Configure New Administrator Users in BroadWorks

Contents

Introduction

This document describes different kinds of administrator accounts in BroadWorks Application Server (AS) and steps on how to create new accounts.

Background Information

Cisco BroadWorks is an application installed on top of Linux OS and it can be accessed via several interfaces. Therefore, it comes with multiple different administrator accounts:

- Root user - account created during OS installation. It gives full access to the system so it must be used with cautioun. It is out of the scope of this article; you must apply guidelines from your OS vendor to manage root access and keep it secure. For example, you can refer to Red Hat's superuser access document if your BroadWorks is installed on top of Red Hat Enterprise Linux (RHEL).
- BroadWorks administrator (also known as bwadmin) - account used to manage BroadWorks application and to access it via Command Line Interface (CLI).
- System administrator - account used to log into BroadWorks application via Web interface.
- Reseller / Enterprise / Service Provider / Group administrator - account used to manage particular Reseller / Enterprise / Service Provider / Group.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Basic BroadWorks administration.
- Basic Linux commands.

Components Used

The information in this document is based on BroadWorks AS version R24.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

BroadWorks Administrator

Configure

Initial BroadWorks administrator account is created during BroadWorks installation. In order to create additional accounts, use these steps:
Step 1. Log into BroadWorks CLI with your root credentials.

Step 2. Navigate to **/usr/local/broadworks/bw_base/sbin** directory:

```
[root@as1 ~]# cd /usr/local/broadworks/bw_base/sbin
```

Step 3. Run **bwuseradd –h** command to list configuration options:

```
[root@as1 sbin]# ./bwuseradd –h Missing argument: role bwuseradd Version 1.14 USAGE: bwuseradd
<newusername> <-r, --role BWORKS|BWSUPERADMIN|OPERATOR|VIEWER> [-p, --passwd password] [-d, --
default] [-c, --centralized] [-v, --verbose] [-h, --help] Parameters: <newusername> : the new
user name -r, --role : the user assigned role -p, --passwd : the user password. Enclose the
password in single quotes if it contains special characters. -d, --default : reset passwd -c, --
centralized : for centralized user management -v, --verbose : run in verbose mode -h, --help :
print this Help Description: Invokes Unix/ldap commands to create a local/centralized bw user
Example: bwuseradd -r OPERATOR --passwd admin123 admin
```

When you create the new account, you have to select one of the four roles:

- BWSUPERADMIN - This role has root access for the installation file. This role is used to

install and upgrade Cisco BroadWorks.
- BWORKS - This role can start, stop, and perform modifications with the CLI or other tools available on Cisco BroadWorks servers.
- OPERATOR - This role can configure Cisco BroadWorks configuration files but cannot start or stop Cisco BroadWorks.
- VIEWER - This role can view the current configuration but cannot perform any modifications.

You can consult UNIX User Account Configuration Guide to learn more about commands used in this section.

Step 4. Run **bwuseradd** command to create new user:

```
[root@as1 sbin]# ./bwuseradd -r BWORKS --passwd bwadmin1 bwadmin1 Changing password for user
bwadmin1. passwd: all authentication tokens updated successfully. User will be required to
change password upon next login Expiring password for user bwadmin1. passwd: Success WARNING:
Please make sure this user is created on all servers. WARNING: Do not forget to run 'config-ssh
-createKeys <peer list>' for the new user.
```

Step 5. If AS is installed in cluster mode, run the same command on the secondary node:

```
[root@as2 sbin]# ./bwuseradd -r BWORKS --passwd bwadmin1 bwadmin1 Changing password for user
bwadmin1. passwd: all authentication tokens updated successfully. User will be required to
change password upon next login Expiring password for user bwadmin1. passwd: Success WARNING:
Please make sure this user is created on all servers. WARNING: Do not forget to run 'config-ssh
-createKeys <peer list>' for the new user.
```

Step 6. Log in as new user; you are prompted to reset your password:

```
bwadmin1@as1's password: You are required to change your password immediately (administrator
enforced) WARNING: Your password has expired. You must change your password now and login again!
Changing password for user bwadmin1. Current password: New password: Retype new password:
```

Step 7. Run **bin** command to navigate to **/usr/local/broadworks/bw_base/bin** on primary AS:

```
bwadmin1@as1.mleus.lab$ bin bwadmin1@as1.mleus.lab$ pwd /usr/local/broadworks/bw_base/bin
```

