Installing iDENprotect$^{\text{server}}$ 1.2.0 on RHEL 7 or CentOS 7

iDENprotect Ltd.

Version 1.2.0, August 10th, 2017

Table of Contents

This document describes how to install a standalone iDENprotect$^{\text{server}}$ either on a physical Red Hat Enterprise Linux (RHEL) server or on a virtualised platform using hypervisor software such as VMWare ESXi. The document assumes general knowledge of RHEL server administration, as well as knowledge in hypervisor technology if deploying iDENprotect$^{\text{server}}$ to a virtual machine.

This document only discusses the initial installation of iDENprotect$^{\text{server}}$. For more in-depth information on iDENprotect$^{\text{server}}$ architecture and configuration, see iDENprotect Administrator Guide.

Before Starting

System Requirements

The minimum system requirements for installing the iDENprotect$^{\text{server}}$ on physical or virtual hardware are:

- 64-bit Dual Core CPU
- 4 GB RAM
- 60 GB free hard disk space
- 64-bit RHEL 7.2 operating system
- No additional web servers or other applications running on the server

Pre-installation Tasks

> Before proceeding further with the iDENprotect$^{\text{server}}$ installation process, make sure the following Pre-installation Tasks have been completed.

- The server has RHEL 7 operating system installed. If RHEL 7 is not installed yet, see Installing RHEL
- If installing on CentOS 7, the server must have access to internet. For installation on RHEL 7 the server does not require access to internet if installing the standalone installation ISO.
- The server has the following network settings configured correctly:
  - static IP address
  - subnet mask
  - default gateway
  - DNS server IP addresses
- NTP (Network Time Protocol) is enabled on the server

  > For instructions on configuring NTP, see Configuring NTP at RHEL System Administrator's Guide.

- The server has a valid FQDN (Fully Qualified Domain Name) with unique hostname

  > This can be tested this with the command `ping [server's FQDN]`. If the command returns with a valid reply, the network connection works and the server's FQDN can be resolved.
  >
  > If the server has just been set up, this step may fail even though the FQDN has been configured correctly. In this case, see Hostname Configuration to configure it.

- Knowledge of the full DN (Distinguished Name) policies for digital certificates.
- Knowledge of the email gateway to be used for sending emails from the iDENprotect$^{\text{server}}$ with iDENprotect Activation Codes. Email Gateway details for setup:
  - username

  - password
  - host
  - Port
  - email to be used as the "from" address.

If iDENprotect^{server} is used with Active Directory or other LDAP authentication services, make sure the following LDAP details are known:

- IP Address and FQDN of the LDAP server
- Service account username and password to query the LDAP database
- LDAP OU (Organisational Unit) that contains the users
- LDAP Group where users can be auto-enrolled (The entitlement group)

❗ iDENprotect^{server} operation requires valid DNS and FQDN settings, and correct data within digital certificates. While the settings can be changed later, it is recommended to set everything up during installation.

Hostname Configuration

If iDENprotect^{server} is being installed on a new server that has only recently been set up, it's possible that the server's hostname may not yet be registered in an organisation's DNS service. To confirm if the hostname is registered, use the ping command as follows:

```
ping [server's FQDN]
```

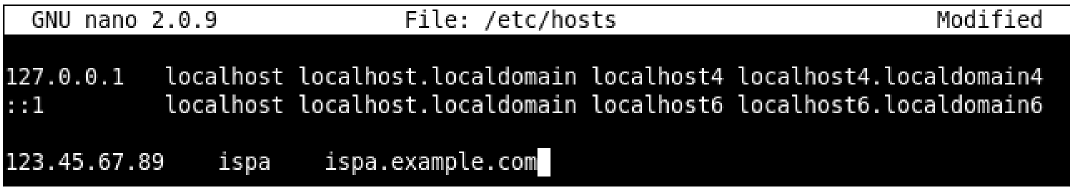
If the ping command returns with a valid reply, the DNS of the server is functioning correctly and this section can be ignored.

If the ping command returns with an error such as `unknown host`, the FQDN of the server is not yet registered in DNS. **Due to the nature of EJBCA It is recommended as good practice to set the server's hostname in the `/etc/hosts` name mapping file, even if DNS has been setup.**

1. Open `/etc/hosts` in a text editor, such as `nano` or `vi`

   ```
   sudo nano /etc/hosts
   ```

2. Enter the server's public IP address in a new row in the file, and add the hostname and FQDN after it:

   ```
     GNU nano 2.0.9              File: /etc/hosts                          Modified

   127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4
   ::1         localhost localhost.localdomain localhost6 localhost6.localdomain6

   123.45.67.89    ispa    ispa.example.com
   ```

   Figure 1. Editing hosts file

3. Save the file and and exit (`CTRL+O` and `CTRL+X` in `nano`)

To get the server's IP address, type `ip addr show` and find the right network interface from the list.

Java Configuration

iDENprotect$^{\text{server}}$ components use JDK (Java Development Kit) 1.7.0, which must be installed on the system before installing iDENprotect$^{\text{server}}$.

However, having both JDK 1.7.0 and JDK 1.8.0 or later installed on the system at the same time is known to cause some conflicts during iDENprotect$^{\text{server}}$ installation, so it is recommended to uninstall all Java 1.8.0 (and later) components:

1. Check currently installed Java version(s):

   ```
   java -version
   ```

2. If Java 1.8.0 (or later) is installed, remove it:

   ```
   sudo yum remove java-1.8.0*
   ```

3. If JDK 1.7.0 is not installed, install the JRE:

   ```
   sudo yum install java-1.7.0-OpenJDK
   ```

4. Verify that only Java 1.7.0 is installed on the system:

   ```
   java -version
   ```

The `\*` wildcard is required to remove JDK (`java-1.8.0-OpenJDK` package) in addition to other Java 1.8.0 components.

If an older Java version is running on the server, it can be left there.

Remove any Existing MySQL Configuration

iDENprotect$^{\text{server}}$ uses MariaDB as its internal database. Having MySQL Server installed on the system is known to cause some conflicts with MariaDB installation, so it is recommended to uninstall the `mysql-server` packages before proceeding with iDENprotect$^{\text{server}}$ installation:

1. Check currently installed MySQL version(s)

   ```
   mysql -V
   ```

2. If the command lists any existing MySQL Server components, remove them

```
sudo yum remove mysql-server*
```

Many RHEL server options come with MySQL preinstalled, so it might be on the system even it has not explicitly been installed at any point.

CentOS Prerequisites for Offline Installation

iDENprotect^{server} is developed and tested primarily on Red Hat Enterprise Linux. While it is possible to install iDENprotect^{server} on CentOS servers, we recommend using RHEL.

Installing iDENprotect^{server} on CentOS requires disabling a number of base CentOS repositories before installation to avoid package conflicts. To disable the repositories:

1. Open `/etc/yum.repos.d/CentOS-Base.repo` in a text editor such as `nano`

   ```
   sudo nano /etc/yum.repos.d/CentOS-Base.repo
   ```

2. Locate repositories labeled `[base]`, `[updates]` and `[extras]`
3. Disable each repository
4. Refresh repositories

   ```
   sudo yum clean all
   ```

Installing iDENprotect^{server}

The installation process takes around 30 minutes depending on server performance. During installation, the following iDENprotect^{server} components are installed:

- iDENprotect^{server} core and iDENprotect^{server} Management Console
- iDENprotect^{server} internal database
- iDENprotect^{server} security hardening functions
- (optional) iDENprotect's Certificate Authority application (EJBCA - Enterprise Java Beans Certificate Authority)

The iDENprotect^{server} is installed from an ISO image file or a DVD disc.

