Changing the C Interface IP Address: step-by-step

Topic 45020 / Updated: 23-March-2011

Applies To:	Websense V10000 v7.6 Websense V10000 G2 v7.6 Websense V5000 G2 v7.6

Sometimes it is necessary to change the C interface IP address. What is affected and what must be done depends on the configuration of your appliances and the details of your deployment. **The number of activities that must be performed and the service disruption can be significant. If possible, retain the current C interface IP address.**

In most cases, off-box components that depend on or directly service an appliance should be uninstalled prior to changing the C interface IP address and reinstalled after the IP address change is completed. These components include:

- Off-box TRITON Unified Security Center
- Filtering Service
- Network Agent
- Real Time Monitor
- DC Agent
- Logon Agent
- eDirectory Agent
- Radius Agent
- Remote Filtering Service
- Sync Service
- Linking Service

Important

It is strongly recommended that you back up your appliance and affected off-box components before making any changes.

Follow the steps in the scenario below that matches your deployment.

Scenario 1: One appliance, Web Security only with on-box TRITON Unified Security Center and off-box Log Server

This configuration is for small deployments and Proof of Concept projects.

Step-by-step instructions:

1. If Web DLP is configured, unregister Content Gateway with the Data Security Management Server:
   a. Log on to Content Gateway Manager and go to **Configure** > **Security** > **Data Security**.
   b. Note the Data Security Management Server IP address. You must also know the administrator user name and password.
   c. Click **Unregister**.
2. On the Log Server machine, stop the Log Server service:
   a. From the Windows Start menu, select **Programs** > **Websense** > **Utilities** > **Log Server Configuration**.
   b. On the Connections tab, click **Stop**.
3. Change the IP address of interface C:
   a. Log on to the Appliance Manager and go to **Configuration** > **Network Interfaces**.
   b. In the Appliance Controller Interface (C) section, at the top of the page, change the **IP Address** field and associated fields, as needed.
   c. Click **Save**. The Appliance Manager applies the change to all appliance components. This process takes several minutes.
4. On the Log Server machine, edit websense.ini and start the Log Server service:
   a. In the Windows file system, go to C:\Program Files\Websense\bin

b. In a text editor such as Notepad, open websense.ini and locate the entry for "PolicyServerIP =". Change the value to the new IP address of the C interface. Save and close the file.

c. Start Log Server by going to the Windows Start menu and selecting **Programs** > **Websense** > **Utilities** > **Log Server Configuration**. On the Connections tab, click **Start**.

5. If Web DLP is configured, re-register Content Gateway with the Data Security Management Server and redeploy Web DLP:

   a. Log on to Content Gateway Manager and go to **Configure** > **Security** > **Data Security**.

   b. Enter the Data Security Management Server IP address, Data administrator user name and password.

   c. Click **Register**.

   d. Log on to the TRITON Unified Security Center and go to TRITON - Data Security.

   e. Go to **Settings** > **Deployment** > **System Modules**.

   f. Click **Deploy**.

   g. Restart all Content Gateway services, or the Content Gateway module.

> **Note**
> Although the new Policy Server IP address is available when you next log on to TRITON Unified Security Center, the previous Policy Server is not deleted from TRITON - Web Security. You can delete the invalid Policy Server details on the **Settings** > **General** > **Policy Servers** page.

Scenario 2: One appliance, Web Security only with off-box TRITON Unified Security Center and off-box Log Server

This is a recommended deployment for small and medium sized networks.

Step-by-step instructions:

1. If Web DLP is configured, unregister Content Gateway with the Data Security Management Server:

   a. Log on to Content Gateway Manager and go to **Configure** > **Security** > **Data Security**.

   b. Note the Data Security Management Server IP address. You must also know the administrator user name and password.

   c. Click **Unregister**.

2. On the Log Server machine, stop the Log Server service:

a. From the Windows Start menu, select **Programs** > **Websense** > **Utilities** > **Log Server Configuration**.

b. On the Connections tab, click **Stop**.

