

1. **Finalize the Default Policy:** There are several new policy items for you to configure. Also, if you plan to have multiple policies (e.g. for different users), create those now.
2. **Customize the Email Templates:** You can optionally customize the emails that get automatically sent to your users.
3. **Create User Groups:** If you will be managing lots of users, organize your users in Groups.
4. **Add Additional Admins:** Make sure to have several System Admins so you do not lose access to your account.
5. **Add Users:** Once your policies and groups have been set, add users and then give them Imation Enterprise devices.

Click the **Review Default Policy** button to modify the policy and enable Silver Bullet Remote Administrative Controls (to allow admins to remotely reset passwords, recover, or detonate devices) and Password Aging and Reuse settings.

Steps	
9	**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 device. Once activated, you can use the Admin Console to 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 the 2nd System Admin device

It is very important to set up a 2nd System Admin device; 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 Admin users automatically receive an email message containing device activation codes.

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

Steps	Description
1	Retrieve the Activation Email that was sent during the Account setup.
2	Complete steps 1 through 7 in the procedure, "Activating the 1st System Admin device" on page 39. You do not need to review and modify the Default Policy as this should have been completed by the 1st System Admin after the device was activated.

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 Enterprise Server Kit came with four devices for this purpose). If you lose these System Admin devices, you cannot manage any user 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.

MANAGE A MIXED DEVICE ENVIRONMENT

If you are an existing customer with active S200/D200 devices, Admins (System Admin or Admin) must use a 200 Series device to manage these devices. An S200/D200 device can be used to manage all device types but can only be managed by another 200 Series device. For more information, see about managing S200/D200 devices, see the "Managing Devices" chapter of the *IronKey Enterprise Server Admin Guide*.

BACKUP

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

To back up the config file, type the following at 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.

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 "Configuration and command reference" on page 52 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.
4. Shutdown Enterprise Server. To safely shut down the server enter this command:
   ```
   sysconf shutdown
   ```

USEFUL PSCP.EXE COMMANDS

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

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:\iksupport_<ES hostname>_<###>.tar.gz
```

Downloading All Files from the Download Folder

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

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

Upgrading IronKey Enterprise Server

Upgrading IronKey Enterprise Server from a previous version to version 6.0 involves uninstalling the existing server and deploying (ESXi environment) or installing (ACE environment) the new version. Once installed, you must re-configure the server settings.

IMPORTANT: Before you begin, 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. You must also unlock your new Setup Device using the same password as the one used to unlock your original Setup Device.

Steps		Description
1	Fill out the Installation worksheet on page 10.	Make sure you have a backup of the certificate files initially uploaded to the Server: `server.crt` and `issuer.crt`
2	Stop the application server.	Enter this CLI command: `service stop appserver`
3	Shut down the Enterprise Server VM.	Enter this CLI command `sysconf shutdown` **NOTE:** If using VMware ACE, this command shuts down the Server and exits the VMware ACE application. In an ESXi environment, this command shuts down the Server.
4	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.

Steps		Description
5	Upgrade the database. Use the SQL Server Management Studio to run the script named "db_upgrade_from_v52_to_v6.sql" (located in the \Utils folder). **NOTE:** If you are upgrading from an earlier version, you must upgrade the database in sequence. For example, to upgrade from version 2.0 to version 6.0, you must run the following scripts in order: 1. `db_upgrade_from_v2_to_v3.sql` 2. `db_upgrade_from_v3_to_v4.sql` 3. `db_upgrade_from_v4_to_v5.sql` 4. `db_upgrade_from_v5_to_v51.sql` 5. `db_upgrade_from_v51_to_v52.sql` 6. `db_upgrade_from_v52_to_v6.sql`	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_v52_to_v6.sql** file to the query window. 4. Click the **Execute** button next to the drop-down database selection list. The length of time this takes to complete varies with the size of the database. Any errors returned are displayed.
6	Uninstall Enterprise Server v5.2.	
7	Deploy or install the new Enterprise Server using the files on the Setup device that was provided with your Server Upgrade package.	**ESXi environment:** Insert and unlock the Enterprise Setup device. In vSphere Client, deploy the Enterprise Server OVA file, located on the Server Setup device in the IronKey_ES OVA folder, to the host. See also "Deploying Enterprise Server in an ESXi environment" on page 22. **VMware ACE environment:** Insert and unlock the Enterprise Setup device. Open the IronKey Control Panel and on the **Applications** page click **Install IronKey Enterprise Server with ACE Environment** to start installing the new version of Enterprise Server. See also, "Installing Enterprise Server with ACE environment" on page 26. **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.
8	Start the IronKey Enterprise Server VM.	**ESXi environment:** In vSphere Client, right-click the Server and click **Power** > **Power On**. **VMware ACE environment:** Double-click the **IronKey_ES VM** shortcut to start the VM. Create and confirm a new activation password for the VMware ACE Player that you will use each time you start the IronKey Enterprise Server VM.

Steps		Description
9	At the IronKey Enterprise Server CLI, log in using the CLI username and password provided in your Welcome Email. You will 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	

10	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) of the previous server.

11	Configure the server's 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`

12	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 (GMT) using the `sysconf` time command. Enterprise Server will show the correct time once you set the date or add the NTP server.
		Example:
		`sysconf time 14:11:00 31 August 2014`

Steps		Description

13	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)?`

14	Configure the database server.	`application database configure <DB server IP or hostname> <port ID> <database username> <password> mssql <database name>`
		Example:
		`application database configure 10.1.1.89 1433 db_usr mypasswd mssql es_master`

15	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 sitename from the previous server.
		Command Example:
		`application siteName set myhost.domain.com`

16	Securely copy the certificate files to the /upload directory on the VM.	Use a Secure Copy (SCP) utility (such as command-line-based PSCP or GUI-based WinSCP) to securely copy the files to /upload.
17	Install the certificates.	`application certificate install`
18	Enable HTTPS.	`application ssl enable`
19	Start the application server.	`service start appserver`
20	Update your license. **IMPORTANT:** You must add a new license to your server to be able to initialize new devices. See the *IronKey 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.
21	Reboot Enterprise Server.	`sysconf reboot`

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 v5.2, you will need to re-upload this file as it is removed when v5.2 was uninstalled during the server upgrade process. For more information, see "Uploading device software updates" on page 50.

Uploading device software updates

The software update process for devices 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. Once the update package has been uploaded to the Server, see the *IronKey Enterprise Admin Guide* for information on approving the update so that users can download and install it to their device.

Both the software update package and the database script are available on the *support site*. There are two files:

- **Update package file**—upload and install this file to 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_YYYYMMDD.tgz`
- Update script: `\\Device Updates\ikupdate_db_YYYYMMDD.sql`

Where "YYYYMMDD" represents the Year, Month, and Day of the release of the update package and script.

NOTE: When you upgrade Enterprise Server from v5.2 to v6, any software update package that was added to the server is removed when the v5.2 server is uninstalled. You must re-upload the software update package and install it to the new v6 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 file `ikupdate_db_YYYYMMDD.sql` (located on the *support site*) to the query window.
5. Click the Execute button next to the database selection list.
6. The length of time this takes to complete will vary with the size of the database. Any errors

returned are displayed.

TO UPLOAD AND INSTALL THE UPDATE PACKAGE

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

   ```
   service stop appserver
   ```

2. Upload the update package file `ikupdate_YYYYMMDD.tgz` (located on the *support site*) 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_YYYYMMDD.tgz>
   admin@x.x.x.x:/upload
   ```

