How to Configure Authentication and Access Rights

The FTP Gateway service provides a section which lets you set up local and external authentication schemes, configure welcome messages and specify access and authentication exceptions. You can also create user-specific profiles to specify restrictions and permissions f or FTP connections , e.g. access to certain actions and destinations, that should apply to connected users.

Configure Authentication Settings

To configure FTP authentication settings for users and networks, complete the instructions given in the following sections.

Step 1. Configure Authentication Exceptions

Configure access and authentication exceptions for denied source networks and IP addresses that do not require authorization on the FTP gateway.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > FTP-Gateway > FTP Gateway Settings**.
2. Click **Lock**.
3. In the left navigation, click **Authentication**.
4. In the **Denied source-networks** table, click **+** and add all IP addresses and networks from which users should not be allowed to connect to the FTP gateway.
5. In the **No local authorization needed** table, add all IP addresses and networks from which users do not need to be authenticated.

6. Proceed with **Step 2** or **Step 3**.

Step 2. (optional) Configure Welcome Messages

Configure welcome messages to be displayed to users who are allowed to connect.

1. Click **Edit** in the **Welcome message** section on the **Authentication** page.
2. In the upcoming window, configure your welcome messages that should be displayed after successful FTP connections.
3. Click **OK**.

4. Proceed with **Step 3**.

Step 3. Configure User Authentication

Configure authentication schemes for users who are allowed to access FTP,

1. Click **Edit** in the **Authentication Service settings** section on the **Authentication** page.

2. From the **Authentication Scheme** list, select the authentication scheme to be used for FTP connections.

   You can select MS Active Directory, LDAP, Radius, RSA SecurID, TacPlus, NGF Local, or MSNT. (MSNT does not provide group information.)
3. In the **Authentication Service Listen IP** field, specify the listen IP address for the authentication service. By default, the listen IP address is *127.0.0.1*.

4. From the **User List Policy** list, select the policy for handling users who have been added to the **User List** table. You can select:
   - *deny-explicit*
   - *allow-only*
5. In the **User List** table, click **+** and add the login names for users who should be handled according to the **User List Policy** setting.
6. Click **OK**.
7. Click **Send Changes** and **Activate**.

Configure Permissions and Restrictions

Create access profiles and specify permissions and restrictions that apply to all or specific users, groups and/or IP addresses when connected to the FTP Gateway service.

When configuring user-specific or default profiles, the following permissions and restrictions can be set:

- **Destination** – The IP address or DNS resolvable hostname of the FTP destination to which the restrictions will apply. This setting is only applicable to the Special Destinations section.
- **Redirection** – This setting allows connection redirection to another host. This setting is only applicable to the Special Destinations section.
- **Policy** – Grants or denies access to the destination (default: *allow*).
- **Initial directory** – The initial directory that can be accessed after logging into the destination. This setting is only applicable to the **Special Destinations** section.
- **Top most directory** – The highest directory level that can be accessed. This setting is only applicable to the **Special Destinations** section.
- **Deny file-<action>** – Enable this setting to deny a specific action.
- **Deny structure mount** – Enable this setting to prohibit structure mounts.
- **Deny make/delete dir** – Enable this setting to allow/deny directory creations.
- **Deny file-extensions** – In this field, you can enter a space delimited list of prohibited file extensions. Only enter the name of the extension without the leading dot. For example: *mp3 exe doc*
- **Timeout (sec.)** – The length of time in seconds that a connection can remain idle until it is terminated (default: 0).

Create a User-specific Profile

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > FTP-Gateway > FTP Gateway Settings**.
2. In the left navigation, click **Userspecific**.
3. Click **Lock**.
4. In the **User specific** table, click **+** , enter a sequence number for the profile, e.g. 01 for the first entry, and click **OK**.

   To determine if a connection matches a profile, the profiles are processed from top to bottom in the order that they are listed in the table (similar to how firewall rules are processed). The sequence is determined by the profile names, which must be numeric.

5. In the **Configuration Assignment** section, add the users to which the profile restrictions and permissions should apply:
   - In the **Affected Groups** table, add the affected groups.
   - In the **Affected Users** table, add the affected users.

- In the **Affected IPs for Anonymous** table, add the affected IP addresses that do not required authentication for accessing the FTP gateway.

6. In the **Special Destinations** section, click **+** .
7. In the **Destination field**, enter the IP address or DNS resolvable hostname of the FTP destination to which the restrictions will apply.
8. Configure the restrictions and permissions that should apply to the specified users and IP addresses for connections to this destination. (These settings override any default access restrictions.)
9. Click **OK**.
10. In the **Other Destinations** section, set default restrictions and permissions for connections to all other FTP destinations that are not listed in the **Special Destinations** section.
11. In the **Time Restrictions** section, configure the following settings if applicable:
    - **Use Local Time** – To use the local time zone settings of the system to determine when to apply the time restrictions, select this check box. Otherwise, select a time zone from the **Time Zone** list.
      - **Time Zone** – Unless you are using the local time zone settings of the system, select a time zone to determine time restrictions.
    - **Time Settings** – To set the times during which the configured restrictions and permissions are applied, click **Always**. In the **Time Interval** window, select the days and hours.
12. Click **OK**.
13. Click Send **Changes** and **Activate**.

Configure Default Permissions and Restrictions

If a connection does not match any user-specific profile, it is handled with the default restrictions and permissions. To configure default access restrictions, complete the following steps:

1. On the **Userspecific** page, click **Edit** next to **Default User specific**.
2. In the **Destination** section, click **+** to open the **Destination** configuration window.
3. In the **Destination field**, enter the IP address or DNS resolvable hostname of the FTP destination to which the restrictions will apply.
4. Configure the restrictions and permissions for connections to this destination.
5. Click **OK**.
6. In the **Other Destinations** section, set default restrictions and permissions for connections to all other FTP destinations that are not listed in the **Special Destinations** section.
7. In the **Time Restrictions** section, configure the following settings if applicable:
    1. **Use Local Time** – To use the local time zone settings of the system to determine when to apply

the time restrictions, select this check box. Otherwise, select a time zone from the **Time Zone** list.
   - **Time Zone** – Unless you are using the local time zone settings of the system, select a time zone to determine time restrictions.
2. **Time Settings** – To set the times during which the configured restrictions and permissions are applied, click **Always**. In the **Time Interval** window, select the days and hours.

8. Click **OK**.

9. Click Send **Changes** and **Activate**.

FTP Gateway connections are now handled according to the settings that are specified in these profiles.