TREND MICRO™

9.1 InterScan™ Messaging Security Virtual Appliance

High Availability Guide

Hybrid SaaS Email Security

Messaging Security

Document Part No.: MSEM97551/160906

Release Date: September 2016

Protected by U.S. Patent No.: Patents pending

This documentation introduces the main features of the product and/or provides installation instructions for a production environment. Read through the documentation before installing or using the product.

Detailed information about how to use specific features within the product may be available in the Trend Micro Online Help and/or the Trend Micro Knowledge Base at the Trend Micro website.

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please contact us at docs@trendmicro.com.

Evaluate this documentation on the following site:

http://www.trendmicro.com/download/documentation/rating.asp

Table of Contents

IMSVA High Availability Guide

High availability is a top priority for many business operations. From small, specialized businesses to global enterprises, competition requires more and more companies to service customers, partners, and endpoints around the clock. The increased reliance on server-based systems to power business requires that server services are continuously running. Mission-critical applications, such as corporate databases and email, must often reside on systems and network structures that are designed for high availability. Organizations find that they have to plan and configure their systems with high availability in mind, so that they can rely on them for continuous service.

This document describes high availability support that Trend Micro™ InterScan™ Messaging Security Virtual Appliance (IMSVA) provides in version 8.5 Service Pack 1 and later.

Topics include:

Background

This section describes the parent-child deployment for IMSVA and the IMSVA components in the deployment.

IMSVA Deployment

IMSVA can be deployed in a geographically distributed enterprise environment, which is known as a parent-child deployment.

In a parent-child deployment, the parent device assumes the roles of central controller and data repository. All configuration information including policy data is stored in a database hosted on the parent device in the IMSVA deployment. All child devices

communicate with the parent device directly or indirectly for system and policy configurations.

For performance considerations, the parent device usually does not process email messages, but works as a configurable central controller. The child devices process received email messages.

Only one parent device is allowed in a parent-child deployment. As a result, the availability of the parent device is critical to the entire deployment. However, the absence of the parent device is not necessarily equal to the outage of the entire deployment.

Components in the Parent-Child Deployment

The following components are deployed on the parent device:

- IMSVA admin database, which stores the following data:
  - Policies
  - System configuration
  - Logs, including system event logs and message tracking logs
  - Quarantined email message indices
  - Report statistics
  - IP Profiler statistics
- Domain Name Service (DNS) server

  Implemented with Berkeley Internet Name Domain (BIND) to provide the DNS service for the IP Profiler function.
- Lightweight Directory Access Protocol (LDAP) cache

  Implemented with OpenLDAP to provide a consolidated view for more than one LDAP server. The data in this cache can be used in policy enforcement.

Note

The LDAP cache takes effect only when multiple on-premises LDAP servers are chosen.

The following components are deployed on child devices:

- Policy server
- IP Profiler

Note

When connecting child devices to the LDAP server, make sure that at least one LDAP server is connected. If only one on-premises LDAP server is connected, child devices query the LDAP server. If multiple on-premises LDAP servers are connected, child devices query the local LDAP cache.

High Availability Support

This section provides diagrams to show IMSVA deployment without and with high availability support, and describes the considerations to take for the deployment.

High availability support is available in IMSVA version 8.5 Service Pack 1 and later. It automatically takes effect when the child device fails to connect to the database on the parent device.

Goals for High Availability

To guarantee high availability in a parent-child deployment when the parent device goes down, make sure the following goals, listed in descending order of importance, are achieved:

1. The child devices are not affected and can process email messages normally.
2. The child devices can still process email messages even if they are rebooted.
3. System configurations are still available from the child devices.

No configuration changes are required to equip the existing IMSVA deployments with high availability. When the parent device goes offline:

- Child devices keep processing email messages without being affected.
- Child devices can be rebooted freely.
- No compromise in LDAP query for policy enforcement.
- No compromise to configuration settings.
- No loss to log access, including Mail Transfer Agent (MTA) events, message tracking events, or policy events after the parent device recovers.