   (for additional information about the PSCP utility commands, see "Useful PSCP.EXE Commands" on page 44).

   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` (the uploaded update package `ikupdate_YYYYMMDD.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_YYYYMMDD.tgz`

6. When you are prompted by the VM User Interface to restart the appserver, type the following command: `service start 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 Enterprise Server Admin Guide* for information about testing and updating device firmware/ software settings.)

Configuration and command 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 44.

Background

Some CLI commands require write access on the Virtual Machine that hosts Enterprise Server before you can run the commands. For example, `application certificate install` requires certificate files to be copied to Enterprise Server before it starts. Similarly, some CLI commands require data to be copied out of Enterprise Server after running them. For example, `supportInfo` creates a file with information required for a support ticket and places it in the /download directory.

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 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 HTTPS.

```
application ssl disable
```

Description:
Disable HTTPS.

```
application ssl show
```

Description:

Display HTTPS configuration.

```
application certificate
```

Description:

Get all certificate management commands.

```
application certificate install [force]
```

Description:

Before running the command, combine the key and certificate (PEM format) into a file called *server.crt*. Using an SCP utility, copy the file to the *upload* directory on the server: `/upload/server.crt`. Install the server certificate. **NOTE:** You should save a copy of your key and certificate file in a secure file location as a backup.

The `force` option bypasses certificate chain validation.

```
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 malwareScanner
```

Description:

Display and set the malware scanner *ini* URL and virus definition URL.

```
application malwareScanner show
```

Description:

Display the malware scanner *ini* URL and virus definition URL.

```
application malwareScanner set
```

Description:

Set the malware scanner *ini* URL and virus definition URL.

```
application malwareScanner set iniURL <value>
```

Description:

Set the malware scanner *ini* URL.

```
application malwareScanner set definitionURL <value>
```

Description:

Set the malware scanner virus definition URL.

Arguments:

`value`	URL for the malware scanner virus definition file.

```
application reset
```

Description:

Resets all configuration parameters. **NOTE:** You will have to go through the configuration settings again once you execute this command.

```
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. Use the site name that is printed on the certificate issued by your CA (for example, *ironkey.domain.com*).

```
application siteName show
```

Description:

Display the current site name.

```
application version
```

Description:

Get application version.

Logout Commands

```
exit
```

Description:

Log out of the current CLI session.

```
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 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 shutdown
```

Description:

Shuts down the server.

```
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, 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 boot
```

Description:

Show boot log.

```
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.