Mounting Installation Media

- If installing from a DVD, mount the DVD drive `/dev/sr0` contents in the `/mnt/iso` directory

```
sudo mkdir /mnt/iso
sudo mount -r -t iso9660 -o loop /dev/sr0 /mnt/iso
```

- If installing from a ISO image file, mount the image contents in the `/mnt/iso` directory

```
sudo mkdir /mnt/iso
sudo mount -r -t iso9660 -o loop [/path/to/iso_image.iso] /mnt/iso
```

Launching the Installer

The install package contains a text wizard script `wizard.sh` for performing a guided iDENprotect^{server} installation. **It must be launched from the mounted directory:**

```
cd /mnt/iso
sudo sh wizard.sh
```

Execution of the wizard script opens a main menu where options can be selected to install and define organisation-specific setup parameters. The two selectable components are the iDENprotect^{server} and the EJBCA PKI Certificate Authority. Unless there is a specific reason for separating their functions on different servers, installing both components on the same server is the simplest way to run iDENprotect^{server}.

> For the purpose of this guide, the components will be installed on the same server. If there are requirements to split the installation across multiple servers, please contact an iDENprotect representative for support and assistance.

In the main menu:

1. Selects the components to be installed (iDENprotect^{server} and EJBCA server for the purpose of this document).

2. Opens [Setup Parameters] view (mandatory before install).
3. Starts the installation process.

Step 1 - select the components to be installed

If the installation is to be built with an EJBCA Certificate Authority then both options should be selected here. If an EJBCA installation already exists, then only the option to install iDENprotect^{server} should be selected.

Step 2 - Configure the Setup Parameters

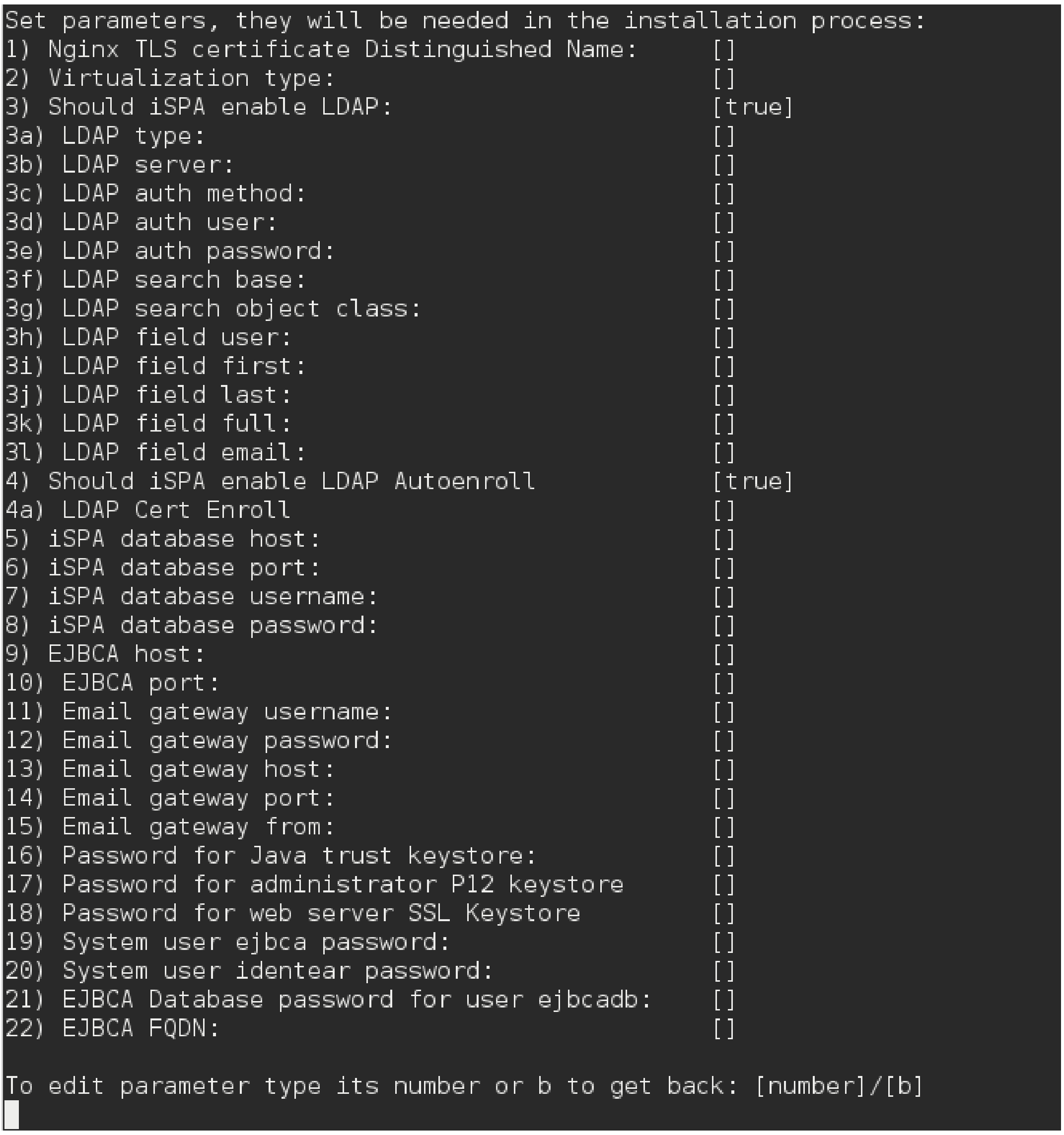
The Setup Parameters define how the installed iDENprotect^{server} operates in the environment. The parameters include configuration options such as database connection settings, web server TLS certificate name, and optional LDAP connection settings. **All of the Setup Parameters must be configured in this step.**

⚠

All passwords entered during installation should match the following security requirements:

- At least 8 characters long
- Includes at least 1 lowercase, 1 uppercase and 1 numeric character
- Do not use special characters.

Failing to meet the password requirements will cause the installation to fail.



```
Set parameters, they will be needed in the installation process:
1) Nginx TLS certificate Distinguished Name:     []
2) Virtualization type:                          []
3) Should iSPA enable LDAP:                      [true]
3a) LDAP type:                                   []
3b) LDAP server:                                 []
3c) LDAP auth method:                            []
3d) LDAP auth user:                              []
3e) LDAP auth password:                          []
3f) LDAP search base:                            []
3g) LDAP search object class:                    []
3h) LDAP field user:                             []
3i) LDAP field first:                            []
3j) LDAP field last:                             []
3k) LDAP field full:                             []
3l) LDAP field email:                            []
4) Should iSPA enable LDAP Autoenroll            [true]
4a) LDAP Cert Enroll                             []
5) iSPA database host:                           []
6) iSPA database port:                           []
7) iSPA database username:                       []
8) iSPA database password:                       []
9) EJBCA host:                                   []
10) EJBCA port:                                  []
11) Email gateway username:                      []
12) Email gateway password:                      []
13) Email gateway host:                          []
14) Email gateway port:                          []
15) Email gateway from:                          []
16) Password for Java trust keystore:            []
17) Password for administrator P12 keystore      []
18) Password for web server SSL Keystore         []
19) System user ejbca password:                  []
20) System user identear password:               []
21) EJBCA Database password for user ejbcadb:    []
22) EJBCA FQDN:                                  []

To edit parameter type its number or b to get back: [number]/[b]
```

Figure 2. iDENprotect^{server} Setup Parameters

Table 1. iDENprotect^{server} Setup Parameters

ID	Name	Example values	Description
1	Nginx TLS certificate Distinguished Name	`/C=US/O=ExampleOrg/OU=IT/CN=iden.example.com`	TLS certificate name used for securing HTTPS web access to the iDENprotect^{server} Maintenance Console interface. The certificate must follow the DN (Distinguished Name) conventions and include at least the following parameters, separated by forward slashes: • C (Country) • O (Organisation) • OU (Organisational Unit) • CN (Common Name) - This must match the FQDN of the iDENprotect^{server}
2	Virtualisation type	`vmware/virtualbox/none`	Configures iDENprotect^{server} for VMWare or Oracle VirtualBox systems

