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

Topic 60046 | Updated: 20-July-2012

Applies To:	Websense V10000 v7.7 Websense V10000 G2 v7.7 Websense V5000 G2 v7.7

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
- Filtering Plug-In
- 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*
- *Scenario 2: One appliance, Web Security only with off-box TRITON Unified Security Center, and off-box Log Server*
- *Scenario 3: One or many appliances, Email Security Gateway only with off-box TRITON Unified Security Center, and off-box Log Server*
- *Scenario 4: One appliance, Web Security and Email Security with off-box TRITON Unified Security Center, and off-box Log Server*
- *Scenario 5: Multiple appliances in a cluster, Web Security only, off-box TRITON Unified Security Center, and off-box Log Server*
- *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*

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

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

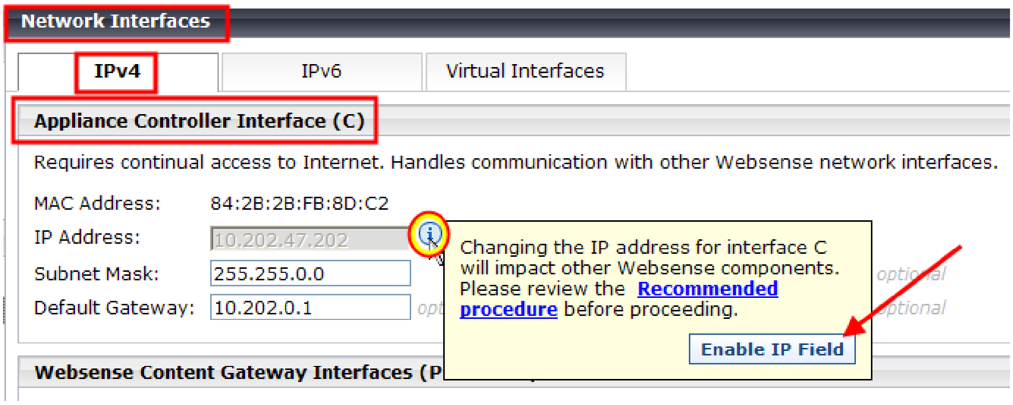
Step-by-step instructions:

1. Perform a full backup of the appliance and save it to an off-appliance location.
2. On the Log Server machine, stop the Log Server service.

   Use the **Windows Services** applet to stop the **Websense Log Server** service (**Start** > **Administrative Tools** > **Services**).
3. Change the C interface IP address:

   a. Log on to the Appliance Manager and go to **Configuration** > **Network Interfaces** > **IPv4**.

   b. In the **Appliance Controller Interface (C)** section, place the mouse pointer over the "i" icon until the text box appears.



Appliance Controller Interface (C)

Requires continual access to Internet. Handles communication with other Websense network interfaces.

MAC Address: 84:2B:2B:FB:8D:C2

IP Address: 10.202.47.202

Subnet Mask: 255.255.0.0

Default Gateway: 10.202.0.1

Changing the IP address for interface C will impact other Websense components. Please review the Recommended procedure before proceeding.

Websense Content Gateway Interfaces (P

   c. Click **Enable IP Field** and change the **IP Address** and associated fields, as needed.

   d. Click **OK**. 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 (x86)\Websense\Web Security\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. Use the **Windows Services** applet (**Start** > **Administrative Tools** > **Services**) to start the **Websense Log Server** service.

5. Restart all Content Gateway services.

> ✓ **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. As a precaution, perform a full backup of the appliance and all off-box components. Save the backups to a network location.

2. If Web DLP is configured (only with Web Security Gateway Anywhere), unregister Content Gateway with the Data Security Management Server:

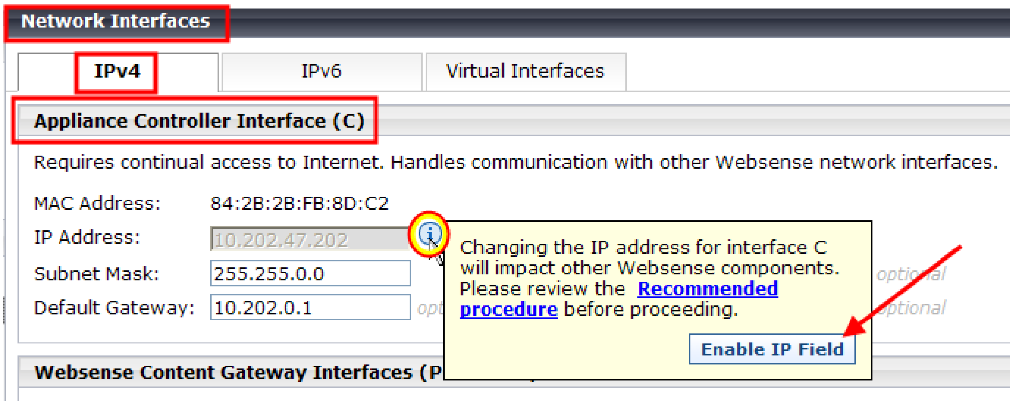
   a. Log on to **Content Gateway Manager** and go to **Configure** > **My Proxy** > **Basic**.

   b. In the **Features** > **Networking** section, turn off **Data Security** and restart Content Gateway.

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

   Use the **Windows Services** applet to stop the **Websense Log Server** service (**Start** > **Administrative Tools** > **Services**).

4. On the TRITON Unified Security Center machine, run the version 7.7 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 C interface IP address:
   a. Log on to the Appliance Manager and go to **Configuration > Network Interfaces > IPv4**.
   b. In the **Appliance Controller Interface (C)** section, place the mouse pointer over the “i” icon until the text box appears.



Appliance Controller Interface (C)

Requires continual access to Internet. Handles communication with other Websense network interfaces.

MAC Address: 84:2B:2B:FB:8D:C2

IP Address: 10.202.47.202

Subnet Mask: 255.255.0.0

Default Gateway: 10.202.0.1

Changing the IP address for interface C will impact other Websense components. Please review the Recommended procedure before proceeding.

Websense Content Gateway Interfaces (P

   c. Click **Enable IP Field** and change the **IP Address** and associated fields, as needed.
   d. Click **OK**. 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 7.7 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 (x86)\Websense\Web Security\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. Use the **Windows Services** dialog box (**Start > Administrative Tools > Services**) to start the **Websense Log Server** service.
8. If Web DLP was configured, re-enable Data Security:
   a. Log on to **Content Gateway Manager** and go to **Configure > My Proxy > Basic**.

b. In the **Features** > **Networking** section, turn on **Data Security**, select **Integrated on-box,** and restart Content Gateway. Wait for the restart to complete.

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

d. Go to **Settings** > **Deployment** > **System Modules** and click **Deploy**.

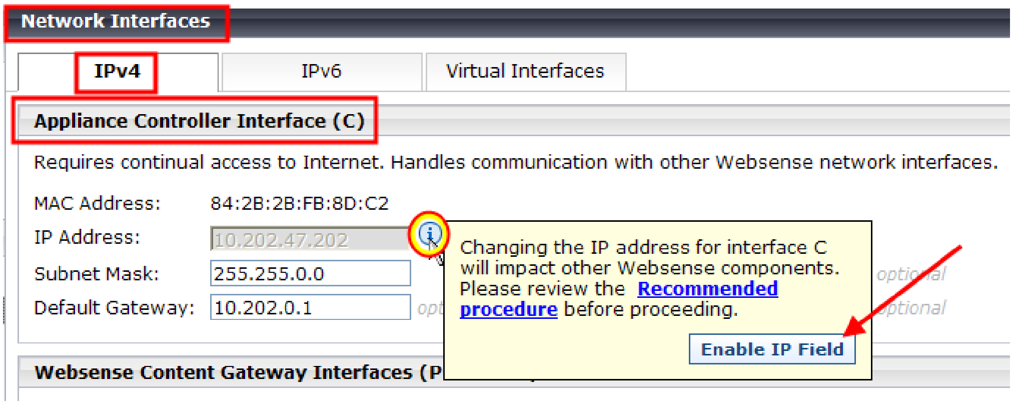
If the above procedure fails, see the "Manual registration" section of this article in the Websense Technical library.

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. As a precaution, perform a full backup of the appliance and all off-box components and save the backups to a network location.
2. If Email DLP is used:
   a. In TRITON - Email Security, go to **Settings** > **General** > **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** > **Deployment** > **System Module** and delete the entry for Email Security.
3. Change the C interface IP address:
   a. Log on to the Appliance Manager and go to **Configuration** > **Network Interfaces** > **IPv4**.
   b. In the **Appliance Controller Interface (C)** section, place the mouse pointer over the "i" icon until the text box appears.



