Ironkey EMS On-Prem Setup Guide

version 7.2

DataLocker Inc.

June, 2018

Contents

About This Guide

This guide is written for IT Administrators and describes how to install and set up an IronKey EMS On-Prem server. It also describes best practices for deploying and managing devices in your enterprise environment. This document also lists the commands available to customize and configure the server.

Related Documentation

The following documents are also available:

- *IronKey EMS On-Prem Quick Start Guide*
- *Ironkey EMS On-Prem Admin Guide*
- *DataLocker Device User Guides (H300/H350, Sentry EMS, Sentry ONE)*

About IronKey EMS On-Prem

Overview

IronKey EMS On-Prem is the world's most secure enterprise server solution for managing supported USB flash drives, hard drives, and portable workspaces. Installed and managed in your own data center, you can protect your organization's portable data and ensure that IronKey EMS security policies are enforced.

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 through a web-based administrative management console:

- 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 EMS On-Prem Admin Guide*, available in the Admin Console, or with your IronKey EMS On-Prem installation package.

System Requirements

IronKey EMS On-Prem uses virtual machine technology and can be installed in the following operating environments:

- Running in VMware® vSphere® ESXi Hypervisor (version 5.0 or higher) environment
- Running in VMware® Workstation 12 Player (or higher) environment

The following table outlines the minimum requirements needed to install and use IronKey EMS On-Prem.

Requirement	Description
Database	Microsoft SQL Server 2005, Microsoft SQL Server 2008, or Microsoft SQL Server 2012, Microsoft SQL Server 2016 (beta support),Microsoft SQL Server Express 2005, Microsoft SQL Server Express 2008, Microsoft SQL Server Express 2012, or Microsoft SQL Server Express 2016 **Note:** Only the default database instance is supported by this guide. SSL encrypted connections are not supported.
Host system requirements in ESXi environment	
vSphere ESXi version 5.0 or higher (the ESXi version must support the Guest OSCentOS v6.6 On-Prem is installed). See the VMware Compatibility Guide 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 EMS On-Prem. Information on installing ESXi is outside the - the OS on which IronKey EMS scope of this guide, see VMware productdocumentation.

Requirement	Description
Ethernet physical network adapter	1Gb or faster
Memory	4GB phyiscal RAM
Physical datastore space	70GB available space
Host system requirement in VMware Workstation Player environment	
VMware Workstation 12 player (Or higher)	Host machine must meet the minimum system requirements for this version in addition to minimum requirements provided by VMware. See VMware product documentation for more details: http://www.vmware.com **Note:** You must have VMware Workstation 12 Player already installed and set up on your host before you deploy IronKey EMS On-Prem. Information on installing VMware Workstation is outside the scope of this guide, see VMware product documentation.
Operating system	Windows Server 2008 or Windows Server 2012
Ethernet physical network adapter	1Gb or faster
Memory	4GB phyiscal RAM
Hard Disk	30GB free disk space required; 60GB recommended

Common Terminology

Item	Description
Server Admin	The administrator who manages the host machine and CLI for IronKey EMS On-Prem.
System Admin	The administrator who manages end-users and their devices once the server is set up and running.
Device	Generic term for all supported drives that can be managed by IronKey EMS On-Prem.
CLI	The Command Line Interface used to configure the system.

What's In The Box?

The IronKey EMS On-Prem Server Kit contains six IronKey S250/D250 devices:

- One Setup device (labeled "Carrier/Setup") that contains the necessary software for installing

IronKey EMS On-Prem

- Five devices (four labeled "Sys. Admin" and one labeled "User") are available for use by System Admins or general users. While System Admins are not required to have an activated device to manage your EMS Account, the device provides a secure second factor by which they can access the management console.

IronKey EMS On-Prem Support

DataLocker is committed to providing world-class support to its IronKey EMS On-Prem customers. Technical support solutions and resources are available through the DataLocker Support website, located at http://support.datalocker.com. For more information, see Contact Information.

Standard Users

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

System Administrators

Administrators can contact support by:

- Filing a support request at support.datalocker.com.
- Sending an email to support@datalocker.com

Important: Always reference your IronKey EMS 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 EMS Account number, video tutorials and product documentation, and contact information for DataLocker Technical Support.

Contact Information

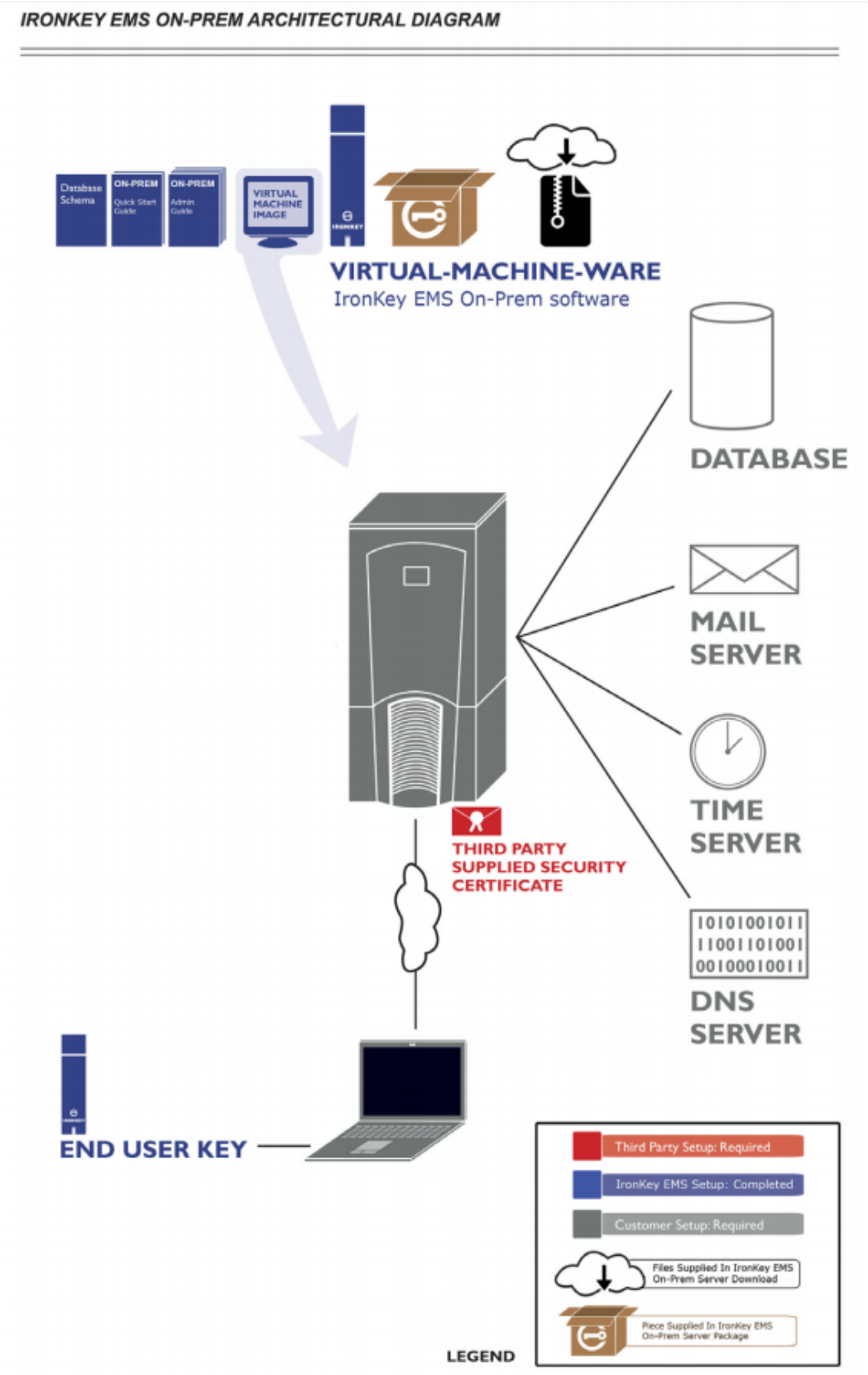
support.datalocker.com - Support information, knowledge base and video tutorials

support@datalocker.com - All licensing and account questions Product feedback and feature requests

datalocker.com - General information

Product Architecture

This architectural diagram shows a system-level map of IronKey EMS On-Prem.



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 the next page to help you collect and organize this information. The Setup Check List on the page following the Installation Worksheet 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).
- The Welcome Email you received from Customer Service at DataLocker.
- The Setup Device or download package that contains the IronKey EMS On-Prem software. 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 IronKey EMS On-Prem.

IronKey EMS Account Number (from Welcome Email)	
Download link to IronKey EMS On-Prem or password for the Setup Device if you received a Server Kit (from Welcome Email)	
CLI User Name (from Welcome Email)	
CLI Password (from Welcome Email)	
Host Name (to be assigned to IronKey EMS On-Prem)	
DNS server IP	
Static IP Address (assigned to IronKey EMS On-Prem)	
Subnet Mask (for IronKey EMS On-Prem)	
Default Gateway IP (for IronKey EMS On-Prem)	
NTP server IP or FQDN (optional)	
SMTP server IP or FQDN (check if your SMTP requires a password)	
Database server FQDN or IP	
Database Port	
Database User Name and Password (required: db_owner privileges)	
Database Name (example: `ent_server`)	
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 DataLocker.

( ) IronKey EMS On-Prem software downloaded or received in the Server Kit

( ) Installation Worksheet filled out

( ) External ports open (see IronKey EMS On-Prem Ports)

( ) Third-party SSL Certificate ready (see Certificate Acquisition And Renewal)

( ) SQL Server database configured (see Database Setup)

( ) IronKey EMS On-Prem VM installed

( ) IronKey EMS On-Prem configured with required information

( ) IronKey EMS Account successfully created

( ) EMS Account number entered from Welcome Email

( ) EMS License Request created and sent to DataLocker Customer Service

( ) License Key from DataLocker Customer Service entered in On-Prem

( ) Default User Policy created

( ) Contact information for two System Admins entered

( ) First System Admin's online account activated-can access Admin Console

( ) Second System Admin online account activated-can access Admin Console

( ) IronKey EMS On-Prem Admin Guide reviewed for deployment

IronKey EMS On-Prem Ports

The ports referred to in this section are those that are required to connect to IronKey EMS On-Prem. For full functionality of devices (for example, Silver Bullet Services 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 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 AntiMalware Updates for more information.

Application	DNS Name	Configuration	Ports
Admin Portal	<server>.<full domain name>	HTTPS	443/TCP
Services	<server>.<full domain name>	HTTPS and Client Authentication	2000/TCP*
Device Updates Phase 1	<server>.<full domain name>	HTTPS and Client Authentication	2001/TCP
Device Updates Phase 2	<server>.<full domain name>	HTTPS	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 with Cisco firewalls if phone traffic is on the IronKey EMS On-Prem network. To resolve the conflict, you can disable Cisco firewall port 2000/TCP packet inspection with 'no inspect skinny' or set IronKey EMS On-Prem Server to use port 9701/TCP. IMPORTANT: Do *not* change the default port after devices have been activated. Otherwise, activated devices that use a different port setting may be unable to connect. For information about switching the default port, see the *command summary for setting an alternate port* in the Commands Summary.

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 EMS On-Prem 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, Be-Trusted, Aba.com, AddTrust, Baltimore, DST, GTE, GlobalSign, Sonera, TC TrustCenter, DigiCert

Before purchasing a certificate please read the following knowledge base article to make sure your certificate is fully compatible with all of your devices.

datalocker.com/help/ems-certificates

Acquiring And Installing An SSL Certificate

1. Download the OpenSSL binary for Windows at the URL below and install OpenSSL at the default location on a computer running Microsoft Windows 7 64 bit, Server 2008, or Server 2012.

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

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

   Windows 7, Server 2008, 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:

   Windows 7, Server 2008, 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 sitename, as the SSL Certificate's Common Name. You should enter the Organization Name (your company name). Your Certificate Authority provider may 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 EMS On-Prem" on page 31 for more information about the following installation steps that complete your server configuration.

6. Use the following commands to upload the certs to the EMS server. For more information, see Useful CLI Commands.

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

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


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 IronKey EMS On-Prem 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 IronKey EMS On-Prem.

   ```
   sysconf reboot
   ```

8. Restart the application server.

   ```
   service start appserver
   ```

Database Setup

Before you install IronKey EMS On-Prem, 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. SSL encrypted connections are not supported.

If you are setting up the database on an existing named instance, see the Knowledge Base Article on the support site for more information.