Note

Depending on the size of logs and the length of the outage, it may take hours to days to upload delayed logs to the parent device.

Deployment Diagram (High Availability Not Supported)

The following diagram shows the original components and connections deployed within IMSVA in parent-child mode before high availability is supported.

Note

High availability support is available in IMSVA version 8.5 Service Pack 1 and later.

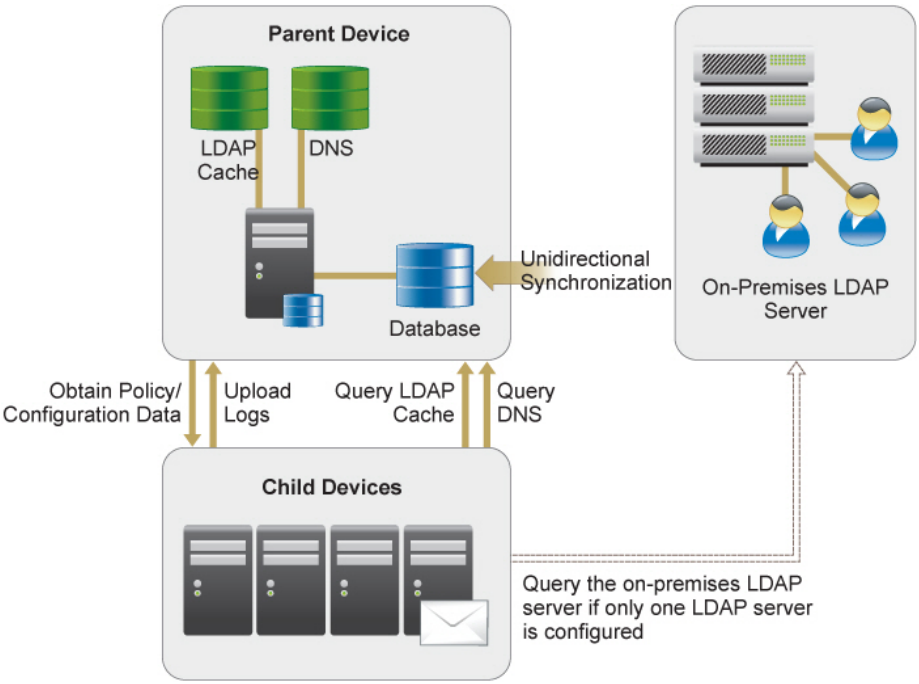


FIGURE 1. Original components and connections

Deployment Diagram (High Availability Supported)

The following diagram shows the current components and connections within IMSVA in high availability mode.

