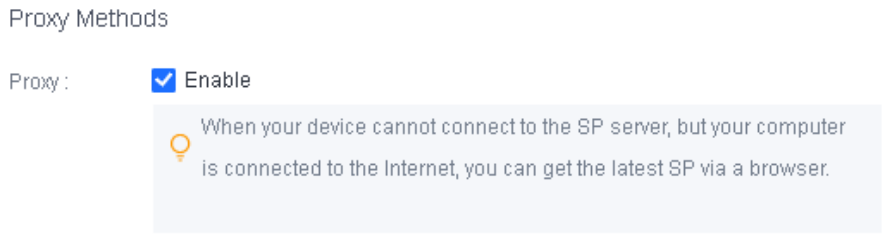
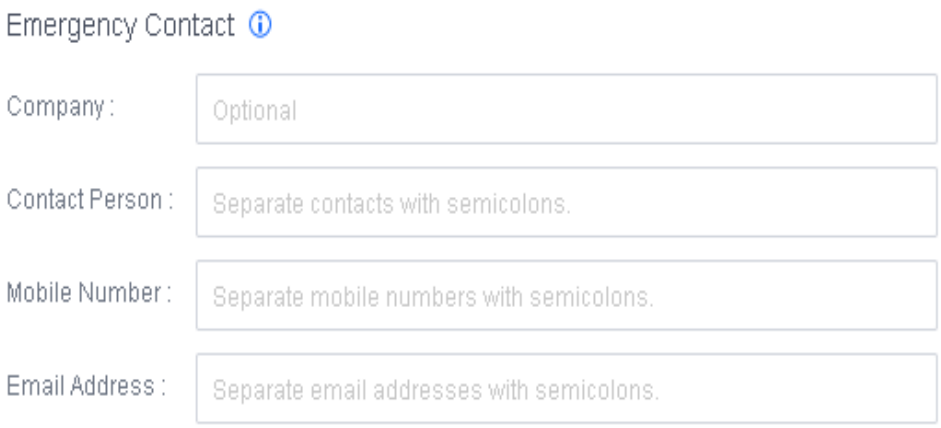
If Endpoint Secure Manager cannot directly connect to the Internet, but the local computer has Internet access, you can enable a browser proxy, so that Endpoint Secure Manager obtains service pack updates through the proxy, as shown in the following figure.



We recommend that you provide an emergency contact, as shown in the following figure. If we have released an emergency pack, but you do not enable automatic upgrade, we can contact you at the earliest opportunity to prevent business interruptions.



4.3 Update the Signature Databases

4.3.1 Update the Antivirus Database

The antivirus database can be updated online and offline.

Online update

By default, if Endpoint Secure Manager is connected to the Internet, the antivirus database is automatically updated online.

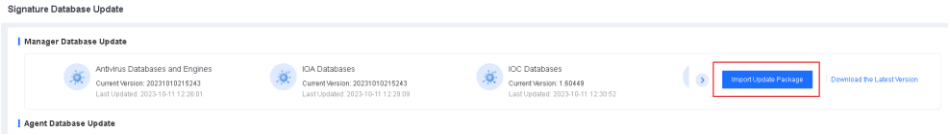
Offline update

If Endpoint Secure Manager is disconnected from the Internet, you can manually update the antivirus database offline by performing the following steps:

1. Download the offline antivirus database or engine and verify its MD5 value.

   To download the antivirus database, visit https://community.sangfor.com and go to **Self Services** > **Download** > **Endpoint Secure** > **Anti-virus Database**.

2. Log in to Endpoint Secure Manager. Go to **System** > **System Updates** > **Signature Database Update**, and click **Import Update Package**. Then, select the antivirus database downloaded in Step 1. After the antivirus database and engine are imported to Endpoint Secure Manager, Endpoint Secure Agent will automatically update the antivirus database and engine, as shown in the following figure.