Important: To ensure that the front-end code base of IronKey EMS On-Prem 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 < 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" Database Role:

```
use < 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

Note: You can also grant Server role privileges to the user. This step is optional. For example you can assign the *sysadmin* role so the user also has full rights to all other databases on the Server. See the step in the GUI procedure for assigning Server role.

5. Set the default database for the login (created in Step 1) to the IronKey EMS On-Prem database:

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

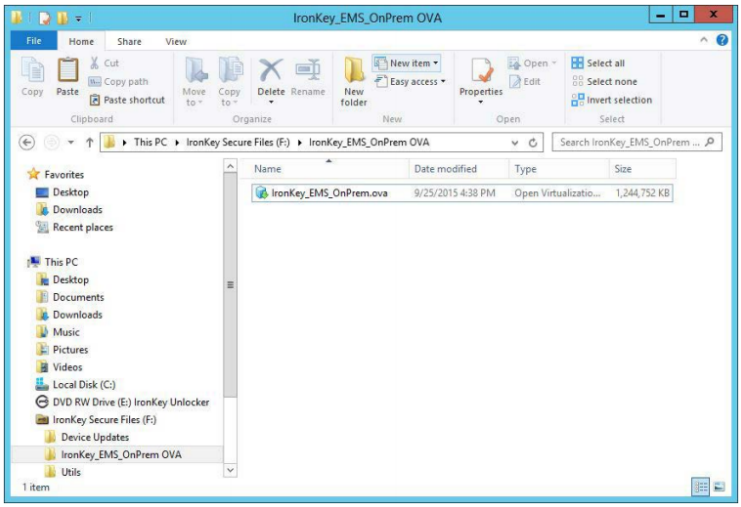
reference: http://msdn.microsoft.com/en-us/library/ms189828.aspx

Database Setup: GUI Steps

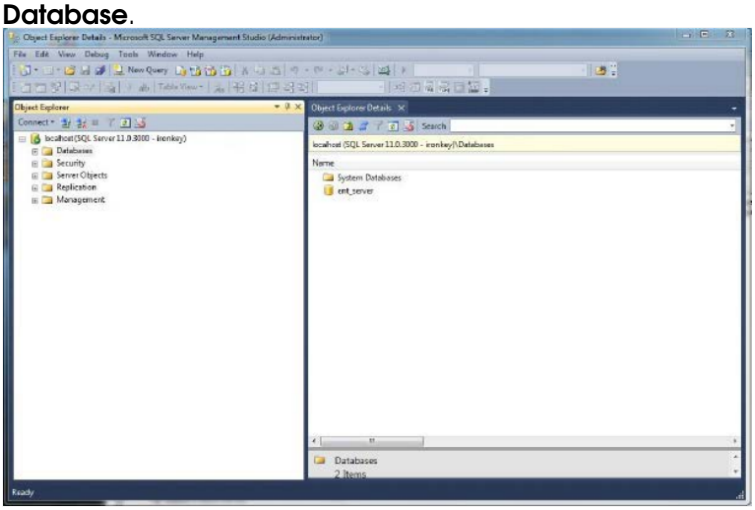
1. Restore the database backup on an existing SQL Server:

- **1.1:** In the **Utils** folder of the IronKey EMS On-Prem download file (or on the Setup device if you received the Server Kit), locate the IronKey EMS On-Prem schema, `IronKey_EMS_OnPrem_V72.bak` (a backup of a blank database).

Note: The device password to unlock the Setup device is provided in your Welcome email.

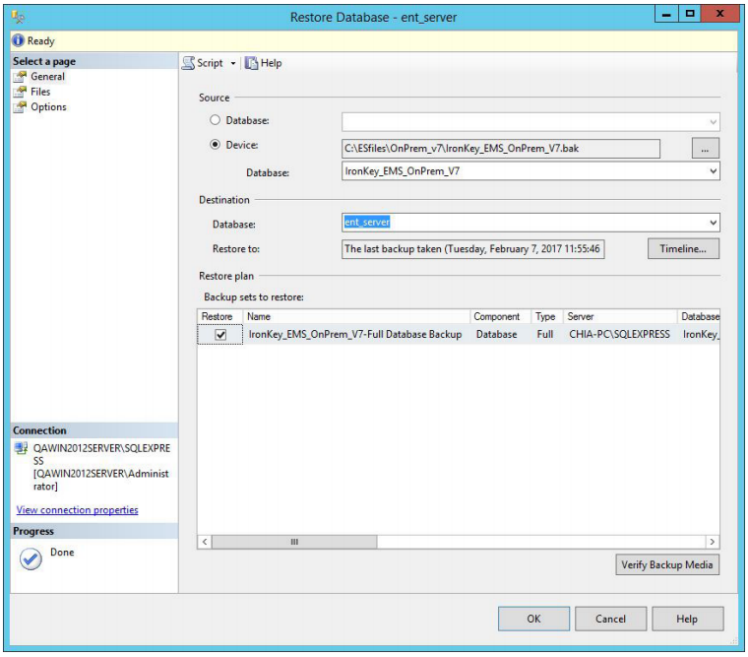


- **1.2:** In SQL Server Management Studio, right-click the **Databases** folder, and then click **Restore Database**.

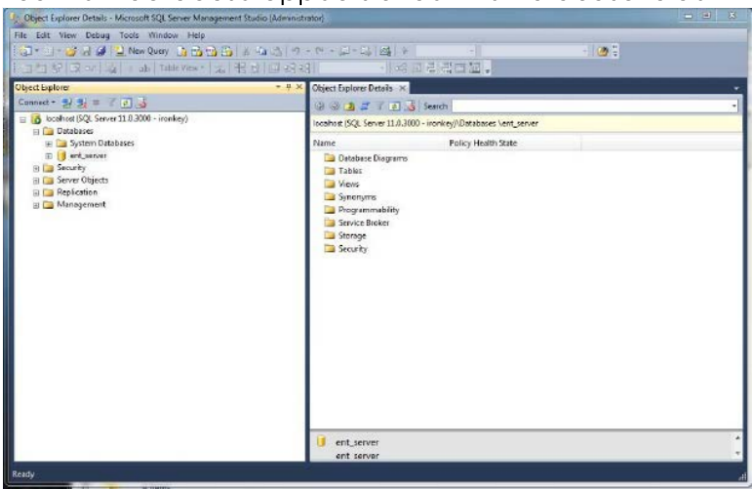


- **1.3:** In the **Restore Database** dialog box, do the following:
  - Click **Device** and browse to the `IronKey_EMS_OnPrem_V72.bak` file.
    (In the **Select Backup devices** dialog box, click the **Add** button, browse to the database backup file, and then click **OK**.)
  - Enter the name for 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.

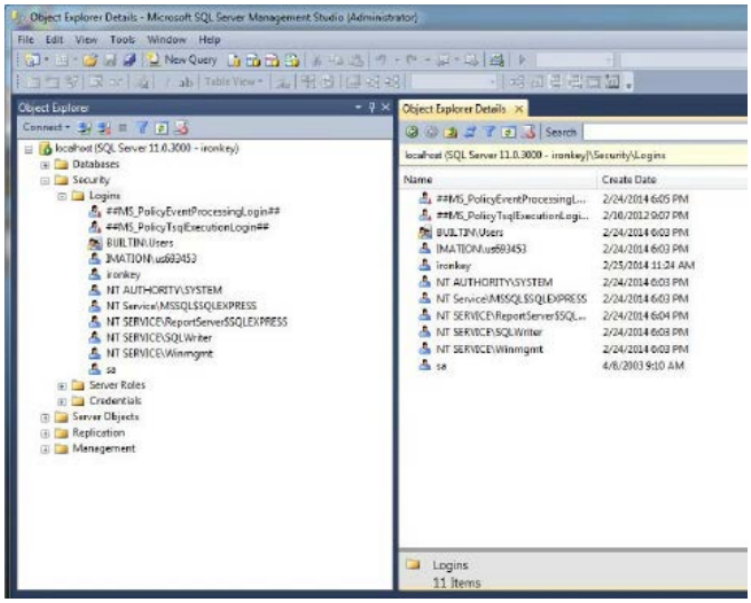


- **1.4:** Click **OK** to return to the main window.
  Your new database appears under the **Database** folder.

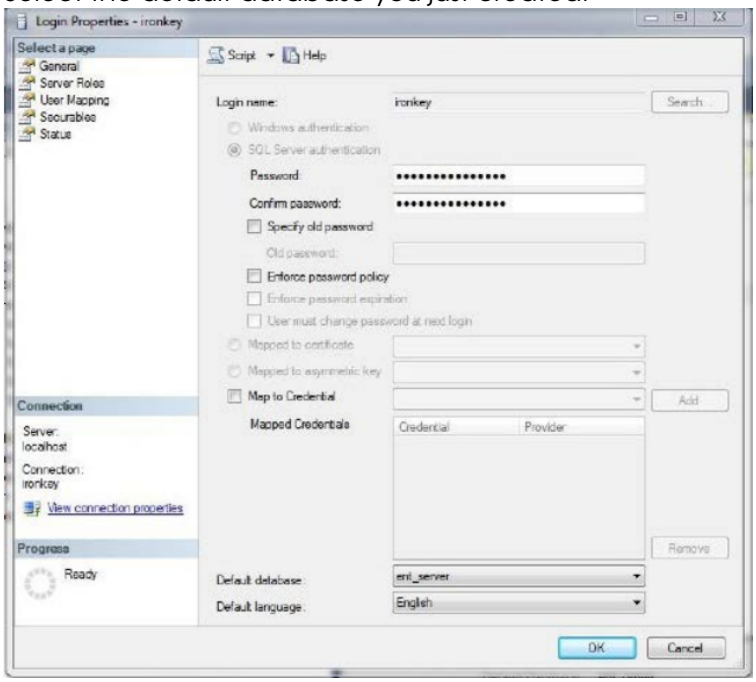


2. Create a SQL Server login and grant the Database User the “db_owner” Database Role

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

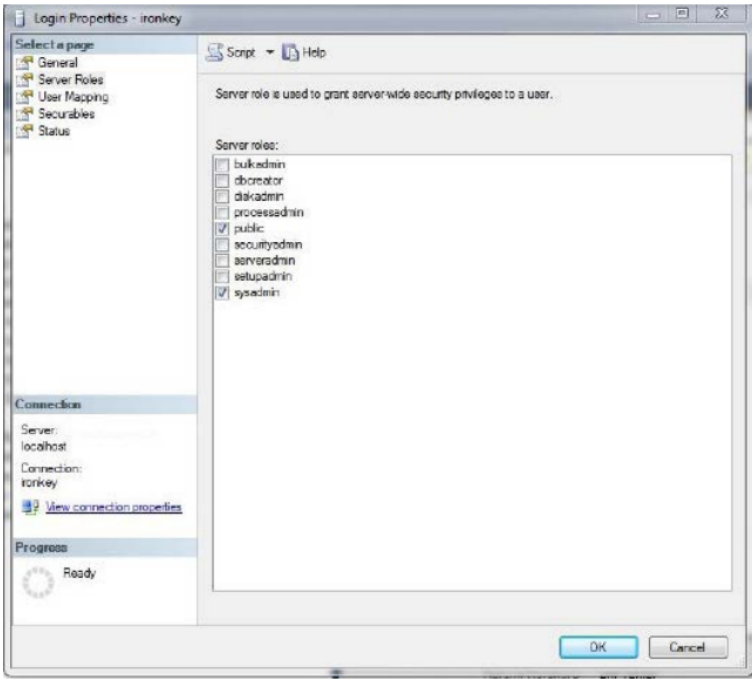


- **2.2:** On the **General** page, do the following:
  - Enter a login name for the user.
  - Select **SQL Server authentication** and enter a password.
  - Select the default database you just created.



- **2.3:** On the **Server Roles** page, make sure that public is selected. If you want the user to also manage other databases on the server, select **sysadmin**.

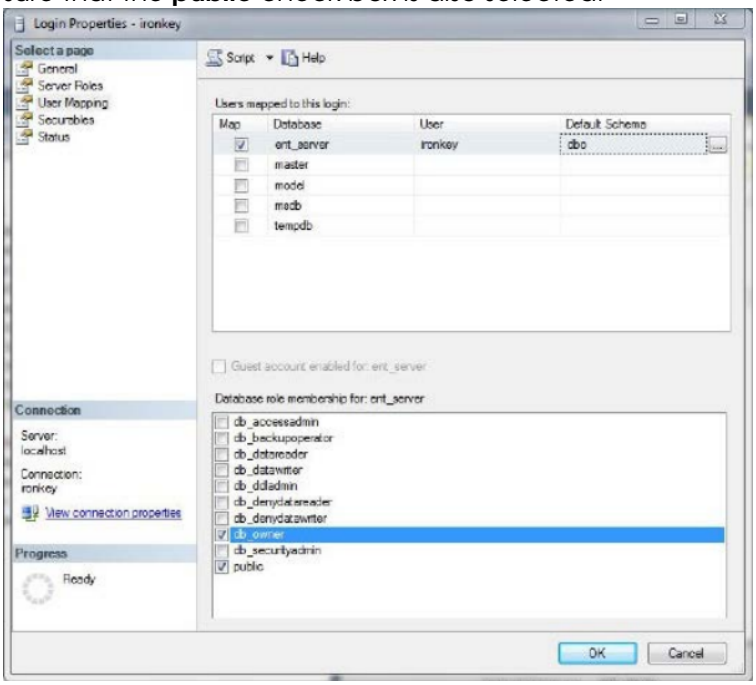
  Note: If you are using another management console, the available options might vary.



- **2.4:** To map the user to the database owner role, select **User Mapping** in the left panel, and then select the newly created user in the right panel.

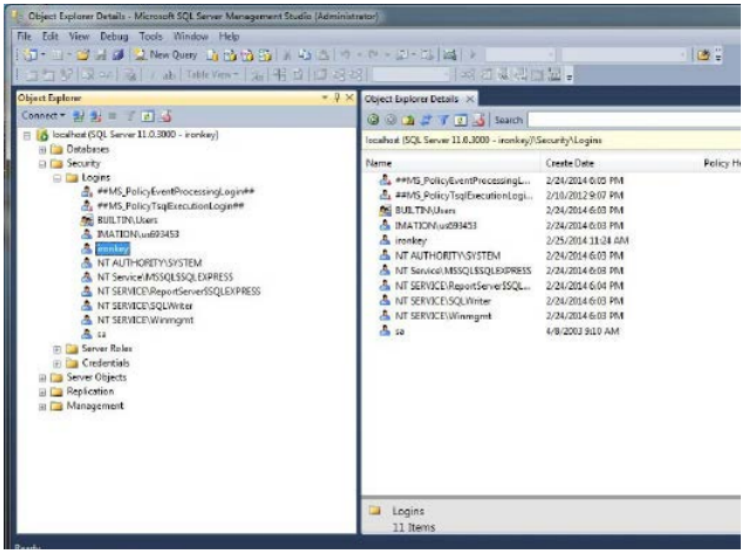
  Make sure **dbo** is entered for the **Default Schema**.

  In the **Database role membership for** section, click the check box for **db_ owner** and make sure that the **public** check box is also selected.



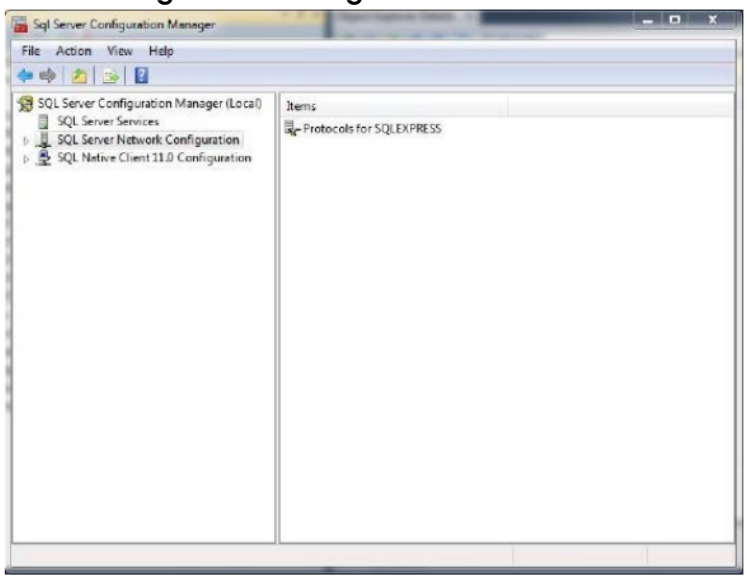
- **2.5:** Click **OK** to return to the main window.

  Your new user appears under the **Logins** folder and is also mapped to the the database.

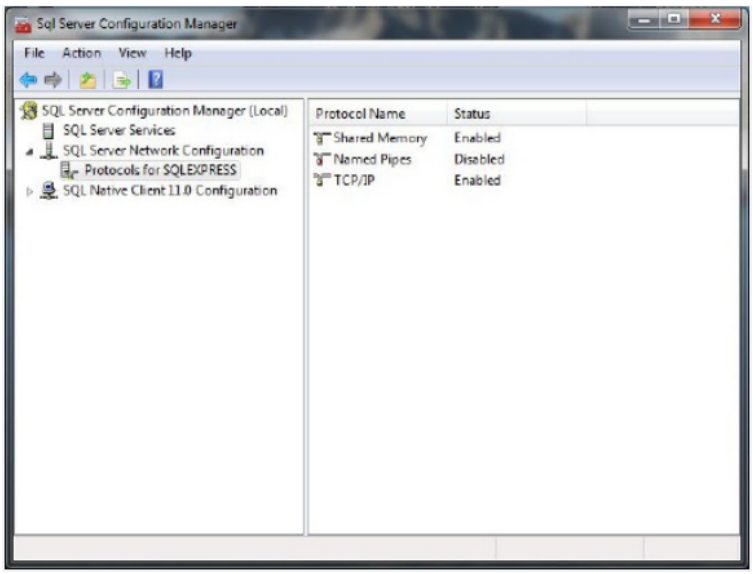


3. Set the default database for the login (created in Step 2) to the IronKey EMS On-Prem database.

- **3.1:** Open SQL Server Configuration Manager. (Location: Go to **Start** screen > **Apps** > **SQL Server Configuration Manager**



- **3.2:** Expand **SQL Server Network Configuration**, and then click Protocols for SQLEXPRESS. If you are not using SQLEXPRESS, select **Protocols for MSSQLSERVER**.

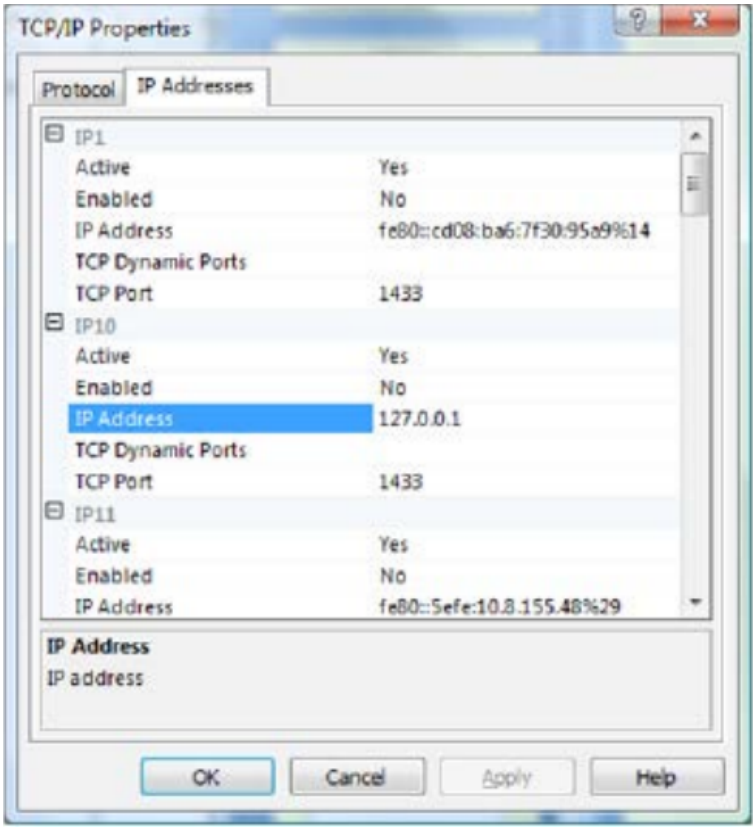


- **3.3:** In the right pane, right-click the **TCP/IP Protocol Name** and choose **Enable**.
- **3.4:** Double-click **TCP/IP** in the right pane and in the TCP/IP Properties dialog box, click the **IP Addresses** tab.

  Configure the following fields for each for of the IP numbers that apply:

  - **IP localhost (IP10 in this example):**
    - **IP address:** 127.0.0.1
    - **TCP Dynamic Ports:** blank (should not be zero)
    - **TCP Port:** number of the port.
  - **IP2 (This number may be different depending on your configuration)**
    - **IP address:** IP of the system where SQL server is installed
    - **TCP Dynamic Ports:** blank (should not be zero)
    - **TCP Port:** number of the port
  - ***IPAll***
    - **TCP Dynamic Ports:** blank (should not be zero)
    - **TCP Port:** number of the port.

  Note: You will need the port number to configure the database connection in IronKey EMS On-Prem. The default port is 1433.



- **3.5:** Open SQL Server Management Studio and do the following:
  - Make sure **Server type** is set to **Database Engine** and **Server name** is set to **the server instance name**.
  - Select **SQL Server Authentication** in the **Authentication** list.
  - To verify that the user was created correctly, enter the username and password you created earlier.
  - Select **Remember password**.
  - Click **Connect**.

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. Verify the following, and try to connect again:
  - A user account other than the system administrator account is being used.
  - The user account has the database owner (dbo) role and public privileges on the database server. The user may optionally have system administrator privileges on the database server.
  - 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: 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 EMS On-Prem

