How to Configure the CC Syslog Service

https://campus.barracuda.com/doc/73719514/

The CC Syslog Service is installed and configured on the box layer of the Barracuda Firewall Control Center.

Configure the CC Syslog Service

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > CC Syslog Service**.
2. Click **Lock**.
3. In the left menu expand **Configuration Mode** section and click **Advanced View**.
4. From the **Configuration** menu on the left, select **Basic Setup** and specify the parameters as described in the **Basic Setup** section.
5. Select **Trusted Data Reception** from the **Configuration** menu on the left and specify the parameters as described in the **Trusted Data Reception Settings** section.
6. Select **Local Storage** from the **Configuration** menu on the left and specify the parameters as described in the **Local Storage Settings**section.
   This tab is used for configuring the local behavior of the syslog service on the Barracuda Firewall Control Center box. This tab is only editable if parameter **Store on Disk** (see section **Basic Setup**) is set to **yes**.
7. Select **HA Synchronization** from the **Configuration** menu on the left and specify the parameters as described in the **HA Synchronization Settings** section.
   The log message synchronisation between HA partners is configured via this tab.
8. Select **Relaying Setup** from the **Configuration** menu on the left and specify the parameters as described in the **Relaying Setup** section.
9. Select **Relay Filters** from the **Configuration** menu on the left and specify the parameters as described in the **Relay Filter Settings**section.
10. Select **Relay Destinations** from the **Configuration** menu on the left and specify the parameters as described in the **Relay Destination Settings**section.
11. Select **Relay Streams** from the **Configuration** menu on the left, and specify the following settings:
    - **Name** – Here the name of the stream is displayed.
    - **Log Destinations** – Here the available log destinations (defined in the section Relay Destinations) can be selected.
    - **Log Filters** – Here the available log filters (defined in Relay Filters) can be selected.

    Configuring section **Relay Streams** concludes the configuration of log streaming. However, this section requires parameter **External Relaying** (see section **Basic Setup**) to be set to **yes** in order to become active. For creating a new relay stream, click the **+** icon and enter a name for the relay stream.
12. Click **OK**.
13. Click **Send Changes** and **Activate**.

CC Syslog Service Settings

The following sections provide more information on the settings that you can configure in the **CC Syslog Service Settings** configuration windows:

Basic Setup

Operational Setup

Parameter	Description
Idle Mode	Syslogging is activated by default (setting **no**, that means *not idle*). When active, the service listens for incoming log messages from its managed boxes and, therefore, processes them as configured through the following parameters. Nonetheless, even when idle (setting **yes**, that means *idle*) it also listens for incoming messages to avoid *ICMP Port Unreachable* messages from being sent back to the connecting systems. It then simply discards the received messages.
Run as User	(Only available in **Advanced View** mode) This parameter defines the username that will be used when synchronising the log with the HA partner system. By default, this parameter is set to system user *msyslog*. By ticking the checkbox **Other** (to the right), you may enter any other name. Once set, do not change.
User ID	(Only available in **Advanced View** mode) Here the ID of the system user (parameter **Run as User**, see above) is defined (default: **7999**).
Service Key	This parameter is required for authentication purposes against connecting clients using the SSL connections. In order to create a new 1024-bit SSL private key, simplly click **New Key**. On the right of this line, the hash of the certificate is displayed. By default creating a new SSL private key results in a freshly generated *Service Certificate* (see below) that is automatically signed with the new private key.
Service Certificate	This certificate is required for SSL connections, regardless whether they are passive or active ones. Via button **Show ...** the certificate is displayed, and via button **Edit ...** the certificate may be modified. Again, to the right, the hash mark is displayed. Both the SSL Private Key **AND** SSL Certificate must have the same hash mark.

Support Trusted Data Reception	If set to **yes** (default) the service will listen for incoming SSL connections on configured IPs and defined SSL Listen Port (port 5143; Trusted Data Reception view). This option is not needed when managed boxes deliver log content through a box management tunnel. Boxes without a management tunnel should use the SSL option for delivery. In this case you should not set this option to no and likewise configure the affected boxes to use SSL for log delivery.
Store on Disk	Setting this parameter to **yes** (default: **no**) causes writing the incoming log messages to the specified logging path (customizable via parameter **Local Log Directory**, see **Local Storage** section below). By default the path for logging is */var/phion/mlogs*.
Sync to HA Partner	This parameter enables the real-time transfer of log messages to the HA partner. As a matter of fact, this parameter is only available if parameter Store on Diskis set to **yes**. Synchronising takes place via a SSHv2 tunnel between the HA partners. For more information, see: High Availability.
External Relaying	This parameter enables the optional transfer of log messages to external loghosts (default: **no**).

Plain Data Reception

This parameter set is only available in **Advanced View** mode.

