Sterling Integrator®

Using Adapter Limitation Policies

Version 5.1

Sterling Commerce
An IBM Company

About FTP and SFTP Adapter Limitation Policies – Overview

When using the FTP Server adapter or the SFTP Server adapter, you can define limitations for their usage. These limitation policies control various types of access. Policies can be applied to all of the server adapters of one protocol type (SFTP or FTP), or just to specific instances that you identify.

The following limitation policies can be defined for cluster and non-cluster environments:

- **Bandwidth Limiting** enables you to limit the inbound transfer speed from a specific trading partner for an IP address or range or set of users. Limits can be allocated by your system administrator based on your company's performance and tuning requirements. For example, You can set a low bandwidth for all IP addresses except for a few selected ones, which belong to high priority customers. (Both IPv4 and IPv6 are supported.)
- **Command Limiting** enables you to limit specific FTP commands or SFTP commands for an IP address or range of addresses or for a set of users. IP addresses define the who, while the command limiting policy defined what they can do.
- **Data Limiting** enables you to limit the total amount of inbound data that can be sent by a trading partner (IP address or range) or a set of users in a day. By doing this, you can save important resources that could be consumed if there are no restrictions.
- **Lockout** enables you to prevent hacking attacks on servers. By locking out users after a certain number of invalid attempts, you prevent them from trying different combinations of passwords as part of a brute force attack. User lockout can be time based or it can be permanent lockout.

You can have multiple limitation policies to define complex rules. For example, you could create the following bandwidth policies:

- If TP1 (trading partner) connects, allow TP1 1 MB/s bandwidth.
- But if TP2 or TP3 connects, allow them each 256 KB/s bandwidth.
- For all other trading partners, give only 10 KB/s as default.

Before you configure limitation policies, consider the following:

- You can only set one lockout policy at the protocol level.
- You can have as many instance level policies defined for a protocol as necessary.
- You can apply as many instance level policies to a specific instance of an adapter as necessary. The basic criteria to select between protocol level and instance level policies is:
  - If you want to have a restriction put on all instances of an adapter (FTP/SFTP server), you define a protocol level policy. This is a default restriction.
  - If you want to loosen some restrictions on certain instances of the adapter, may be for a high priority trading partner, you can define a instance level policy applicable for the user Id or IP address for the trading partner.
- Once you have defined a protocol level policy, it becomes effective immediately for all instances of the protocol server adapter. After defining an instance level policy, you must add it to the adapter instances that you want covered by the policy. For existing adapters, this is done by editing the adapter configuration in the Admin Console. For new adapters, select the policy during the initial adapter configuration.

Defining or updating policies is done in the Admin Console, under **Deployment** > **Adapter Utilities** > **Policy Configuration**.

Adapter Limitation Policy Examples

The following are some scenarios, when you might want to use a limitation policy.

Scenario	Use this Policy Type:
You may need to limit the speed at which data comes into your system.	Bandwidth
You may want to restrict the amount of data a Trading Partner can send and save your disk/DB space.	Data Limit
You may need to prevent the trading partner from listing or reading files in the FTP server or you want the trading partner to only send you files. Or the other way round, you may want the trading partner to only read data and prevent the trading partner from changing it in any way.	Command Limit
You may want to prevent hacking attacks on your server by locking users permanently or only for 5 mins every time they make 3 invalid attempts.	Lockout
You can create policies when you want to restrict a trading partner or any third party client connecting to the servers (Server adapters) from using your resources or executing undesirable commands.	Command Limit

Information You Need to Gather Before Defining Adapter Policies

Before you define new policies in the Admin Console, you need to know what type of policy you are defining and then gather the following information:

	Policy Type X= info required			
Information Needed for Defining a Policy	Bandwidth Limiting	Lockout	Command Limiting	Data Limit
Which type of policy are you defining Bandwidth, Command, Data, or Lockout?	X	X	X	X
Will this policy be applied to an IP address or Users?	X		X	X
Which protocol will the policy will be applied to: SFTP or FTP?	X	X	X	X
Is the policy applied to a protocol or instance?	X	X	X	X
What is the maximum number of login attempts before lockout?		X		