ID	Name	Example values	Description
3	Should iDENprotect^{server} enable LDAP	`true/false`	Enables additional LDAP setup parameters if `true` - required for LDAP integration and user search from iDENprotect^{server}
4	Should iDENprotect^{server} enable LDAP Autoenroll	`true/false`	Enables additional LDAP autoenrollment parameters if `true` - required for auto-enrolment entitlements group
5	iDENprotect^{server} database host	`127.0.0.1`	IP address or hostname of the server that hosts the iDENprotect^{server} database. Usually both the iDENprotect^{server} application and its database are installed on the same server.
6	iDENprotect^{server} database port	`3306`	Port number for the iDENprotect^{server} database. **note: the port must be 3306 for MariaDB.**
7	iDENprotect^{server} database username	`AUTH_SERVER`	Name of the internal iDENprotect^{server} database account
8	iDENprotect^{server} database password		Password for the internal iDENprotect^{server} database account. Minimum password requirements must be met.
9	EJBCA host	`127.0.0.1`	IP address or hostname of the EJBCA server that functions as the Certificate Authority for iDENprotect^{server}. If EJBCA server is running on the same server as iDENprotect^{server}, enter the server's IP address or hostname.
10	EJBCA port	`8443`	Port number used by EJBCA for incoming connections. EJBCA includes a web management panel that is accessible in this port. **Note: this port must be 8443 for EJBCA.**
11	Email gateway username	`idenprotect-admin@example.com`	Email account username for communicating with registered users of the iDENprotect^{server}
12	Email gateway password		Password of the email account
13	Email gateway host	`mail.example.com`	URL of the outbound email server
14	Email gateway port	`25`	Outbound email port (25 = unsecured SMTP)
15	Email gateway from	`idenprotect-admin@example.com`	"From" address for emails sent from the iDENprotect^{server} account
16	Password for Java trust keystore		Password for the internal Java runtime keystore used by EJBCA. Minimum password requirements must be met.
17	Password for administrator P12 keystore		Password for EJBCA administrator P12-format certificate, which is created during installation. The certificate is required for connecting to the EJBCA web management panel. Minimum password requirements must be met.
18	Password for web server SSL keystore		Password for web server's TLS certificate private key. Minimum password requirements must be met.

ID	Name	Example values	Description
19	System user ejbca password		Password for the EJBCA operator UNIX account `ejbca`, which is created during installation. Minimum password requirements must be met.
20	System user identear password		Password for the iDENprotect$^{\text{server}}$ operator UNIX account `identear`, which is created during installation. Minimum password requirements must be met.
21	EJBCA database password for user ejbcadb		Password for the internal EJBCA database account. Minimum password requirements must be met.
22	EJBCA FQDN	`iden.example.com`	Fully Qualified Host Name of the EJBCA server that functions as the Certificate Authority for iDENprotect$^{\text{server}}$. If EJBCA server is running on the same server as iDENprotect$^{\text{server}}$, enter the server's FQDN.

If parameters 3 or 4 are set as `true`, additional LDAP setup parameters become visible. Set the following parameters to integrate iDENprotect$^{\text{server}}$ with your LDAP backend such as Active Directory.

Table 2. Additional LDAP parameters

ID	Name	Example values	Description
3a	LDAP type	`real`	This is a LDAP type parameter for future compatibility. Only currently used value is `real`
3b	LDAP server	`ldap://10.0.1.5:389`	LDAP server IP address and port
3c	LDAP auth method	`simple` / `sasl` / `anonymous`	LDAP authentication method for the authentication user account. Supported methods are Anonymous, Simple and SASL authentication. Dependent on the organisation's LDAP policy.
3d	LDAP auth user	`CN=idenprotect,OU=Service Accounts,DC=example,DC=com`	Full DN (Distinguished Name) for the LDAP authentication user account, with fields separated by commas
3e	LDAP auth password		Password for the LDAP authentication user account
3f	LDAP search base	`OU=Users,DC=example,DC=com`	Full DN for the LDAP search base object
3g	LDAP search ObjectClass	`person` / `top` / `use` / `organisationalPerson`	LDAP search target objectClass
3h	LDAP field user	`uid`	Field name for user ID in the LDAP database
3i	LDAP field first	`givenName`	Field name for user first name in the LDAP database
3j	LDAP field last	`sn`	Field name for user surname in the LDAP database
3k	LDAP field full	`fullName`	Field name for user display name in the LDAP database
3l	LDAP field email	`mail`	Field name for user email address in the LDAP database

ID	Name	Example values	Description
4a	LDAP Cert Enroll	`CN=iDEN_User_Allow,OU=Group,DC=example,DC=com`	Full certificate DN for the LDAP autoenrollment group.

Please check all the values after you have entered them as the installation script will not stop to prompt for further confirmation in case of erroneous values. If the install script fails at some point, the installation process will need to restart from the beginning.

Step 3 - Run the Installation

The install process takes about 30 minutes, depending on the network speed and hardware capability. At some points, especially when initialising the EJBCA database, the installer may seem stuck for up to 3 minutes. This is nothing to be alarmed of as it is intentional.

The installer finishes when the text `Installation completed` is printed on the screen.

Post-install Configuration

Before the iDENprotect$^{\text{server}}$ can be started for the first time, the following must be configured to ensure that the iDENprotect$^{\text{server}}$ is protected against threats and vulnerabilities, and additionally that the CA component functions correctly.

1. Start iDENprotect$^{\text{server}}$ for the first time to verify that installation completed successfully.
2. If using EJBCA, Configure EJBCA Certificate and End Entity profiles.
3. If using Microsoft Exchange, configure Microsoft Exchange to accept anonymous SMTP traffic from iDENprotect$^{\text{server}}$.
4. Install a trusted certificate for the iDENprotect$^{\text{server}}$.

Configuring Firewall

Firewall configuration in RHEL 7 is managed via FirewallD. Apply the recommended following rules for the protection of iDENprotect$^{\text{server}}$. The rules are added with the '--permanaent' switch to ensure the rules are active after a reboot.

1. Ensure the server has public zone set as default:

   ```
   firewall-cmd --get-default-zone
   ```

   The result should read `public`

2. Add the services that are allowed to access the server:

   ```
   firewall-cmd --zone=public --permanent --add-service=https
   ```

3. Add allowed incoming ports:

   ```
   firewall-cmd --zone=public --permanent --add-port=8443/tcp
   firewall-cmd --zone=public --permanent --add-port=443/tcp
   firewall-cmd --zone=public --permanent --add-port=22/tcp
   ```

4. Add allowed outgoing ports:

   ```
   firewall-cmd --permanent --direct --add-rule ipv4 filter OUTPUT 0 -p tcp -m
   tcp  --dport=25 -j ACCEPT
   firewall-cmd --permanent --direct --add-rule ipv4 filter OUTPUT 1 -p tcp -m
   tcp --dport=53 -j ACCEPT
   ```

5. Ensure all added ports are listed in the firewall status message:

   ```
   firewall-cmd --zone=public --permanent --list-all
   firewall-cmd --permanent --direct --get-all-rules
   ```

6. Restart the firewall and nginx web server services:

   ```
   systemctl restart firewalld.service
   systemctl restart nginx.service
   ```

If the iDENprotect^{server} is to be connected remotely over SSH after installation, enable incoming port 22 and save the firewall settings:

```
iptables -I INPUT 1 -p tcp --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables-save
```

Starting iDENprotect^{server} for the First Time

iDENprotect^{server} is started with the `/opt/identear/ispa.sh` script that's created during the installation process. If the installation script (wizard.sh) was executed using the root user then the script must be ran using the root user. Otherwise, it is recommended to run the script using the `identear` user account created during iDENprotect^{server} installation:

1. Open a terminal window.
2. Run the startup script:

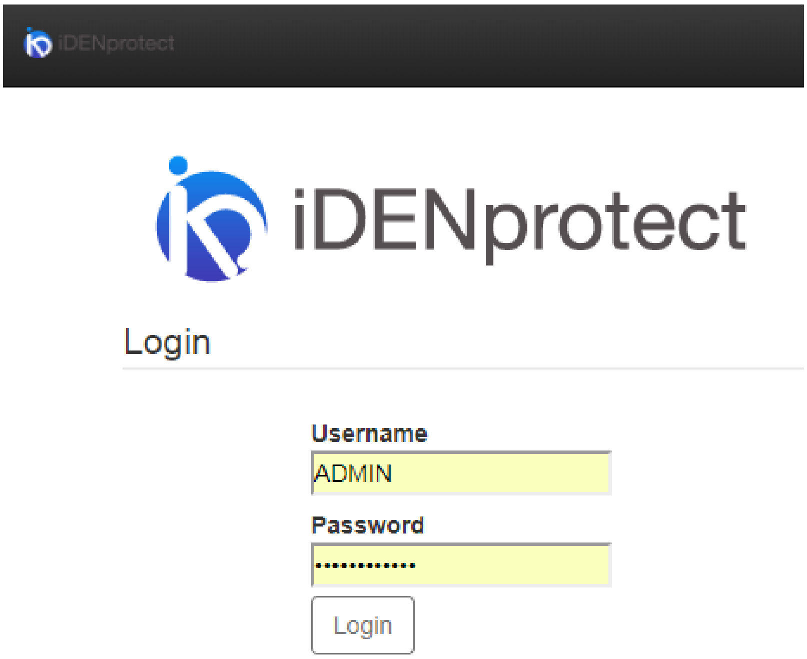
   ```
   cd /opt/identear
   sh ispa.sh
   ```

The startup script takes about 30 seconds to launch iDENprotect^{server}. The script launches iDENprotect^{server} as a background process and keeps the current terminal window active.

To check the iDENprotect^{server} status when it is running, poll the `/opt/identear/ispa_log.out` log file (for example, with command `cat  /opt/identear/ispa_log.out`. When the iDENprotect^{server} startup process is finished, the last message on the log file says `Successfully released change log lock`.

Accessing iDENprotect^{server}

To open the iDENprotect^{server} Management Console, open a web browser and go to the iDENprotect^{server} URL or IP address set during installation, such as `https://iden.mydomain.com`. The webpage shows the iDENprotect^{server} Management Console login screen.



Login

Username

ADMIN

Password

••••••••••••

Figure 3. iDENprotect^{server} login screen

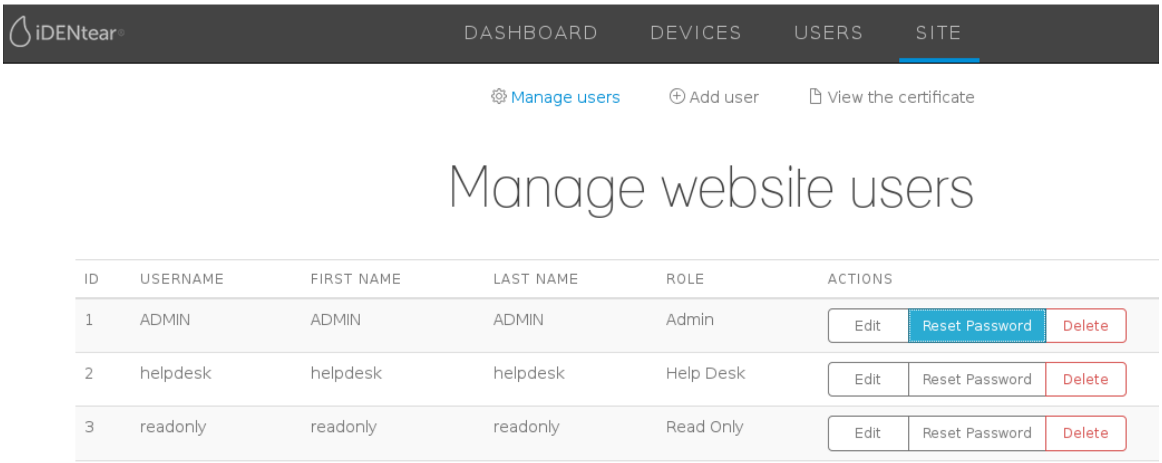
Log in with the default administrator user account:

- User name: *ADMIN*
- Password: *1detearAdm1n*

Changing Default Admin Password

It is highly recommended that the iDENprotect^{server} Management Console Administrator password should be changed from the default:

1. Open the **Site** panel.
2. **Manage Users** subview is opened by default. Locate the `ADMIN` user from the list.
3. Click the **Reset Password** button and enter a new password for the `ADMIN` account.



Manage website users

ID	USERNAME	FIRST NAME	LAST NAME	ROLE	ACTIONS
1	ADMIN	ADMIN	ADMIN	Admin	Edit Reset Password Delete
2	helpdesk	helpdesk	helpdesk	Help Desk	Edit Reset Password Delete
3	readonly	readonly	readonly	Read Only	Edit Reset Password Delete

Figure 4. Resetting ADMIN password

Configuring Microsoft Exchange

The iDENprotect$^{\text{server}}$ is configured by default to send email on port 25 of the selected SMTP Server using SMTP Basic Authentication.

If the SMTP Server in use is Microsoft Exchange, authentication between Exchange and the iDENprotect$^{\text{server}}$ may cause issues. In these specific scenarios, a Receive Connector should be configured that accepts anonymous users.

Configuring the Full Receive Connector is referenced within the following Microsoft TechNet resource. As a general guide, the process can be outlined as:

1. Open **Exchange Management Console**
2. Open **Server Configuration**
3. Select **Hub Transport**
4. Select **Receive Connectors**
5. Add new **Custom Receive Connector**
6. Provide a name for the Connector, for example **iDENprotect Connector**
7. Go to the **Network** tab
8. Enter the internal IP Address of iDENprotect$^{\text{server}}$ in the list **Receive mail from remote servers that have these IP addresses**
9. Go to the **Authentication Tab**
10. Select **Basic Authentication**
11. Go to the **Permission Groups** tab and select as appropriate e.g. Anonymous Users

Installing a Trusted Certificate

In order to handle web connections securely, the iDENprotect$^{\text{server}}$ must use a valid publicly trusted digital certificate. If no valid certificate has been configured, iDENprotect devices will not be able to communicate with the iDENprotect$^{\text{server}}$.

Generating Private Key and CSR

1. In the iDENprotect$^{\text{server}}$ terminal, create a new 2048-bit RSA key using OpenSSL:

   ```
   openssl req -new -newkey rsa:2048 -nodes -keyout server.key -out server.csr
   ```

   Change the name of `server.key` and `server.csr` to the hostname of iDENprotect$^{\text{server}}$. For example, if the hostname is `iden.domain.com`, name the files `iden.key` and `iden.csr`.

   This starts the process of generating 2 files: a **private key** file for decrypting TLS traffic and a CSR (Certificate Signing Request) file

2. Enter the organisational and geographic information for the certificate
3. When prompted for the **Common Name**, enter the fully qualified domain name of the iDENprotect$^{\text{server}}$. For example, `iden.domain.com`.
4. Enter an email address for contact information regarding the certificate

Signing the CSR

Once the CSR file is created, send it to the CA (Certificate Authority) that is to be used for TLS web connection certificates. The reply from the CA typically contains the signed certificate chain in a `.pem` or `.crt` file. This file is the **public key** of iDENprotect^{server}. Store it on the iDENprotect^{server} computer. If an option is given to sign a certificate for a specific web server, select NGINX bundle.