Parameter	Description
Supported Protocols	Via this parameter you define what kind of sockets are available for incoming log messages. Available options are **UDP&TCP** (opens an UDP and a TCP socket; default), **UDP** (opens an UDP socket only) and **TCP** (opens a TCP socket only).
UDP Port	This parameter is only available as long as the parameter **Supported Protocols** contains an UDP option and defines the port that is to be used for receiving log messages (default: **5144**). If you change this port assignment to another port (be sure to use a port higher than 1024) you need to adjust the local firewall rule set on the CC box.
TCP Port	This parameter is only available as long as the parameter **Supported Protocols** contains a TCP option and defines the port that is to be used for receiving log messages (default: **5144**). If you change this port assignment to another port (be sure to use a port higher than 1024) you need to adjust the local firewall rule set on the CC box.

Trusted Data Reception Settings

Trusted Data Reception (Only available in Advanced View mode)

Parameter	Description

SSL Listen Port	This parameter defines the listening port for SSL connections (default: **5143**).
SSL Busy Timeout [s]	This timeout defines for how long (in seconds) an SSL connection may be in busy condition until it is terminated (default: **300**).
SSL Close Timeout [s]	This timeout defines for how long (in seconds) an SSL connection may be in close condition until it is terminated (default: **60**).
SSL Idle Timeout[s]	This timeout defines for how long (in seconds) an SSL connection may be in idle condition until it is terminated (default: **43200**).

SSL Client Authentication

Parameter	Description
Service Certificate	Via this menu the to-be-used service certificate is selected (default: **Use_MC_SSL_Cert**; that means the SSL certificate of the Barracuda Firewall Control Center will be used for authentication. When using option **Use_MC_SSL_Cert** it is highly recommended to use **verify_peer_certificate** as type of **Client Authentication**. When updating (not newly installing) the system from any version prior to version 2.4.2 (all versions up to 2.4.1-x) the CC SSL Certificate is not yet present. To create the certificate, open the **CC Identity** file and make a dummy change followed by activation. Barracuda CloudGen Firewall versions 2.4.2 and higher already contain the certificate, so it need not be activated.
Client Authentication	Here you define the way clients will authenticate themselves (default: **verify_peer_with_locally_installed_certificate**).
Trusted Clients	This section is used for importing/exporting the client certificates required for authentication when using SSL-based log delivery to the CC.

Local Storage Settings

Parameter	Description
Local Log Directory	(Only available in **Advanced View** mode) This field holds the path where the logs of the syslog service are written to (default: */var/phion/mlogs*). This directory belongs to the configured system user (parameter **Run as User**, see section **Basic Setup**).
Use Time Received	(Only available in **Advanced View** mode) Take into consideration that this parameter is only available if parameter **Store on Disk** is set to **yes**. Each log message has a send-time stamp when it is written to disk: • *send_stamp log_message*: **yes** – *send_stamp* is rewritten using local CC receive time. • *send_stamp log_message*: **no** (default) – *send_stamp* is not modified.

Prepend Received Time	(Only available in **Advanced View** mode) This parameter is only available if parameter **Store on Disk** is set to **yes**. Each log message gets its own time stamp(s) when it is written to disk (*receive_time_stamp* showing CC receiving time; *send_stamp* showing Box sending time): • receive_time_stamp send_stamp log_message when set to **yes** (default). • *send_stamp log_message* when set to **no**.
File Sync Frequency[lines]	(Only available in **Advanced View** mode) This parameter defines the number of lines after which the synchronisation is started. The default value of **0** indicates that there is currently no delay set.
Log Keep Duration	Via this parameter you define for how long the log files are kept on the local system. The following periods are available: • **day** – log file name: .$HOUR.log; after 23 h the log files created by syslog are overwritten. • **week** (default) – log file name: .$WEEKDAY.$HOUR.log; after one week the log files (that is mon, tue, wed, ...) created by syslog are overwritten. After one week the log files are overwritten • **no-limit** – log file name: .log; This setting is very specific and, therefore, should be used by experts only (contacting Barracuda Networks Technical Support is highly recommended).

HA Synchronization Settings

Parameter	Description
SSH Authentication Key	Here the SSH key management is provided. By clicking **New Key** you may create a new key for the SSH connection. Alternatively, you may import already existing keys (either from clipboard or file) or export the newly generated key (either to clipboard or file, password protected or not, or the public key only). These import/export options are available within the menu **Ex/Import**. For informational purpose the key's hash is displayed to the right of this line.
SSH Host Key	Here the SSH host key management is provided. By clicking **New Key** you may create a new SSH key. Alternatively, you may import already existing keys (either from clipboard or file) or export the newly generated key (either to clipboard or file, password protected or not, or the public key only). These import/export options are available within the **Ex/Import** menu. For informational purpose the key's hash is displayed to the right of this line.
SSH Listen Port	(Only available in **Advanced View** mode) This parameter defines the port that will be used for establishing the SSH connection (default: **5145**).
Use Compression	Here you may activate/deactivate data compression (standard gzip quality) for the SSH connection (default: **yes**).