	Policy Type X= info required			
Information Needed for Defining a Policy	**Bandwidth Limiting**	**Lockout**	**Command Limiting**	**Data Limit**
Is the user lockout permanent or time-based?		X		
Is the policy only applied to specific users? If yes, you need the list of users.	X		X	X
Is the policy only applied to specific IP addresses? If yes, you need the list of IP addresses.	X		X	X
Does this policy limit commands? If yes, you need to know the commands and the users or IP addresses that will be limited.			X	
Does this policy limit the amount of inbound data that can be received per day an IP address? If yes, what is the maximum amount of inbound data for 24 hours.				X

About IP Address Range for Policies

Three of the policy types support limitation by IP addresses ranges or patterns. An IP address range is a semicolon separated list of IP ranges and patterns. The following examples illustrate valid IP address formats. These can be semicolon separated and combined into a single IP pattern.

Type of IP Address	**Format Example**	**Notes**
One IP address	10.20.30.44	
Clear range	10.20.30.0-10.20.30.45	
Clear range	10:20::40:10 – 10:20::40:ffff	Where ffff is a bit hexadecimal number with all bits set to 1. (Decimal value = 65535)
Range	10.20.30.*	Range is 10.20.30.0 – 10.20.30.255
Range	10:20::*	Range is 10:20:0:0:0:0:0:0-10:20:0:0:0:0:0:ffff
Range	10:20:*	Range is 10:20:0:0:0:0:0:0-10:20:ffff:ffff:ffff:ffff:ffff:ffff
Range	10:30:40::30:43:*	Range is 10:30:40:0:0:30:43:0-10:30:40:0:0:30:43:ffff

How are multiple policies applied to an Adapter Instance?

If there are multiple policies of a single policy type applied to an adapter instance, the following rules are used to select a single policy to be applied to a user or IP address:

1. **IP based policy gets priority:** The system first selects the policies that are applicable/defined for the IP address of the client. If none are found, the system selects the policies that are applicable/defined for the UserId used by the client. If none are found, no policies are applied.

   Note: The first rule is not applicable to Lockout Policy as it is not IP address or User based.

2. **Instance level policy gets priority:** From the list of IP based or user based policies from the previous rule (IP based policy get priority), the system selects instance level policies. If there are none, the system selects protocol level policies.

   Note: At this point the system will have selected either instance level policies or protocol level policies but not both (for evaluation).

3. **Most restrictive policy gets applied:** If the system still has multiple policies after applying the previous rule (instance level policy), the system selects the most restrictive policy. This is possible if the IP address falls in an overlapping range or the same user is selected for many policies.

   - For command limiting policy, the system combines all commands in the command list of each policy and treats this as a single policy.
   - For bandwidth and data limit policies, the system applies the one with the minimum amount (of bandwidth/data) configured.
   - For lockout policy, since there can be only one instance level policy per instance and only one protocol level policy for the system, there is no conflict at this point.

About Command Limiting Policies – Overview

You can use Command Limiting Policies to prevent specific IP addresses or users from executing certain commands on an Application SFTP or FTP server. This is useful in situations where you want to prevent read/write access to your Application FTP/SFTP servers.

The command limiting policies define:

- Which protocol the policy applies to: FTP or SFTP
- IP addresses or users to be denied access to the specified commands
- Commands to be blocked
- Whether the policy applies to all instances of the adapter (protocol level) or only to adapter instances that you choose (instance level)

When planning command limiting policies, remember that all instances of the protocol (SFTP/FTP) are affected by the policy.

Defining a Command Limiting Policy

To define a command limiting policy:

1. On the Application Admin Console, select **Deployment** > **Adapter Utilities** > **Policy Configuration**.
2. Next to **New Policy**, click **Go!**
3. Select **Command Limiting Policy** and click **Next**.
4. Enter the **Policy Name**.
5. Enter **Description**.
6. Select the **Policy Mode**: IP Address or Range or User Based.
7. Select the **Protocol**: FTP or SFTP.
8. Select the **Level at which this policy is applied**: Protocol or Instance.
9. Click **Next**.
10. The next screen displayed depends on the **Policy Mode** you selected.
    - If you selected **User Based**, select the users affected by this policy and click **Next**.
    - If you selected **IP Address or Range**, enter the IP address or range and click **Next**.
11. Select the commands that users or IP addresses will **NOT** be able to execute on the specified servers and click **Next**. The commands displayed are dependant on the protocol you selected.
12. Review the policy configuration.
13. Click **Finish** to create the policy.

