information on exporting tech info for SecureSphere MXs, see Exporting Technical Information from Management Servers.

To export technical information for a Gateway:

1. In the **Main** workspace, select **Setup > Gateways**.
2. In the **Gateways** pane, select the **Gateway** whose get tech info you want to export.

   Note: The Gateway must be in the status Running.

3. In the **Details** pane, next to **Tech Info (zip)**, click **Download**.

   SecureSphere prepares the information for download. Once complete a dialog box appears with a link. Click the link and download the zip file to the desired location. You can then mail it to Imperva support for analysis.

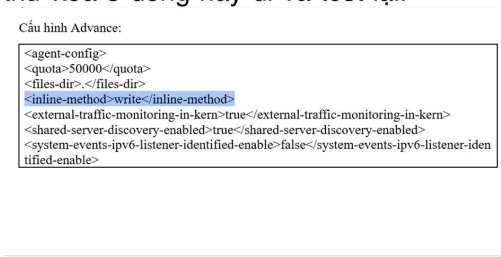
request that you provide them with technical information that is automatically generated by SecureSphere, so they can analyze logs and other information. You can export this information from the SecureSphere Management Server using the GUI. This procedure describes how to export technical information for a SecureSphere Management Server from the GUI. For information on exporting technical information from SecureSphere Gateways architectures, see Exporting Technical Information from Gateway.

To export technical information from Management Servers:

1. In the **Admin** workspace, select System Performance > Management Server.
2. From the top of the **Details** pane, click **MX Tech Info**.

   SecureSphere prepares the information for download. Once complete a dialog box appears with a link. Click the link and download the zip file to the desired location. You can then mail it to Imperva support for analysis.

- Agent Advanced configuration: Các dòng này anh thêm vào có ý nghĩa gì, thêm theo 1 template có sẵn hay hãng hướng dẫn? Anh thử xóa 3 dòng này đi và test lại.


Cấu hình Advance:

```
<agent-config>
<quota>50000</quota>
<files-dir>.</files-dir>
<inline-method>write</inline-method>
<external-traffic-monitoring-in-kern>true</external-traffic-monitoring-in-kern>
<shared-server-discovery-enabled>true</shared-server-discovery-enabled>
<system-events-ipv6-listener-identified-enable>false</system-events-ipv6-listener-identified-enable>
```

```
<userspace-oracle-injection-technology>active</userspace-oracle-injection-technology>
<oracle-advanced-monitoring>1</oracle-advanced-monitoring>
</agent-config>
```

- Em thấy có enable mode oracle shared server, anh xem có chính xác log như trong guide này không nhé: https://docs-cybersec.thalesgroup.com/bundle/v14.19-dam-user-guide/page/76950.htm


If you see the following message under an agent's Activity Log:

An active shared server has been detected on the Oracle database server. Please disable the Oracle shared server option on that server or enable shared server channel discovery via the on-premises Agents Advanced Configuration, otherwise some or all of the data associated with the Oracle database will not be monitored.

you ca ... Oracle shared server monitoring using the following procedure.

Nếu có thì anh cấu hình thêm channel aging để tự động xóa các interface không cần thiết (trong link đã có hướng dẫn).

- Khi tạo policy block jump, nếu block thành công alert hiển thị như thế nào, anh chụp đầy đủ giúp em thông tin alert
- Xóa các interface thừa trong tab Data Interfaces (Last activity là none hoặc các port không liên quan tới service đang dùng), disable interface discovery

If you see the following message under an agent's Activity Log:

> **An active shared server has been detected on the Oracle database server. Please disable the Oracle shared server option on that server or enable shared server channel discovery via the on-premises Agents Advanced Configuration, otherwise some or all of the data associated with the Oracle database will not be monitored.**

you can activate Oracle shared server monitoring using the following procedure.