Before installing IronKey EMS On-Prem, 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_EMS_OnPrem_V72.bak* file, located in the *Utils* folder of the server download (or on the secure volume of the Setup device if you received the IronKey EMS On-Prem Server Kit), 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 EMS On-Prem after installation. See Database Setup for information about setting up the database.

IronKey EMS On-Prem software leverages virtual server technology. IronKey EMS On-Prem is a virtual server that runs on CentOS 6.6 operating system. There are two methods to deploy or install the server. Choose the method that meets your operating environment.

- To deploy the Server in a VMware vSphere ESXi environment, see Deploying IronKey EMS On-Prem In An ESXi Environment.
- To deploy the Server in a VMware Workstation Player environment, see Deploying IronKey EMS On-Prem In VMware Workstation Player Environment.

Installation files for these environments are available as a download (or on the Setup device in the Server Kit). Once installed, you must do the following:

- Configure IronKey EMS On-Prem
- request a license and set up the IronKey EMS Account
- Activate the first and second System Admin online account

Important: If you plan on deploying High Availability (HA) with your server, you must install and configure a second IronKey EMS On-Prem server after you finish the first installation. You must also update the license of the second server. Both servers will point to the same database. For more information, see Deploying A High Availability Solution.

Deploying IronKey EMS On-Prem In An ESXi Environment

The IronKey EMS On-Prem download (or Setup device if you received a Server Kit) includes an Open Virtualization Appliance (OVA) file, `IronKey_EMS_OnPrem.ova`, to deploy IronKey EMS On-Prem on the VMware ESXi host. OVA is an archive file that contains the Open Virtualization File (OVF) and supporting files required to deploy IronKey EMS On-Prem. 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 EMS On-Prem.

Note: IronKey EMS On-Prem is supported only on vSphere ESXi version 5.0 or higher.

1. If you received IronKey EMS On-Prem as a download, go to step 3.

   If you received the IronKey EMS On-Prem Server Kit, insert the Setup device into the USB port of the host computer.

   If you do not see a prompt to unlock the device, in a file manager, go to **My Computer** and double-click the **IronKey** icon, then double click **IronKey.exe**.

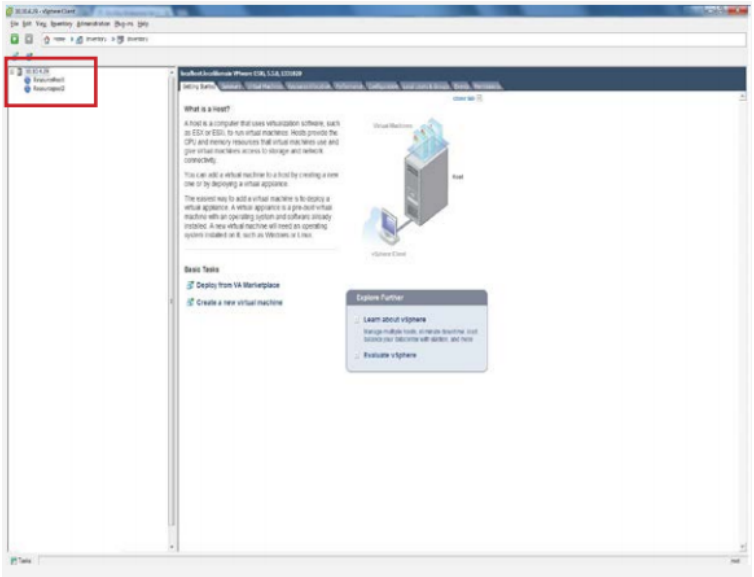
2. Enter the Setup device password, and then click the Unlock button. The Control Panel opens.

   The password is the same as your account number, which you received in the Server Kit and in the Welcome Email.

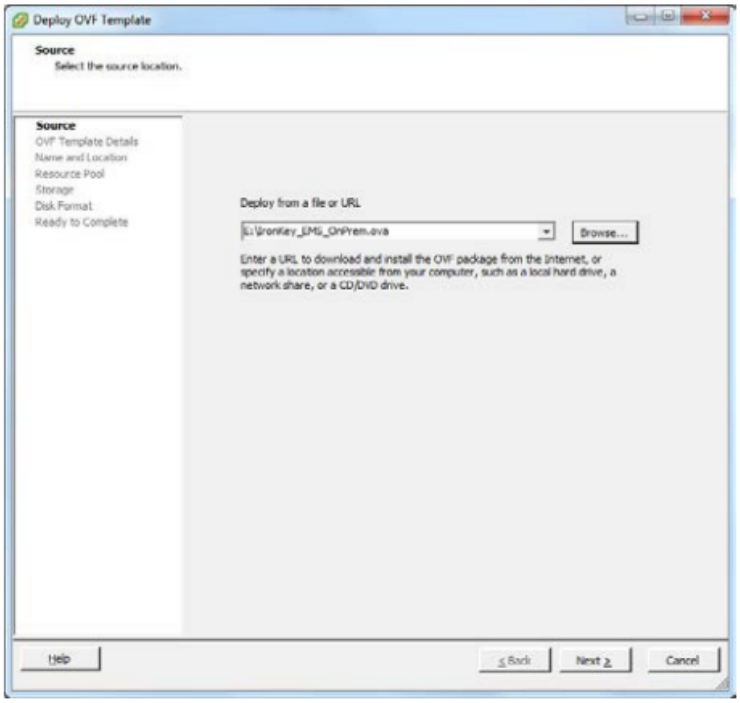
3. Login to the VMware vSphere ESXi server using VMware vSphere Client. You will be asked for the IP address/name of the host as well as the User name and Password.

4. In vSphere Client, click **File, Deploy OVF Template**.

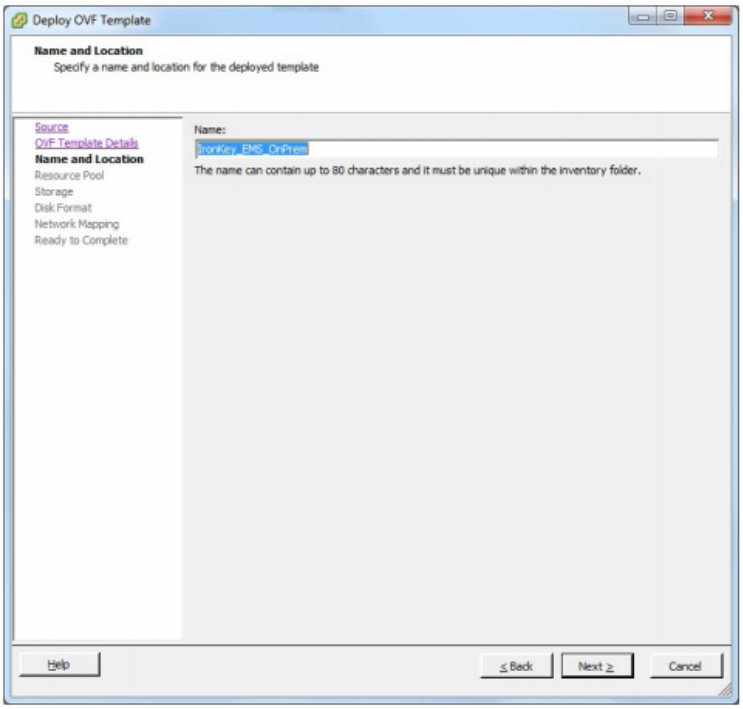
   Note: If you have multiple Resource Pools in your ESXi environment, choose the Resource Pool to which you want to deploy the Server, and then click **File, Deploy OVF Template**. If you do not select a Resource Pool, you will be prompted to do so later in the setup.



5. On the Deploy OVF Template screen, click **Browse**. Navigate to the **IronKey_EMS_OnPrem OVA** folder of the server download file (or on the Setup device if you received the Server Kit) and select the **IronKey_EMS_OnPrem.ova** file, then click **Next**.

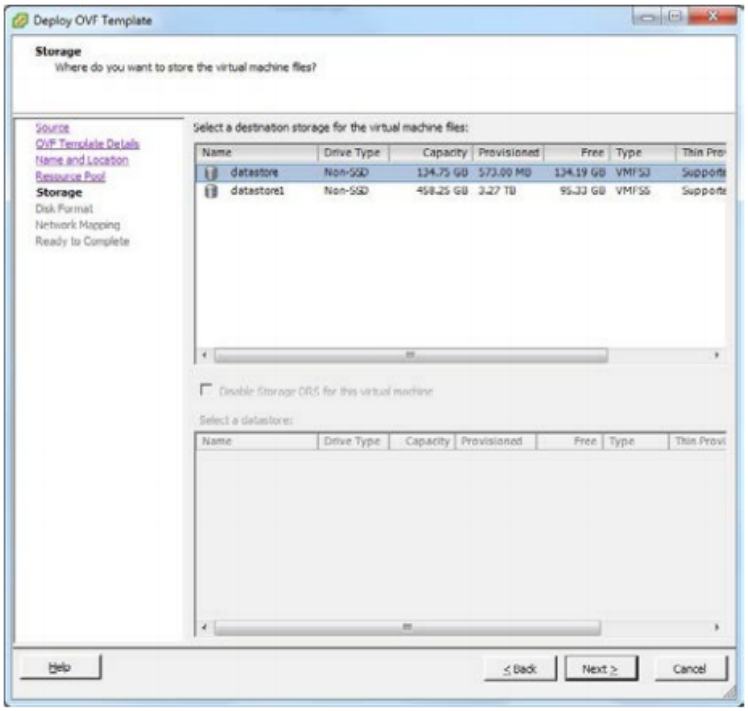


6. Click **Next** after verifying the details of the IronKey EMS On-Prem virtual machine template.
7. On the **Name and Location** screen, enter a virtual machine name that is unique to your ESXi inventory and click **Next**.



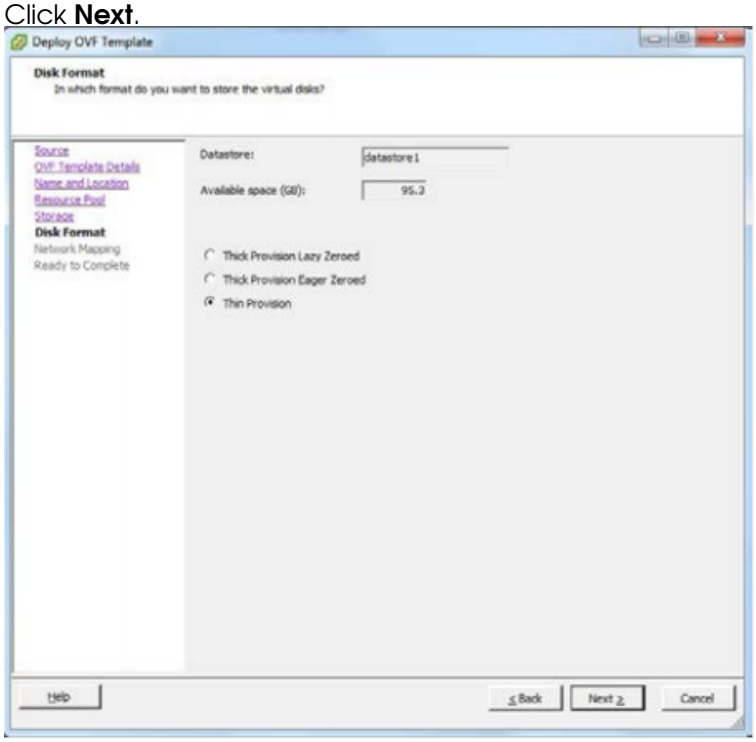
8. If prompted to select a Resource Pool, select it and click **Next**.
9. Select the destination storage for the virtual machine files. This screen will not display on ESXi servers with a single datastore.

Click **Next**.



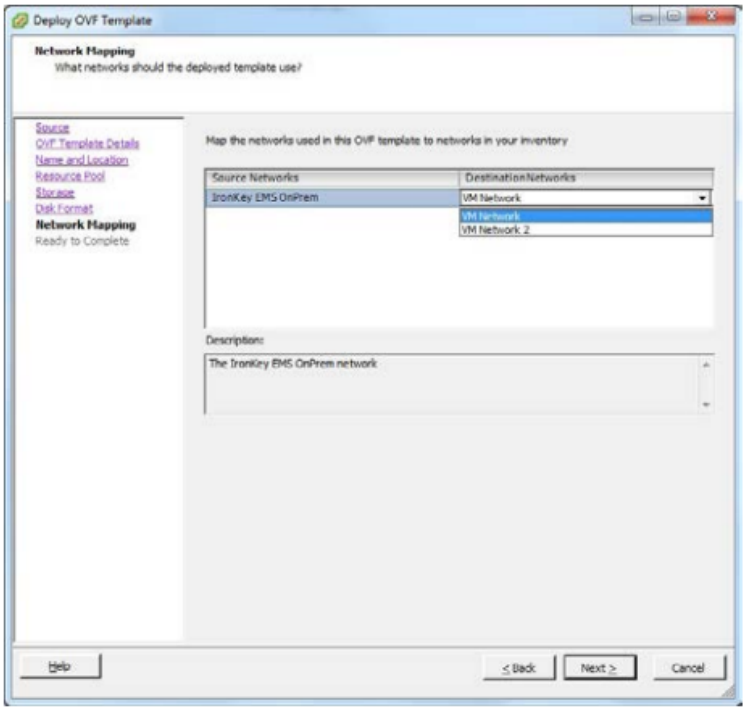
10. On the **Disk Format** screen, it is recommended that you choose the **Thin Provision** option to reduce the install time and to minimize disk space usage.

    Click **Next**.



11. On the **Network Mapping** screen, select the network that you want IronKey EMS On-Prem to use from the **Destination Networks** list box. This screen will not display on ESXi servers with only one VM network.

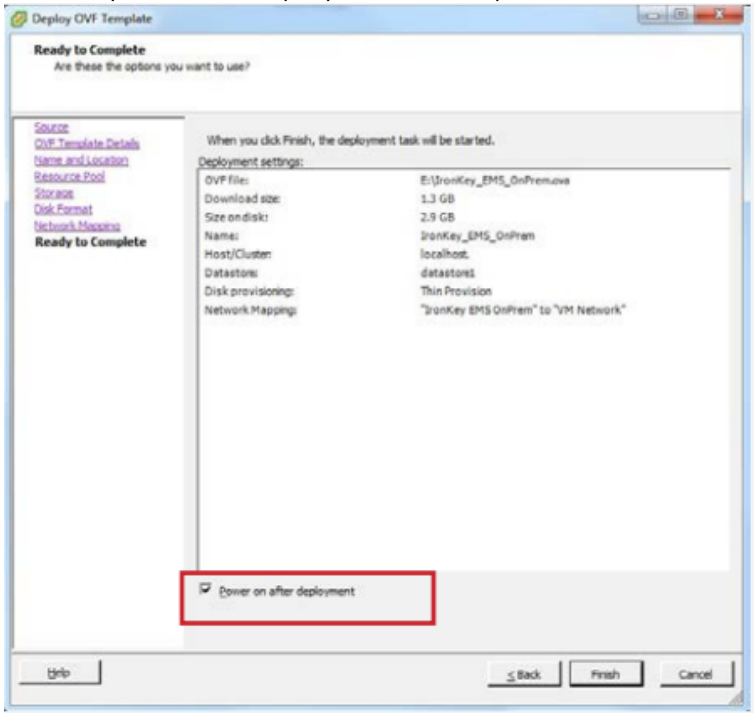
Click **Next**.



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.



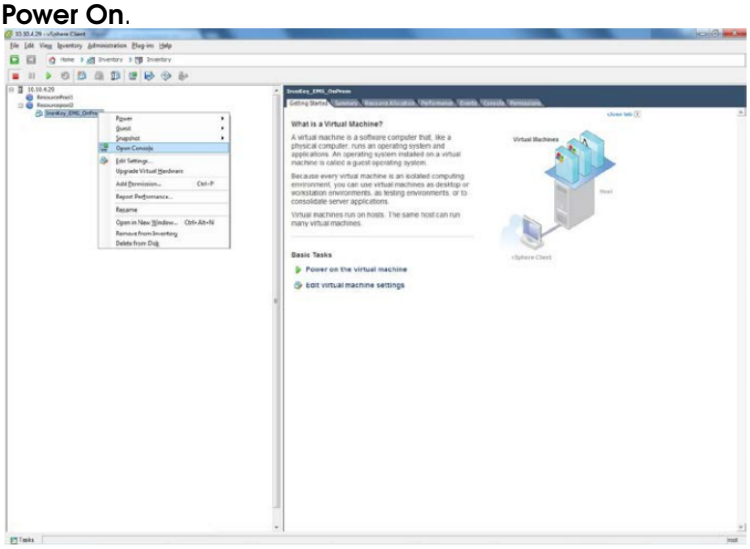
13. An installation status dialog box will display to indicate how much time is left in the install process. Total time will vary depending on the ESXi CPU and the server disk throughput.

14. When the **Deployment Completed Successfully** dialog box displays, click **Close**.

Logging In The First Time

1. In vSphere Client, right-click IronKey EMS On-Prem VM and click **Open Console**.

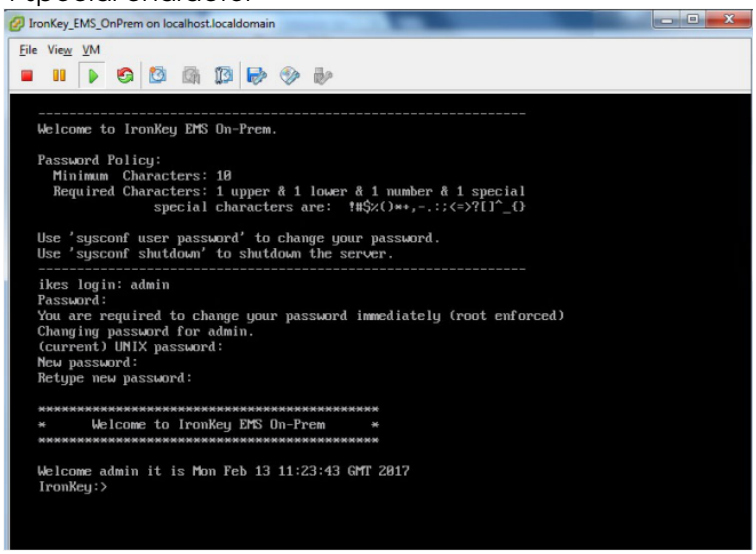
   Note: If IronKey EMS On-Prem is not already turned on, right-click the VM and click **Power, Power On**.



2. When the IronKey EMS Command Line Interface (CLI) appears for IronKey EMS On-Prem, 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



Deploying IronKey EMS On-Prem In VMware Workstation Player Environment