Disabling a Command Limiting Policy

To disable a command limiting policy:

1. On the Application Admin Console, select **Deployment** > **Adapter Utilities** > **Policy Configuration**.
2. In the **List** panel, in **By Policy Type**, select **Command Limiting Policy** and click **Go**! A list of the command limiting policies are displayed.
3. Clear the **Enabled** checkbox for the policy you want to disable.

Enabling a Command Limiting Policy

To enable a command limiting policy that has been disabled:

1. On the Application Admin Console, select **Deployment** > **Adapter Utilities** > **Policy Configuration**.
2. In the **List** panel, in **By Policy Type**, select **Command Limiting Policy** and click **Go**! A list of the command limiting policies are displayed.
3. Check **Enabled** for the policy you want to enable.

Editing a Command Limiting Policy

To edit a command limiting policy:

1. On the Application Admin Console, select **Deployment** > **Adapter Utilities** > **Policy Configuration**.
2. In the **List** panel, in **By Policy Type**, select **Command Limiting Policy** and click **Go**! A list of the command limiting policies are displayed.
3. Select **Edit** for the command limiting policy you want to enable.
4. Review and update as required.
5. Review the updates.
6. Click **Finish** to update the policy.

Deleting a Command Limiting Policy

Before you can delete a command limiting policy, you must disable it.

To delete a command limiting policy:

1. On the Application Admin Console, select **Deployment** > **Adapter Utilities** > **Policy Configuration**.
2. In the **List** panel, in **By Policy Type**, select **Command Limiting Policy** and click **Go**! A list of the command limiting policies are displayed.
3. If the policy you want to delete is enabled, clear the **Enabled** checkbox.
4. Select **Delete** for the policy you want to delete.
5. Review and confirm that you want to delete the policy, as the action can not be reversed.
6. Click **Delete**.

About Bandwidth Limiting Policies – Overview

You can use Bandwidth Limiting policies to prevent specific IP addresses (generally, for specific trading partners) from transferring files inbound to Application FTP/SFTP servers at high speeds, which can take up bandwidth that might be required for high priority customers or trading partners.

You can customize a bandwidth throttling policy by setting:

- IP addresses or users.
- Maximum bandwidth that should be allowed for any IP in this range (in kilobytes per second). The bandwidth is given to every session from any IP in the range or any user in the selected set. For example, if the bandwidth limit is 100KBs, and three IP addresses ar selected, each IP address gets a bandwidth of 100KBs.
- Maximum concurrent connections allowed from this IP address.
- Whether the lockout is permanent or for a specified time period.
- Which protocol the policy applies to: FTP or SFTP.

When planning bandwidth throttling policies, consider the following:

- For protocol level policies, all instances of the protocol (SFTP/FTP) are affected.
- Instance level policies take precedence over protocol level policies.

Defining a Bandwidth Limiting Policy

To create a new bandwidth limiting policy:

1. On the Application Admin Console, select **Deployment** > **Adapter Utilities** > **Policy Configuration**.
2. Next to **New Policy**, click **Go!**
3. Select **Bandwidth Limiting Policy** and click **Next**.
4. Enter the **Policy Name**.
5. Enter **Description**.
6. Select the **Policy Mode**: IP Address or Range or User Based.
7. Enter the **Maximum Bandwidth** allowed for this IP address, or any IP address in this range, in kilobytes per second (KB/s).
8. Enter the **Maximum** number of **Concurrent Connections** allowed for this IP address, or any IP address in this range.
9. Select the **Protocol**: FTP or SFTP.
10. Select the **Level at which this policy is applied**: Protocol or Instance.
11. Click **Next**.
12. The next screen displayed depends on the **Policy Mode** you selected.
    - If you selected **User Based**, select the users affected by this policy and click **Next**.
    - If you selected **IP Address or Range**, enter the IP address or range and click **Next**.