Requires continual access to Internet. Handles communication with other Websense network interfaces.

MAC Address: 84:2B:2B:FB:8D:C2

IP Address: 10.202.47.202

Subnet Mask: 255.255.0.0

Default Gateway: 10.202.0.1

Changing the IP address for interface C will impact other Websense components. Please review the Recommended procedure before proceeding.

   c. Click **Enable IP Field** and change the **IP Address** and associated fields, as needed.

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

4. In the TRITON - Email Security interface, go to **Settings** > **General** > **Email Appliances** and click on the host name link to change the appliance IP address.
5. If Email DLP is used, in TRITON - Email Security, go to **Settings** > **General** > **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:

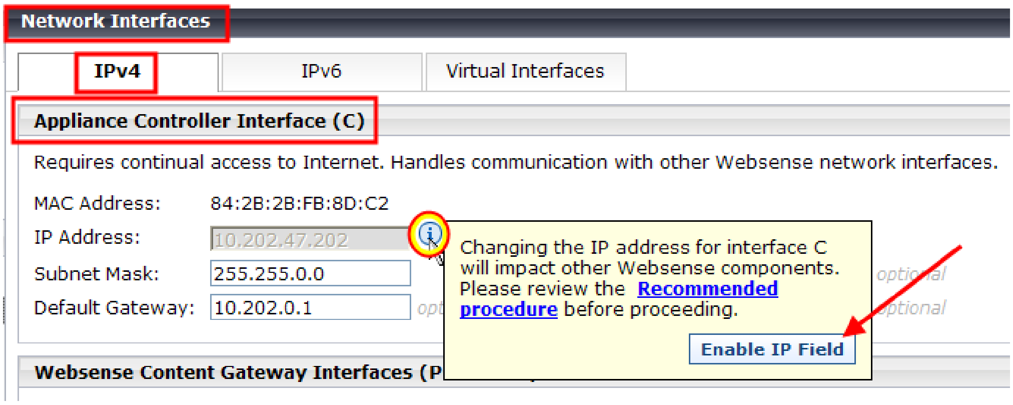
1. As a precaution, perform a full backup of the appliance and all off-box components. Save the backups to a network location.
2. If Web DLP is configured (only with Web Security Gateway Anywhere), unregister Content Gateway with the Data Security Management Server:
   a. Log on to **Content Gateway Manager** and go to **Configure** > **My Proxy** > **Basic**.

   b. In the **Features** > **Networking** section, turn off **Data Security** and restart Content Gateway.
3. If Email DLP is used (only with Email Security Gateway Anywhere):
   a. In TRITON - Email Security, go to **Settings** > **General** > **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** > **Deployment** > **System Module** and delete the entry for Email Security.
4. On the Log Server machine, stop the Log Server service.

   Use the **Windows Services** applet to stop the **Websense Log Server** service (**Start** > **Administrative Tools** > **Services**).
5. On the TRITON Unified Security Center machine, run the version 7.7 TRITON Installer and uninstall TRITON Unified Security Center and associated components (see the component list). Make a list of all uninstalled components.
6. Change the C interface IP address:
   a. Log on to the Appliance Manager and go to **Configuration** > **Network Interfaces** > **IPv4**.

b. In the **Appliance Controller Interface (C)** section, place the mouse pointer over the “i” icon until the text box appears.



Requires continual access to Internet. Handles communication with other Websense network interfaces.

MAC Address: 84:2B:2B:FB:8D:C2

IP Address: 10.202.47.202

Subnet Mask: 255.255.0.0

Default Gateway: 10.202.0.1

Changing the IP address for interface C will impact other Websense components. Please review the Recommended procedure before proceeding.

c. Click **Enable IP Field** and change the **IP Address** and associated fields, as needed.

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

7. On the TRITON Unified Security Center machine, run the version 7.7 TRITON Installer and reinstall TRITON Unified Security Center and associated components. Refer to the list you made in step 5.

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

8. In the **TRITON - Email Security** interface, go to **Settings** > **General** > **Email Appliances** and click on the host name link to change the appliance IP address.