The IronKey EMS On-Prem download (or the Setup device if you received an IronKey EMS On-Prem Server Kit) includes an Open Virtualization Appliance (OVA) file, `IronKey_EMS_OnPrem.ova`, to deploy IronKey EMS On-Prem on VMware Workstation 12 Player. OVA is an archive file that contains the Open Virtualization File (OVF) and supporting files required to deploy IronKey EMS On-Prem. This section assumes that VMware Workstation 12 Player is already installed and running on the host system.

Note: IronKey EMS On-Prem is supported only on VMware Workstation 12 Player (or higher).

1. If you received IronKey EMS On-Prem Server as a download, go to step 3.

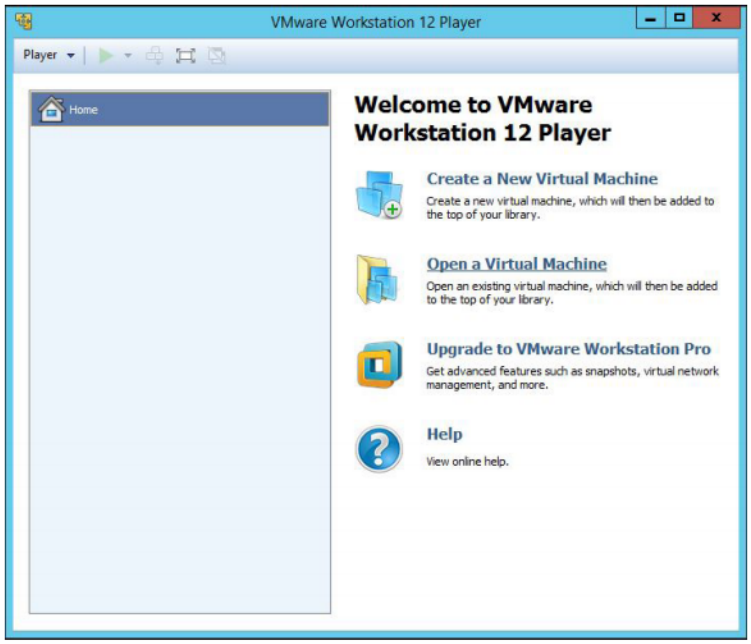
   If you received the IronKey EMS On-Prem Server Kit, insert the Setup device into the USB port of the host computer.

   If you do not see a prompt to unlock the device, in a file manager, go to **My Computer** and double-click the **IronKey** icon, then doubleclick **IronKey.exe**.

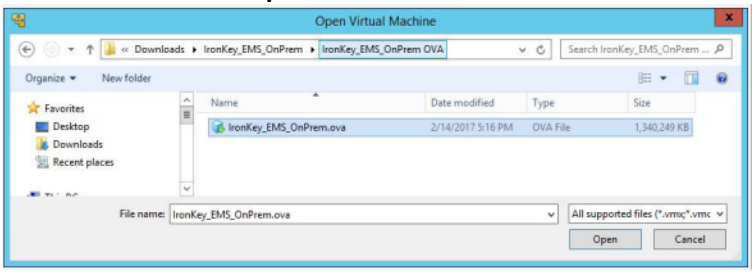
2. Enter the Setup device password, and then click the **Unlock** button. The Control Panel opens.

   The password is the same as your account number, which you received in the Server Kit and in the Welcome Email.

3. Start VMware Workstation Player. On the Welcome screen, select **Open a Virtual Machine**.

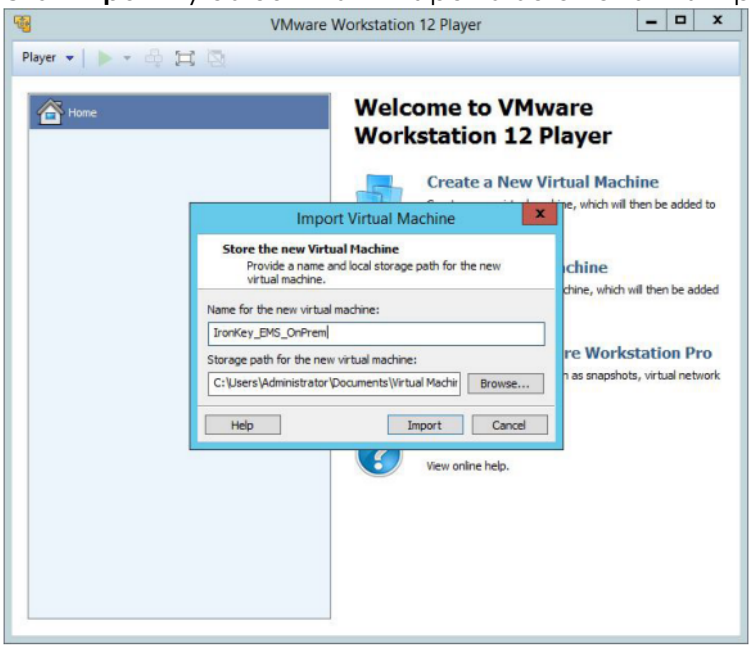


4. Navigate to the **IronKey_EMS_OnPrem OVA** folder of the IronKey EMS On-Prem download file (or on the Setup device if you received the Server Kit), select the **IronKey_EMS_OnPrem.ova** file, and then click **Open**.



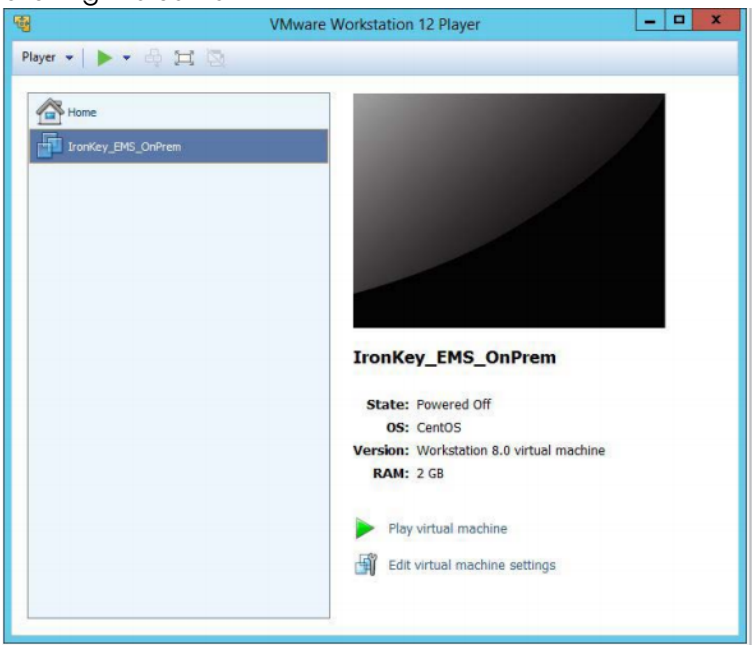
5. On the **Import Virtual Machine** screen, do the following:
   - Type a name for the IronKey EMS On-Prem virtual machine, for example "IronKey_ EMS".
   - Provide a path to the location where the VM will be stored or click **Browse** to navigate to the storage location.

   Click **Import**. By default the VM is powered off after it's imported.



6. To start the IronKey EMS On-Prem VM, select it from the list and click **Play virtual machine**.

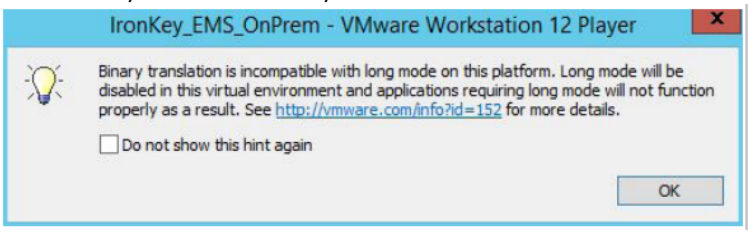
   Hint: You can start the Server by right-clicking the Server and choosing **Power On** or double-clicking the Server.



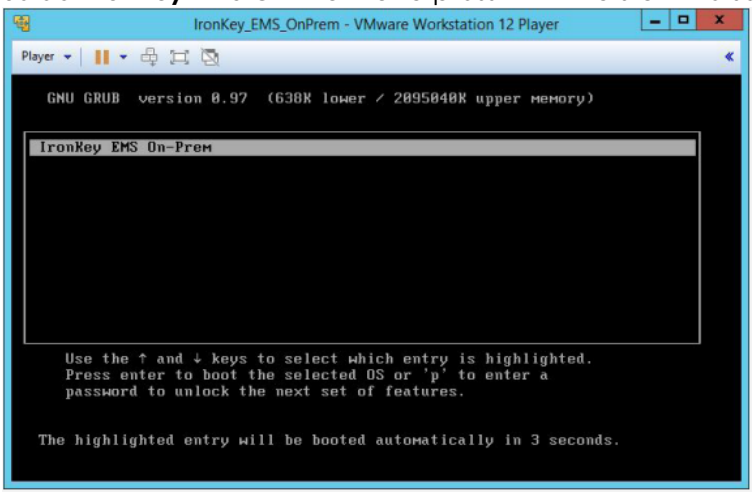
   Note: You may see a warning about binary translation incompatibility if the "Virtualization Technology" setting is disabled in the BIOS of the host system. This is because IronKey EMS On-Prem uses a 32-bit operating system and this feature is not supported with a 32-bit OS. To

avoid seeing the warning when you start the Server, do one of the following:

- Click the **Do not show this hint again** check box if you do not require the Virtualization Technology setting to be enabled in the BIOS. Then click **OK**.
- Enable the Virtualization Technology setting in the BIOS. The warning will not display the next time you start IronKey EMS On-Prem.



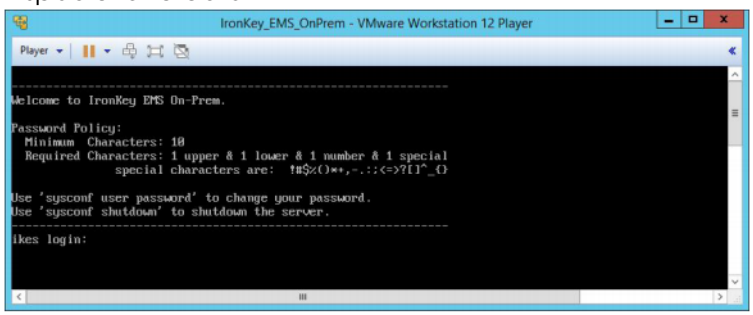
7. Select **IronKey EMS On-Prem** and press **ENTER** to start the server.



8. At the IronKey EMS Command Line Interface (CLI) for IronKey EMS On-Prem, 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



Configuring IronKey EMS On-Prem

Once you have successfully deployed or installed IronKey EMS On-Prem, 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 Configuration And Command Reference.

Once you log into the CLI, enter the commands to configure IronKey EMS On-Prem. 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 , represent arguments to be replaced with your own data.

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

If you are deploying a high availability solution, you will need to install and configure a second server. It is recommended that you follow the steps as outlined in the Deploying A High Availability Solution section.

1. Log in to IronKey EMS On-Prem using the command line interface (CLI).

2. Set the host name.

   ```
   network hostname <VM hostname>
   ```

   Example:

   ```
   network hostname ikes1.domain.com
   ```

   Critical: When using this command, make sure you enter a Fully Qualified Domain Name (FQDN), not just the hostname of the IronKey EMS On-Prem.

   FQDN Example: (correct)

   ```
   network hostname ikes1.domain.com
   ```

   Hostname only Example (incorrect):

   ```
   network hostname ikes1
   ```

3. Configure a static IP address

   ```
   network interface static <static IP> <IP mask> <Gateway>
   ```

   This is the IP address that the siteName will point to in the DNS server.

   Example:

   ```
   network interface static 192.168.200.101 255.255.255.0 192.168.200.1
   ```

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. IronKey EMS On-Prem 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:port>`

   Example:
   `sysconf smtp set server01.corp.ironkey.com:465`

   `Does the relayhost <your_SMTP_server> require authentication (y/n)?`

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 IronKey EMS On-Prem to use that port.

   This manual uses `ent_server` as the example `<database name>`, check with your DB admin to verify the database name.

   Example:
   `application database configure 10.1.1.89 1433 db_usr mypasswd mssql ent_server`

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 site name must match the Common Name in the SSL Certificate.

   Note: Your certificate must have a valid public domain. To use the Silver Bullet Services, you must be able to expose the server on the Internet and allow firewall routing for that URL.

   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`

Example:

```
pscp.exe -scp server.crt admin@192.168.200.101:/upload

pscp.exe -scp issuer.crt admin@192.168.200.101:/upload
```

See Certificate Acquisition And Renewal and Useful PSCP.EXE Commands for more information.

10. Install the certificates.

    ```
    application certificate install
    ```

11. Enable HTTPS.

    ```
    application ssl enable
    ```

12. Start IronKey EMS On-Prem.

    ```
    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 command as needed for your configuration:

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 EMS On-Prem

Whether IronKey EMS On-Prem is installed in an ESXi or VMware Workstation Player, 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 VMware Workstation Player, closing the application is not a recommended method of shutting down the Server.

Setting Up Your IronKey EMS Account

After you have configured IronKey EMS On-Prem, you must set up your IronKey EMS Account. You must have the required license and security information from DataLocker Customer Service to set

up and activate your IronKey EMS 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 user policy and create the first two System Admin accounts. The user policy controls the password requirements and access restrictions that will be applied to the online account requirements for Administrators.

If you are installing a second server to deploy a high-availability solution, you do not need to set up a second IronKey EMS Account. Both servers will use the same database. However, you must update the license on the second server. For more information, see Deploying A High Availability Solution.

Note: After you receive the Welcome Email containing your server account number, you are ready to start the IronKey EMS Account setup. During the setup, you will send a license request to DataLocker. In return, DataLocker Customer Service will send a License Response email that contains your server license. Once you receive the email, you can complete your account setup.

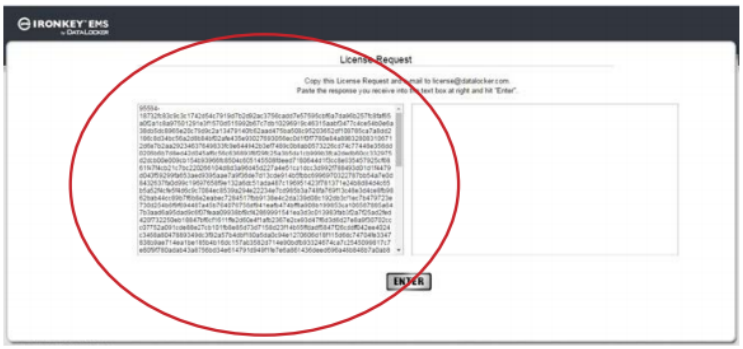
1. Go to **https: //< applicationsiteName >/enterprisesetup** (where **<application siteName>** is the value you entered in step 8 of the Configuring IronKey EMS On-Prem procedure).

   From the Welcome email, copy the 10-digit account number (in the format XXXXX-XXXXX) and paste it into the **IronKey EMS Account Number** box.

   Click **Enter**.

2. On the License Request page, copy the string from the text box on the left and email it to license@datalocker.com

3. Check your inbox for a message from DataLocker. This may take 24-48 hours to complete.

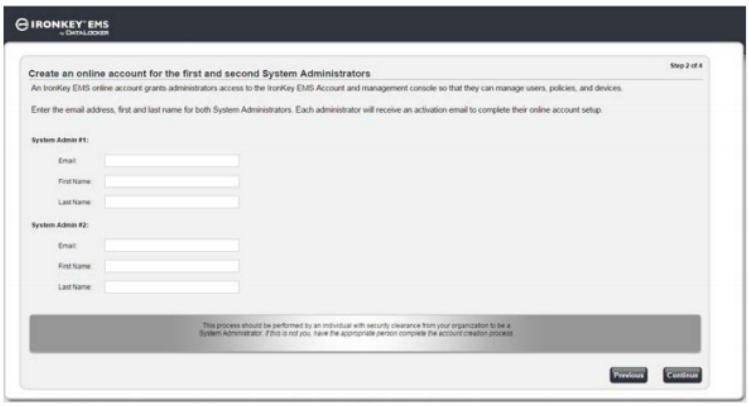
   You need the license key contained in this email to complete the installation.

4. On the **License Request** page, copy the license key that you received from DataLocker and paste it into the text box on the right.

   Click **Enter**.

5. Read the license agreement, and then select the check box to confirm that you are authorized to set up your organization's IronKey EMS account.

   Click **Continue**.



6. On the **Create an online account for the first and second System Administrators** page, enter an email address and the First and Last name of the first and second System Administrator.

   Click **Continue**.

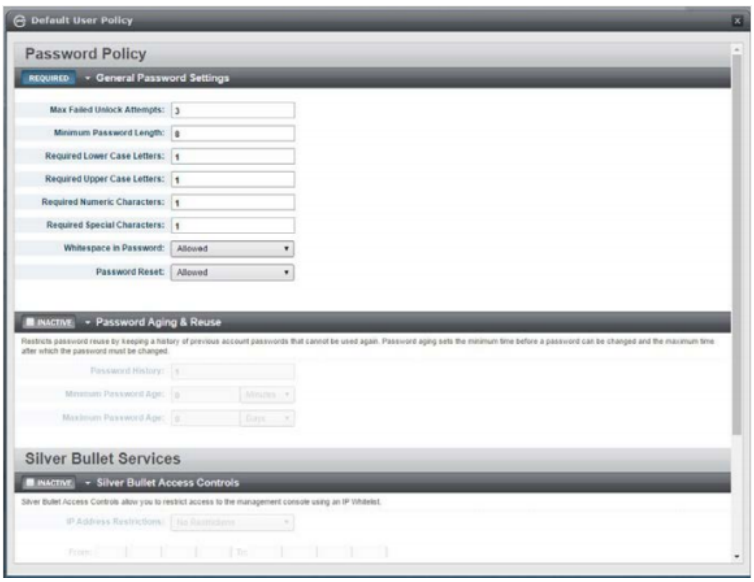
7. On the **Create the Default User Policy** page, click **Create Policy** to open the policy setup.

   Note: The Default User Policy will be applied to the 1st and 2nd System Admin when they activate their online account.

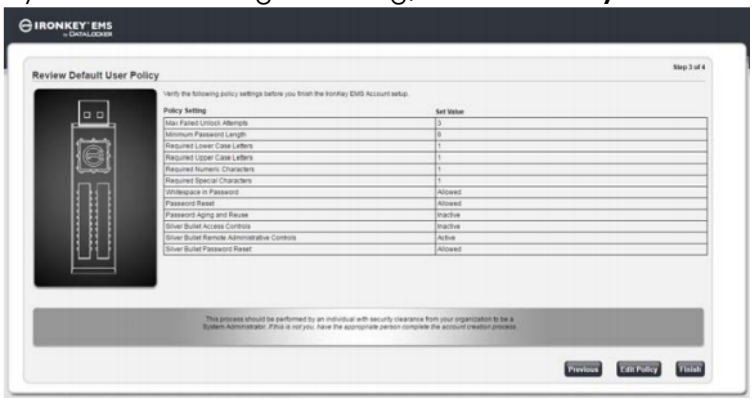
8. On the **Default User Policy** page, scroll through and review each section. Configure the settings that you want to be included in the Default User Policy for your EMS Account.

   Each policy section displays the system default settings.

   When you finish setting all user policy options, scroll to the end of the Default User Policy and click **OK** to continue with the EMS Account Setup.



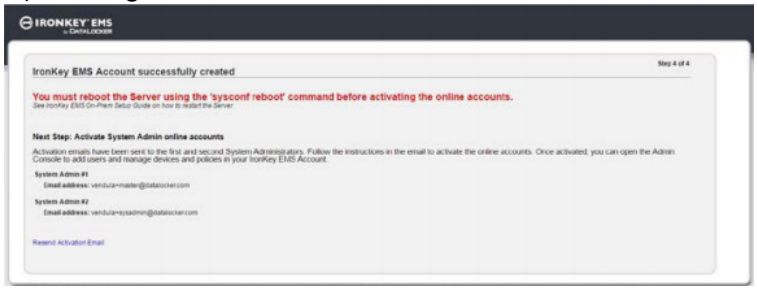
9. On the **Review Default User Policy** page, verify the policy settings and do one of the following.
   - If you are satisfied with the policy selections, click **Finish** to complete the EMS Account Setup.
   - If you need to change a setting, click **Edit Policy**.



10. A confirmation message will indicate that your EMS Account has been successfully created.

    Each System Admin will receive an email message with instructions on how to activate their online account.

    Note: It is recommended that you keep this confirmation page open until the System Admin users have received the activation email. If they do not receive it, you can resend the email by clicking **Resend Activation Email**.



11. Reboot IronKey EMS On-Prem.

Enter this CLI command:

```
sysconf reboot
```

Important: If you do not reboot the Server before users activate devices, the activation process will fail. Be sure to perform this step before activating any devices.

Activating The 1st And 2nd System Admin Online Account

After you set up the EMS Account, the first and second System Admin users will receive an email with instructions about how to activate their online account. The online account allows administrators to log in to the management console to manage the IronKey EMS account, policies, users, and devices.

Activating an account involves creating login credentials for the management console. Make sure that these users have received the activation email message before continuing. The email address for the first and second System Admin users was added during the EMS Account Setup.

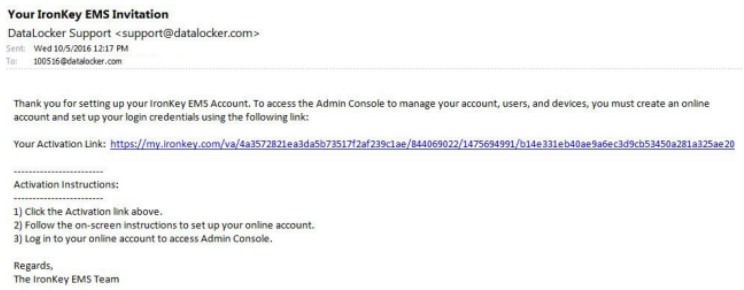
Activating An Online Account

To be completed by the first and second System Admin users.

1. Open the activation email that was sent during the setup of the EMS Account.

   Note: If you did not receive an email, check your spam or bulk mail folder.

2. In the email message, click the Activation link. The **Online Account Setup** page will open in a Web browser.


Your IronKey EMS Invitation
DataLocker Support <support@datalocker.com>
Sent: Wed 10/5/2016 12:17 PM
To: 100516@datalocker.com

Thank you for setting up your IronKey EMS Account. To access the Admin Console to manage your account, users, and devices, you must create an online account and set up your login credentials using the following link:

Your Activation Link: https://my.ironkey.com/va/4a3572821ea3da5b73517f2af239c1ae/844069022/1475694991/b14e331eb40ae9a6ec3d9cb53450a281a325ae20

Activation Instructions:
---
1) Click the Activation link above.
2) Follow the on-screen instructions to set up your online account.
3) Log in to your online account to access Admin Console.

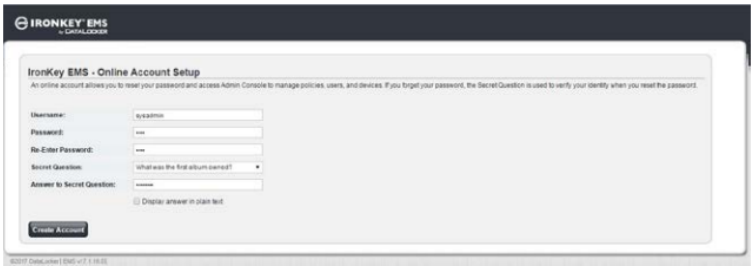
Regards,
The IronKey EMS Team

3. On the **Online Account** Setup screen, do the following:

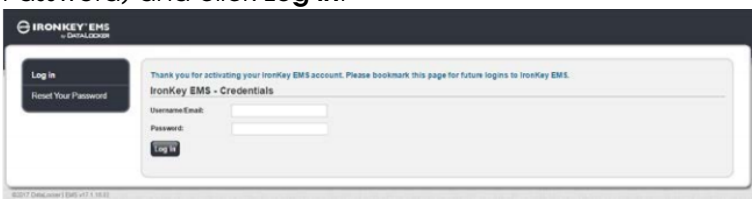
   - In the **Username** text box, create a user name for your account.
   - In the **Password** text box, create an account password and confirm the password. Passwords are case-sensitive and must comply with the password policy defined during the EMS Account setup.
   - Select a question from the **Secret Question** list box or create your own secret question.
   - In the **Answer to Secret Question** text box, provide the response to the secret question. The secret question will be used to verify your identity if you have to reset your password.

   Click **Create Account**.

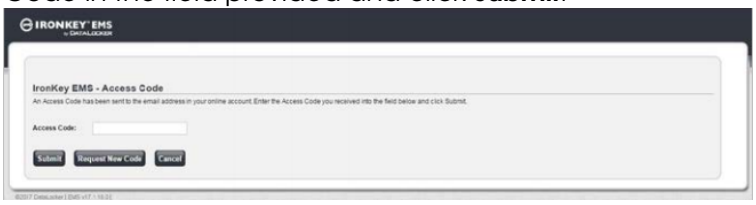
   A confirmation message will display to indicate that you have successfully created your online account.



4. To log in to the management console, enter your IronKey EMS credentials (Username and Password) and click **Log in**.



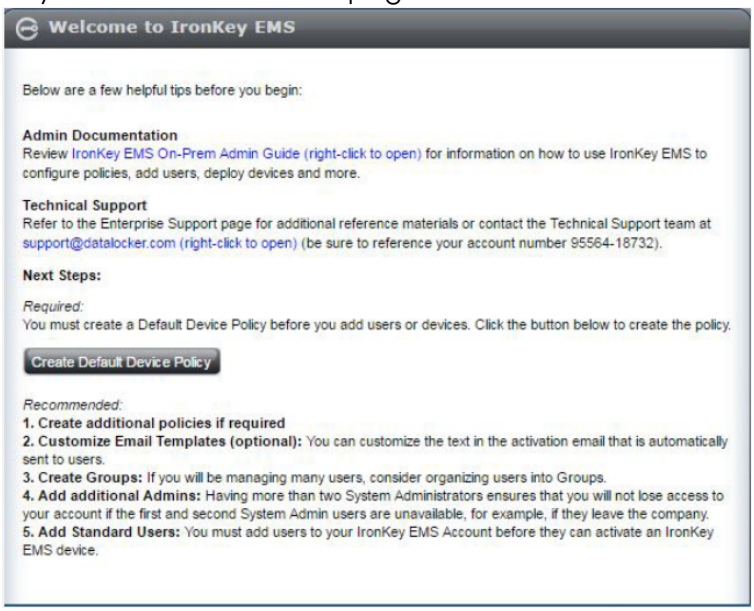
5. On the **Access Code** page, follow the instructions onscreen to retrieve and paste the Access Code in the field provided and click **Submit**.



A Welcome page will appear with information and instructions on next steps.

6. If you are the first System Admin to activate your online account and access the Admin Console, the Welcome page will prompt you to create a Default Device Policy. Click **Create Default Device Policy** to continue.

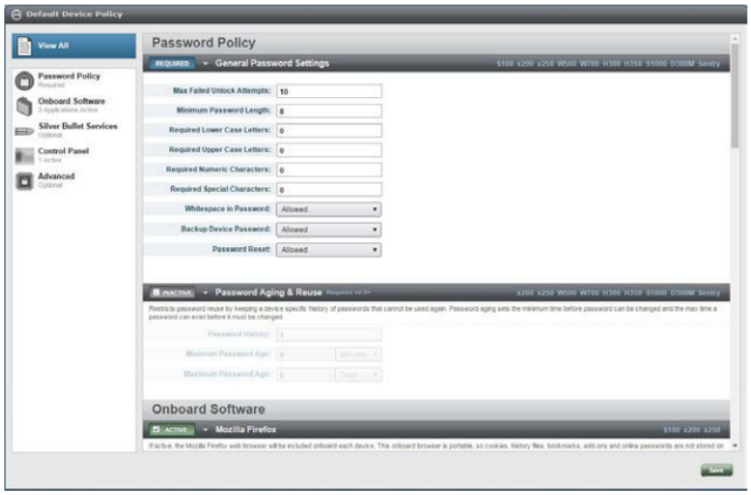
Note: If you are the second System Admin to activate your online account, you will not be prompted to create the Default Device Policy. The management console will appear as soon as you close the Welcome page.



7. On the **Default Device Policy** page, scroll through and review each section. Configure the settings and applications that you want to be included in the Default Device Policy for your EMS Account.

   Each policy section displays the system default settings and lists the devices to which these settings apply.

   Important: In the **Password Policy** section, under **General Password Settings**, configure the **Max Failed Unlock Attempts** setting with a balance of security and end-user convenience in mind. If the user exceeds the maximum, the device will "self-destruct" and all data will be permanently lost. The drive can no longer be used. D300M and Sentry devices do not self-destruct but will reset to a factory state, erasing all onboard data.



8. When you finish setting all device policy options, scroll to the end of the Default Device Policy and click **Save**.

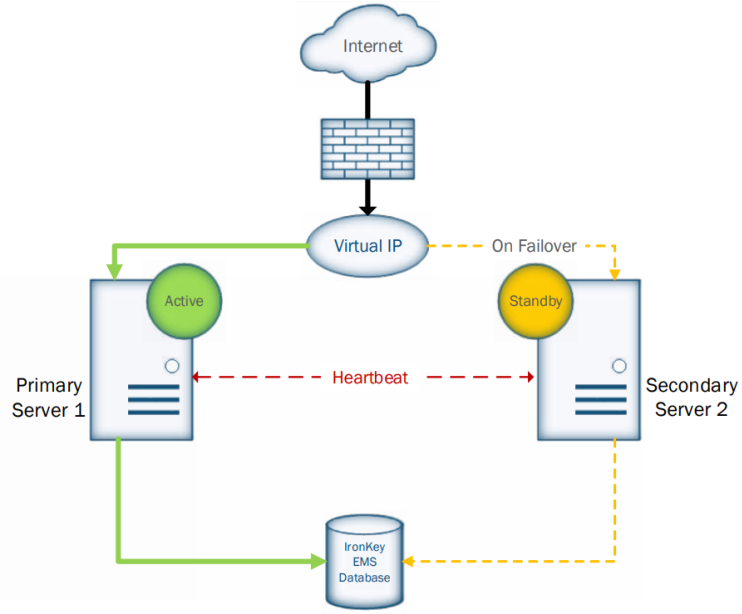
   You will receive a notice that your Default Device Policy was added successfully.

9. The management console will open in your web browser. You can now start adding users and managing your EMS account. For information about adding users, see the IronKey EMS On-Prem Admin Guide.

Deploying A High Availability Solution

High availability (HA) is the ability for supported IronKey EMS devices to access IronKey EMS On-Prem without experiencing a loss of service. Deploying IronKey EMS On-Prem's HA solution minimizes service disruptions if the server becomes unavailable. The IronKey EMS On-Prem HA solution uses an Active-Standby server configuration. The solution requires two installations of IronKey EMS On-Prem. One server is designated as the primary or active server and the other as the secondary or standby server. If the active server fails, the standby server becomes active and begins successfully resuming server processes. This process is referred to as "failover." When the primary server comes back online, the active secondary server automatically switches back to a "standby" state and the primary server will reclaim it's "active" status again. This process is called "failback."

The primary and secondary servers communicate using heartbeat detection. When the secondary server can no longer detect the heartbeat of the primary server, it automatically takes over as the active server. Both servers have an independent local IP address but share a virtual IP (VIP) address. IronKey EMS devices connect to the VIP address. The active server advertises the VIP address. The standby server takes over the VIP address only if the active server becomes unresponsive in a failover situation. The following illustration gives an overview of the HA solution.



Requirements

The HA solution requires two (minimum) installed and configured IronKey EMS On-Prem instances or peers. If you are a new customer, you should install and configure the primary server first. Follow the instructions outlined in section Installing IronKey EMS On-Prem and Configuring IronKey EMS On-Prem.

Both servers must be running version 6.1 or higher to deploy HA. If you are an existing customer and your installed server is running version 6.0 or earlier, you must upgrade to IronKey EMS On-Prem version 6.1 before you can enable HA. See, Upgrading IronKey EMS OnPrem. Both servers will point to the same database.

Once you set up the primary server, including creating your EMS account and activating System Admin devices, you are ready to deploy HA on the server.

Important: You do not need to create a new EMS account on the secondary server. However, you must update the license file in order to activate devices. It is recommended that you follow the steps in the section To Install And Configure The Secondary Server to configure and update the license file on the secondary server before deploying HA on this server.

The following restrictions apply when setting up your HA environment:

- Only IPv4 addresses are supported.
- Both servers share the VIP address and must be on the same subnetwork. The active server will advertise the VIP.

Before You Begin

You will need the following information when you deploy HA.

- Host name of the primary server. This is the host name of the server that will be the preferred active peer in the HA cluster.
- IP address of the primary server.
- Host name of the secondary server. This is the host name of the server that will be the standby peer in the HA cluster.
- IP address of the secondary server.
- Virtual IP (VIP) address that the active server will advertise. Devices will connect to the VIP address.

Note: You must update your DNS server so make sure that the siteName points to the address of the VIP once HA is enabled on both servers. This ensures that all device traffic is directed to the VIP.

Configurable HA Settings

The settings in the following table include all the configurable settings that are available with HA. Those marked with an " * " represent the settings that are required when deploying HA on each server. Some HA settings have preset default values assigned to them. You can change these default values using the appropriate `sysconf ha` CLI command. See the `sysconf ha` section for more information about HA CLI commands.

HA Setting	Description
peerip*	This is the IP address of the peer in an HA cluster. For example, on the primary server, the `peerip` is the IP address of the secondary server. The IP address must use Internet Protocol version 4 (IPv4).
peerhostname*	This is the host name of the peer server in an HA cluster. For example, on the primary server, the `peerhostname` is the host name of the secondary server.
VIP*	This is the Virtual IP (VIP) address that is shared between the HA peers. Only one peer advertises the VIP. In a failover situation, the standby peer will take over the VIP and become the Active peer. **Important:** When using HA, make sure that the `siteName` traffic is directed to the VIP address and not to a specific host address.

HA Setting	Description
preferred*	This is the host name of the server that you want to be the preferred peer. When active, the preferred peer will advertise the VIP address and run services. This setting must be the same for all peers in the HA cluster. **Note:** If `autofailback` is "On" the preferred peer will resume these services when it is back up and active after a "failover" event. If `autofailback` is "Off", then the preferred setting is used only in a situation where both servers startup at the same time.
autofailback	Determines whether the HA VIP will automatically fail back to the preferred peer (On), or remain on the current node (Off) until the current node fails or you change the state to "standby" using `sysconf ha standby`. In a failover situation, if you set autofailback to "On" for the preferred (active) server and "On" for the secondary (standby) server, the secondary server will automatically return to its standby state after it detects that the preferred server is back up and running. The preferred peer will take the VIP from the secondary server after the preferred peer comes back online. This setting should have the same value for both peers in the HA cluster, that is, either both set to "On" or both set to "Off". Autofailback does not apply when a server is set to "standby." *Default setting is "Off".*
keepalive	Sets the time in seconds between HA peer heartbeat checks. The heartbeat check determines the health of the peer to and whether the peer is responding. *Default value is 10 seconds (This is the recommended setting)*
deadtime	Determines the time in seconds that an HA server will wait before marking its peer as unresponsive (or dead) after consistently failing to respond during HA `keepalive` health checks. When the `deadtime` limit is exceeded, the HA server will take the VIP from the unresponsive peer and become the active server. The `deadtime` value must be less than or equal to the `initdead` value. *Default value is 300 seconds. It is recommended that do not set deadtime to less than (or equal to) 60 seconds.*
initdead	Sets the time in seconds that an HA server will wait before doing an initial peer heartbeat check. This setting allows the server network interface and upstream network infrastructure to pass traffic. The `initdead` value must be greater than or equal to the `deadtime` value. *Default value is 300 seconds. It is recommended that do not set initdead to less than (or equal to) 60 seconds.*

*These settings are required when deploying HA on both servers.

Deploying HA

You deploy HA on each IronKey EMS Server peer using CLI commands to configure the servers. For a complete list of HA commands, see the `sysconf ha` entries in the command line reference

section at the end of this guide. You must enable HA on each server to successfully deploy a high availability solution.

It is recommended that you deploy HA on your primary (preferred) peer first before you install and configure the secondary (standby) peer, and deploy HA. Before you begin, make sure that the siteName in the DNS server is pointing to the IP address of the primary server and that users can activate devices on this server. The following list outlines the tasks involved in an HA deployment. You should complete these tasks in the order listed.

Deployment Steps

- Deploy HA on primary server
- Install and configure the secondary server
- Re-generate the server license on the secondary server
- Deploy HA on secondary server
- Modify siteName in DNS server to point to VIP

See Example Of An HA Deployment for a walk-through of how one customer deployed HA in their organization.

To Deploy HA On The Primary IronKey EMS On-Prem Server

1. Log in to the primary IronKey EMS On-Prem Server using the command line interface (CLI).

   Note: The primary server is the active server that will advertise the VIP address.

2. Set the peerip address for the *secondary server* in the HA cluster.

   ```
   sysconf ha peerip <valid IPv4 address>
   ```

   Example:

   ```
   sysconf ha 192.168.200.102
   ```

   Note: Both the primary and secondary servers must use the same subnetwork.

3. Set the peerhostname for the secondary (standby) server in the HA cluster.

   ```
   sysconf ha peerhostname <hostname>
   ```

   Example:

   ```
   sysconf ha peerhostname ikes2.domain.com
   ```

4. Set the VIP address to be advertised by the active server.

   ```
   sysconf ha vip <valid IPv4 address>
   ```

   Example:

   ```
   sysconf ha vip 192.168.200.100
   ```

5. Set the hostname of the preferred server.

   ```
   sysconf ha preferred <hostname>
   ```

   Example:

   ```
   sysconf ha preferred ikes1.domain.com
   ```


6. Turn on autofailback.

   ```
   sysconf ha autofailback On
   ```

   Note: The default `autofailback` setting is Off. For more information, see sysconf ha autofailback <on or off> in the Commands Summary section.

   When autofailback is turned on, the preferred server will automatically reclaim the active server role after the failover event is resolved and the preferred server is up.

7. Enable HA on the primary server.

   ```
   sysconf ha enable
   ```

8. Confirm the status of the primary server.

   ```
   sysconf ha status
   ```

To Install And Configure The Secondary Server

If you have not done so already, install the secondary server. See Installing IronKey EMS On-Prem. Configure the server using the following procedure.

1. Log in to IronKey EMS On-Prem using the command line interface (CLI).

2. Set the host name.

   ```
   network hostname <VM hostname>
   ```

   Example:
   ```
   network hostname ikes2.domain.com
   ```

   Critical: When using this command, make sure you enter a Fully Qualified Domain Name (FQDN), not just the hostname of the IronKey EMS On-Prem.

   The host name must be unique. It cannot be the same as the hostname of the primary server.

   FQDN Example: (correct)
   ```
   network hostname ikes2.domain.com
   ```

   Hostname only Example (incorrect):
   ```
   network hostname ikes2
   ```

3. Configure a static IP address

   ```
   network interface static <static IP> <IP mask> <Gateway>
   ```

   Example:
   ```
   network interface static 192.168.200.102 255.255.255.0 192.168.200.1
   ```

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. IronKey EMS On-Prem 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:port number>
   ```