> If the CSR file contents are being copy-pasted, make sure to include all of them. Many CSRs fail because the BEGIN and END lines were not included in the request.

Installing the Certificates

To set up TLS for iDENprotect^{server}, both keys must be stored on the server and configured in nginx:

1. Copy the `.key` file and the CRT or PEM received from the CA in the `/var/certs` directory
2. Edit `/etc/nginx/nginx.conf` and add the locations for the keys `ssl_certificate` and `ssl_certificate_key`

   ```
   ssl_certificate: /var/certs/my_domain_name.pem; (or bundle.crt)
   ssl_certificate_key: /var/certs/my_domain_name.key;
   ```

   > Adjust the file names to match the certificate files on your file system.

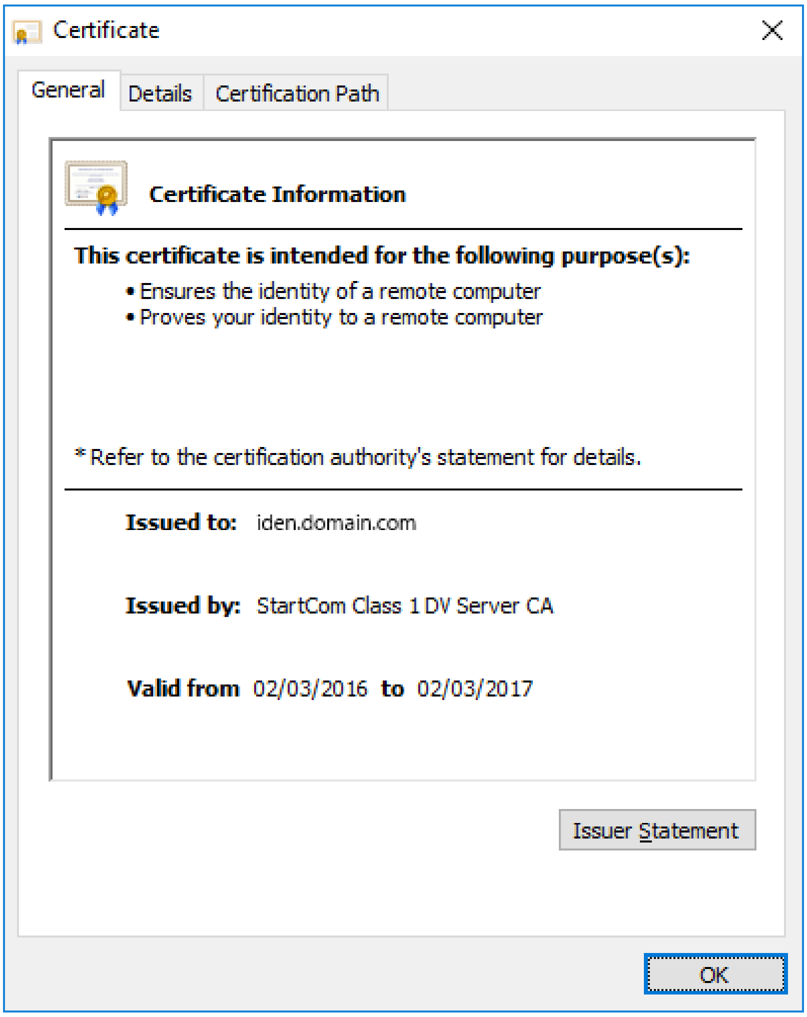
3. Restart the nginx web server:

   ```
   systemctl restart nginx
   ```

Testing the Certificate

Open a web browser and enter the URL for the iDENprotect^{server}. The browser should not alert to any certificate validation errors.

Depending on the browser, there should be a padlock or similar icon in the address bar, which means that the iDENprotect^{server} now has a trusted certificate for the web site.



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer
- Proves your identity to a remote computer

* Refer to the certification authority's statement for details.

Issued to: iden.domain.com

Issued by: StartCom Class 1 DV Server CA

Valid from 02/03/2016 **to** 02/03/2017

Figure 5. Certificate information

Troubleshooting

'sudo' Commands Do Not Work

In some RHEL installations, access to the `sudo` command is restricted. Usually this results in error message "Username is not in the sudoers file."

The default RHEL setup is to allow `sudo` commands only for users belonging to the `wheel` group. Since the initial `wheel` group contains no user accounts, no users can perform `sudo` actions.

To add a user to the `wheel`:

1. Log in as root, or change to the root account with the `su` command.
2. Add the user account to `wheel` with the `usermod` command:

   ```
   usermod -aG wheel <USERNAME>
   ```

For more information on diagnosing `sudo` issues, see Configuring sudo Access in Red Hat Enterprise Linux Getting Started Guide.

There is no Network Connectivity

Check that you have Internet connectivity by pinging a publicly available IP address such as `8.8.8.8`:

```
ping 8.8.8.8
```

Also check that your server is configured so that the it can resolve its own FQDN and ping itself (replace `iden.example.com` with your own server hostname):

```
ping iden.example.com
```

If the ping request returns replies, verify that the response address of the ping is the same IP address as the server's network interface IP address:

```
ifconfig -a
```

If the ping request times out, add the server's network interface IP address, the server's hostname, and the server's FQDN to `/etc/hosts`:

```
nano /etc/hosts
```

See Hostname Configuration for more information.

EJBCA Installation is not Finishing Correctly

Most of the EJBCA issues are due to one of two things:

1. Unresolvable or inconsistent hostname/FQDN (Fully Qualified Domain Name)
2. EJBCA passwords not meeting complexity requirements

Unresolvable hostname

During installation, the server hostname/FQDN is set in install wizard setup parameters 1, 9, and 22. If there are inconsistencies between the parameters, the EJBCA installation fails.

You can find the FQDN parameters on the server with the following commands:

Table 3. Verifying EJBCA FQDN Parameters

Command	Description	Example value
`hostname`	Hostname of your EJBCA server	`iden.example.com`
`cat /opt/identear/ispa.sh`	Environment variable `EJBCA_HOST` in the `/opt/identear/ispa.sh` launch script	`export EJBCA_HOST=ispa.example.com`
`cat /etc/hosts`	Hostname and FQDN mapped to your IP address in the server's `etc/hosts` file	`12.34.56.78 iden iden.example.com`

If the hostname/FQDN in `hosts` or `ispa.sh` differs from the server's hostname, correct it in the files and try restarting iDENprotect$^{\text{server}}$. If EJBCA still doesn't work, repeat the whole installation process.

Strength and validity of EJBCA Passwords.

EJBCA requires stronger passwords than other parts of the Wizard installation. All EJBCA passwords must be at least 8 characters and contain numbers and both uppercase and lowercase letter.

Using special characters is generally good policy, but some special characters are may be stored incorrectly, which causes EJBCA to fail. We advise against using special characters in iDENprotect$^{\text{server}}$ passwords.

An example of a suitable password would be: `s3cR3TP445W0rD`

iDENprotect$^{\text{server}}$ doesn't Integrate with LDAP

First, verify that LDAP integration, and optionally also LDAP autoenrollment (setup parameters \#3 and \#4) were enabled during installation. Read the contents of the `/opt/identear/ispa.sh` configuration file:

```
cat /opt/identear/ispa.sh
```

You should see parameters `-Dldap.enabled` and optionally `-Dldap.autoenroll.enabled` set as `true`.

LDAP parameters are not enabled

If parameters `-Dldap.enabled` and `-Dldap.autoenroll.enabled` are set as `false`, we recommend reinstalling the iDENprotect^{server}. When entering setup parameters during reinstall, make sure that you enable LDAP:

```
3) Should {server} enable LDAP:                [true]
4) Should {server} enable LDAP Autoenroll      [true]
```

LDAP parameters are enabled, but LDAP integration still fails

There are a number of essential parameters that iDENprotect^{server} uses when connecting to the LDAP server. If any of them are incorrect, LDAP connection likely fails.

