NextGen Admin Settings

https://campus.barracuda.com/doc/53248525/

The following sections provide information on how to configure Barracuda NextGen Admin settings using the NextGen Admin User Interface configuration. To access the configuration menu, click the **OPTIONS** tab at the top left, and then selecting **Settings**.

Client Settings

To configure the connection and display for NextGen Admin, specify the client settings according to your requirements.

Compression

Enable Compression activates or deactivates data compression for NextGen Admin connections (Default: *inactive*) and increases efficiency like responsive management, especially over 'thin' lines. This feature is backward-compatible. Even older NextGen Firewall releases not capable of handling compressed management connections can still be properly connected. When compression is active, the connection status icon at the top right changes to an icon with a cyan background.

> To activate compression, disconnect and reconnect to your system after enabling this setting.

Cryptography

Click **Advanced Cryptographic Settings** to edit the following advanced crypto API settings:

- **Disable Smartcard /Token** – Selecting this check box deactivates the advanced cryptographic API settings.
- **Cryptographic Service Provider** – Barracuda Networks supports all cryptographic service providers (CSPs) using the Microsoft crypto API. All CSPs installed on your local workstation are listed.
- **Key Length** – The key length depends on the selected CSP. Minimum, maximum, and default values for key lengths are displayed in the Cryptographic Service Provider list.
- **Default Store** – The default store for certificates (defaults to MY).
- **Specifies the provider type** – Location of the certificate. You can select one of the following settings:
  - CERT_STORE_PROV_SYSTEM – Certificate available in MS Management Console.
  - CERT_STORE_PROV_PHYSICAL – Certificate available on eToken/Smartcard.
- **Flags** – Availability of the certificate. Possible values are 'current user only' or 'local workstation', regardless of the logged-in user. You can select one of the following settings:

    - CERT_SYSTEM_STORE_CURRENT_USE – Certificate is dedicated to this user only.
    - CERT_SYSTEM_STORE_LOCAL_MACHINE – Certificate is dedicated to local workstation.
- **Select Smartcard Reader** – If smartcard readers are available, you can select one from this list. If the list is inactive, there are no smartcard readers available.

Connectivity Options

- **Use SPoE as default** – Use SPoE as default if NextGen Admin should use a single point of entry to connect to the NextGen Firewall or Control Center. TCP port 807 is used to access the firewall, and TCP port 806 for the NextGen Control Center. SPoE is required when deploying in the public cloud. When the unit cannot be reached via SPoE ports, NextGen Admin reverts to the previous connection method. Following a successful connection, the connection method is saved to the registry and re-used for the next connection to that firewall or Control Center.
- **Socket Connect Timeout** – Duration in seconds that a login attempt can last until it is stopped due to failure and an error message is displayed (Default: *6* seconds).

The socket connect timeout also has an impact on PAR file creation of comprehensive configurations. If necessary, you can temporarily set to *200* seconds or longer. See Backups and Recovery.

- **Configuration Read Timeout** – Duration in seconds that a connection attempt (with the **Connect** button) can last after a failure until it is stopped and an error message is displayed (default: 30 seconds). In addition, this setting also determines the read timeout of the configuration file on the **Box Control > Licenses** page. For more information, see How to License a NextGen Firewall.
- **Statistic Timeout** – Duration in seconds that a statistic view attempt can last until the attempt is stopped and an error message is displayed (Default: 30 seconds). Increase this setting if you expect large statistics files.
- **Max. Automatic Reconnects** – The maximum time NextGen Admin automatically reconnects after a session has been interrupted, e.g., in case of connection attempts during updates.

System

- **Disable Windows 7 taskbar preview** – To disable the taskbar preview in Windows 7, select this check box.
- **Disable Events System Tray Icon** – To disable the icon in the system tray that indicates an active event, select this check box.
- **Always use Session Password** – To always use the last known password when reconnecting to a system after a session has been disconnected, select this check box. The password is only saved until you close NextGen Admin.
- **Switch tab title order** – To invert the labeling of opened tabs, select this check box. Either the system name or the system IP address will be on top.
- **Print Header** – In this field, you can enter a custom header for prints. A header is especially useful for identifying owners when multiple administrators use one printer.

Date Format

Specifies how the date and time are formatted in various overview listings (for example, CC Control).

Configuration Settings

- **Advanced Mode Configuration** – To activate **Advanced Configuration Mode** throughout the client, select this check box.
- **Enable Configuration Scripting** – To enable the functionality to script the configuration, select this check box.
- **Read Only Colour** – To define the background color for configuration files in read-only mode, click **Read Only Colour**.