4.3.2 Update the IOA or IOC Database

The IOA or IOC database can be updated online and offline.

Online update

By default, if Endpoint Secure Manager is connected to the Internet, the database is automatically updated online.

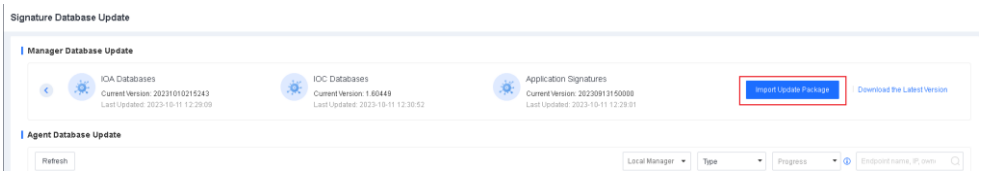
Offline update

If the Manager is disconnected from the Internet, you can manually update the database offline by performing the following steps:

1. Download the IOA or IOC database and verify its MD5 value.

   To download the database, visit https://community.sangfor.com and go to **Self Services** > **Download** > **Endpoint Secure** > **IOC / IOA Database**.

2. Log in to Endpoint Secure Manager. Go to **System** > **System Updates** > **Signature Database Update**, and click **Import Update Package**. Then, select the database downloaded in Step 1. After the IOA or IOC database is imported to Endpoint Secure Manager, Endpoint Secure Agent will automatically update the IOA or IOC database, as shown in the following figure.



4.4 Update the Vulnerability Database

The vulnerability database can be updated online and offline.

Online update

By default, if Endpoint Secure Manager is connected to the Internet, the vulnerability database and patch package are automatically updated online.

Offline update

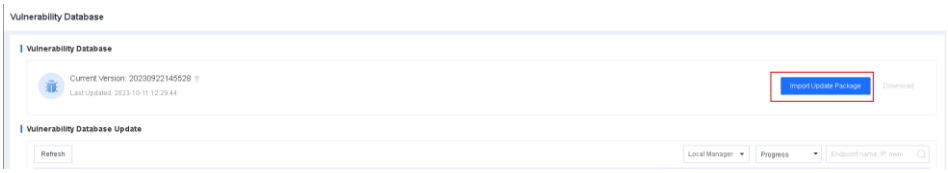
If Endpoint Secure Manager is disconnected from the Internet, you can manually update the vulnerability database offline by performing the following steps:

1. Download the vulnerability database or patch package and verify its MD5 value.

   To download the vulnerability database, visit https://community.sangfor.com and go to **Self Services** > **Download** > **Endpoint Secure** > **Vulnerability Database**.

2. Log in to Endpoint Secure Manager. Go to **System** > **System Updates** > **Vulnerability Database**, and click **Import Update Package**. Then, select

the database downloaded in Step 1. After the database is imported to Endpoint Secure Manager, Endpoint Secure Agent will automatically update the database, as shown in the following figure.



5 High-risk Operations

Before you use Endpoint Secure, learn about and avoid the high-risk operations described in the table below. Otherwise, your business may be impacted or, in severe cases, interrupted.

Table 6: High-risk Operations

Module	Level 1 Directory	Level 2 Directory	Risky Operation	Description	Risk Level	Response
Policies	General Policies	Anti-Malware	The action for a detected threat file is set to **Auto Fix - Security First**.	A business file may be quarantined due to a false positive, which can cause a system error.	High	Set the action for a detected threat file to **Auto Fix - Business Continuity First**.
Policies	General Policies	Anti-Malware	The engine is set to **High Detection Rate** for daily operations.	The virus detection rate is higher in **High Detection Rate** mode, resulting in more false positives. We recommend using this mode only when you test the virus detection rate.	High	Do not set the engine to **High Detection Rate** for daily operations.
Policies	General Policies	Realtime Protection	In the **Realtime File Protection** section, the action to take for a	A business file may be quarantined due	High	Set the action for a detected threat file to