3. On the TRITON Unified Security Center machine, run the version 7.6 TRITON Installer and uninstall TRITON Unified Security Center and associated components (see the component list). Make a list of all uninstalled components.
4. Change the IP address of interface C:
   a. Log on to the Appliance Manager and go to **Configuration** > **Network Interfaces**.
   b. In the Appliance Controller Interface (C) section, at the top of the page change the **IP Address** field and associated fields, as required.
   c. Click **Save**. The Appliance Manager applies the change to all appliance components. This process takes several minutes.
5. On the TRITON Unified Security Center machine, run the version 7.6 TRITON Installer and reinstall TRITON Unified Security Center and associated components. Refer to the list you made in Step 3.

> **Note**
> If TRITON Unified Security Center was not uninstalled prior to changing the IP address of interface C, uninstall and reinstall TRITON now.

6. On the Log Server machine, edit websense.ini and start the Log Server service:
   a. In the Windows file system, go to C:\Program Files\Websense\bin.
   b. In a text editor such as Notepad, open websense.ini and locate the entry for "PolicyServerIP =". Change the value to the new IP address of the C interface. Save and close the file.
   c. Start Log Server by going to the Windows Start menu and selecting **Programs** > **Websense** > **Utilities** > **Log Server Configuration**. On the Connections tab, click **Start**.
7. If Web DLP is configured, re-register Content Gateway with the Data Security Management Server and redeploy Web DLP:
   a. Log on to Content Gateway Manager and go to **Configure** > **Security** > **Data Security**.
   b. Enter the Data Security Management Server IP address, Data administrator user name and password.
   c. Click **Register**.
   d. Log on to the TRITON Unified Security Center and go to TRITON - Data Security.
   e. Go to **Settings** > **Deployment** > **System Modules**.
   f. Click **Deploy**.
   g. Restart all Content Gateway services, or the Content Gateway module.

Scenario 3: One or many appliances, Email Security Gateway only with off-box TRITON Unified Security Center and off-box Log Server

This is a recommended deployment for small and medium sized networks.

Step-by-step instructions:

1. If Email DLP is used:
   a. in TRITON - Email Security, go to **Settings** > **Data Security** and unregister DLP. Note the Data Security Management Server IP address. You must also know the administrator user name and password.
   b. In TRITON - Data Security, go to **Settings** > **System Module** and delete the entry for Email Security.
2. Change the IP address of interface C:
   a. Log on to the Appliance Manager and go to **Configuration** > **Network Interfaces**.
   b. In the Appliance Controller Interface (C) section, at the top of the page change the **IP Address** field and associated fields, as needed.
   c. Click **Save**. The Appliance Manager applies the change to all appliance components. This process takes several minutes.
3. In the TRITON - Email Security interface, go to **Settings** > **Email Appliances** and change the appliance IP address.
4. If Email DLP is used, in TRITON - Email Security, go to **Settings** > **Data Security** and re-register DLP.

Scenario 4: One appliance, Web Security and Email Security with off-box TRITON Unified Security Center and off-box Log Server

Step-by-step instructions:

1. If Web DLP is configured, unregister Content Gateway with the Data Security Management Server.
   a. Log on to Content Gateway Manager and go to **Configure** > **Security** > **Data Security**.
   b. Note the Data Security Management Server IP address. You must also know the administrator user name and password.
   c. Click **Unregister**.
2. If Email DLP is configured, unregister Email Security with the Data Security Management Server.

a. In TRITON - Email Security, go to **Settings** > **Data Security** and unregister DLP. Note the Data Security Management Server IP address. You must also know the administrator user name and password.

b. In TRITON - Data Security, go to **Settings** > **System Module** and delete the entry for Email Security.

3. On the Log Server machine, stop the Log Server service:

   a. From the Windows Start menu, select **Programs** > **Websense** > **Utilities** > **Log Server Configuration**.

   b. On the Connections tab, click **Stop**.