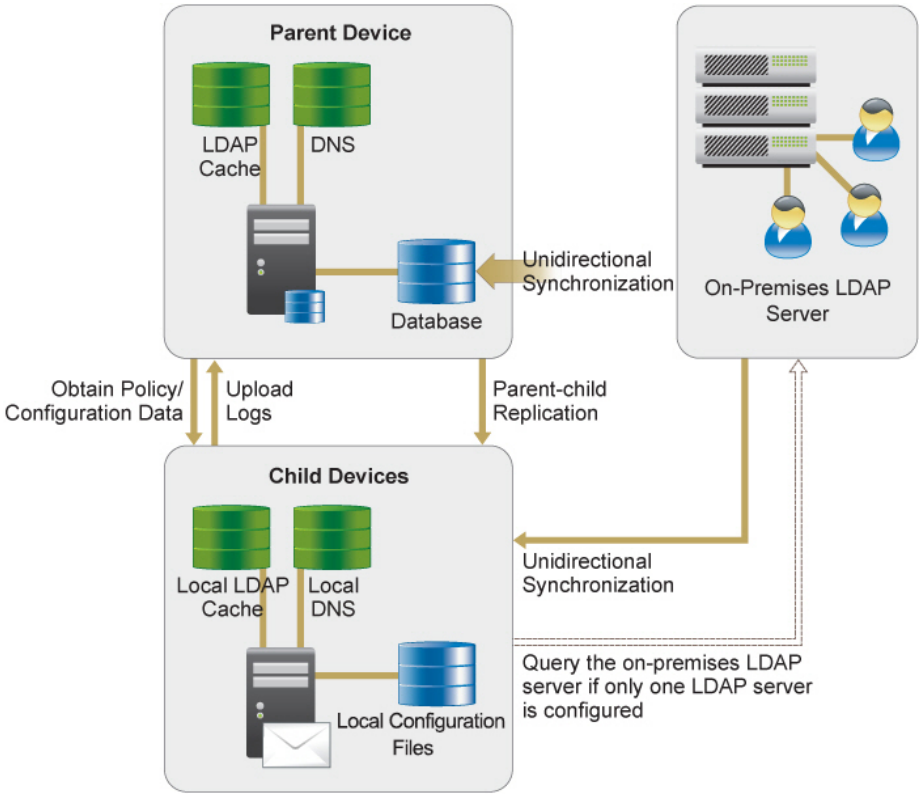


FIGURE 2. Current components and connections

To achieve the goals defined in *Goals for High Availability on page 3*, a child device is enhanced to:

- Prevent policies and other configurations stored on local policy servers from being lost.

- Provide a local DNS server for IP Profiler.
- Provide a local LDAP server for LDAP-related features.
- Query the local DNS server when a DNS query is requested from IP Profiler.

Note

The DNS query requires a synchronization between the local DNS server on the child device and the DNS server hosted on the parent device.

- Query the local LDAP server (or the on-premises LDAP server if only one LDAP server is configured) when an LDAP query is requested.

Considerations for High Availability

- Create an estimate for the maximum outage of the parent device.

  Although email messages are continuously flowing through the network, you temporarily lose the ability to access the management console and trace email routing during the outage. In addition, logs generated during the outage are stored on child devices and are not uploaded to the parent device until it recovers. To guarantee high availability, it is necessary to calculate the maximum parent device outage.

Note

For details about how to calculate the maximum outage based on the number of received email messages, see *Calculating Downtime of the Parent Device on page 8*.

- Frequently back up configurations to local disks.

  Frequent backups help shorten the time for recovering the parent device. For the detailed steps of automating an export action, see *Enabling the Automatic Export and Import Function on page 20*.

- Use the same IP address that was previously allocated to the parent device.

If you cannot recover the failed parent device, use the hot standby for the device instead. Use the same IP address as the original parent device to avoid potential communication issues among IMSVA components.

For details about how to connect to a new parent device, see *Connecting Child Devices to a New Parent Device on page 13*.

Calculating Downtime of the Parent Device

When the parent device fails, various logs generated by the MTA and Scan Daemon are temporarily stored to local hard disks. After being consolidated, these logs are stored in internal cache. When the parent device recovers, these logs are uploaded to the central database. Based on the log file size limit, you must bring the parent device back before the logs are purged. The maximum time that these logs can be retained on child devices depends on the following factors:

- Log retention period

  To configure the retention period of logs, open the management console, go to **Logs** > **Settings**, and specify the value for **Number of days to keep log files**.

- Free disk space

  Email messages are also stored on local hard disks. When the available disk space is lower than the specified threshold (10240 MB by default), IMSVA sends a notification message. To configure the threshold value, go to **Administration** > **Notifications**, click the **Events** tab, and then specify a value for **Data partition free space on any host is less than**.

- Internal log cache size

  By default, the internal log cache size is 2 GB. To configure this value, go to **Logs** > **Settings** and specify a value for **Maximum log file size for each service**.

The log record for each email message occupies an average of 200-byte disk space. Based on the average message traffic size, you can predict the duration to store logs during the downtime of the parent device.