FW Rule Editor

- **Maximum number of network objects to fill into source and destination Combo Box** – Defines the maximum number of network objects to be listed for **Source** and **Destination** when creating firewall rules. You can leave this setting as default.
- **Double Click to use Rule Dialog instead of Inplace Edit** – Switch between in-place editing and opening the Rule Editor when double-clicking inside a cell in the rule list.

Behavior on Slow Connection

- **Do always automatic data refresh on activation and timer intervals** – If enabled, content of the user interface will always be automatically refreshed.
- **Disable automatic data refresh for Box/CC Connections slower than <value> Latency in ms** – In this field, specify a threshold in milliseconds after which automatic data refresh is disabled for connections. The NextGen Firewall or Control Center connection will be probed on the first connection attempt.

Keyboard Navigation

- **Disable Keyboard Navigation by <Alt> Key** – To display the keyboard navigation when you press **Alt**, select this check box.

Ribbon Bar

- **Show Big Symbols** – To display large icons in the ribbon bar, select this check box.

Restore Defaults

- **Restore Dialog Positions, Restore List Columns, Restore Config Element Sizes** – To restore default settings, click the corresponding button.

Custom IP Lookup Link

- **Disable Custom IP Lookup Link in Firewall Live and History. Takes effect with next**

opened session! – To disable the custom IP lookup link in the **Firewall > Live** and **History** view, select this check box.
- **IPv4 Lookup URL** – In this section, you can enter an HTTP/S URL to perform a custom IP address lookup (for example whatismyipaddress.com). By default, IP addresses are looked up at https://db-ip.com/.

To use the lookup function for an IP address from the Live or History screen, you must set parameter **DNS Resolve IPs** to **yes** (see: History Page).

- **<ipv4 addr>** – The IPv4 address.

External SSH Client

- **Command to open SSH-Client** – In this field, enter the command to open the SSH client. Use %IP address and %user to dynamically insert IP addresses and login name. Format: 'path' parameters. e.g., 'C:\putty.exe' %user@%IP address.

Printing

- **Anonymize IP Addresses on Printing** – When selecting this check box, IP addresses are anonymized by replacing the last 4 digits by xxx. E.g., 80.90.100.xxx when printing lists.

Log in

- **Save session information** – Save the IP address in the **recent connection** section of the login page.
- **Save user name** – Save the username last used to log into the IP address with the recent connection information.
- **Import recent sessions** – Click to import recently accessed firewalls and Control Centers from the registry.

Netmask Notations

- **Use Netmask Notation** – From this list, you can select either the CIDR or Inverted CIDR (phion) netmask notation. (Default: CIDR). The inverted CIDR notation, which may be used for configuration purposes within the NextGen Firewall F-Series, is different from the CIDR netmask notation. As a rough guide, keep in mind that the higher the inverted CIDR notation, the bigger the network (contrary to CIDR notation). Some log files can still use the inverted CIDR notation, but generally CIDR notation is used. The inverted CIDR notation can be calculated as follows: `Inverted CIDR = 32 - CIDR`

Quad	CIDR	Inverted CIDR
255.255.255.255	**32**	**0**
255.255.255.254	**31**	**1**
255.255.255.252	**30**	**2**

255.255.255.248	**29**	**3**
255.255.255.240	**28**	**4**
255.255.255.224	**27**	**5**
255.255.255.192	**26**	**6**
255.255.255.128	**25**	**7**
255.255.255.0	**24**	**8**
255.255.254.0	**23**	**9**
255.255.252.0	**22**	**10**
255.255.248.0	**21**	**11**
255.255.240.0	**20**	**12**
255.255.224.0	**19**	**13**
255.255.192.0	**18**	**14**
255.255.128.0	**17**	**15**
255.255.0.0	**16**	**16**
255.254.0.0	**15**	**17**
255.252.0.0	**14**	**18**
255.248.0.0	**13**	**19**
255.240.0.0	**12**	**20**
255.224.0.0	**11**	**21**
255.192.0.0	**10**	**22**
255.128.0.0	**9**	**23**
255.0.0.0	**8**	**24**
254.0.0.0	**7**	**25**
252.0.0.0	**6**	**26**
248.0.0.0	**5**	**27**
240.0.0.0	**4**	**28**
224.0.0.0	**3**	**29**
192.0.0.0	**2**	**30**
128.0.0.0	**1**	**31**
0.0.0.0	**0**	**32**

Barracuda Activation

Expanding the **Barracuda Activation** drop-down menu lets you configure the settings for Barracuda Activation. The settings in this section control the behavior or completely disable the Barracuda

Activation process.