4. On the TRITON Unified Security Center machine, run the version 7.6 TRITON Installer and uninstall TRITON Unified Security Center and associated components (see the component list). Make a list of all uninstalled components.

5. Change the IP address of interface C:

   a. Log on to the Appliance Manager and go to **Configuration** > **Network Interfaces**.

   b. In the Appliance Controller Interface (C) section, at the top of the page change the **IP Address** field and associated fields, as needed.

   c. Click **Save**. The Appliance Manager applies the change to all appliance components. This process takes several minutes.

6. On the TRITON Unified Security Center machine, run the version 7.6 TRITON Installer and reinstall TRITON Unified Security Center and associated components. Refer to the list you made in Step 4.

   

   Note

   If TRITON Unified Security Center was not uninstalled prior to changing the IP address of interface C, uninstall and reinstall TRITON now.

7. On the Log Server machine, edit websense.ini and start the Log Server service:

   a. In the Windows file system, go to C:\Program Files\Websense\bin

   b. In a text editor such as Notepad, open websense.ini and locate the entry for “PolicyServerIP =”. Change the value to the new IP address of the C interface. Save and close the file.

   c. Start Log Server by going to the Windows Start menu and selecting **Programs** > **Websense** > **Utilities** > **Log Server Configuration**. On the Connections tab, click **Start**.

8. In the TRITON - Email Security interface, go to **Settings** > **Email Appliances** and change the appliance IP address.

9. If Email DLP is used, in TRITON - Email Security, go to **Settings** > **Data Security** and reregister DLP.

10. If Web DLP is used, reregister Content Gateway with the Data Security Management Server and redeploy Web DLP:

a. Log on to Content Gateway Manager and go to **Configure** > **Security** > **Data Security**.

b. Enter the Data Security Management Server IP address, Data administrator user name and password.

c. Click **Register**.

d. Log on to the TRITON Unified Security Center and go to TRITON - Data Security.

e. Go to **Settings** > **Deployment** > **System Modules**.

f. Click **Deploy**.

g. Restart all Content Gateway services, or the Content Gateway module.

Scenario 5: Multiple appliances in a cluster, Web Security only, off-box TRITON Unified Security Center and off-box Log Server

Covered under this scenario:

1. Changing the C interface of the Full policy source appliance
2. Changing the C interface of User directory and Filtering appliances
3. Changing the C interface of Filtering only appliances

Step-by-step instructions for changing the C interface of the Full policy source appliance:

1. If Web DLP is configured, unregister Content Gateway with the Data Security Management Server.
   a. Log on to Content Gateway Manager and go to **Configure** > **Security** > **Data Security**.
   b. Note the Data Security Management Server IP address. You must also know the administrator user name and password.
   c. Click **Unregister**.
2. On the Log Server machine, stop the Log Server service:
   a. From the Windows Start menu, select **Programs** > **Websense** > **Utilities** > **Log Server Configuration**.
   b. On the Connections tab, click **Stop**.
3. Remove the connection between TRITON - Web Security and any User directory and filtering appliances (this step applies only if you have entered User directory and filtering appliances as secondary Policy Servers in TRITON Unified Security Center):
   a. Log on to TRITON Unified Security Center and go to TRITON - Web Security.
   b. Go to **Settings** > **General** > **Policy Servers**.

c. Note the details of all secondary Policy Server entries

d. Select all User directory and filtering appliance entries and click **Delete**.

e. Click **OK** on the Policy Servers page to cache your changes. Changes are not implemented until you click **Save All**.

