

## Secure Sphere 初期セットアップ手順

ネットワークバリューコンポネンツ  
エンジニアリング部

---

## 目次

---

1.1	初期セットアップ(MX サーバ).....	3
1.2	初期セットアップ(GW) .....	10
1.3	初期セットアップ(OneBox).....	18

## 1.1 初期セットアップ(MX サーバ)

OS インストール後にログインプロンプト画面が表示されますので

以下ユーザアカウントでログインします。初期ユーザ、初期パスワードでログイン後以下のようにパスワードの変更を求められるのでメッセージに従い入力します。

login:**admin**

Password:**admin**

You are required to change your password immediately (root enforced)

Changing password for admin.

(current) UNIX password:**admin** ← (実際にはエコーバックしません)

New password: ← (実際にはエコーバックしません)

Retype new password: ← (実際にはエコーバックしません)

login: **admin**

Password: ←**admin** と入力します

You are required to change your password immediately (root enforced)

Changing password for admin.

(current) UNIX password: ←**admin** と入力します

New password: ←**admin** ユーザの新パスワードを設定します

Retype new password:

Last login: Fri Mar 31 01:22:13 on ttyS0

Welcome to SecureSphere Shell

Type "ftl" to complete deployment

SecureSphere>

SecureSphere>**ftl**

Welcome to Imperva's configuration tool !!!

Initial setup mode.

The machine has been identified as a "management" type appliance.

The SecureSphere "Management Server" component will be activated.

You will now set up the "management" interface, which connects  
the SecureSphere appliances.

The default "management" interface for this appliance is "eth0".

Do you want to change it? [y/n]: **n**

Classless Inter-domain Routing (CIDR) notation explicitly specifies the number of bits in an IP address denoting the network, in contrast to the netmask notation which indirectly specifies the number of bits. For example, a netmask of 255.255.255.0 indicates (for IPv4 addresses) the first 24 bits of an IP address denote the network. In CIDR notation, one simply writes /24 after the IP address (for example, 123.124.125.126/24).

IP configuration for the management interface "eth0".

IP Address [IP Address/CIDR]: **172.16.13.45/24**

Do you want to set IPv6 Address as well? [y/n]: **n**

You can optionally set an Ethernet interface that will connect the appliance to a LAN (Local Area Network). You can use one of the on-board Ethernet interfaces.

Do you want to set a LAN interface? [y/n]: **n**

You can (optionally) set a default gateway.

Do you want to set an IPv4 default gateway? [y/n]: **y**

You will be asked for the IPv4 default gateway's Address and an optional device.

If you specify a device:

It should be one of the onboard Ethernet interfaces (eth0 eth1).

If you don't specify a device:

The default gateway must be reachable through one of the onboard interfaces.

The route will become available when the appliance boots and remain available until it shuts down.

Gateway [IPv4 Address reachable from onboard interface]: **172.16.13.1**

Do you want to specify a device? [y/n]: **n**

You can configure a DNS client. (optional)

Do you want to configure a DNS client? [y/n]: **y**

Domain name [Domain name, or none]: **none**

Domain search list [Space separated list of domains, or none]: **none**

Name servers [Space separated list of IPv4 Addresses, or none]: **172.16.7.99**

Set the password for the Linux "root" user. This password will also be used as the grub bootloader password.

Enter password [Please enter a strong password. Password must be 7 - 14 characters long. It must contain a combination of: numbers, lower-case characters, and at least 1 of the following character groups: upper-case characters or special characters. The password cannot contain 3 or more consecutive repeating characters]: ←**root** ユーザ、**bootloader** のパスワードを入力します

Re-enter password: ←再度 **root** ユーザ、**bootloader** のパスワードを入力します

The user "secure" (the SecureSphere administrative user) is used to register the SecureSphere Gateway with a SecureSphere Management Server.

If the password is changed, the SecureSphere Management Server will be restarted when the changes are applied.