Step 8. Run **config-ssh** command to create common key pair:

```
bwadmin1@as1.mleus.lab$ ./config-ssh -createKeys bwadmin1@as2
============================================= ==== SSH CONFIGURATION TOOL version 2.2.22 ====
=> Setting default settings <= Setting 'StrictHostKeyChecking no' Setting 'ServerAliveInterval
250' => DNS Sanity test <= [###############] [...............] Configured: y, Reachable: y,
Resolved: y, Required: n. Using bwadmin1@as1.mleus.lab as local peer name for as1.mleus.lab. =>
DNS OK <= => Peer reachability test <= [###] [...] => Creating SSH keys <= Creating keys for
bwadmin1@as2... bwadmin1@as2's password: Generating ecdsa key... Generating rsa key... Creating
keys for bwadmin1@as1.mleus.lab... bwadmin1@as1.mleus.lab's password: Generating ecdsa key...
Generating rsa key... => Keying SSH <= Preparing bwadmin1@as1.mleus.lab for keying... Cleaning
public keys for bwadmin1@as2... Sharing keys with bwadmin1@as2... Pushing local public keys...
bwadmin1@as2's password: Pulling remote public keys... bwadmin1@as2's password: Sharing keys
with bwadmin1@as2... [done] => Fully meshing SSH peers <= => Recursing with bwadmin1@as2 <=
Pushing config-ssh script to bwadmin1@as2... Launching config-ssh on bwadmin1@as2... => Setting
default settings <= Adding 'StrictHostKeyChecking no' Adding 'ServerAliveInterval 250' => DNS
Sanity test <= [###############] [...............] Configured: y, Reachable: y, Resolved: y,
Required: n. Using bwadmin1@as2.mleus.lab as local peer name for as2.mleus.lab. => DNS OK <= =>
Peer reachability test <= [###] [...] => Keying SSH <= Preparing bwadmin1@as2.mleus.lab for
keying... Cleaning public keys for bwadmin1@as1.mleus.lab... Sharing keys with
```

```
bwadmin1@as1.mleus.lab... Pushing local public keys... Pulling remote public keys... Sharing
keys with bwadmin1@as1.mleus.lab... [done] => Testing ssh configuration <= Testing
bwadmin1@as2... [done] ==== SSH CONFIGURATION TOOL completed ====
```

Verify

In order to verify new user, log in to CLI with new credentials and run some basic BroadWorks commands:

```
bwadmin1@as1.mleus.lab$ bwshowver AS version Rel_24.0_1.944 Built Sat Jun 6 00:26:50 EDT 2020 -
BASE revision 909962 - AS revision 909962 Patching Info: Active Patches: 701
bwadmin1@as1.mleus.lab$ bwcli
====================================================================== BroadWorks Command Line
Interface Type HELP for more information
====================================================================== AS_CLI>
```