9. 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 (x86)\Websense\Web Security\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. Use the **Windows Services** dialog box (**Start** > **Administrative Tools** > **Services**) to start the **Websense Log Server** service.

10. If Email DLP is used, in **TRITON - Email Security**, go to **Settings** > **General** > **Data Security** and re-register DLP.

11. If Web DLP was configured, re-enable Data Security:

    a. Log on to **Content Gateway Manager** and go to **Configure** > **My Proxy** > **Basic**.

    b. In the **Features** > **Networking** section, turn on **Data Security**, select **Integrated on-box,** and restart Content Gateway. Wait for the restart to complete.

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

d. Go to **Settings** > **Deployment** > **System Modules** and click **Deploy**.

If the above procedure fails, see the “Manual registration” section of this article in the Websense Technical library.

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

Covered in 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

> **Important**
>
> As a precaution, perform a full backup of the appliance(s) that is changing C interface IP address, and backup all off-box components. Save the backups to a network location.

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

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

   a. Log on to **Content Gateway Manager** and go to **Configure** > **My Proxy** > **Basic**.

   b. In the **Features** > **Networking** section, turn off **Data Security** and restart Content Gateway.

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

   Use the **Windows Services** applet to stop the **Websense Log Server** service (**Start** > **Administrative Tools** > **Services**).

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**. Note the details of all secondary Policy Server entries.

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

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

4. On the TRITON Unified Security Center machine, run the version 7.7 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 is changing:

   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.

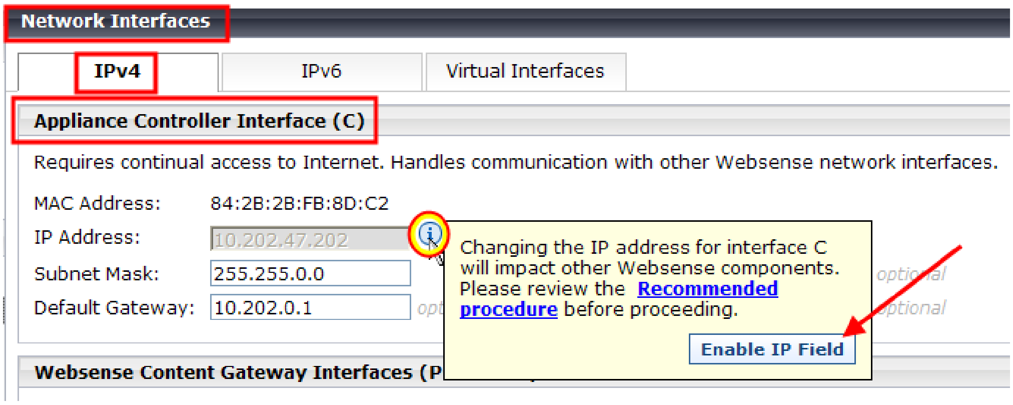
   c. On the appliances set to **User directory and filtering** or **Filtering only**, set the policy source to **Full policy source**.

   d. Click **OK**.

6. Change the C interface IP address on the original Full policy source appliance:

   a. Log on to the Appliance Manager and go to **Configuration** > **Network Interfaces** > **IPv4**.

   b. In the **Appliance Controller Interface (C)** section, place the mouse pointer over the “i” icon until the text box appears.



Requires continual access to Internet. Handles communication with other Websense network interfaces.

MAC Address: 84:2B:2B:FB:8D:C2

IP Address: 10.202.47.202

Subnet Mask: 255.255.0.0

Default Gateway: 10.202.0.1

Changing the IP address for interface C will impact other Websense components. Please review the Recommended procedure before proceeding.

   c. Click **Enable IP Field** and change the **IP Address** and associated fields, as needed.

   d. Click **OK**. 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 **OK**.

8. On the TRITON Unified Security Center machine, run the version 7.7 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 and Deploy**.
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 (x86)\Websense\Web Security\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. Use the **Windows Services** dialog box (**Start** > **Administrative Tools** > **Services**) to start the **Websense Log Server** service.
11. If Web DLP was configured, re-enable Data Security:
    a. Log on to **Content Gateway Manager** and go to **Configure** > **My Proxy** > **Basic**.
    b. In the **Features** > **Networking** section, turn on **Data Security**, select **Integrated on-box,** and restart Content Gateway. Wait for the restart to complete.
    c. Log on to the TRITON Unified Security Center and go to TRITON - Data Security.
    d. Go to **Settings** > **Deployment** > **System Modules** and click **Deploy**.