Enter password [Please enter a strong password. Password must be 7 - 14 characters long. It must contain a combination of: numbers, lower-case characters, and at least 1 of the following character groups: upper-case characters or special characters. The password cannot contain 3 or more consecutive repeating characters]: ←secure パスワードを入力します

Re-enter password: ←再度 secure パスワードを入力します

Set the password for the SecureSphere "system" user (database administrator)

Enter password [Please enter a strong password. Password must be 7 - 14 characters long. It must contain a combination of: numbers, lower-case characters, and at least 1 of the following character groups: upper-case characters or special characters. The password cannot contain 3 or more consecutive repeating characters]: ←system パスワードを入力します

Re-enter password: ←再度 system パスワードを入力します

Assign a name to the host

Host name [Short or FQDN (separated by .) hostname, where each part starts with a letter and consists of the following: letters, digits, \_ or -]: m100-v12-0-42

You will now select a time zone

Please identify a location so that time zone rules can be set correctly.

Please select a continent or ocean.

- 1) Africa
- 2) Americas
- 3) Antarctica
- 4) Arctic Ocean
- 5) Asia
- 6) Atlantic Ocean
- 7) Australia

- 8) Europe
- 9) Indian Ocean
- 10) Pacific Ocean
- 11) none - I want to specify the time zone using the Posix TZ format.

5

#? Please select a country.

- |                |                     |                          |
|----------------|---------------------|--------------------------|
| 1) Afghanistan | 18) Israel          | 35) Palestine            |
| 2) Armenia     | 19) Japan           | 36) Philippines          |
| 3) Azerbaijan  | 20) Jordan          | 37) Qatar                |
| 4) Bahrain     | 21) Kazakhstan      | 38) Russia               |
| 5) Bangladesh  | 22) Korea (North)   | 39) Saudi Arabia         |
| 6) Bhutan      | 23) Korea (South)   | 40) Singapore            |
| 7) Brunei      | 24) Kuwait          | 41) Sri Lanka            |
| 8) Cambodia    | 25) Kyrgyzstan      | 42) Syria                |
| 9) China       | 26) Laos            | 43) Taiwan               |
| 10) Cyprus     | 27) Lebanon         | 44) Tajikistan           |
| 11) East Timor | 28) Macau           | 45) Thailand             |
| 12) Georgia    | 29) Malaysia        | 46) Turkmenistan         |
| 13) Hong Kong  | 30) Mongolia        | 47) United Arab Emirates |
| 14) India      | 31) Myanmar (Burma) | 48) Uzbekistan           |
| 15) Indonesia  | 32) Nepal           | 49) Vietnam              |
| 16) Iran       | 33) Oman            | 50) Yemen                |
| 17) Iraq       | 34) Pakistan        |                          |

19

#?

The following information has been given:

Japan

Therefore TZ='Asia/Tokyo' will be used.

Local time is now: Fri Mar 31 11:03:58 JST 2017.

Universal Time is now: Fri Mar 31 02:03:58 UTC 2017.

Is the above information OK?



1) Yes

2) No

1

#?

You can configure an NTP client. (recommended)

Do you want to configure an NTP client? [y/n]: **y**

NTP servers [Space separated list of IPv4 Addresses]: **172.16.7.99**

NOTE:

The SecureSphere Management Server has been activated on this machine.  
The database is about to be created. This may take a while.

NOTE:

A transaction that will activate these settings is about to start.

You can use another terminal session to monitor it with:

impctl show log.

NOTE:

During the settings activation, the hardening settings will be configured.  
Part of these settings include setting a timeout on inactive shell sessions  
as well as denying access to 'root' user over SSH.  
If you have open shell sessions, please close them all after all the settings  
have been activated in order for the hardening settings to be properly  
applied.

Press <ENTER> to continue: **←Enter を押します**

-----設定が反映されるまで 40~60 分程度必要となります-----

【図 1 初期セットアップ(MX サーバ)】

## 1.2 初期セットアップ(GW)

OS インストール後にログインプロンプト画面が表示されますので

以下ユーザアカウントでログインします。初期ユーザ、初期パスワードでログイン後以下のようにパスワードの変更を求められるのでメッセージに従い入力します。

login:admin

Password:admin

You are required to change your password immediately (root enforced)

Changing password for admin.