For example, company A has an average of 55,000 email messages per day per IMSVA server. After calculation, the total log size is 11 MB per day. The peak number of email messages for company A is 2,760 per hour per IMSVA server. Based on the peak value,

the maximum number of email messages is 66,240 per day per IMSVA server. After calculation, these email messages produce 13 MB of logs every day. With its internal log cache, the IMSVA server can store these logs for approximately 150 days. However, IMSVA automatically purges logs older than 90 days. As a result, a 90-day retention period is available.

Company B has twice the average message traffic as A and an even higher peak number of email messages during peak hours. The average message traffic is 110,000 email messages per day, and the peak number of email messages is 9,000 per hour. Based on the peak value, the maximum number of email messages is 220,000 per day per IMSVA server. After calculation, these email messages produce 44 MB of logs every day. IMSVA can store these logs for approximately 45 days in its internal log cache.

Note

The data for IP Profiler cannot be updated during the downtime of the parent device.

The Trend Micro Virtual Analyzer agent is suspended during the downtime. When the parent device recovers, restart the Virtual Analyzer agent manually. For details, see *Restarting the Deep Discovery Advisor Agent on page 23*.

The Trend Micro Management Communication Protocol (MCP) agent is suspended during the downtime. When the parent device recovers, restart the MCP agent manually. For details, see *Restarting the MCP Agent on page 23*.

Email messages are not encrypted during the downtime. Outgoing email messages that match encryption policies are considered as exceptions, and the default scan action is "Quarantine and Notify".

If your client uses POP3 to receive email messages, change the client's POP3 server from the parent device to the child device.

Optional Operations

This section describes the operations that you can choose to perform when the parent device goes offline.

Adding a Hard Disk to a Child Device

Perform the following procedure if the hard disk on a child device is insufficient.

Procedure

1. Start a shell window and log on as the root user.
2. Check disk partitions under `/dev`:

   ```
   ls /dev/sd*
   ```

   Note

   By default, you can find sda, sda1, sda2 disk partitions.

3. Install a new hard disk.
   a. Power off the device the IMSVA server.
   b. insert a hard disk.
   c. Power on the server.
4. After IMSVA restarts, check the new hard disk under `/dev` in the shell window:

   ```
   ll /dev/sd*
   ```

   In the output, you can find the new disk, for example, sdb.

   Note

   The following commands use sdb as the disk name if it is not changed.

5. Create a primary partition on the new hard disk.
   a. Type the following:

      ```
      fdisk /dev/sdb
      ```

   b. Type `m` and press **Enter** to display the primary command action menu.

      Note

      For available actions, see *Command Actions on page 12*.

   c. Type `n` to add a new partition and press **Enter**.

The following output appears:

```
e extended

p primary partition (1-4)
```

d. Type `p` to add a primary partition and press **Enter**.

The following output appears:

```
Partition number (1-4):
```

e. Type `1` as the partition number and press **Enter**.

The following output appears:

```
First cylinder (1-5221, default 1):

Using default value 1

Last cylinder or +size or +sizeM or +sizeK (1-5221,
default 5221):

Using default value 5221
```

f. Type `w` to update the partition table and press **Enter**.

The following output appears:

```
The partition table has been altered!

Calling ioctl() to re-read partition table.

Syncing disks.
```

g. Use the following command to check the new partition (sdb1):

```
ll /dev/sd*
```

6. Format the new hard disk with the ext3 file system:

```
mkfs.ext3 /dev/sdb1
```

7. Create a physical volume on the partition:

```
pvcreate /dev/sdb1
```

8. Add the new physical volume to a volume group:

   ```
   vgextend IMSVA /dev/sdb1
   ```

9. Allocate space to spool or app_data.

   Note

   app_data is the directory where IMSVA stores mail areas and queues.

   a. Run the following commands to stop services:

      ```
      imssctl.sh stop
      service crond stop
      ```

   b. Run the following command to unmount app_data:

      ```
      umount /var/app_data
      ```

   c. Run the following commands to allocate space to app_data:

      ```
      lvextend -L +100G /dev/mapper/IMSVA-App_data
      e2fsck -f /dev/mapper/IMSVA-App_data
      resize2fs /dev/mapper/IMSVA-App_data
      ```

      Note

      In the preceding commands, 100G means 100 GB. It is the size of space needed to allocate to app_data.

   d. Run the following command to mount app_data:

      ```
      mount -t ext3 /dev/mapper/IMSVA-App_data /var/app_data
      ```

10. Restart the IMSVA server.

Command Actions

```
a toggle a bootable flag
```

```
b edit bsd disklabel

c toggle the dos compatibility flag

d delete a partition

l list known partition types

m print this menu

n add a new partition

o create a new empty DOS partition table

p print the partition table

q quit without saving changes

s create a new empty Sun disklabel

t change a partition's system id

u change display/entry units

v verify the partition table

w write table to disk and exit

x extra functionality (experts only)
```

Connecting Child Devices to a New Parent Device

If the old parent device cannot be recovered, install a new parent device. Perform the following procedure to connect the child devices to the new parent device.

Before proceeding with the following procedure, make sure that you have imported configurations from the original parent device to the new parent device. For details about how to automatically export and import configurations, see *Enabling the Automatic Export and Import Function on page 20*.

Note

In the following steps, 10.204.168.98 is an example of the new parent device's IP address, and 10.204.168.100 is an example of a child device's IP address.

Note that all the logs and quarantined messages on the original parent device cannot be found on the management console of the new parent device.

Procedure

1. Install a new parent device that uses a different IP address from the original parent device.

   a. Install the same build as the original parent device on the new parent device.

   Note

   Use a different IP address for the new parent device to prevent services on child devices from malfunctioning if the child devices connect to the new parent device before it is available.

   b. Import the original configurations on the new server.

2. Add IP addresses of all child devices to the new parent device.

   a. Log on to the parent device's management console.

   b. Go to **Administration** > **IMSVA Configuration** > **Connections**.

      The **Components** tab appears by default.

   c. Click the **Child IP** tab.

   d. Under **Add IP Address**, specify a child device's IP address.

   e. Click **>>**.

      The IP address appears in the IP address table.

   f. Click **Save**.

3. Obtain information from the child device.

a. Open the `imss.ini` file and find **scanner_id** as shown in the following figure:

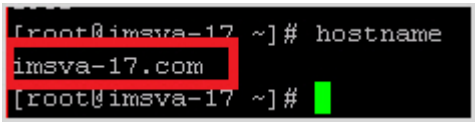
```
# vi /opt/trend/imss/config/imss.ini
```

Note

All figures in this section are provided as examples for your reference.

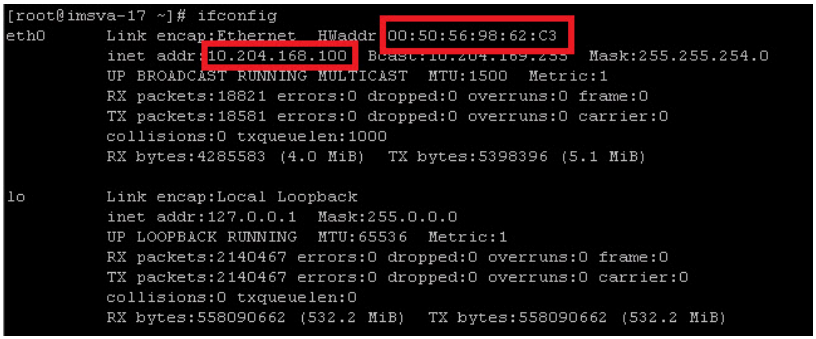
b. Obtain **hostname** and use it as **scanner_name**:

```
# hostname
```



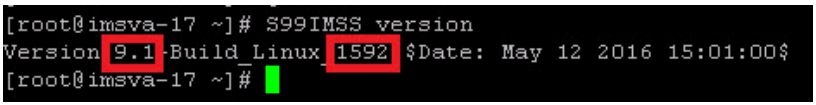
c. Obtain the device IP address and MAC address and use them as **ip_addr** and **mac_addr** respectively:

```
# ifconfig
```



d. Obtain the application version and use it as **app_ver**:

```
#S99IMSS version
```