The LDAP connection parameters are set in the `/opt/identear/ispa.sh` script. They are the lines beginning with `-Dldap`. Make sure that each of them matches your LDAP server configuration.

For more information, see idenprotect-administrator-guide.pdf in iDENprotect^{server} Administrator Guide.

ispa.sh Script doesn't Launch iDENprotect^{server} Succesfully

After you have launched iDENprotect^{server} with the `/opt/identear/ispa.sh` script, you should see some diagnostic texts followed by the `Successfully released change log lock` text in the terminal. After this, the iDENprotect^{server} Management Console should be available for web browser login in the IP address or hostname of your server.

If the `ispa.sh` script returns errors and doesn't launch the iDENprotect^{server} correctly, the reason may be firewall settings or SELinux (Security-Enhanced Linux) settings which have been set in the installation phase.

Checking SELinux settings

Check the status of SELinux:

```
sestatus
```

This returns either `SELinux status: permissive` or `SELinux status: enabled` depending on whether SELinux is running on permissive or fully enabled mode, respectively.

If SELinux was set as `enabled`, set it to `permissive`. Then restart nginx web server:

```
setenforce 0
systemctl restart nginx
```

Next, restart iDENprotect^{server} with the `/opt/identear/ispa.sh` script. If the iDENprotect^{server} launches normally, you can leave SELinux set as `permissive` and continue using iDENprotect^{server}.

Checking Firewall settings

If iDENprotect^{server} launch still fails, check if your Linux Firewall is blocking it:

```
systemctl stop firewalld
systemctl restart nginx
```

Next, restart iDENprotect$^{\text{server}}$ with the `/opt/identear/ispa.sh` script. iDENprotect$^{\text{server}}$ should launch normally. If iDENprotect$^{\text{server}}$ launches normally after disabling the firewall, one or more firewall rules are causing conflicts with iDENprotect$^{\text{server}}$ configuration.

We don’t recommend running iDENprotect$^{\text{server}}$ without a firewall. You should go through the firewall settings listed in `iptables` and remove all that are not listed in section [Firewall Configuration].

For more information on configuring firewall on RHEL 7, see:

https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Security_Guide/sec-Using_Firewalls.html

I can’t Access iDENprotect$^{\text{server}}$ Management Console with Web Browser

If the nginx web server is running but not set up correctly, you will see an error reporting *502 Bad Gateway* in the iDENprotect$^{\text{server}}$ URL (`https://iden.example.com`).

First, make sure that you are connecting to the HTTPS address of the server (**https**://iden.example.com)

Next, check the iDENprotect$^{\text{server}}$ hostname settings from [Why isn’t my EJBCA installation finishing correctly?]. If there are discrepancies in the hostname configuration files, correct them.

If you are connecting to the iDENprotect$^{\text{server}}$ from an external computer, there may be a temporary issue with the iDENprotect$^{\text{server}}$ DNS resolution. Try to connect only with the iDENprotect$^{\text{server}}$ IP address (`https://12.34.56.78`)

Appendix A: Installing RHEL

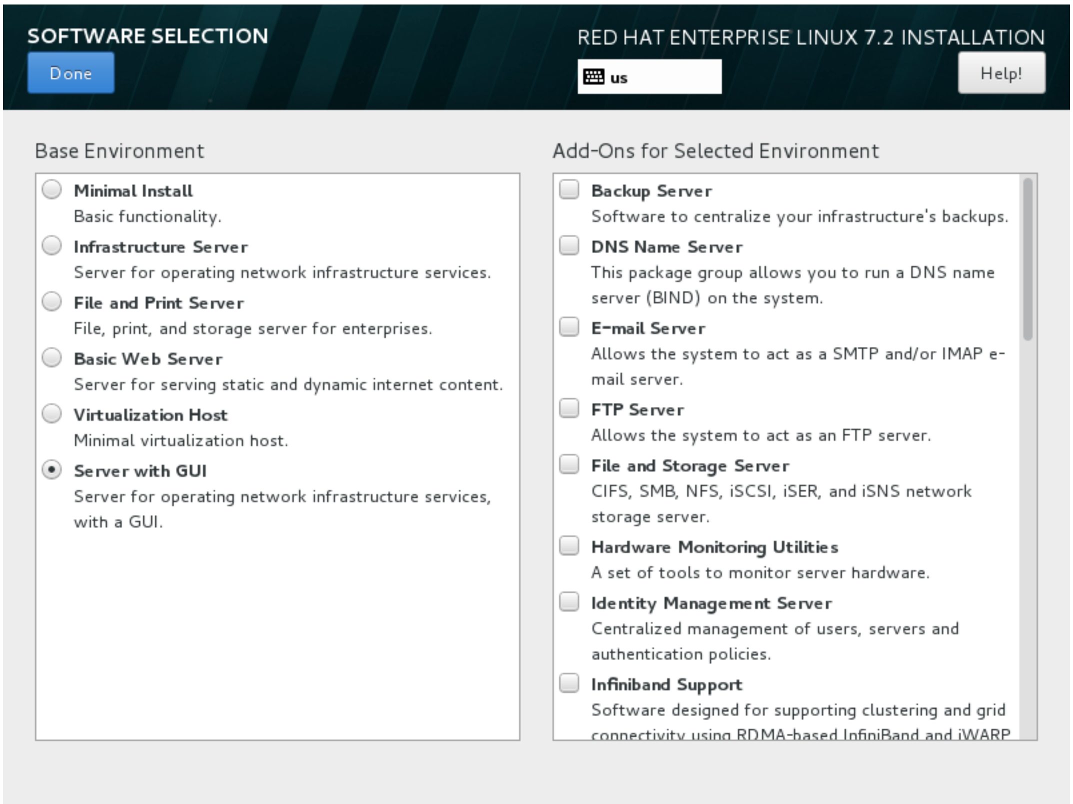
> This section can be skipped if a RHEL 7 Linux system already exists that meets the [prerequisites].

This section provides a brief walkthrough of installing RHEL 7 on an empty hard drive. For complete installation instructions, refer to RHEL 7 Installation Guide.

After launching the RHEL 7 installer and selecting the install language, the **Installation Summary** screen is displayed. Do the following steps to launch the RHEL 7 installation process:

1. Set up the localisation settings:
   a. Open the **Date & Time** window and select the time zone
   b. Open the **Keyboard** window and select the keyboard layout
2. Select the server base environment type:
   a. Open the **Software Selection** window
   b. Select either **Minimal Install** or **Server with GUI**

   iDENprotect$^{\text{server}}$ itself does not require a GUI, but having access to a graphical internet browser (which comes bundled on **Server with GUI**) on the server is helpful when performing initial iDENprotect$^{\text{server}}$ setup.



Base Environment

○ **Minimal Install**
Basic functionality.

○ **Infrastructure Server**
Server for operating network infrastructure services.

○ **File and Print Server**
File, print, and storage server for enterprises.

○ **Basic Web Server**
Server for serving static and dynamic internet content.

○ **Virtualization Host**
Minimal virtualization host.

● **Server with GUI**
Server for operating network infrastructure services, with a GUI.

Add-Ons for Selected Environment

□ **Backup Server**
Software to centralize your infrastructure's backups.

□ **DNS Name Server**
This package group allows you to run a DNS name server (BIND) on the system.

□ **E-mail Server**
Allows the system to act as a SMTP and/or IMAP e-mail server.

□ **FTP Server**
Allows the system to act as an FTP server.

□ **File and Storage Server**
CIFS, SMB, NFS, iSCSI, iSER, and iSNS network storage server.