(current) UNIX password:admin ←(実際にはエコーバックしません)

New password: ←(実際にはエコーバックしません)

Retype new password: ←(実際にはエコーバックしません)

login: **admin**

Password: ←**admin** と入力します

You are required to change your password immediately (root enforced)

Changing password for admin.

(current) UNIX password:←**admin** と入力します

New password:←**新しいパスワードを設定します**

Retype new password:

Last login: Fri Mar 31 04:09:54 on ttyS0

Welcome to SecureSphere Shell

Type "ftl" to complete deployment

SecureSphere>

SecureSphere>**ftl**

Welcome to Imperva's configuration tool !!!

Initial setup mode.

The machine has been identified as a "Gateway" type appliance (asset-tag: X4500).

Do you want to activate the SecureSphere Management Server [y/n]: **n**

Is this gateway deployed in order to replace another gateway ? [y/n]: **n**

You will now set up the "management" interface, which connects the SecureSphere appliances.

The default "management" interface for this appliance is "eth0".

Do you want to change it? [y/n]: **n**

Classless Inter-domain Routing (CIDR) notation explicitly specifies the number of bits in an IP address denoting the network, in contrast to the netmask notation which indirectly specifies the number of bits. For example, a netmask

of 255.255.255.0 indicates (for IPv4 addresses) the first 24 bits of an IP address denote the network. In CIDR notation, one simply writes /24 after the IP address (for example, 123.124.125.126/24).

IP configuration for the management interface "eth0".

IP Address [IP Address/CIDR]: **172.16.13.46/24**

Do you want to set IPv6 Address as well? [y/n]: **n**

You can optionally set an Ethernet interface that will connect the appliance to a LAN (Local Area Network). You can use one of the on-board Ethernet interfaces.

Do you want to set a LAN interface? [y/n]: **n**

You can (optionally) set a default gateway.

Do you want to set an IPv4 default gateway? [y/n]: **y**

You will be asked for the IPv4 default gateway's Address and an optional device.

If you specify a device:

It should be one of the onboard Ethernet interfaces (eth0 eth1).

If you don't specify a device:

The default gateway must be reachable through one of the onboard interfaces.

The route will become available when the appliance boots and remain available until it shuts down.

Gateway [IPv4 Address reachable from onboard interface]: **172.16.13.1**

Do you want to specify a device? [y/n]: **n**

You can configure a DNS client. (optional)

Do you want to configure a DNS client? [y/n]: **y**

Domain name [Domain name, or none]: **none**

Domain search list [Space separated list of domains, or none]: **none**

Name servers [Space separated list of IPv4 Addresses, or none]: **172.16.7.99**

Set the password for the Linux "root" user. This password will also be used as the grub bootloader password.

Enter password [Please enter a strong password. Password must be 7 - 14 characters long. It must contain a combination of: numbers, lower-case characters, and at least 1 of the following character groups: upper-case characters or special characters. The password cannot contain 3 or more consecutive repeating characters]: ←**root ユーザ、bootloader** のパスワードを入力します

Re-enter password: ←再度 **root ユーザ、bootloader** のパスワードを入力します

The user "secure" (the SecureSphere administrative user) is used to register the SecureSphere Gateway with a SecureSphere Management Server.

Enter password [Please enter a strong password with 7 - 14 characters]: ←**secure ユーザ** のパスワードを入力します

Re-enter password: ←再度 **secure ユーザ** のパスワードを入力します

Set the password for the imperva user.

The imperva user is responsible for communication with remote agents.

Enter password [Please enter a strong password. Password must be 7 - 14 characters long. It must contain a combination of: numbers, lower-case characters, and at least 1 of the following character groups: upper-case characters or special characters. The password cannot contain 3 or more consecutive repeating characters or "nochange"]:  
←**imperva ユーザ** のパスワードを入力します

Re-enter password: ←再度 **imperva ユーザ** のパスワードを入力します

Assign a name to the host

**NOTE:**

The host name you will set will also be used as the Gateway name.

If you enter a Fully Qualified Domain Name (FQDN) the leftmost part of the name will be used for hostname.

For example, if you enter "mycomputer.mydomain.com" the host name will be "mycomputer".