   Example:
   ```
   sysconf smtp set server01.corp.ironkey.com:465
   ```

   ```
   Does the relayhost <your_SMTP_server> require authentication (y/n)?
   ```

7. Configure the database server.

   ```
   application database configure <DB server IP or hostname> <port ID> <database username>
   <password> mssql <database name>
   ```

   Note: Both the primary and secondary server must connect to the same database. Make sure that the database configuration uses the same parameters as the database configured for the primary server.

   Example:
   ```
   application database configure 10.1.1.89 1433 db_ usr mypasswd mssql ent_server
   ```

8. Set the external name of the server as accessed by devices.

   ```
   application siteName set <site name>
   ```

   Important: The siteName must be the same as the siteName of the primary server. If the siteName is different, devices will not be able to connect to the server. Make sure that your site name uses a Fully Qualified Domain Name (FQDN). The site name must match the Common Name in the SSL Certificate.

   Note: Your certificate must have a valid public domain. To use the Silver Bullet Services, you must be able to expose the server on the Internet and allow firewall routing for that URL.

   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`

Example:

```
pscp.exe -scp server.crt admin@192.168.200.102:/upload

pscp.exe -scp issuer.crt admin@192.168.200.102:/upload
```

See Certificate Acquisition And Renewal and Useful PSCP.EXE Commands for more information.

Make sure that you use the same SSL certificate that was used on the primary server.

10. Install the certificates.

```
application certificate install
```

11. Enable HTTPS.

```
application ssl enable
```

12. Start IronKey EMS On-Prem.

```
service start appserver
```

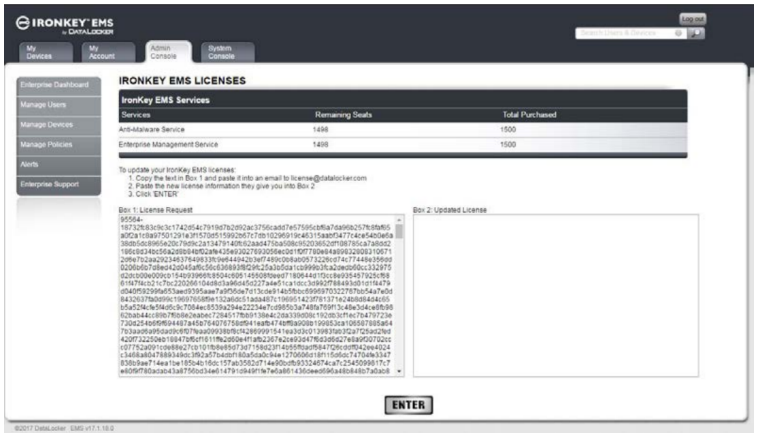
Once you've configured the secondary server, you must re-generate the license from the Admin Console. To access Admin Console, change the `hosts` file on the system to which your System Admin device is connected by adding a host entry that points to the IP address of the secondary server. Device traffic will now be going through the secondary IP server address.

Using the examples in Step 2 and 3, the host entry would be

```
192.168.200.102 myhost.domain.com.
```

To Re-Generate The License File Of The Secondary Server

1. Log in to the Admin Console.
2. In Admin Console, click **Enterprise Support** from the left menu.
3. Click the **Manage Licenses** button to view your Services list.
4. Copy the License Request text from Box 1 and paste it into an email message addressed to Customer Service at license@datalocker.com



5. Paste the new license information from the Customer Service Reply email in Box 2, and then click the **Enter** button.

To Deploy HA On The Secondary Server

1. Log in to the secondary IronKey EMS On-Prem Server using the command line interface (CLI).

   Note: The secondary server is the Standby server that will become active in a failover situation.

2. Set the peerip address for the *primary* server in the HA cluster.

   ```
   sysconf ha peerip <valid IPv4 address>
   ```

   Example:

   ```
   sysconf ha 192.168.200.101
   ```

   Note: Both the primary and secondary servers must use the same subnetwork.

3. Set the peerhostname for the primary (Active) server in the HA cluster.

   ```
   sysconf ha peerhostname <hostname>
   ```

   Example:

   ```
   sysconf ha peerhostname ikes1.domain.com
   ```

4. Set the VIP address to be advertised by the Active server.

   ```
   sysconf ha vip <valid IPv4 address>
   ```

   Example:

   ```
   sysconf ha vip 192.168.200.100
   ```

5. Set the hostname of the preferred server.

   ```
   sysconf ha preferred <hostname>
   ```

   Example:

   ```
   sysconf ha preferred ikes1.domain.com
   ```

   Note: When autofailback is turned on, the preferred server will automatically reclaim the active server role after the failover event is resolved and the preferred server is up. Once the secondary (standby) server detects the heartbeat of the preferred server, the preferred server

will take back the VIP and become the active server. The secondary server will switch back to "standby" status.

The default `autofailback` setting is *Off*. See sysconf ha autofailback in the Commands Summary section for information about turning this setting On.

6. Turn on autofailback.

   ```
   sysconf ha autofailback On
   ```

   Note: The default `autofailback` setting is Off. For more information, see sysconf ha autofailback in the Commands Summary section.

   When autofailback is turned on, the preferred server will automatically reclaim the active server role after the failover event is resolved and the preferred server is up.

7. Enable HA on the secondary server.

   ```
   sysconf ha enable
   ```

8. Confirm the status of the secondary server.

   ```
   sysconf ha status
   ```

After you enable HA on the secondary server, open the `hosts` file on the system to which your System Admin device is connected and change the host entry. Instead of pointing to the IP address of the secondary server, for example `192.168.200.102 myhost.domain.com`, point to the VIP that both servers will use, for example `192.168.200.100 myhost.domain.com`.

Verify that device traffic is using the VIP by accessing Admin Console and monitoring that the device connects using the VIP (for example `192.168.200.100`). Once you have verified on the secondary server that device traffic is using the VIP, you can remove the host entry from the `hosts` file and make the actual change in the DNS server.

Modify SiteName In DNS Server To Point To VIP

Locate the siteName entry in the DNS server and replace the IP address of the primary server with the VIP. This will route device traffic through the VIP to complete the HA deployment.

- Old DNS entry <IP Address Primary server><FQDN siteName>
  For example: `192.168.200.101 myhost.domain.com`
- New DNS entry <VIP><FQDN siteName>
  For example: `192.168.200.100 myhost.domain.com`

Example Of An HA Deployment

In this example, two installed IronKey EMS On-Prem Servers (Server 1 and Server 2) have been licensed and configured with the following settings:

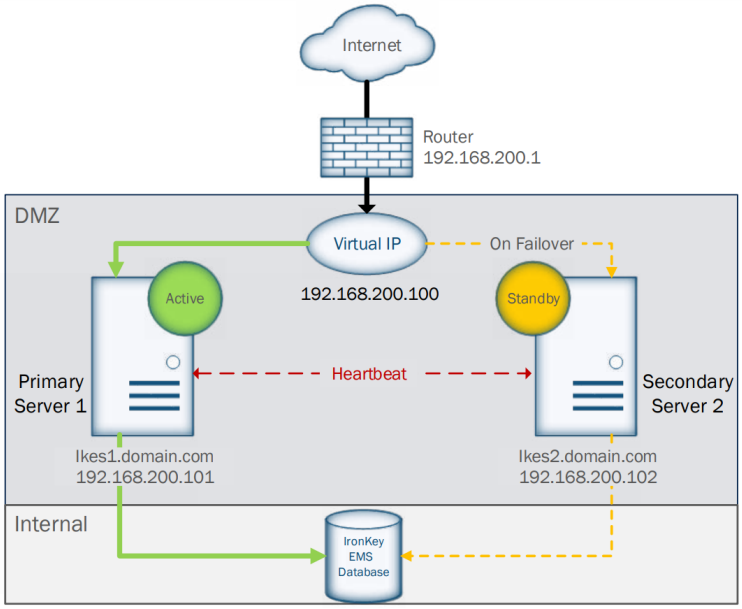
- **Router IP address:** 192.168.200.1
- **Server 1 hostname:** ikes1.domain.com
- **Server 1 IP address:** 192.168.200.101
- **Server 2 hostname:** ikes2.domain.com
- **Server 2 IP address:** 192.168.200.102
- **VIP address:** 192.168.200.100

- **siteName:** myhost.domain.com
- **DNS**: myhost.domain.com (192.168.200.100)

Note: The siteName is pointing to the address of the VIP. This ensures that all device traffic is directed to the VIP.

When deploying HA for this server cluster, Server 1 is configured as the primary server and is the preferred active peer (ikes1.domain.com). Server 2 is the secondary server that will be on standby in case the active server becomes unresponsive. Autofailback is turned on to ensure that Server 1 will reclaim its active status on failback when it is able to resume operations after a failover event.

The following diagram illustrates the deployed HA server implementation.



Steps To Deploy HA

On Server 1 (Primary), log into the CLI and type the following commands:

1. Set the IP address of the HA **Secondary** peer.

   ```
   sysconf ha peerip 192.168.200.102
   ```

2. Set the host name of the HA **Secondary** peer.

   ```
   sysconf ha peerhostname ikes2.domain.com
   ```

3. Set the IP address of the Virtual IP (VIP).

   ```
   sysconf ha vip 192.168.200.100
   ```

4. Set the domain name for the preferred peer. This value name be the same on both the Primary and Secondary server.

   ```
   sysconf ha preferred ikes1.domain.com
   ```


5. Set autofailback to "On".

   ```
   sysconf ha autofailback on
   ```

6. Enable HA on the primary server.

   ```
   sysconf ha enable
   ```

On Server 2 (Secondary), log into the Server using the CLI and type the following commands:

1. Set the IP address of the HA **Primary** peer.

   ```
   sysconf ha peerip 192.168.200.101
   ```

2. Set the host name of the HA **Primary** peer.

   ```
   sysconf ha peerhostname ikes1.domain.com
   ```

3. Set the IP address of the Virtual IP (VIP).

   ```
   sysconf ha vip 192.168.200.100
   ```

4. Set the domain name for the preferred peer. This value name be the same on both the Primary and Secondary server.

   ```
   sysconf ha preferred ikes1.domain.com
   ```

5. Set autofailback to "On".

   ```
   sysconf ha autofailback on
   ```

6. Enable HA on the secondary server.

   ```
   sysconf ha enable
   ```

Conclusion

HA is now enabled on both servers. The Primary server is the preferred peer. The Primary server will become the Active server and take the VIP. The Secondary server will automatically go to Standby mode. Each server will continue monitoring the heartbeat of its peer.

Hint: To verify the status of the primary or secondary server, type the following command on the server whose status you want to confirm: `sysconf ha status`.

HA Recovery Scenarios

When you run the `sysconf ha status` command, it returns the mode that the server is in: Active, Standby, or Local. It also identifies if the server is holding the VIP. When HA is running as expected, the status on the primary server is in "Active" mode and the server is holding the VIP. The status on the secondary server is in "Standby" mode and the server is *not* holding the VIP.

A server will typically go into Local mode only when a recovery or Active-Active server scenario occurs. However, on first setup, after you first configure and enable HA on both peers, the servers will also transition to Local mode. This is expected and occurs because HA is enabled first on Server

1, so there is a period of time where it cannot detect Server 2 and considers the server "dead." When Server 2 comes online, Server 1 will detect that its peer is now running, but recognizes this as a recovery scenario, similar to the network outage scenario. Both servers go into Local mode with the preferred server (Server 1) holding the VIP.

In a recovery scenario, one or both of the servers are trying to resolve a disruption in service. The HA parameters that you configure, such as autofailback "On" or "Off", as well as the type of disruption will determine how each server recovers in these situations and which server holds the VIP.

The following table describes the expected outcomes when one or both of the servers experience issues. The server names, IP addresses, and domain names that are used in these scenarios are from the Example Deployment section.

1. **HA is disabled on both servers.**

   When both servers are disabled, neither are holding the VIP. If the siteName DNS record (myhost. domain.com) points to the VIP (IP address: 192.1689.200.100), devices will not be able to reach either server in the HA cluster because the servers are not listening for device traffic.

   Resolution: Enable HA on both peers to ensure that the HA solution is running and devices can connect to the server. If you need to disable HA on both servers, make sure that your DNS server points the siteName to the IP address of the server that you want to keep running. This will ensure that devices can still connect to the server that you specify once HA is disabled.

2. **Active server loses network connectivity (HA is enabled on both, Server 1 is preferred)**

   When the Active server experiences a network outage, the Active server (Server 1) and Standby server (Server 2) can no longer communicate even though Server 1 is still running. Both servers will start the `deadtime` countdown. When Server 1 exceeds `deadtime`, it remains Active and marks its peer "dead." When Server 2 exceeds `deadtime`, it becomes Active and also marks its peer "dead." Both servers are now holding the VIP and both are in Active mode. However, due to the network outage with Server 1, only Server 2 is receiving traffic.