    If the above procedure fails, see the "Manual registration" section of this article in the Websense Technical library.

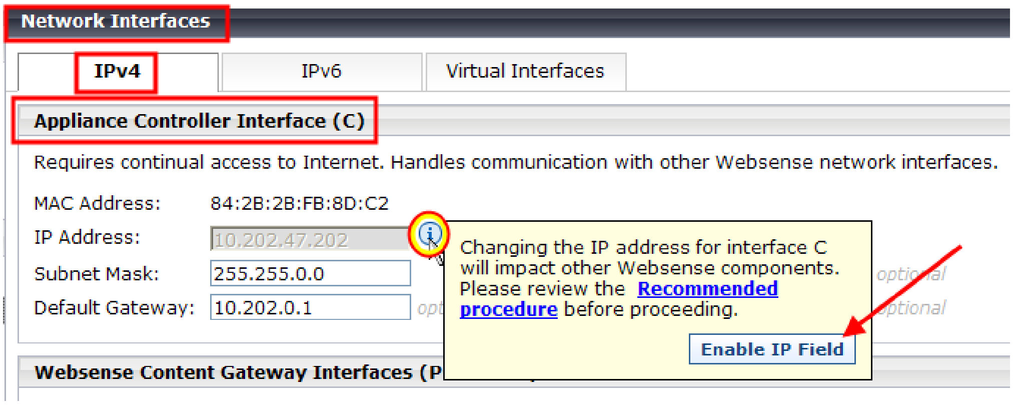
Step-by-step instructions for changing the C interface of the User directory and filtering appliance:

1. On the TRITON Unified Security Center machine, run the version 7.7 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 **OK**.
3. Change the C interface IP address on the User directory and filtering appliance:
    a. Log on to the Appliance Manager and go to **Configuration** > **Network Interfaces** > **IPv4**.

    b. In the **Appliance Controller Interface (C)** section, place the mouse pointer over the “i” icon until the text box appears.



Appliance Controller Interface (C)

Requires continual access to Internet. Handles communication with other Websense network interfaces.

MAC Address: 84:2B:2B:FB:8D:C2

IP Address: 10.202.47.202

Subnet Mask: 255.255.0.0

Default Gateway: 10.202.0.1

Changing the IP address for interface C will impact other Websense components. Please review the Recommended procedure before proceeding.

    c. Click **Enable IP Field** and change the **IP Address** and associated fields, as needed.

    d. Click **OK**. 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.

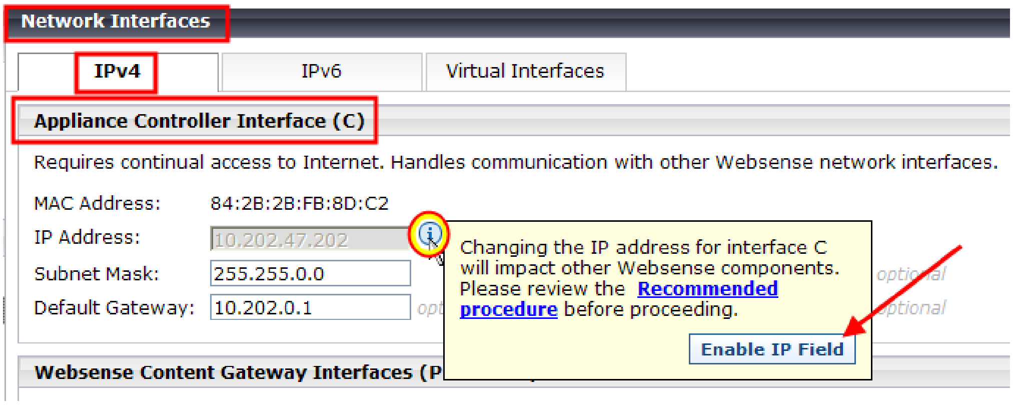
    d. Click **OK**.

5. On the TRITON Unified Security Center machine, run the version 7.7 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 7.7 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 C interface IP address on the Filtering only appliance:
   a. Log on to the Appliance Manager and go to **Configuration > Network Interfaces > IPv4**.
   b. In the **Appliance Controller Interface (C)** section, place the mouse pointer over the “i” icon until the text box appears.