Host name [Short or FQDN (separated by .) hostname, where each part starts with a letter and consists of the following: letters, digits, \_ or -]: **x4500-v12-0-42-13-46**

Gateway configuration

You will now set the IP Address of the Management Server.

**NOTE:**

The Management Server must be accessible over the management interface of this Gateway

Enter the Management Server's IP Address [IPv4 Address]: **172.16.13.45**

Choose a gateway operation mode

The SecureSphere gateway operation modes are:

- 1) Sniffing.
- 2) Bridge STP.
- 3) Bridge IMPVHA.
- 4) Reverse Proxy Kernel.

Operation mode: **3**

You will now select a time zone

Please identify a location so that time zone rules can be set correctly.

Please select a continent or ocean.

- 1) Africa
- 2) Americas
- 3) Antarctica
- 4) Arctic Ocean
- 5) Asia
- 6) Atlantic Ocean
- 7) Australia
- 8) Europe
- 9) Indian Ocean
- 10) Pacific Ocean
- 11) none - I want to specify the time zone using the Posix TZ format.

5

#? Please select a country.

- |                |                     |                          |
|----------------|---------------------|--------------------------|
| 1) Afghanistan | 18) Israel          | 35) Palestine            |
| 2) Armenia     | 19) Japan           | 36) Philippines          |
| 3) Azerbaijan  | 20) Jordan          | 37) Qatar                |
| 4) Bahrain     | 21) Kazakhstan      | 38) Russia               |
| 5) Bangladesh  | 22) Korea (North)   | 39) Saudi Arabia         |
| 6) Bhutan      | 23) Korea (South)   | 40) Singapore            |
| 7) Brunei      | 24) Kuwait          | 41) Sri Lanka            |
| 8) Cambodia    | 25) Kyrgyzstan      | 42) Syria                |
| 9) China       | 26) Laos            | 43) Taiwan               |
| 10) Cyprus     | 27) Lebanon         | 44) Tajikistan           |
| 11) East Timor | 28) Macau           | 45) Thailand             |
| 12) Georgia    | 29) Malaysia        | 46) Turkmenistan         |
| 13) Hong Kong  | 30) Mongolia        | 47) United Arab Emirates |
| 14) India      | 31) Myanmar (Burma) | 48) Uzbekistan           |
| 15) Indonesia  | 32) Nepal           | 49) Vietnam              |

16) Iran                      33) Oman                      50) Yemen

17) Iraq                      34) Pakistan

19

#?

The following information has been given:

Japan

Therefore TZ='Asia/Tokyo' will be used.

Local time is now:              Fri Mar 31 13:30:22 JST 2017.

Universal Time is now:      Fri Mar 31 04:30:22 UTC 2017.

Is the above information OK?

1) Yes

2) No

1

#?

You can configure an NTP client. (recommended)

Do you want to configure an NTP client? [y/n]: **y**

NTP servers [Space separated list of IPv4 Addresses]: **172.16.7.99**

NOTE:

The SecureSphere Gateway has been activated on this machine.

The selected operation mode is Bridge IMPVHA.

The Gateway will be registered and started.

NOTE:

A transaction that will activate these settings is about to start.



You can use another terminal session to monitor it with:

`impctl show log.`

NOTE:

During the settings activation, the hardening settings will be configured.

Part of these settings include setting a timeout on inactive shell sessions as well as denying access to 'root' user over SSH.

If you have open shell sessions, please close them all after all the settings have been activated in order for the hardening settings to be properly applied.

Press <ENTER> to continue: ←Enter を押します

-----設定が反映されるまで 5~10 分程度必要となります-----

【図 2 初期セットアップ(GW)】

## 1.3 初期セットアップ(OneBox)

OS インストール後にログインプロンプト画面が表示されますので

以下ユーザアカウントでログインします。初期ユーザ、初期パスワードでログイン後以下のようにパスワードの変更を求められるのでメッセージに従い入力します。

login:**admin**

Password:**admin**

You are required to change your password immediately (root enforced)

Changing password for admin.