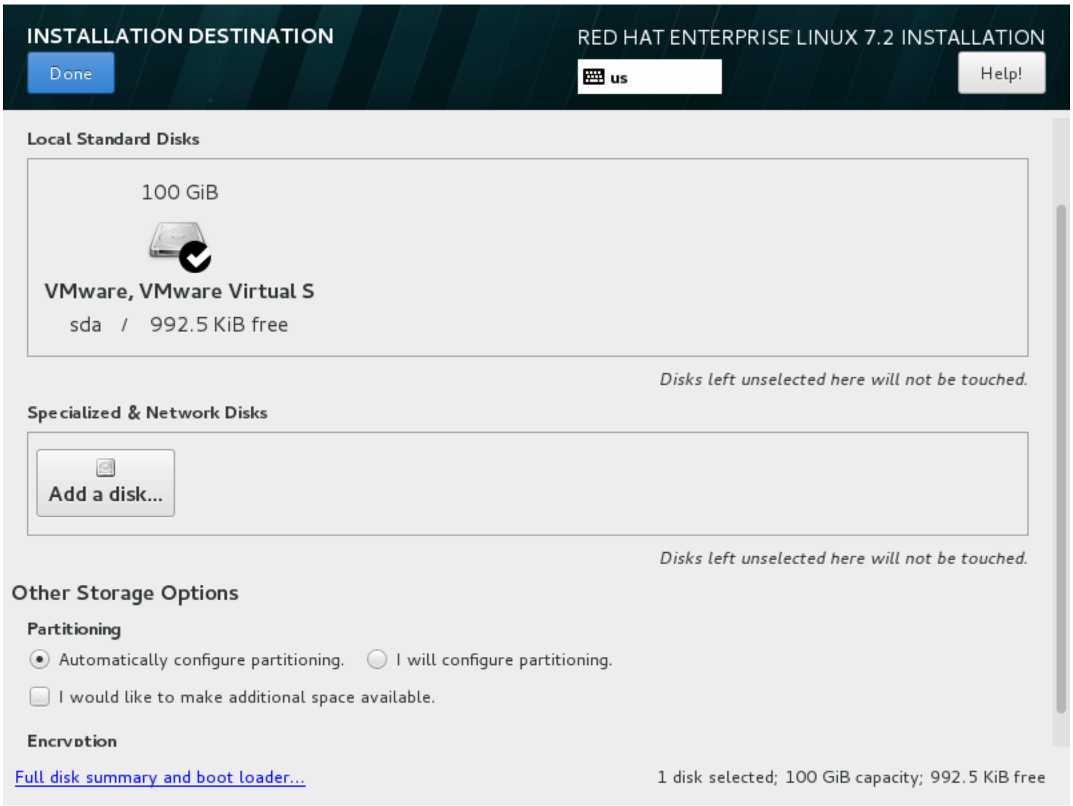
□ **Hardware Monitoring Utilities**
A set of tools to monitor server hardware.

□ **Identity Management Server**
Centralized management of users, servers and authentication policies.

□ **Infiniband Support**
Software designed for supporting clustering and grid connectivity using RDMA-based InfiniBand and iWARP

Figure 6. Selecting server type

3. Set up automatic partitioning:
   a. Open the **Installation Destination** window
   b. Leave all settings as they are and click **Done**


INSTALLATION DESTINATION
Done
RED HAT ENTERPRISE LINUX 7.2 INSTALLATION
us
Help!

Local Standard Disks

100 GiB

VMware, VMware Virtual S

sda / 992.5 KiB free

Disks left unselected here will not be touched.

Specialized & Network Disks

Disks left unselected here will not be touched.

Other Storage Options

Partitioning

● Automatically configure partitioning. ○ I will configure partitioning.

□ I would like to make additional space available.

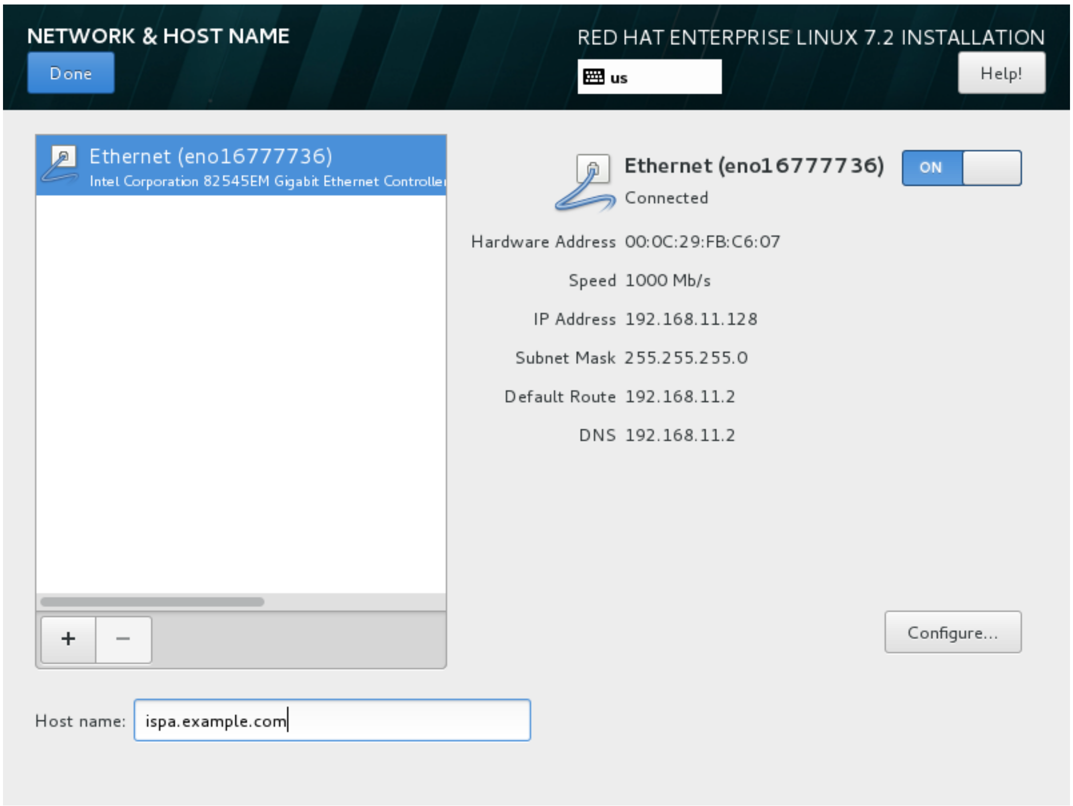
Encryption

Full disk summary and boot loader...

1 disk selected; 100 GiB capacity; 992.5 KiB free

Figure 7. Setting up partitioning

4. Set up the network settings:
   a. Open the **Network & Hostname** window
   b. Enter the FQDN (Fully-Qualified Domain Name) of the server in the **Host name** field