To activate Oracle shared server monitoring:

1. In the **Main** workspace, select **Setup > Agents**.
2. In the **Agents** window, select the agent you want to configure.
3. In the lower pane, click the **Settings** tab.
4. In the bottom right hand corner of the **Settings** tab, expand the **Advanced Configuration** option. A text field opens.
5. Type the following text:

   ```
   <shared-server-discovery-enabled>true</shared-server-discovery-enabled>
   ```

   where `true` means monitoring enables and `false` means monitoring

1. In the **Main** workspace, select **Setup > Agents**.
2. In the **Agents** window, select the agent you want to configure.
3. In the lower pane, click the **Settings** tab.
4. In the bottom right hand corner of the **Settings** tab, expand the **Advanced Configuration** option. A text field opens.
5. Type the following text:

   ```
   <shared-server-discovery-enabled>true</shared-server-discovery-enabled>
   ```

   where `true` means monitoring enables and `false` means monitoring disabled.

6. Restart the agent to apply the new configuration.

> **Note:** When enabling shared server discovery it is recommended to enable channel aging. For more information, see Channel Aging.

Channel Aging

Also available in: v14.19 - Other

Last Updated Feb 01, 2026 1 minute read

Public # Database Activity Monitoring # v14.19 # User Guide # Documentation

SecureSphere can be configured to discover new data interfaces and assign them to services for monitoring. If after adding an agent channel, later the SecureSphere Agent cannot see it (for example, if the port was closed), the channel will be retained in SecureSphere, even if a new interface was registered. Over time these non-active "channels" can build up. Subsequently, you can use the **Data Interface and Retention** feature to determine guidelines by which the SecureSphere Agent checks periodically if a channel is still being used, and if not then deletes it. For instructions on configuring Channel Aging, see Data Interface Retention and Aging.

Data Interface Retention and Aging

You can configure SecureSphere so that when an Agent discovers a new data interface, SecureSphere immediately auto-assigns a service to it so that its traffic is immediately monitored by the Agent using that service's policies. You do this by selecting a **Default Server Group** in the **General Settings** section of the **Settings** tab for that Agent, then selecting a default service for the various service types.

The rules for data interface deletion are:

- By default, a data interface that no longer has a service assigned to it is deleted after a pre-defined and configurable period of time.

  You can configure SecureSphere such that, if subsequently the Agent cannot see that data interface for some reason (for example: you closed that port), as long as the data interface has a service applied to it, the channel is not deleted.

- If the aging time passes and the Agent does not detect that the data interface has been restored, the data interface is deleted.
- If the Agent itself is disconnected, no data interface disconnection occurs. Once the Agent is reconnected and sends its first report (this occurs every 120 seconds by default (this can be customized), data

- If the aging time passes and the Agent does not detect that the data interface has been restored, the data interface is deleted.
- If the Agent itself is disconnected, no data interface disconnection occurs. Once the Agent is reconnected and sends its first report (this occurs every 120 seconds by default (this can be customized), data interface deletion commences. If the data interface was discovered in this interval, of course it is not deleted.
- Data interface deletion only occurs if the Agent has at least one active data interface. If it has none, then none of its inactive data interfaces are deleted.

You can configure data interface deletions via the **agents-gateway.properties** file on the MX service in the **/opt/SecureSphere/server/SecureSphere/jakarta-tomcat-secsph/webapps/SecureSphere/WEB-INF/properties/** directory.

Disable data interface deletion by setting the property `channel.aging.enabled` to `False`.

The aging time is set by default to one week, 10080 minutes. You can configure this by changing the value for the property of `channel.aging.time.in.minutes`. Note that the minimum value is 1 minute, even if you set the

You can configure data interface deletions via the **agents-gateway.properties** file on the MX service in the **/opt/SecureSphere/server/SecureSphere/jakarta-tomcat-secsph/webapps/SecureSphere/WEB-INF/properties/** directory.

Disable data interface deletion by setting the property `channel.aging.enabled` to `False`.

The aging time is set by default to one week, 10080 minutes. You can configure this by changing the value for the property of `channel.aging.time.in.minutes`. Note that the minimum value is 1 minute, even if you set the property for zero. A value below 30 hours or 1800 minutes is not recommended for versions earlier than 14.8.

If you change any of these values, restart the MX service using the **impctl server restart** command.

If you want to prevent data interface discovery entirely, deselect the **Enable Discovery of Data Interfaces** check box, in the **Database Settings** section of the **Settings** tab for that Agent.

For the API function call, see https://docs.imperva.com/bundle/v14.19-dam-api-reference-guide/page/61666.htm