- **Policy for Contact Information** – From this drop-down list you can select from the following options:
  - **Do not store. Ask every time** – Does not store customer information locally. For each license activation, the user information needs to be entered.
  - **Store, but ask for confirmation** – Stores customer information locally. The information does not need to be entered for each activation, but needs to be confirmed instead.
  - **Store and use always automatically** – Stores customer information locally.
- **CC: Create PAR Files** – When the check box is selected, no warning will be displayed on creation of box PAR files without configured serial numbers.
- **Proxy Settings** – When the check box is selected, proxy settings configured in Internet Explorer will be inherited to the client.

Admin and CC Settings

When expanding the **Admin and CC Settings** section, you can configure the password and key for administrators of a NextGen Control Center and stand-alone Barracuda NextGen Firewall F.

Configure Stand-Alone Barracuda NextGen Firewall F-Series Admin Settings

To configure the administrator settings for a stand-alone Barracuda NextGen Firewall F-Series:

1. From the list below the **Legacy Configuration** section, select **Change Admin Credentials for Local Admin (Single Box)**.
2. In the **Box IP Address** field, enter IP address of the firewall.
3. In the **Change Administrator Password** section, you can change the password.
4. In the **Change Administrator Key** section, you can change the keys.

Configure Barracuda NextGen Control Center Admin Settings

To configure the administrator settings for a Barracuda NextGen Control Center:

1. From the list below the **Legacy Configuration** section, select **Change Admin Credentials for CC Admin**.
2. In the **CC Selection** section, select the NextGen Control Center. In the **Address** field, the IP address of the system appears.
   If you want to remove the NextGen Control Center from this list, click **Remove Selected**. To log back into a removed system, you must accept its certificate again.
3. To view the certificate for the system, click **Show Certificate**.
4. In the **Change Administrator Password** section, you can change the password.
5. In the **Change Administrator Key** section, you can change the keys.

Certificates and Private Keys

This drop-down menu contains the private key administration. Login and authentication of the administrator on a NextGen Firewall are processed using a two-factor authentication technique. The authenticity of the admin workstation is verified using a challenge-response method. In addition to this, administrators must authenticate themselves using a personal password.

> It is also possible to use eToken and smartcards.

Creating a Certificate

> New certificates are usually not generated with NextGen Admin. They will normally be available on the domain controller and will then be transferred to the specified default store.

In order to generate a new certificate/key by using Microsoft Strong Cryptographic Provider v1.0, click **Create New Certificate/Key**. This opens a window requiring several values to be entered. After confirming your entry, the new certificate will be displayed in the list. The columns within the main tab derive from the information entered while creating the certificate. However, two columns differ:

- **Hash** – Contains short information concerning the key in order to make it easier to verify whether keys are equal.
- **Key Container** – Displays the unique name of the CSP key container.

To delete a certificate, select the required certificate in the list and click **Delete Certificate/Key**.

> Certificates cannot be viewed and exported using NextGen Admin. You can use Microsoft Management Console (MMC) for this purpose instead. Refer to the manuals provided by the manufacturer for further information.

Using Keys on a Barracuda NextGen Firewall F-Series

Keys in PEM format cannot be used on NextGen Firewall F systems. However, NextGen Admin enables conversion of already-existing keys into certificates. If you have older keys sitting in your registry, NextGen Admin provides an additional button within this dialog named **Migrate Keys to Cert**. Click this button to open a password request for the available keys. After entering the proper password, the keys are converted into certificates. The subsequent dialog (**Registry Keys converted to Microsoft Certificate Management - Remove Registry Keys?**) offers two options:

- **Yes** – Removes the keys in PEM format from the registry.
- **No** – Keeps the keys in PEM format in the registry.

Public Host Keys

When expanding the **Public Host Keys** drop-down field, the following sections are available:

Public Keys

This section shows all firewalls that were previously accessed using this computer. The list includes the box IP address, a short hash of the key, and the unique box fingerprint. Use the **Remove Selected** option for deleting a selected entry from the list. A security request will pop up the next time you log into the box. The **Import PEM** option allows you to import PEM files. Security is increased by using certificates in this place, at the same time a security request is avoided.

SSH Keys

This section shows all firewalls that were previously accessed using an SSH connection from this computer. The list includes the SSH IP address and the unique SSH fingerprint. In addition to the **Remove Selected** and **Import PEM** options (both having the same purpose as described above), the **Enter Finger Print** option is also available here. Click to enter the unique fingerprint and the corresponding IP address manually into a dialog box.

Barracuda NG Admin Maintenance

This drop-down menu offers you an option to install the currently running instance of NextGen Admin into the so-called Global Assembly Cache (GAC), to uninstall it again from there, and to delete further instances that have been detected on the workstation. Usually, there is no need to install NextGen Admin because the executable can simply be copied to and executed on a workstation, thereby fulfilling the hardware and OS requirements without requiring any further preparations.