Ethernet (eno16777736)
Intel Corporation 82545EM Gigabit Ethernet Controlle

Ethernet (eno16777736) ON
Connected

Hardware Address 00:0C:29:FB:C6:07

Speed 1000 Mb/s

IP Address 192.168.11.128

Subnet Mask 255.255.255.0

Default Route 192.168.11.2

DNS 192.168.11.2

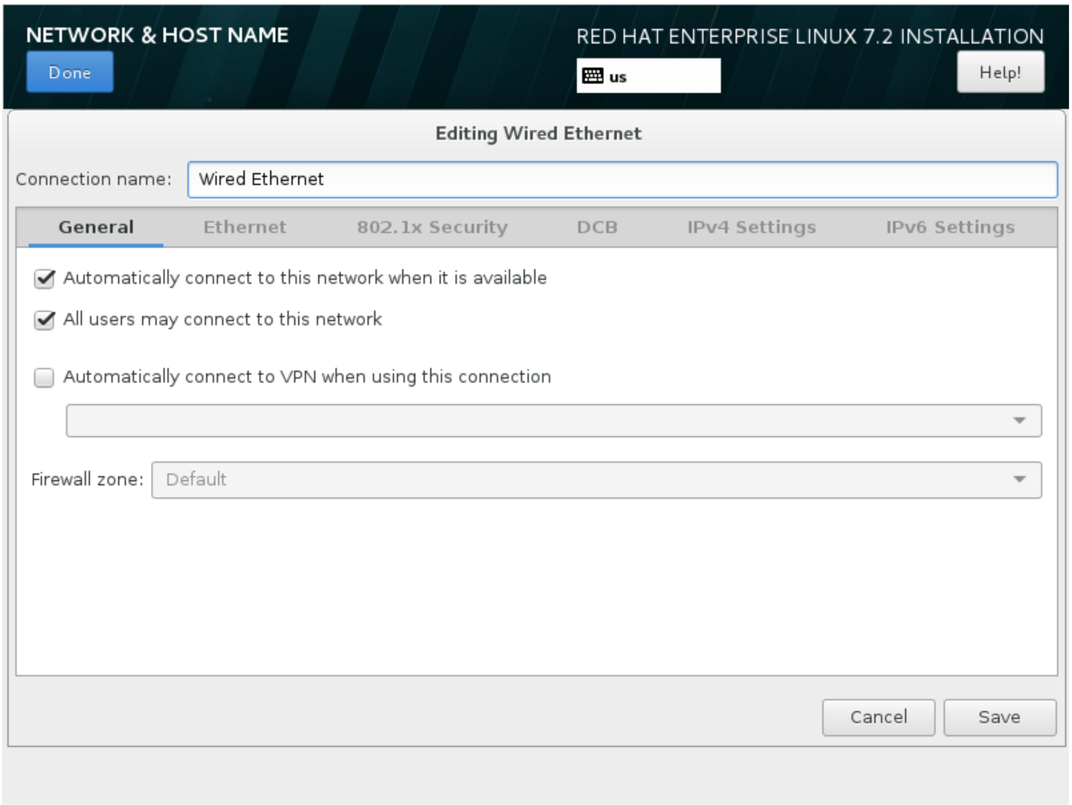
Host name: ispa.example.com

Figure 8. Setting up FQDN

c. Enable the Ethernet interface by clicking on the **On/Off** button

d. Click **Configure**

e. In the **General** tab, enable the **Automatically connect to this network when it is available** checkbox



Connection name: Wired Ethernet

☑ Automatically connect to this network when it is available

☑ All users may connect to this network

□ Automatically connect to VPN when using this connection

Firewall zone: Default

Figure 9. Enabling the network connection

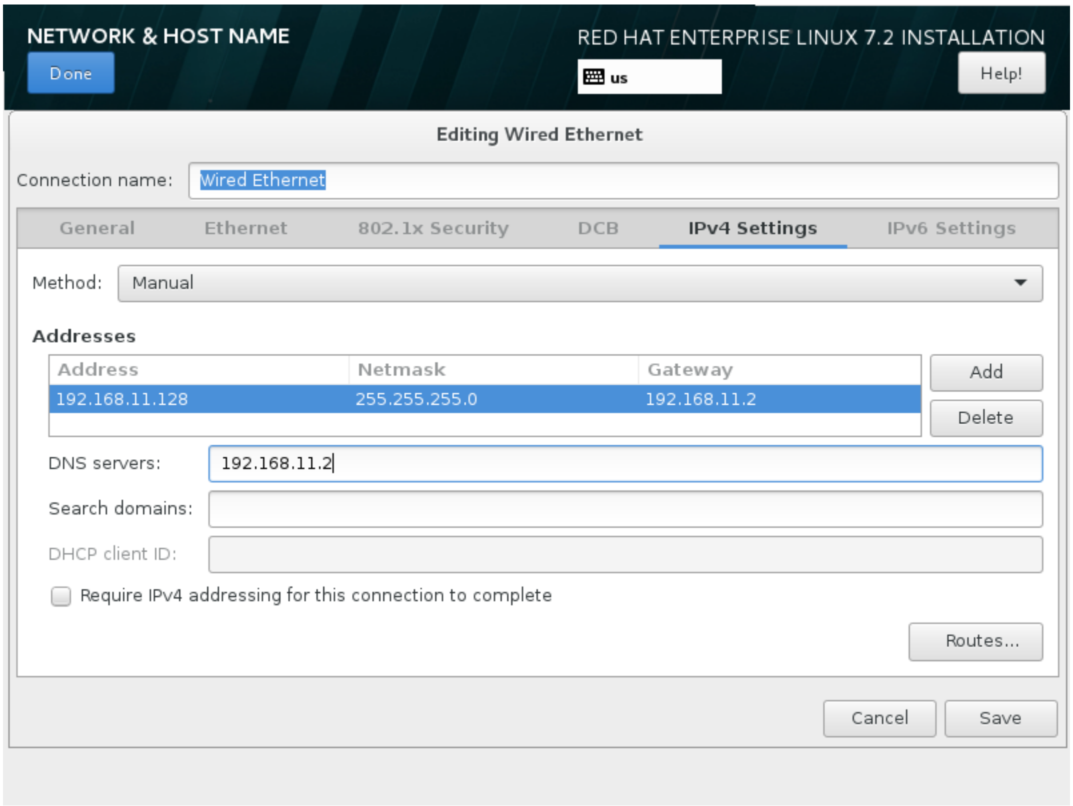
f. In the **IPv4 Settings** tab, set up static IP address for the server:

  i. Choose the **Manual** option in the **Method** drop-down menu

  ii. Click **Add** to add a new IP address

  iii. Enter the **Address**, **Netmask**, and **Gateway** of the server

  iv. Enter at least 1 DNS server IP address in the **DNS servers** field



Connection name: Wired Ethernet

Method: Manual

Addresses

Address	Netmask	Gateway
192.168.11.128	255.255.255.0	192.168.11.2

DNS servers: 192.168.11.2

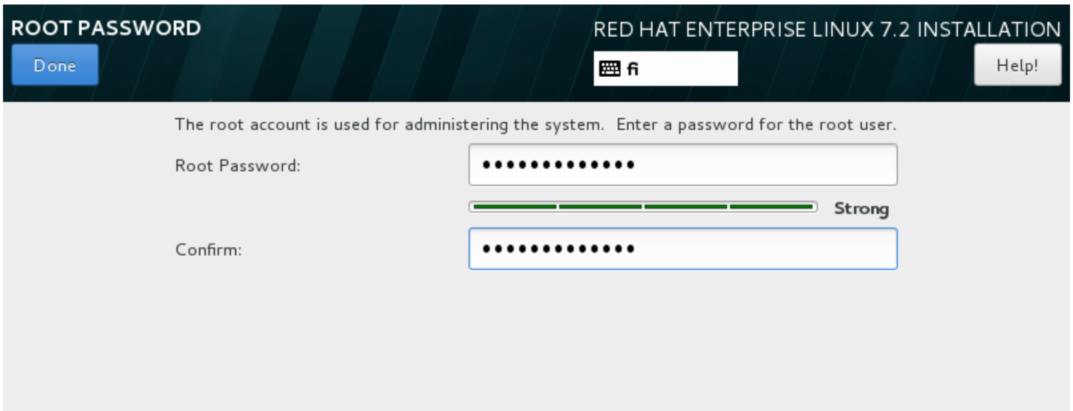
Search domains:

DHCP client ID:

□ Require IPv4 addressing for this connection to complete

Figure 10. Configuring IP addresses

5. Click **Begin Installation**
6. Set up a password for the built-in `root` user account:
   a. Open the **Root Password** window
   b. Enter and confirm a secure root password in the **Root Password** and **Confirm** fields



The root account is used for administering the system. Enter a password for the root user.

Root Password: •••••••••••••

Confirm: •••••••••••••

Figure 11. Setting root password

7. Wait for the installation to finish and reboot the server