Appliance Controller Interface (C)

Requires continual access to Internet. Handles communication with other Websense network interfaces.

MAC Address: 84:2B:2B:FB:8D:C2

IP Address: 10.202.47.202

Subnet Mask: 255.255.0.0 optional

Default Gateway: 10.202.0.1 optional

Changing the IP address for interface C will impact other Websense components. Please review the Recommended procedure before proceeding.

Websense Content Gateway Interfaces (P

   c. Click **Enable IP Field** and change the **IP Address** and associated fields, as needed.
   d. Click **OK**. 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 7.7 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 **Status > Dashboard > System** page, click the IP address under **Filtering Service Status**. Check that 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

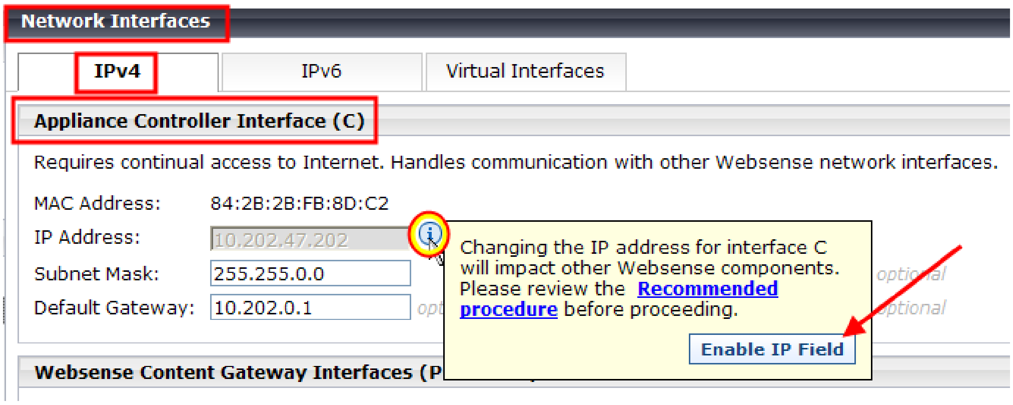
✓ **Note**

No appliance is set to Full policy source.

Step-by-step instructions:

1. As a precaution, perform a full backup of affected appliances, as well as all off-box components. Save the backups to a network location.
2. If Web DLP is configured (only with Web Security Gateway Anywhere), unregister Content Gateway with the Data Security Management Server:
   a. Log on to **Content Gateway Manager** and go to **Configure > My Proxy > Basic**.
   b. In the **Features > Networking** section, turn off **Data Security** and restart Content Gateway.
3. On the TRITON Unified Security Center machine, run the version 7.7 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.
4. 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 **OK**.
5. Change the C interface IP address:
   a. Log on to the Appliance Manager and go to **Configuration > Network Interfaces > IPv4**.

b. In the **Appliance Controller Interface (C)** section, place the mouse pointer over the “i” icon until the text box appears.



Appliance Controller Interface (C)

Requires continual access to Internet. Handles communication with other Websense network interfaces.

MAC Address: 84:2B:2B:FB:8D:C2

IP Address: 10.202.47.202

Subnet Mask: 255.255.0.0

Default Gateway: 10.202.0.1

Changing the IP address for interface C will impact other Websense components. Please review the Recommended procedure before proceeding.

Websense Content Gateway Interfaces (P

c. Click **Enable IP Field** and change the **IP Address** and associated fields, as needed.

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

6. 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 4.

   d. Click **OK**.

7. On the TRITON Unified Security Center machine, run the version 7.7 TRITON Installer and reinstall all off-box components that are registered to the reconfigured appliance. 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.

8. If Web DLP was configured, re-enable Data Security:

   a. Log on to **Content Gateway Manager** and go to **Configure** > **My Proxy** > **Basic**.

   b. In the **Features** > **Networking** section, turn on **Data Security**, select **Integrated on-box,** and restart Content Gateway. Wait for the restart to complete.

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

   d. Go to **Settings** > **Deployment** > **System Modules** and click **Deploy**.

If the above procedure fails, see the section titled “Manual registration” in this article in the Websense Technical library.