13. Review the policy configuration.
14. Click **Finish** to create the policy.

Disabling a Bandwidth Limiting Policy

To disable an bandwidth limiting policy:

1. On the Application Admin Console, select **Deployment** > **Adapter Utilities** > **Policy Configuration**.
2. In the **List** panel, in **By Policy Type**, select **Bandwidth Limiting Policy** and click **Go**! A list of the bandwidth limiting policies are displayed.
3. Clear the **Enabled** checkbox for the policy you want to disable.

Enabling a Bandwidth Limiting Policy

To enable bandwidth limiting policy that has been disabled:

1. On the Application Admin Console, select **Deployment** > **Adapter Utilities** > **Policy Configuration**.
2. In the **List** panel, in **By Policy Type**, select **Bandwidth Limiting Policy** and click **Go**! A list of the bandwidth limiting policies are displayed.
3. Check **Enabled** for the policy you want to enable.

Editing a Bandwidth Limiting Policy

To edit a bandwidth limiting policy:

1. On the Application Admin Console, select **Deployment** > **Adapter Utilities** > **Policy Configuration**.
2. In the **List** panel, in **By Policy Type**, select **Bandwidth Limiting Policy** and click **Go**! A list of the bandwidth limiting policies are displayed.
3. Select **Edit** for the bandwidth limiting policy you want to edit.
4. Review and update as required.
5. Review the updates.
6. Click **Finish** to update the policy.

Deleting a Bandwidth Limiting Policy

Before you can delete a bandwidth limiting policy, you must disable it.

To delete a bandwidth limiting policy:

1. On the Application Admin Console, select **Deployment** > **Adapter Utilities** > **Policy Configuration**.
2. In the **List** panel, in **By Policy Type**, select **Bandwidth Limiting Policy** and click **Go**! A list of the bandwidth limiting policies are displayed.
3. If the policy you want to delete is enabled, clear the **Enabled** checkbox.

4. Select **Delete** for the policy you want to delete.
5. Review and confirm that you want to delete the policy, as the action can not be reversed.
6. Click **Delete**.

About Data Limit Policies – Overview

You can use Data Limit policies to limit the total amount of inbound data that can be sent by a trading partner in one day. By doing this, you can save important resources that could be consumed if there are no restrictions.

Data Limit policies use a data counter to track the amount of data sent by the users or IP addresses for which a data limit policy is applicable. This data counter tracks the amount (bytes) of data transferred by all users or IP addressees associated with a policy. A separate data counter is associated with every combination of a policy and an instance/protocol. Review the following scenarios so you understand when the data counter is reset to zero (0):

Data Limit Policy Update Scenario	Is the data counter reset?
You update an IP address list (Policy Mode).	No
You update the User list (Policy Mode).	No
You update the policy from instance to protocol (Level at which this policy is applied).	Yes, the data counter is reset to zero on the day you update the policy.
You update the policy from protocol to instance (Level at which this policy is applied).	Yes, the data counter is reset to zero on the day you update the policy.
You update the policy from a user based policy to an IP address based policy.	Yes, the data counter is reset to zero on the day you update the policy.
You update the policy from a IP address based policy to an User based policy.	Yes, the data counter is reset to zero on the day you update the policy.

For example, if the data limit is 100MB per day, if there are 10 IPs in the range or 10 users are selected in the policy, all of them together can only send 100MB per day. What this means is if one (or few) of the IPs or users defined in the policy uses up the 100 MB limit on a day, the rest cannot transfer any files until the next day.

You can customize a data limit policy by setting:

- IP addresses or users.
- Maximum amount of inbound data that should be allowed for any IP in this range (in kilobytes per day).
- Whether the policy applies to all instances of the adapter (protocol level) or only to adapter instances that you choose (instance level).
- Which protocol the policy applies to: FTP or SFTP.
- If multiple data limiting polices have been applied, then the policy with the lowest data limit is what takes precedence.

When planning data limit policies, consider the following:

- A day is a 24 hours time period. The day starts when the first document is received. Time is 00:00 hours.
- For protocol level policies, all instances of the protocol (SFTP/FTP) are affected.