(current) UNIX password:**admin** ←(実際にはエコーバックしません)

New password: ←(実際にはエコーバックしません)

Retype new password: ←(実際にはエコーバックしません)

login: **admin**

Password: **admin**

You are required to change your password immediately (root enforced)

Changing password for admin.

(current) UNIX password: ←**admin** と入力します

New password:

Retype new password:

Last login: Tue Apr 18 07:54:38 on ttyS0

Welcome to SecureSphere Shell

Type "ftl" to complete deployment

SecureSphere>

SecureSphere>**ftl**

Welcome to Imperva's configuration tool !!!

Initial setup mode.

The machine has been identified as a "Gateway" type appliance (asset-tag: X2500).

Please choose the SecureSphere component-set you would like to activate. Note that the use of SecureSphere components is restricted by the license you install on the appliance. Please see the Quick Start Guide for more information.

- 1) Gateway only.
- 2) Onebox (Management Server and Gateway).**
- 3) Discovery and Assessment Server (DAS).

Your choice: **2**

You will now set up the "management" interface, which connects the SecureSphere appliances.

The default "management" interface for this appliance is "eth0".

Do you want to change it? [y/n]: **n**

Classless Inter-domain Routing (CIDR) notation explicitly specifies the number of bits in an IP address denoting the network, in contrast to the netmask notation which indirectly specifies the number of bits. For example, a netmask of 255.255.255.0 indicates (for IPv4 addresses) the first 24 bits of an IP address denote the network. In CIDR notation, one simply writes /24 after the IP address (for example, 123.124.125.126/24).

IP configuration for the management interface "eth0".

IP Address [IP Address/CIDR]: **172.16.13.54/24**

Do you want to set IPv6 Address as well? [y/n]: **n**

You can optionally set an Ethernet interface that will connect the appliance to a LAN (Local Area Network). You can use one of the on-board Ethernet interfaces.

Do you want to set a LAN interface? [y/n]: **n**

You can (optionally) set a default gateway.

Do you want to set an IPv4 default gateway? [y/n]: **y**

You will be asked for the IPv4 default gateway's Address and an optional device.

If you specify a device:

It should be one of the onboard Ethernet interfaces (eth0 eth1).

If you don't specify a device:

The default gateway must be reachable through one of the onboard interfaces.

The route will become available when the appliance boots and remain available until it shuts down.

Gateway [IPv4 Address reachable from onboard interface]: **172.16.13.1**

Do you want to specify a device? [y/n]: **n**

You can configure a DNS client. (optional)

Do you want to configure a DNS client? [y/n]: **y**

Domain name [Domain name, or none]: **none**

Domain search list [Space separated list of domains, or none]: **none**

Name servers [Space separated list of IPv4 Addresses, or none]: **172.16.7.99**

Set the password for the Linux "root" user. This password will also be used as the grub bootloader password.

Enter password [Please enter a strong password. Password must be 7 - 14 characters long. It must contain a combination of: numbers, lower-case characters, and at least 1 of the following character groups: upper-case characters or special characters. The password cannot contain 3 or more consecutive repeating characters]: ←root ユーザ、**bootloader** のパスワードを設定します

Re-enter password:←再度 root ユーザ、**bootloader** のパスワードを設定します

The user "secure" (the SecureSphere administrative user) is used to register the SecureSphere Gateway with a SecureSphere Management Server.

If the password is changed, the SecureSphere Management Server will be restarted when the changes are applied.

Enter password [Please enter a strong password. Password must be 7 - 14 characters long. It must contain a combination of: numbers, lower-case characters, and at least 1 of the following character groups: upper-case characters or special characters. The password cannot contain 3 or more consecutive repeating characters]: ←secure パスワードを入力します

Re-enter password: ←再度 secure パスワードを入力します

Set the password for the imperva user.

The imperva user is responsible for communication with remote agents.

Enter password [Please enter a strong password. Password must be 7 - 14 characters long. It must contain a combination of: numbers, lower-case characters, and at least 1 of the following character groups: upper-case characters or special characters. The password cannot contain 3 or more consecutive repeating characters or "nochange"]:  
←imperva ユーザのパスワードを入力します

The password has not been changed.