System Administrator

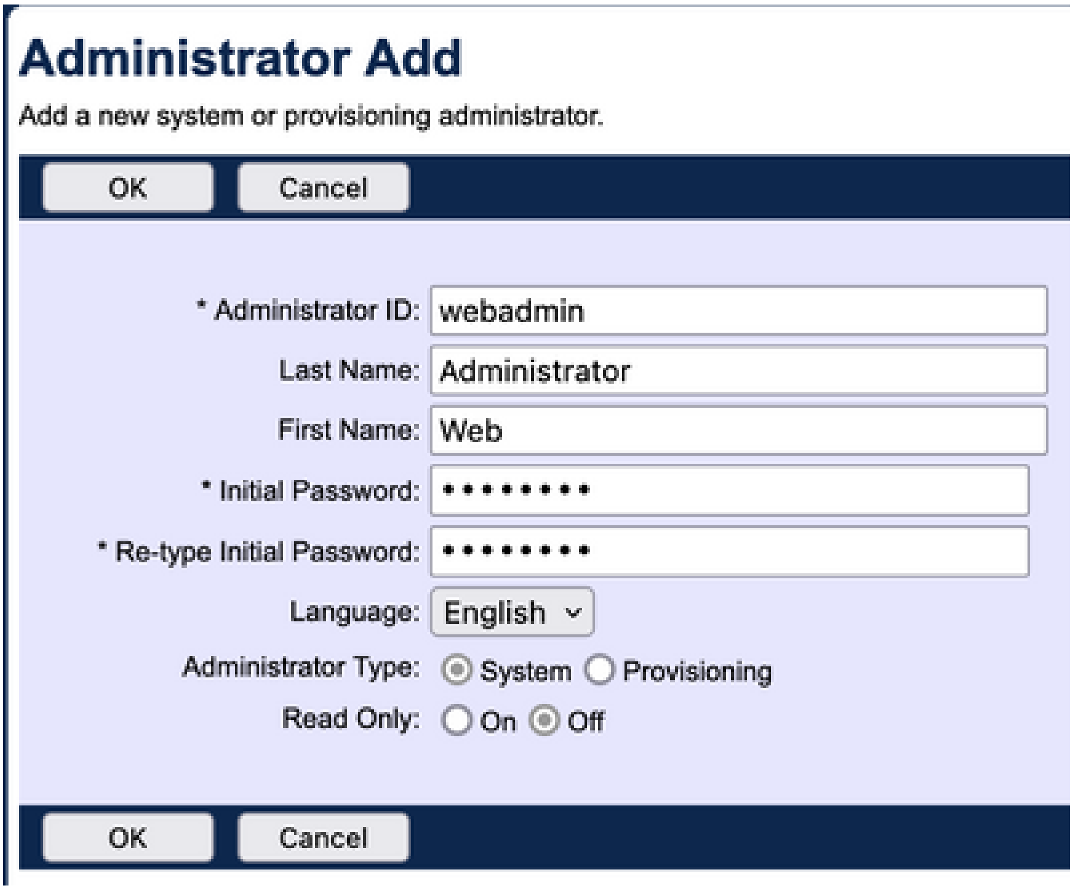
Configure

Step 1. Navigate to **https://*<AS_FQDN>*/Login** page and log into AS Web interface.

Step 2. Navigate to **System > Profile > Administrators**.

Step 3. Click **Add** button.

Step 4. Populate all fields:



Administrator Add

Add a new system or provisioning administrator.

* Administrator ID: webadmin

Last Name: Administrator

First Name: Web

* Initial Password: ••••••••

* Re-type Initial Password: ••••••••

Language: English

Administrator Type: ● System ○ Provisioning

Read Only: ○ On ● Off

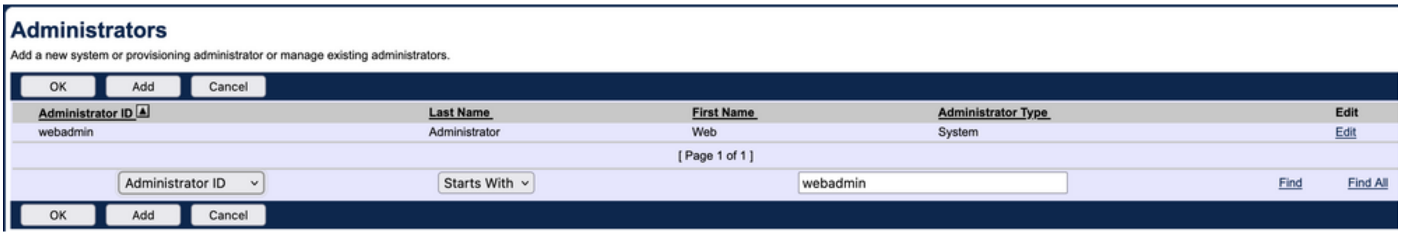
There are two types of Administrator to select:

- System gives the administrator full access to the system.
- Provisioning gives the administrator limited access to the system for the purpose to add new customers and manage customer accounts.

Step 5. Click **OK** to save changes.

Verify

Navigate to **System > Profile > Administrators** and search for newly created account:



Administrators

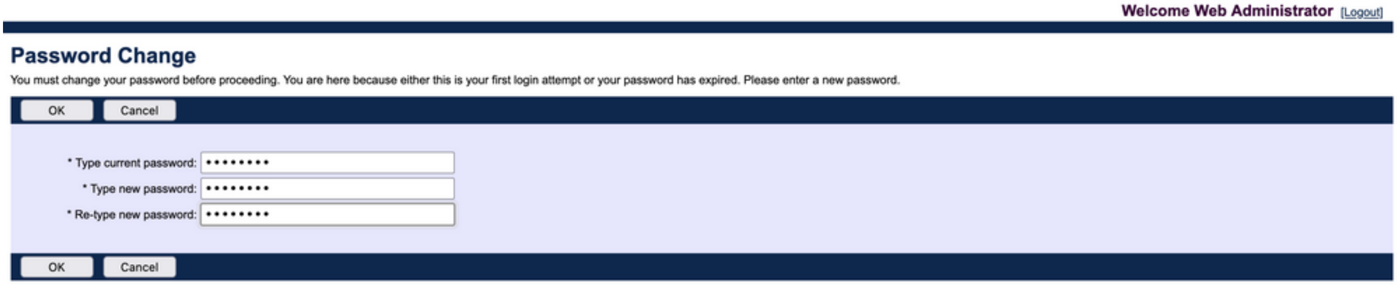
Add a new system or provisioning administrator or manage existing administrators.

Administrator ID	Last Name	First Name	Administrator Type	Edit
webadmin	Administrator	Web	System	Edit

[Page 1 of 1]

Administrator ID · Starts With · webadmin · Find · Find All

Log out and log in back with new set of credentials (you are prompted to change your password):



Password Change

You must change your password before proceeding. You are here because either this is your first login attempt or your password has expired. Please enter a new password.

* Type current password: ••••••••

* Type new password: ••••••••

* Re-type new password: ••••••••

Navigate through menu to confirm all the required options are available.

You can also verify new credentials over CLI. Open BroadWorks CLI (BWCLI) and run **login** command with new set of credentials:

```
AS_CLI> login webadmin Password: webadmin logging in...
```

Reseller / Enterprise / Service Provider / Group Administrator

Configure

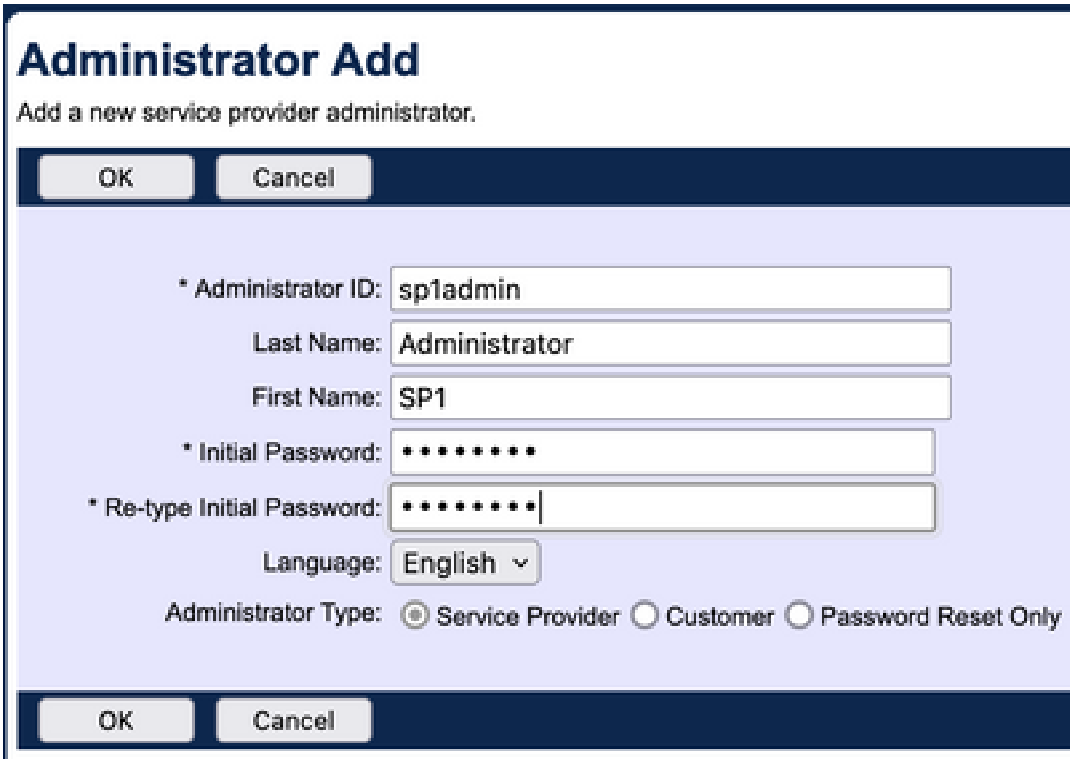
Step 1. Navigate to **https://*<AS_FQDN>*/Login** page and log into AS Web interface.