4. Update the tb_component_list database table on the new parent device.

a. Log on to the database.

```
# /opt/trend/imss/PostgreSQL/bin/psql imss sa
```

b. Check the settings in the database table:

```
# select * from tb_component_list;
```

Note

The components and processes shown in the preceding figure include:

- daemon: Scanning Daemon
- policy: Policy Service
- euq: End-User Quarantine
- nrs: Email Reputation Service
- ipprofiler: IP Profiler

The value 1 means the component or process is not running, and the value 2 means it is running.

c. Update the tb_component_list table.

```
Insert into tb_component_list
(scanner_id,scanner_name,ip_addr,daemon,policy,euq,nrs,
ipprofiler,os_ver,app_ver,mac_addr)
VALUES(2,'imsva-17.com','10.204.168.100',2,2,2,2,2,
'2.6.32','9.1.0.1592','00:50:56:98:62:C3');
```

Note

- Replace the preceding values in bold with the information you obtained in Step *3 on page 14*.
- Make sure that other string values are consistent with those on the parent device.

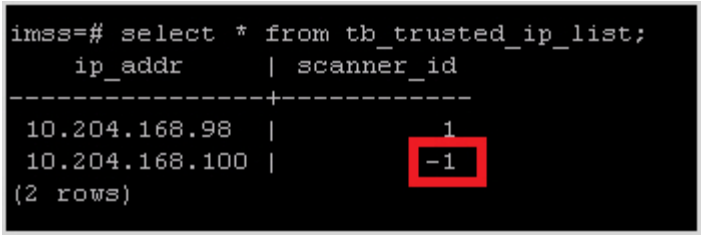
5. Update the tb_trusted_ip_list database table on the new parent device.

a. Log on to the database.

```
# /opt/trend/imss/PostgreSQL/bin/psql imss sa
```

b. Check the settings in the database table:

```
# select * from tb_trusted_ip_list;
```



Note

If the value for **scanner_id** is different from the value obtained in Step *3 on page 14*, go to the next step. If they are the same, skip the next step.

c. Update the tb_trusted_ip_list table.

```
update tb_trusted_ip_list set scanner_id=2 where
ip_addr='10.204.168.100';
```

Note

The value for **scanner_id** is replaced by that obtained in Step *3 on page 14*.

d. Update the tb_scanner_id_seq table.

```
select nextval('tb_scanner_id_seq') as nextid;
```

6. Optional: Manually complete the following settings on the new parent device if you have configured them before:

   - TMCM settings
   - Encryption settings
   - Deep Discovery Advisor settings

Note

If you have configured two LDAP servers, some features may be disabled during import. Check features in the following paths and enable them if they were disabled:

- **Administration** > **Connections** > **LDAP**
- **Cloud Pre-Filter** > **Policy List** > **Policy** > **Conditions** > **Valid Recipient** > **Scheduled maintenance**
- **Administration** > **SMTP Routing** > **Message Rule** > **Relay Control** > **Reject unknown recipients**

7. Replace the current parent device's IP address with the original parent device's IP address.

   a. Go to **Administration** > **IMSVA Configuration** > **Configuration Wizard**.

   b. Click **Next**.

      The **Local System Settings** screen appears.

   c. Change the parent device's IP address.

8. Use the following command on both the parent and child devices to restart all services:

   ```
   # imssctl.sh restart
   ```

9. Verify that services are in "Start" state on the **System Status** screen.

Note

If the End-User Quarantine (EUQ) service is enabled, proceed to Step *10 on page 19* to Step *13 on page 20*. Otherwise, skip these steps.

10. Attach the child device's EUQ database.

    a. Log on to the parent device's management console.

    b. Go to **Administration** > **IMSVA Configuration** > **Connections**.

    c. Click the **Database** tab.

    d. Click **Attach** under **EUQ Database**.