Press <Enter> to continue:

Set the password for the SecureSphere "system" user (database administrator)

Enter password [Please enter a strong password. Password must be 7 - 14 characters long. It must contain a combination of: numbers, lower-case characters, and at least 1 of the following character groups: upper-case characters or special characters. The password cannot contain 3 or more consecutive repeating characters]: ←system パスワードを入力します

Re-enter password: ←system パスワードを入力します

Assign a name to the host

NOTE:

The host name you will set will also be used as the Gateway name.

For example, if you enter "mycomputer.mydomain.com" the host name will be "mycomputer".

Host name [Short or FQDN (separated by .) hostname, where each part starts with a letter and consists of the following: letters, digits, \_ or -]: **v12-onebox**

Gateway configuration

Choose a gateway operation mode

The SecureSphere gateway operation modes are:

- 1) Sniffing.
- 2) Bridge STP.
- 3) Bridge IMPVHA.
- 4) Reverse Proxy Kernel.

Operation mode: **2**

You will now select a time zone

Please identify a location so that time zone rules can be set correctly.

Please select a continent or ocean.

- 1) Africa
- 2) Americas
- 3) Antarctica
- 4) Arctic Ocean
- 5) Asia
- 6) Atlantic Ocean
- 7) Australia
- 8) Europe

- 9) Indian Ocean
- 10) Pacific Ocean
- 11) none - I want to specify the time zone using the Posix TZ format.

5

#? Please select a country.

- |                |                     |                          |
|----------------|---------------------|--------------------------|
| 1) Afghanistan | 18) Israel          | 35) Palestine            |
| 2) Armenia     | 19) Japan           | 36) Philippines          |
| 3) Azerbaijan  | 20) Jordan          | 37) Qatar                |
| 4) Bahrain     | 21) Kazakhstan      | 38) Russia               |
| 5) Bangladesh  | 22) Korea (North)   | 39) Saudi Arabia         |
| 6) Bhutan      | 23) Korea (South)   | 40) Singapore            |
| 7) Brunei      | 24) Kuwait          | 41) Sri Lanka            |
| 8) Cambodia    | 25) Kyrgyzstan      | 42) Syria                |
| 9) China       | 26) Laos            | 43) Taiwan               |
| 10) Cyprus     | 27) Lebanon         | 44) Tajikistan           |
| 11) East Timor | 28) Macau           | 45) Thailand             |
| 12) Georgia    | 29) Malaysia        | 46) Turkmenistan         |
| 13) Hong Kong  | 30) Mongolia        | 47) United Arab Emirates |
| 14) India      | 31) Myanmar (Burma) | 48) Uzbekistan           |
| 15) Indonesia  | 32) Nepal           | 49) Vietnam              |
| 16) Iran       | 33) Oman            | 50) Yemen                |
| 17) Iraq       | 34) Pakistan        |                          |

19

#?

The following information has been given:

Japan

Therefore TZ='Asia/Tokyo' will be used.

Local time is now: Tue Apr 18 16:57:25 JST 2017.

Universal Time is now: Tue Apr 18 07:57:25 UTC 2017.

Is the above information OK?



1) Yes

2) No

1

#?

You can configure an NTP client. (recommended)

Do you want to configure an NTP client? [y/n]: y

NTP servers [Space separated list of IPv4 Addresses]: 172.16.7.99

NOTE:

The SecureSphere Management Server has been activated on this machine.

The database is about to be created. This may take a while.

NOTE:

The SecureSphere Gateway has been activated on this machine.

The selected operation mode is Bridge STP.

The Gateway will be registered and started.

NOTE:

A transaction that will activate these settings is about to start.

You can use another terminal session to monitor it with:

impctl show log.

NOTE:

During the settings activation, the hardening settings will be configured.

Part of these settings include setting a timeout on inactive shell sessions as well as denying access to 'root' user over SSH.

If you have open shell sessions, please close them all after all the settings have been activated in order for the hardening settings to be properly applied.

Press <ENTER> to continue: ←Enter を押します

-----設定が反映されるまで 40~60 分程度必要となります-----

## 【図 3 初期セットアップ(OneBox)】