4. On the TRITON Unified Security Center machine, run the version 7.6 TRITON Installer and uninstall TRITON Unified Security Center and associated components (see the component list). Make a list of all uninstalled components.
5. Temporarily reconfigure appliances that depend on the appliance whose C interface IP address will change:
   a. Log on to each Appliance Manager and go to **Configuration > Web Security Components**.
   b. Under **Policy Source**, note the policy source IP address for this appliance.
   c. On the appliances set to **User directory and filtering** or **Filtering only**, set the policy source to **Full policy source**.
   d. Click **Save**.
6. Change the IP address of interface C on the original Full policy source appliance:
   a. Log on to the Appliance Manager and go to **Configuration > Network Interfaces**.
   b. In the Appliance Controller Interface (C) section, at the top of the page change the **IP Address** field and associated fields, as needed.
   c. Click **Save**. The Appliance Manager applies the change to all appliance components. This process takes several minutes.
7. Return the policy source settings of each appliance to their original mode:
   a. Log on to each Appliance Manager and go to **Configuration > Web Security Components**.
   b. Under **Policy Source**, set the policy source to its previous setting: either **User directory and filtering**, or **Filtering only**.
   c. Enter the new C interface IP address of the Full policy source appliance.
   d. Click **Save**.
8. On the TRITON Unified Security Center machine, run the version 7.6 TRITON Installer and reinstall TRITON Unified Security Center and associated components. Refer to the list you made in Step 4.

Note

If TRITON Unified Security Center was not uninstalled prior to changing the IP address of interface C, uninstall and reinstall TRITON now.

9. If you removed secondary Policy Server entries in step 3, reinstate the connection between TRITON - Web Security and any User directory and filtering appliances:
   a. Log on to TRITON Unified Security Center and go to TRITON - Web Security.

b. Go to **Settings** > **General** > **Policy Servers**.

c. Click **Add**.

d. Enter the secondary appliance details noted in step 3.

e. Click **OK** to save the Policy Server details.

f. Repeat the process for all of the secondary Policy Servers you removed in step 3, then click **OK** on the Policy Servers page to cache your changes. Changes are not implemented until you click **Save All**.

10. On the Log Server machine, edit websense.ini and start the Log Server service:

    a. In the Windows file system, go to C:\Program Files\Websense\bin

    b. In a text editor such as Notepad, open websense.ini and locate the entry for "PolicyServerIP =". Change the value to the new IP address of the C interface. Save and close the file.

    c. Start Log Server by going to the Windows Start menu and selecting **Programs** > **Websense** > **Utilities** > **Log Server Configuration**. On the Connections tab, click **Start**.

11. If Web DLP is used, reregister Content Gateway with the Data Security Management Server and redeploy Web DLP:

    a. Log on to Content Gateway Manager and go to **Configure** > **Security** > **Data Security**.

    b. Enter the Data Security Management Server IP address, Data administrator user name and password.

    c. Click **Register**.

    d. Log on to the TRITON Unified Security Center and go to TRITON - Data Security.

    e. Go to **Settings** > **Deployment** > **System Modules**.

    f. Click **Deploy**.

    g. Restart all Content Gateway services, or the Content Gateway module.

Step-by-step instructions for changing the C interface of the User directory and filtering appliance:

1. On the TRITON Unified Security Center machine, run the version 7.6 TRITON Installer and uninstall TRITON Unified Security Center and associated components that depend on or directly service the appliance that is being configured (for example, Network Agent). Make a list of all uninstalled components.
2. Temporarily reconfigure Filtering only appliances that depend on the User directory and Filtering appliance whose C interface IP address will change:

    a. Log on to each Appliance Manager and go to **Configuration** > **Web Security Components**.

    b. Set the policy source to **Full policy source**.

    c. Click **Save**.

3. Change the IP address of interface C on the User directory and filtering appliance:

a. Log on to the Appliance Manager and go to **Configuration** > **Network Interfaces**.

b. In the Appliance Controller Interface (C) section, at the top of the page change the **IP Address** field and associated fields, as needed.

c. Click **Save**. The Appliance Manager applies the change to all appliance components. This process takes several minutes.

4. Return the policy source settings of each Filtering only appliance to their original mode:

   a. Log on to each Appliance Manager and go to **Configuration** > **Web Security Components**.

   b. Under **Policy Source**, set the policy source to **Filtering only**.

   c. Enter the new C interface IP address of the User directory and filtering appliance.

   d. Click **Save**.