Step 2. Navigate to **System > Profile** and further to **Reseller**, **Enterprises**, **Service Providers** or **Group** you would like to create administrator for. Service Provider is used in this configuration example, but configuration for other entities is identical.

Step 3. Choose Service Provider you would like to add new administrator to.

Step 4. Navigate to **Profile > Administrators** and click **Add** button.

Step 5. Populate all fields:



Administrator Add

Add a new service provider administrator.

* Administrator ID: sp1admin
Last Name: Administrator
First Name: SP1
* Initial Password: ••••••••
* Re-type Initial Password: ••••••••
Language: English
Administrator Type: ● Service Provider ○ Customer ○ Password Reset Only

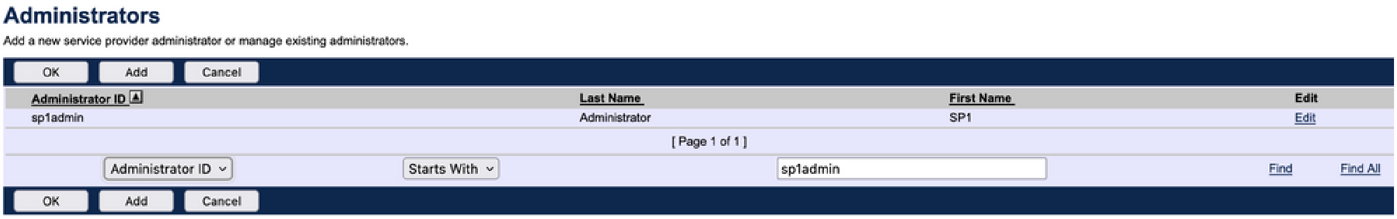
There are three types of Administrators to select for Service Provider / Enterprise (for Reseller and Group there is no selection of type):

- Service Provider creates a normal administrator, with access to the web interface determined by the policies you set on the Administrator Policies page.
- Customer creates a customer administrator. The customer administrator only has access to the Groups, Users, Service Instances, and Change Password pages for their service provider. The customer administrator has access to the group pages for all groups, with the exception of read-only access to the Intercept Group page, and no access the Call Capacity page. You can further restrict the customer administrator access by the policies you set on the Administrator Policies page.
- Password Reset Only allows the administrator to modify user passwords only. The administrator has no access to any other pages, data, or commands within the web interface.

Step 6. Click **OK** to save changes.

Verify

Navigate to **System > Profile > Service Providers** or **Enterprises** and select entity you created administrator account for. Then navigate to **Profile > Administrators** and search for newly created administrator:



Administrators

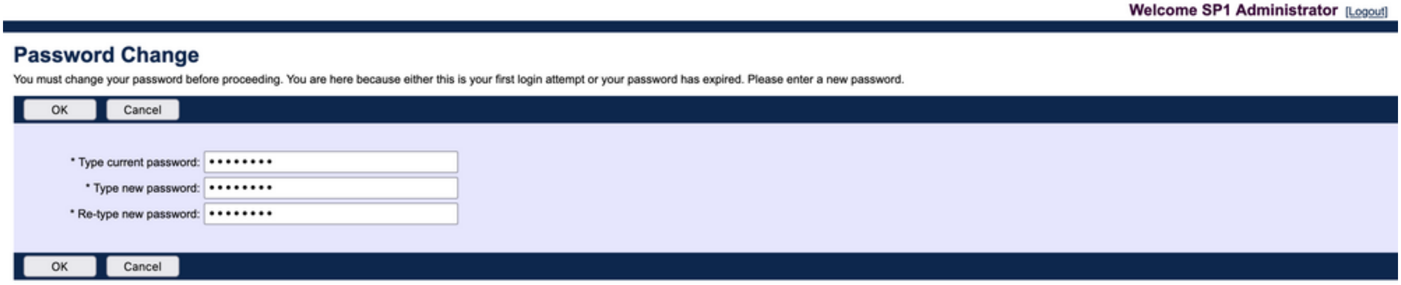
Add a new service provider administrator or manage existing administrators.

Administrator ID	Last Name	First Name	Edit
sp1admin	Administrator	SP1	Edit

[Page 1 of 1]

Administrator ID, Starts With, sp1admin

Log out and log in back with new set of credentials (you are prompted to change your password):



Welcome SP1 Administrator [Logout]

Password Change

You must change your password before proceeding. You are here because either this is your first login attempt or your password has expired. Please enter a new password.