Override SyncIP-Primary / Override SyncIP-Secondary	(Only available in **Advanced View** mode) The default HA sync is carried out between the box IPs of the HA partners. These override parameters allow using the IP addresses of the private uplink connection between the HA partners. Simply enter the proper IP addresses and the log-message transfer is done via the private uplink. This may come handy if the synchronising load is quite high.
TCP Sync Frequency (lines)	This parameter is only available if parameter **Store on Disk** (see section **Basic Setup**) is set to **yes**. This parameter defines the number of log messages after which synchronisation is started. The default value of **0** indicates nothing else than immediate synchronisation as soon as a log message is received.

Relaying Setup

The following parameters are available for relaying configuration to an external host:

Parameter	Description
TCP Retry Interval [s]	Here the time interval (in seconds) is defined at which a TCP retry should be carried out if the connection breaks.

SSL Delivery Setup

Parameter	Description
SSL Peer Authentication	This parameter defines whether authentication takes place when establishing the SSL connection. The following options are available: • **no_peer_verification** (default) • **verify_peer_with_locally_installed_certificate** – Selecting this option requires manual import of a valid SSL certificate from the active connecting system to the active destination system.
SSL Busy Timeout [s]	This timeout defines for how long (in seconds) a SSL connection may be in busy condition until it is terminated (default: **300**).
SSL Close Timeout [s]	This timeout defines for how long (in seconds) a SSL connection may be in close condition until it is terminated (default: **60**).
SSL Idle Timeout[s]	This timeout defines for how long (in seconds) a SSL connection may be in idle condition until it is terminated (default: **43200**).

Relay Filter Settings

Relay Filters

This view offers parameters for configuring profiles, which define the log file type which is to be

transferred/streamed. However, this section requires parameter **External Relaying** (see section **Basic Setup**) to be set to **yes** in order to become active. For creating a new relay filter, click the **+** icon and enter a name for the filter.

Parameter	Description
Filter Box Affiliation	This parameter specifies whether additional information (for example box, cluster, range) is transmitted with the log entries (default: **yes**). Setting this parameter to **yes** activates and requires parameter group **Originator Systems** (see below).
Originator Systems	Take into consideration that this parameter group is only available if parameter **Filter Box Affiliation** is set to **yes**. The configuration dialog for a new and/or existing entry provides the following parameters: • **Hierarchy Structure** – This parameter defines the structure of the log entry. The following structure levels are available for selection: • **Box-Only** – Adds only the box name to the log message. • **Range-Only** – Adds only the range number to the log message. • **Range-Cluster** – Adds both, range number and cluster name to the log message. • **Range-Cluster-Box (def)** – Adds the complete structure to the log message. • **Ranges** – This parameter is only available if parameter **Originator Systems** is set to a value that contains range structure (that means all except for Box-Only) and allows selecting specific ranges. • **Clusters** – This parameter is only available if parameter **Originator Systems** is set to a value that contains cluster structure and allows selecting specific clusters. • **Boxes** – This parameter is only available if parameter **Originator Systems** is set to a value that contains box structure and allows selecting specific boxes.

Data Selection

Parameter	Description
Special File Patterns	Due to the structure of a streamed log message (**///:**), it is possible to restrict log streaming to message containing a certain pattern in their filenames (for example *pattern fw* when having a filename like *server1_fw*) by using this parameter.

Top Level Logdata	The log files offered for selection here are superordinate log files build up of several instances of box and service levels. The following data can be selected: • **Fatal_log**: These are the log contents of the fatal log (log instance name: *fatal*). • **Firewall_Audit_Log**: These are the log contents of the firewall's machine readable audit data stream. Whether data is streamed into the Firewall_Audit_Log has to be configured in the Firewall Parameter Settings on box-level (see SECTION AUDIT INFO GENERATION > Audit-Delivery: Syslog-Proxy). The log instance name corresponding to Syslog-Proxy selected will be trans7. When **Log-File** is selected in the firewall configuration the data will go into a log file named (**Box** > **Firewall** > **audit**, the instance is named *box_Firewall_audit*) and thus this filter setting is not applicable. The pertinent one then would be a selection of category *Firewall* within the box selection portion of the filter.
Affected Box Logfiles	This parameter defines what kind of box logs are to be affected by the syslog daemon. The following options are available: • **All** (any kind of box log is affected) • **None** (default; none is affected) • **Selection** (activates parameter group Box Log Patterns, see below)
Box Log Patterns	Take into consideration that this parameter group is only available if parameter **Affected Box Logfiles** is set to **Selection**. The following parameters are available for configuration: • **Log Groups** – This menu offers every log group for selection that is available on a Barracuda CloudGen Firewall (for example Control, Event, Firewall, ...). • **Log Message Filter** – This parameter is used for defining the affected log types: *Selection* (activates parameter **Selected Message Types**, see below), *All (default), All-but-Internal, Notice-and-Higher, Warning-and-Higher, Error-and-Higher.* As you can see the available options are "group selections". If one explicit log type is required, choose *Selection* and set your wanted type in parameter **Selected Message Types**, see below. • **Selected Message Types** – This parameter allows you to set explicit log types to be affected by syslogging. The types available are: **Panic, Security, Fatal, Error, Warning, Notice, Info, Internal**.
Affected Service Logfiles	This parameter defines what kind of logs created by services are to be affected by the syslog daemon. The following options are available: • **All** (any kind of service log is affected) • **None** (default; none is affected) • **Selection** (activates parameter group **Service Log Patterns**, see below)