5. On the TRITON Unified Security Center machine, run the version 7.6 TRITON Installer and reinstall all off-box components that are registered to the reconfigured appliance. Refer to the list you made in Step 1.

> **Note**
> If TRITON Unified Security Center was not uninstalled prior to changing the IP address of interface C, uninstall and reinstall TRITON now.

Step-by-step instructions for changing the C interface of the Filtering only appliance:

1. On the TRITON Unified Security Center machine, run the version 7.6 TRITON Installer and uninstall TRITON Unified Security Center and associated components that depend on or directly service the appliance that is being configured (for example, Network Agent). Make a list of all uninstalled components.
2. Change the IP address of interface C on the Filtering only appliance:

   a. Log on to the Appliance Manager and go to **Configuration** > **Network Interfaces**.

   b. In the Appliance Controller Interface (C) section, at the top of the page change the **IP Address** field and associated fields, as needed.

   c. Click **Save**. The Appliance Manager applies the change to all appliance components. This process takes several minutes.

3. On the TRITON Unified Security Center machine, run the version 7.6 TRITON Installer and reinstall all off-box components that are registered to the reconfigured appliance. Refer to the list you made in Step 1.
4. Log on to the TRITON Unified Security Center and on the TRITON - Web Security **Today** page, click the IP address under **Filtering Service Summary**. Check the **Content Gateway Connections** field is displaying the correct IP

address. If this field is blank, or if there are issues with Content Gateway and Network Agent, restart the Content Gateway and Network Agent services on this appliance.

Scenario 6: Multiple appliances in a cluster, Web Security only, off-box Policy Broker, off-box TRITON Unified Security Center and off-box Log Server

> **Note**
> No appliance is set to Full policy source.

Step-by-step instructions:

1. If Web DLP is configured, unregister Content Gateway with the Data Security Management Server.
   a. Log on to Content Gateway Manager and go to **Configure** > **Security** > **Data Security**.
   b. Note the Data Security Management Server IP address. You must also know the administrator user name and password.
   c. Click **Unregister**.
2. On the TRITON Unified Security Center machine, run the version 7.6 TRITON Installer and uninstall TRITON Unified Security Center and associated components that depend on or directly service the appliance that is being configured (for example, Network Agent). Make a list of all uninstalled components.
3. Temporarily reconfigure the appliance you want to change:
   a. Log on to the Appliance Manager and go to **Configuration** > **Web Security Components**.
   b. Under **Policy Source**, note the policy source IP address for this appliance.
   c. Set the policy source to **Full policy source**.
   d. Click **Save**.
4. Change the IP address of interface C:
   a. In the Appliance Manager, go to **Configuration** > **Network Interfaces**.
   b. In the Appliance Controller Interface (C) section, at the top of the page change the **IP Address** field and associated fields, as needed.
   c. Click **Save**. The Appliance Manager applies the change to all appliance components. This process takes several minutes.
5. Return the policy source settings of the appliance to its original mode:
   a. In the Appliance Manager, go to **Configuration** > **Web Security Components**.

b. Under **Policy Source**, set the policy source to its previous setting: either **User directory and filtering**, or **Filtering only**.

c. Enter the policy source IP address that you noted in step 3.

d. Click **Save**.

6. On the TRITON Unified Security Center machine, run the version 7.6 TRITON Installer and reinstall all off-box components that are registered to the reconfigured appliance. Refer to the list you made in Step 2.

> **Note**
> If TRITON Unified Security Center was not uninstalled prior to changing the IP address of interface C, uninstall and reinstall TRITON now.

7. If Web DLP is used, reregister Content Gateway with the Data Security Management Server and redeploy Web DLP:

a. Log on to Content Gateway Manager and go to **Configure > Security > Data Security**.

b. Enter the Data Security Management Server IP address, Data administrator user name and password.

c. Click **Register**.

d. Log on to the TRITON Unified Security Center and go to TRITON - Data Security.

e. Go to **Settings > Deployment > System Modules**.

f. Click **Deploy**.

g. Restart all Content Gateway services, or the Content Gateway module.