* Type current password: ••••••••

* Type new password: ••••••••

* Re-type new password: ••••••••

Navigate through menu to confirm that only settings related to particular Service Provider / Enterprise are visible.

Add Administrator Accounts with CLI Commands

All web access accounts can be also created from BWCLI commands. This is not covered in this document in details, but here are respective commands for reference:

- System administrator:

```
AS_CLI/SubscriberMgmt/Administrator> h add When adding a new administrator to the system,
you set the administrator user ID, access level, first and last names, and password.
Parameters description: userId : The user ID for the administrator. type : when set to
"system", allows for complete access to the Application Server CLI and its functions. When
set to "prov", allows only limited access to the Application Server CLI, specifically
functions in the network level only. readOnly : Cannot configure the system. attribute:
Additional attributes to include through the add command. lastName : The user's last name.
firstName: The user's first name. language : Indicates the language to be used for the
administrator. ====================================================================== add
<userId>, String {2 to 80 characters} <type>, Choice = {system, prov} <readOnly>, Choice =
{false, true} [<attribute>, Multiple Choice = {lastName, firstName, language}] <lastName>,
String {1 to 30 characters} <firstName>, String {1 to 30 characters} <language>, String {1
to 40 characters}
```

- Reseller administrator:

```
AS_CLI/SubscriberMgmt/Reseller/Administrator> h add This command is used to add a new
reseller administrator. When this command is used, you are prompted for password
information. Parameters description: resellerId: The ID of the reseller. userId : The user
ID for the reseller administrator. attribute : Additional attributes to include with the
name command. lastName : This parameter specifies the reseller administrator's last name.
firstName : This parameter specifies the reseller administrator's first name. language :
This parameter specifies the reseller administrator's supported language.
====================================================================== add <resellerId>,
String {1 to 36 characters} <userId>, String {2 to 80 characters} [<attribute>, Multiple
Choice = {lastName, firstName, language}] <lastName>, String {1 to 30 characters}
<firstName>, String {1 to 30 characters} <language>, String {1 to 40 characters}
```

- Enterprise / Service Provider administrator:

```
AS_CLI/SubscriberMgmt/ServiceProvider/Administrator> h add When adding a new service
provider administrator to the system, the corresponding service provider administrator's
user ID, first name, and last names are set. You are prompted for password information.
Parameters description: svcProviderId: The service provider. userId : The user ID for the
service provider administrator. adminType : When set to "normal", the service provider
administrator has all standard access rights and privileges. When set to "customer", the
customer administrator only has access to the Group, User, and Change Password web portal
pages. Also, the customer administrator has no access to Call Capacity and has read-only
access to Intercept Group pages. When set to "passwordResetOnly", this value allows the
service provider administrator to reset the user's web and portal password only. attribute :
Additional attributes to include through the add command. lastName : The service provider
administrator's last name. firstName : The service provider administrator's first name.
language : The service provider's supported language.
====================================================================== add <svcProviderId>,
String {1 to 30 characters} <userId>, String {2 to 80 characters} <adminType>, Choice =
{normal, customer, passwordResetOnly} [<attribute>, Multiple Choice = {lastName, firstName,
language}] <lastName>, String {1 to 30 characters} <firstName>, String {1 to 30 characters}
<language>, String {1 to 40 characters}
```

- Group administrator:

```
AS_CLI/SubscriberMgmt/Group/Administrator> h add When adding a new group administrator to
the system, the corresponding group name and service provider, and the group administrator's
user ID, first name, and last name are set. Parameters description: svcProviderId: The ID of
the service provider to whom the group and group administrator belong. groupId : The ID of
the group to which the administrator belongs. userId : The user ID for the group
administrator. attribute : Additional attributes to include through the add command.
lastName : The group administrator's last name. firstName : The group administrator's first
name. language : The supported language for the group administrator.
====================================================================== add <svcProviderId>,
String {1 to 30 characters} <groupId>, String {1 to 30 characters} <userId>, String {2 to
161 characters} [<attribute>, Multiple Choice = {lastName, firstName, language}] <lastName>,
String {1 to 30 characters} <firstName>, String {1 to 30 characters} <language>, String {1
to 40 characters}
```