   ```
   server1> sysconf ha status
   High-Availability is running.
   ACTIVE mode
   Holding VIP 192.168.200.100
   ```

   ```
   server2> sysconf ha status
   High-Availability is running.
   ACTIVE mode
   Holding VIP 192.168.200.100
   ```

   Resolution: When Server 1 regains network connectivity, both peers detect that the other is Active and both will restart HA services to initiate an "Active-Active" recovery. The VIP will be offline for the value of `initdead` (in seconds) while each server comes back up. When both servers can detect their peer, Server 1 will take the VIP because it is the preferred peer. Both servers will remain in Local mode. Local mode means that a recovery has occurred. In this scenario, the servers have recovered from an Active-Active situation.

   ```
   server1> sysconf ha status
   High-Availability is running.
   LOCAL mode
   autofailback or ACTIVE-ACTIVE recovery has occurred.
   Holding VIP 192.168.200.100
   ```

   ```
   server2> sysconf ha status
   High-Availability is running.
   LOCAL mode
   ```



```
autofailback or ACTIVE-ACTIVE recovery has occurred.
Not holding VIP 192.168.200.100
```

3. **Active server is set to standby - Scenario A (HA is enabled, Server 1 is preferred, Autofailback is "On")**

   In this scenario, the HA administrator manually sets the Active server (Server 1) to Standby mode, for example, to perform system maintenance without taking the server offline. Server 2 will automatically be set to Active. When the preferred server is put in Standby mode, it overrides the `autofailback` setting and prevents Server 2 from passing the VIP back to the preferred server even after deadtime is exceeded and Server 1 is running. Only if Server 2 experiences an outage while Server 1 is in Standby mode, or if Server 1 is rebooted will the preferred Server 1 automatically become the active server again and hold the VIP.

   Resolution: When you want Server 1 to take the VIP and become the Active server again, you must manually set Server 2 to Standby so that Server 1 will once again become active and take the VIP.

4. **Active server is set to standby - Scenario B (HA is enabled, Server 1 is preferred, Autofailback is "Off")**

   This scenario is recommended when system maintenance is required on Server 1 and the server must be rebooted multiple times. The HA administrator manually sets the Active server (Server 1) to Standby mode. Server 2 becomes the Active server and takes the VIP. With `autofailback` turned off, unlike Option 1 (above), `autofailback` will not occur when `deadtime` is exceeded and Server 2 detects that Server 1 is running. Even if the preferred server is rebooted, `autofailback` will not cause Server 2 to pass the VIP back to Server 1. This scenario is typically used when an administrator must perform system maintenance on Server 1 that requires the server to be rebooted multiple times.

   Resolution: When you want Server 1 to take the VIP and become the Active server again, put Server 2 in Standby mode. You can also turn autofailback "On."

5. **Active server is rebooted (HA is enabled, Server 1 is preferred)**

   If Server 1 reboots unexpectedly, taking it offline, Server 2 will wait for the `deadtime` value and then become the Active server and hold the VIP.

   Resolution: When Server 1 comes back online, if `autofailback` is "On" for both servers, Server 2 will pass the VIP back to Server 1 when it detects the heartbeat of Server 2. If autofailback is "Off," Server 2 will hold the VIP until it is manually set to Standby mode or experiences a failover.

Best Practices

Deployment Configuration

While IronKey EMS On-Prem can be deployed anywhere on your network, the end-user devices will need to connect to IronKey EMS On-Prem 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 IronKey EMS On-Prem each time they must be unlocked.

DataLocker recommends that you place and protect IronKey EMS On-Prem 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 EMS policies ahead of time (see the *IronKey EMS On-Prem Admin Guide* for more details), and prepare a list of all users and (optionally) their email addresses.

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 EMS On-Prem 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 EMS On-Prem. We recommend that you periodically back up this file and store it securely (ideally on a support EMS 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, IronKey EMS On-Prem 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 EMS On-Prem 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 for a full CLI command reference.

1. *Version Check.* To check the IronKey EMS On-Prem 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 DataLocker Support can use to help you:

   ```
   supportInfo
   ```

3. *Monitoring System Health:* IronKey EMS On-Prem 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 DataLocker Support.

4. *Shutdown IronKey EMS On-Prem.* 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>
```

Certificate Upload

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

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

x.x.x.x is the IronKey EMS On-Prem IP address
is the timestamp

Upgrading IronKey EMS On-Prem

Upgrading IronKey EMS On-Prem from a previous version to the newest version involves uninstalling the existing server and deploying (ESXi environment or VMware Workstation Player) the new version. Once installed, you must re-configure the server settings. The upgrade is available as a download from DataLocker.

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.

1. Fill out the Installation Worksheet.

   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 IronKey EMS On-Prem VM.

   Enter this CLI command:
   `sysconf shutdown`

   Note: 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.

5. Upgrade the database.

   Use the SQL Server Management Studio to run the script named "db_upgrade_ from_v71_to_v72.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 7.2, you must run the following scripts (located in the \Utils\Legacy Files folder) in order:

   1. `db_upgrade_from_v1_to_v2.sql`
   2. `db_upgrade_from_v2_to_v3.sql`
   3. `db_upgrade_from_v3_to_v4.sql`
   4. `db_upgrade_from_v4_to_v5.sql`
   5. `db_upgrade_from_v5_to_v51.sql`
   6. `db_upgrade_from_v51_to_v52.sql`
   7. `db_upgrade_from_v52_to_v6.sql`
   8. `db_upgrade_from_v60_to_v61.sql`
   9. `db_upgrade_from_v61_to_v7.sql`
   10. `db_upgrade_from_v70_to_v71.sql`

   - Click the database you want to update.
   - Click the **New query** button.
   - Copy and paste the text in the **db_upgrade_from_v71_to_v72.sql** file to the query window.
   - 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 IronKey EMS On-Prem v7.1.

7. Deploy the new IronKey EMS On-Prem using the files provided in your Server Upgrade download package.

ESXi environment: In vSphere Client, deploy the IronKey_EMS_OnPrem OVA file to the host. The file is located in the IronKey_EMS_OnPrem OVA folder of the upgrade download package. See also Deploying IronKey EMS On-Prem In An ESXi Environment.

VMware Workstation Player: In VMware Workstation Player, deploy the IronKey_EMS_OnPrem OVA file to the host. The file is located in the IronKey_EMS_OnPrem OVA folder. See Deploying IronKey EMS On-Prem In VMware Workstation Environment.

Note: You may be required to uninstall VMware Player. If you are prompted to do this, use the Windows Control Panel.

8. Start the IronKey EMS On-Prem VM.

   ESXi environment: In vSphere Client, right-click the Server and click **Power > Power On**.

   VMware Workstation Player environment: Select IronKey EMS On-Prem and click **Play virtual machine**.

9. At the IronKey EMS On-Prem 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 ikes1.domain.com
    ```

    Critical: When using this command, make sure you enter the 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 192.168.200.101 255.255.255.0 192.168.200.1
    ```

12. Add the DNS name server.

    ```
    network dns add <DNS server IP>
    ```

    Example:
    ```
    network dns add 10.1.1.100
    ```

13. 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. IronKey EMS On-Prem will show the correct time once you set the date or add the NTP server.

Example:
`sysconf time 14:11:00 31 August 2014`

14. 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:port number>`

    Example:
    `sysconf smtp set server01.corp.ironkey.com:465`

    `Does the relayhost <your_SMTP_server> require authentication (y/n)?`

15. 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 ent_server`

16. 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 siteName must match the Common Name in the SSL certificate.

    Note: Your certificate must have a valid public domain. To use the Silver Bullet Services, you must be able to expose the server on the Internet and allow firewall routing for that URL.

    Command Example:
    `application siteName set myhost.domain.com`

17. Securely copy the certificate files to the `/upload` directory on the VM.

    Use a Secure Copy (SCP) utility (such as commandline-based PSCP or GUI-based WinSCP) to securely copy the files to /upload.

    Example:
    `pcsp.exe -scp server.crt admin@192.168.200.101:/upload`

    `pcsp.exe -scp issuer.crt admin@192.168.200.101:/upload`

18. Install the certificates.

    `application certificate install`

19. Enable HTTPS.

    ```
    application ssl enable
    ```

20. Start the application server.

    ```
    service start appserver
    ```

21. Update your license.

    Important: You must add a new license to your server to be able to initialize new devices. See the *IronKey EMS On-Prem Admin Guide*, "Licensing" section for details.

    - Click the **Admin Console** button in the Control Panel.
    - Click **Enterprise Support** on the Admin Console, and then click the **Manage Licenses** button to view your Services list.
    - 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.

22. Reboot IronKey EMS On-Prem.

    ```
    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 IronKey EMS On-Prem v7, you will need to re-upload this file as it is removed when v7.1 was installed during the server upgrade process. For more information, see Uploading Device Software Updates.

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 EMS On-Prem Admin Guide* for information on approving the update so that users can download and install it to their device.

To get the update package please contact support. 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 from On-Prem v7.1 to v7.2, any software update package that was added to the server is removed when the v7.1 server is uninstalled. You must re-upload the software

update package and install it to the new v7.2 server. However, you do not need rerun 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 at datalocker.com) 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 at datalocker.com) 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).

   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. Log in to 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**.
2. Perform your test to update devices. (See the Updating Devices section of the *IronKey EMS On-Prem 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 IronKey EMS On-Prem using a command line interface. Also see Useful PSCP.EXE Commands.

Background

Some CLI commands require write access on the Virtual Machine that hosts IronKey EMS On-Prem before you can run the commands. For example, `application certificate install` requires certificate files to be copied to IronKey EMS On-Prem before it starts. Similarly, some CLI commands require data to be copied out of IronKey EMS On-Prem 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 supported devices downloads virus definition file updates directly from update.nai.com servers at McAfee.

If you are using IronKey EMS On-Prem to manage supported EMS 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 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 IronKey EMS On-Prem:

   `application malwareScanner set defintionURL <http://<url-to-updatefiles>.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 IronKey EMS On-Prem service and enable the changes:

   `sysconf reboot`

   EMS 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 ssl ciphers show`
Description: Display configured HTTPS Ciphers/Suites and a detailed list of the specific ciphers.

`application ssl ciphers set`
Description: Set HTTPS Ciphers and Suites.

`application ssl ciphers reset`
Description: Reset HTTPS Ciphers and Suites to default.

`application ssl ciphers available`
Description: Display all available HTTPS Ciphers.

`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: ent_server)

`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 malwareScanner test`
Description: Test downloading malwareScanner definitionURL and malwareScanner iniURL files.

`application malwareScanner reset`
Description: Reset malwareScanner URLs to default.

`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 services port show`
Description: Shows the port that is currently set.

`application services port set alternate`
Description: Port is set to alternate value: 9701. Do *not* change the port setting if devices have already been activated using the default port (2000). Otherwise, these devices will no longer be able to connect to the server.

`application services port set default`
Description: Port is set to default value: 2000.

`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.

`network netcat <hostnameorip> <port> <count> <timeout>`
Description: Test any TCP connection to any server, including the On-Prem itself.

Arguments:
`hostnameorip` - Destination Host name or IP address
`port` - Destination TCP Port (ex: 1433)
`count` - Number of connection attempts (CTRL-C to stop)
`timeout` - Connection timeout in seconds

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 ha autofailback <on or off>`
Description: Determines whether the HA VIP will automatically fail back to the preferred peer (On), or remain on the current node (Off) until the current node fails or you run the command `sysconf ha standby`. In a failover situation, if you set autofailback to "On" for both the preferred (active) server and secondary (standby) server, the secondary server will automatically return to its standby state after it detects that the preferred server is back up and running. The preferred peer will take the VIP from the secondary server after the preferred peer comes back online. *Default is "Off".*

`sysconf ha deadtime <seconds>`
Description: Determines the time in seconds that an HA server will wait before marking its peer as unresponsive (or dead) after consistently failing to respond during HA `keepalive` health checks. When the *deadtime* limit is exceeded, the HA server will take the VIP from the unresponsive peer and become the active server. The *deadtime* value must be less than or equal to the *initdead* value.
Default value is 300 seconds.

`sysconf ha disable`
Description: Shuts down the monitoring system and stops the HA services.

`sysconf ha enable`
Description: Starts the monitoring system and the HA services

`sysconf ha initdead <seconds>`
Description: Sets the time in seconds that an HA server will wait before doing an initial peer heartbeat check. This setting allows the server network interface and upstream network infrastructure to pass traffic. The initdead value must be greater than or equal to the deadtime value.
Default value is 300 seconds.

`sysconf ha keepalive <seconds>`
Description: Sets the time in seconds between HA peer heartbeat checks. The heartbeat check determines the health of the peer and whether the peer is responding.
Default value is 10 seconds.

`sysconf ha peerhostname <hostname>`
Description: Sets the host name of the peer in an HA cluster. For example, when configuring the primary (active) server, this is the host name of the secondary (standby) server.

`sysconf ha peerip <IPv4>`
Description: Sets the IP address of the peer in an HA cluster. For example, when configuring the primary (or active) server, this is the IP address of the secondary (or standby) server. IP address must use IPv4.

`sysconf ha preferred <hostname>`
Description: The host name of the server that is to be the preferred peer. When active, the preferred peer will advertise the VIP address and run services. This setting must be the same for all peers in the HA cluster.

Note: If autofailback is "On" for both servers, the preferred peer will resume services when it is back up and active (failback) after a "failover" event. If autofailback is "Off", then the preferred setting is used only in a situation where both servers startup at the same time.

`sysconf ha vip <IPv4>`
Description: Sets the IP address for the Virtual IP (VIP) that will be shared by both HA servers (primary and secondary). Only one peer advertises the VIP.

`sysconf ha standby`
Description: Manually sets the server to standby mode. The other HA peer becomes the active server.

`sysconf ha status`
Description: Displays the operational mode of the HA server, for example Active or Standby.

`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: Disable NTP server.

`sysconf ntp enable`
Description: Enable 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 IronKey EMS On-Prem 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:port>`
Description: Configure SMTP RelayHost and port number.

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.

`application debug show`
Description: Get all available application debug commands. You should only use the debug commands if DataLocker Customer Support has requested that you enable it, for example when attempting to reproduce an issue and provide Customer Support with a supportInfo file.

`application debug enable`
Description: Turns debug mode on. When enabled, log files of actions taken are captured and added to the supportInfo file when you generate a support ticket.

`application debug disable`
Description: Turns debug mode off. Once you have generated a supportInfo file, you should disable debug mode.

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.

DataLocker is committed to creating and developing the best security technologies and making them simple-to-use and widely available. 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 appreciate hearing about your comments, suggestions, and experiences with this product. Feedback: support@datalocker.com

Note: DataLocker 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 DataLocker on the issue discussed as of the date of publication. DataLocker cannot guarantee the accuracy of any information presented after the date of publication. This document is for information purposes only. DataLocker makes no warranties, expressed or implied, in this document. DataLocker, and the DataLocker logo are trademarks of DataLocker Inc. and its subsidiaries. All other trademarks are the property of their respective owners. ™ is a registered trade mark of Kingston Technologies, used under permission of Kingston Technologies. All rights reserved.

IronKey EMS On-Prem v7.2.0.0 software - 2018. IK-EMS-ADM04-1.0