The **Attach EUQ database** screen appears.

e. Use the server IP address that you obtained in Step *3 on page 14* and specify other information as required.

f. Click **OK**.

11. Complete EUQ configurations on the parent device's management console.

a. Log on to the management console.

b. Go to **Administration** > **End-User Quarantine**.

The **EUQ Management** tab appears.

c. Clear the **Enable End-User Quarantine** check box and click **Save**.

d. Select the **Enable End-User Quarantine** check box and click **Save**.

12. Go to **System Status** and verify that the EUQ services are started.

13. Go to **Administration** > **End User Quarantine**. Click **Redistribute all (approved senders and spam)** and click **Redistribute**.

Enabling the Automatic Export and Import Function

IMSVA provides the automatic export and import function for configurations. Automatic export is executed daily at 4:00 a.m., and automatic import is executed daily at 4:30 a.m.

Procedure

1. Install a new parent device.

2. Enable the automatic export and import function on both the original and new parent devices.

   - On the original parent device:

     a. Use the following command to open the `imss.ini` script file:

        # vi /opt/trend/imss/config/imss.ini

     b. Append the following information to the file:

```
[AutoImportExport]
AutoImpExpEnable=on
AutoImpExpDirection=export
AutoImpExpFTPServer=192.168.0.1
AutoImpExpFTPPort=21
AutoImptExpFTPDir=/home/export
AutoImptExpFTPUser=test
AutoImpExpFTPPwd=test
```

Note

The preceding key values in bold are only examples. Replace them with your real settings. For details about those keys, see *Keys and Settings on page 22*.

   - On the new parent device:

     a. Use the following command to open the `imss.ini` script file:

        # vi /opt/trend/imss/config/imss.ini

     b. Append the following information to the file:

```
[AutoImportExport]
AutoImpExpEnable=on
AutoImpExpDirection=import
AutoImpExpFTPServer=192.168.0.1
AutoImpExpFTPPort=21
AutoImptExpFTPDir=/home/export
AutoImptExpFTPUser=test
AutoImpExpFTPPwd=test
```

Note

The preceding key values in bold are only examples. Replace them with your real settings. For details about those keys, see *Keys and Settings on page 22*.

The import function fails if the FTP server has more than one IP address.

Keys and Settings

TABLE 1. Keys for the automatic import and export function

KEY NAME	ACCEPTED VALUE	DEFAULT VALUE	DESCRIPTION
AutoImpExpEnable	on/off	off	on: enable this function off: disable this function
AutoImpExpDirection	export/import	export	export: automatically export data from IMSVA import: automatically import data into IMSVA
AutoImpExpFTPServer	hostname/ip	empty	Host name or IP address of the FTP server
AutoImpExpFTPPort	port number	empty	Port number of the FTP server
AutoImptExpFTPDir	directory	empty	Directory on the FTP server to store exported data
AutoImptExpFTPUser	user name	empty	User name for logging on to the FTP server
AutoImpExpFTPPwd	password	empty	Password for logging on to the FTP server

Restarting the Deep Discovery Advisor Agent

Procedure

1. Log on to the IMSVA child device.
2. Run the following command:

```
# S99DTASAGENT restart
```

Restarting the MCP Agent

Procedure

1. Log on to the IMSVA child device.
2. Run the following command:

```
# S99CMAGENT restart
```

Frequently Asked Questions

This section answers various Frequently Asked Questions.

What do services running on child devices do when the parent device fails?

Services running on child devices are automatically restarted to close broken TCP connections with the parent device. The order that services restart is asynchronous. When the parent device recovers, these services restart asynchronously again to reconnect to it.

TREND MICRO INCORPORATED

225 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 U.S.A.
Phone: +1 (817) 569-8900, Toll-free: (888) 762-8736
Email: support@trendmicro.com

www.trendmicro.com

Item Code: MSEM97551/160906