Service Log Patterns	Take into consideration that this parameter group is only available if parameter **Affected Service Logfiles** is set to **Selection**. • **Log Server-Services** – Here you define server and service where log messages are streamed from. • **Log Message Filter** – This parameter is used for defining the affected log types: ◦ **Selection** (activates parameter **Selected Message Types**, see below) ◦ **All** (default) ◦ **All-but-Internal** ◦ **Notice-and-Higher** ◦ **Warning-and-Higher** ◦ **Error-and-Higher** • **Selected Message Types** – This parameter allows you to set explicit log types to be affected by syslogging. The types available are: **Panic, Security, Fatal, Error, Warning, Notice, Info, Internal**.

Relay Destination Settings

Relay Destination

This view offers parameters for configuring profiles, which define where logging ought to be transferred/streamed to. However, this section requires parameter **External Relaying** (see section **Basic Setup**) to be set to **yes** in order to become active. For creating a new relay destination, click the **+** icon and enter a name for the destination.

Parameter	Description
Connection Type	This menu provides different types for the destination connection: • **Active SSL connect by destination** – if an external system requests logs actively via SSL. • **Stream SSL to passive destination** – for std. secure streaming from CC box to external system via SSL • **Stream plaintext to passive destination** – for streaming without SSL connection (standard syslog stream)
Local SSL Port	(Only available in **Advanced View** mode) This menu defines the port that will be used for establishing the SSL connection between CC box and external system. The available standard port range reaches from 5244 (default) up to 5253. If required, you may enter a custom port by simply ticking the checkbox **Other**. Make sure to use a port higher than 1024.
Destination SSL Certificate	This certificate is used when selecting **Active SSL connect by destination** as **Connection Type**. It holds the certificate of the connecting remote SSL client. This line consists of two buttons: **Show** for displaying the current SSL certificate, and **Ex/Import** for certificate transfer purpose.

Stream to Destination Setup

Parameter	Description
Destination IP	This parameter is only available when **Stream plaintext to passive destination** is selected as **Connection Type**. It allows you to enter the explicit IP address of the log host.
Destination Port	This parameter is only available when **Stream plaintext to passive destination** is selected as **Connection Type**. It holds the port that will be used on the log host when connecting.
Transmission Mode	This parameter is only available when **Stream plaintext to passive destination** is selected as **Connection Type**. It allows you to choose the transmission protocol (**TCP** (default) or **UDP**). When selecting a SSL-capable destination type this parameter is implicitly set to **TCP**.
Destination SSL Certificate	This certificate is used when **Stream SSL to passive destination** is selected as **Connection Type**. It holds the SSL certificate of the destination server. This line consists of two buttons: **Show** for displaying the current SSL certificate, and **Ex/Import** for certificate transfer purpose.
Destination SSL IP	This parameter is only available when **Stream plaintext to passive destination** is selected as **Connection Type**. It is used for entering the IP address of the external system the outgoing SSL tunnel should connect to.
Destination SSL Port	This parameter is only available when **Stream plaintext to passive destination** is selected as **Connection Type**. It is used for entering the port on the external system the outgoing SSL tunnel should connect to.
Loopback SSL Port	This parameter is only available when **Stream plaintext to passive destination** is selected as **Connection Type** and defines the to-be-used port for the loopback interface. The available standard port range spans the ports 5244 (default) up to 5253. If required, you may enter a custom port by simply ticking the checkbox **Other**. Make sure to use a port higher than 1024.
Sender IP	(Only available in **Advanced View** mode) Depending on your policy routing you may need an explicit sender IP address for streaming log files. If so, this address ought to be entered here.

Data Tag Policy

Parameter	Description
Keep Structural Info	The default setting **no** removes the structural information from streamed messages. When set to **yes** the structure information as originally sent to the CC Syslog is preserved. In other words: *<range>///: becomes :.*