- When the inbound data limit is crossed, the Server Adapter sends an error message to the connecting client that the inbound data limit has been crossed. Whether this message is displayed to the user or not depends on the client being used. For SFTP, the client may or may not display the exact message sent by the server. Most FTP clients display the error message, because the FTP protocol is very clear about display of server messages to the user.

Defining a Data Limit Policy

To create a new data limit policy:

1. On the Application Admin Console, select **Deployment** > **Adapter Utilities** > **Policy Configuration**.
2. Next to **New Policy**, click **Go!**
3. Select **Data Limit Policy** and click **Next**.
4. Enter the **Policy Name**.
5. Enter **Description**.
6. Select the **Policy Mode**: IP Address or Range or User Based.
7. Enter the **Inbound Data Limit** that should be allowed for any IP in this range (in kilobytes).
8. Select the **Protocol**: FTP or SFTP.
9. Select the **Level at which this policy is applied**: Protocol or Instance.
10. Click **Next**.
11. The next screen displayed depends on the **Policy Mode** you selected.
    - If you selected **User Based**, select the users affected by this policy and click **Next**.
    - If you selected **IP Address or Range**, enter the IP address or range and click **Next**.
12. Review the policy configuration.
13. Click **Finish** to create the policy.

Disabling a Data Limit Policy

To disable a data limit policy:

1. On the Application Admin Console, select **Deployment** > **Adapter Utilities** > **Policy Configuration**.
2. In the **List** panel, in **By Policy Type**, select **Data Limit Policy** and click **Go**! A list of the data limit policies are displayed.
3. Clear the **Enabled** checkbox for the policy you want to disable.

Enabling a Data Limit Policy

To enable a data limit policy that has been disabled:

1. On the Application Admin Console, select **Deployment** > **Adapter Utilities** > **Policy Configuration**.

2. In the **List** panel, in **By Policy Type**, select **Data Limit Policy** and click **Go**! A list of the data limit policies are displayed.
3. Check **Enabled** for the policy you want to enable.

Editing a Data Limit Policy

Before you edit a data limit policy, review the following scenarios so you understand when the data counter is reset to zero (0):

Data Limit Policy Update Scenario	Is the data counter reset?
You update an IP address list (Policy Mode).	No
You update the User list (Policy Mode).	No
You update the policy from instance to protocol (Level at which this policy is applied).	Yes, the data counter is reset to zero on the day you update the policy.
You update the policy from protocol to instance (Level at which this policy is applied).	Yes, the data counter is reset to zero on the day you update the policy.
You update the policy from a user based policy to an IP address based policy.	Yes, the data counter is reset to zero on the day you update the policy.
You update the policy from a IP address based policy to an user based policy.	Yes, the data counter is reset to zero on the day you update the policy.

To edit a data limit policy:

1. On the Application Admin Console, select **Deployment** > **Adapter Utilities** > **Policy Configuration**.
2. In the **List** panel, in **By Policy Type**, select **Data Limit Policy** and click **Go**! A list of the data limit policies are displayed.
3. Select **Edit** for the data limit policy you want to enable.
4. Review and update as required.
5. Review the updates.
6. Click **Finish** to update the policy.

Deleting a Data Limit Policy

Before you can delete a data limit policy, you must disable it.

To delete a data limit policy:

1. On the Application Admin Console, select **Deployment** > **Adapter Utilities** > **Policy Configuration**.
2. In the List panel, in **By Policy Type**, select **Data Limit Policy** and click **Go**! A list of the data limit policies are displayed.
3. If the policy you want to delete is enabled, clear the **Enabled** checkbox.
4. Select **Delete** for the policy you want to delete.
5. Review and confirm that you want to delete the policy, as the action can not be reversed.
6. Click **Delete**.

About Lockout Policies – Overview

Note: This replaces the Failed Login Tracking and Account Locking option for the SFTP Server adapter.

You can use lockout policies to lockout a user for a length of time or permanently. You can customize a lockout policy by setting:

- Number of signon attempts to allow before a user is locked out.
- Whether the lockout is permanent or for a specified time period.
- Whether the policy applies to all instances of the adapter (protocol level) or only to adapter instances that you choose (instance level).
- Which protocol the policy applies to: FTP or SFTP.

When planning lockout policies, consider the following:

- If the lockout period is permanent, the user is locked out until the lock is cleared by an application administrator.
- For protocol level policies, all instances of the protocol (SFTP/FTP) are affected.
- There can be only one policy defined at the protocol level at any given time.
- Instance level policies take precedence over protocol level policies.

Defining a Lockout Policy

To create a lockout policy:

1. On the Application Admin Console, select **Deployment** > **Adapter Utilities** > **Policy Configuration**.
2. Next to **New Policy**, click **Go!**
3. Select **Lockout Policy** and click **Next**.
4. Enter the **Policy Name**.
5. Enter **Description**.
6. Select the **Maximum** number of **Invalid Login Attempts** allowed.
7. Select the **Lockout Type:** Permanent or Time Based**.**
8. If you selected, Time Based, enter the lockout out **Time Period in Mins** (minutes).
9. Select the **Protocol**: FTP or SFTP.
10. Select the **Level at which this policy is applied**: Protocol or Instance.
11. Click **Next**.
12. Review the policy configuration.
13. Click **Finish** to create the policy.

Clearing a Lock set by a Lockout Policy

The Lockout Policy Manager enables an Policy Lock Manager to clear a lock for a user. Only users who have permission to clear locks, will have the Policy Lock Manager displayed in the Admin Console. After the lock is cleared, the user regains access to the instances.

To clear a lock:

1. In the Admin Console, select **Deployment** > **Adapter Utilities** > **Policy Lock Manager**.
2. Search for the lock by **User Name, Lockout Type**, **Start Date**, or **End Date**. After you enter the search criteria, click **Go!** The lockout information is displayed.
3. Clear the lock checkbox.
4. Click **Finish**.

Disabling a Lockout Policy

To disable an lockout policy:

1. On the Application Admin Console, select **Deployment** > **Adapter Utilities** > **Policy Configuration**.
2. In the **List** panel, in **By Policy Type**, select **Lockout Policy** and click **Go**! A list of the lockout policies are displayed.
3. Clear the **Enabled** checkbox for the policy you want to disable. A warning message is displayed to let you know that any locked users are now unlocked. You need to click **OK** to disable the policy. If you select **Cancel**, the lockout policy remains.

Enabling a Lockout Policy

To enable an lockout policy that has been disabled:

1. On the Application Admin Console, select **Deployment** > **Adapter Utilities** > **Policy Configuration**.
2. In the **List** panel, in **By Policy Type**, select **Lockout Policy** and click **Go**! A list of the lockout policies are displayed.
3. Check **Enabled** for the policy you want to enable.
4. Click **Next**.

Editing a Lockout Policy

To edit a lockout policy:

1. On the Application Admin Console, select **Deployment** > **Adapter Utilities** > **Policy Configuration**.
2. In the **List** panel, in **By Policy Type**, select **Lockout Policy** and click **Go**! A list of the lockout policies are displayed.
3. Select **Edit** for the lockout policy you want to enable.
4. Review and update as required.
5. Review the updates.
6. Click **Finish** to update the policy.

Deleting a Lockout Policy

To delete a lockout policy:

1. On the Application Admin Console, select **Deployment** > **Adapter Utilities** > **Policy Configuration**.
2. In the **List** panel, in **By Policy Type**, select **Lockout Policy** and click **Go**! A list of the lockout policies are displayed.
3. If the policy you want to delete is enabled, clear the **Enabled** checkbox.
4. Click **Next**. A warning message is displayed to let you know that any locked users are now unlocked. You need to click **OK** to confirm the disable.
5. Select **Delete** for the lockout policy you want to delete.
6. Review and confirm that you want to delete the policy, as the action can not be reversed.
7. Click **Delete**.

Frequently Asked Questions (FAQ)

FAQ: Can I import or export Adapter Policies?

Yes, you can import and export adapter policies. From the Admin Console, select **Deployment** > **Resource Manager** > **Import/Export**.

FAQ: What is an Adapter Instance Policy Mapping?

When you are importing and exporting adapter policies, one of the policy resources that you can select is the Adapter Instance Mapping policy. This resource is part of the policy framework. It defines the association between adapter instances and instance level policies.