



HIRSCHMANN

A **BELDEN** BRAND

User Manual

Basic Configuration

HiProvision User Management



The naming of copyrighted trademarks in this manual, even when not specially indicated, should not be taken to mean that these names may be considered as free in the sense of the trademark and tradename protection law and hence that they may be freely used by anyone.

© 2020 Hirschmann Automation and Control GmbH

Manuals and software are protected by copyright. All rights reserved. The copying, reproduction, translation, conversion into any electronic medium or machine scannable form is not permitted, either in whole or in part. An exception is the preparation of a backup copy of the software for your own use.

The performance features described here are binding only if they have been expressly agreed when the contract was made. This document was produced by Hirschmann Automation and Control GmbH according to the best of the company's knowledge. Hirschmann reserves the right to change the contents of this document without prior notice. Hirschmann can give no guarantee in respect of the correctness or accuracy of the information in this document.

Hirschmann can accept no responsibility for damages, resulting from the use of the network components or the associated operating software. In addition, we refer to the conditions of use specified in the license contract.

You can get the latest version of this manual on the Internet at the Hirschmann product site (www.hirschmann.com).

Hirschmann Automation and Control GmbH
Stuttgarter Str. 45-51
72654 Neckartenzlingen
Germany

Contents

1.	INTRODUCTION	4
1.1	General.....	4
1.2	Manual References	4
2.	USER DATABASE AT INITIAL STARTUP	5
3.	LOGON AND ENTER HIPROVISION UM	5
4.	HIPROVISION UM APPLICATION	6
4.1	General.....	6
4.2	Group Access Rights.....	7
4.3	Group Actions.....	7
4.4	User Actions	9
4.4.1	Create User	9
4.4.2	Modify User	10
4.4.3	Delete User	11
4.4.4	Block User / Deny Access.....	11
4.4.5	Unblock User / Grant Access	11
4.4.6	Reset / Clear Saved HiProvision Settings.....	11
4.4.7	Options	12
4.5	Users Log	15
5.	ABBREVIATIONS	15

List of figures

Figure 1 Initial Dashboard View	5
Figure 2 HiProvision Logon Box.....	6
Figure 3 Users Tile: Locked/Unlocked	6
Figure 4 HiProvision UM Default View, Groups	6
Figure 5 (Predefined) Users in Groups	7
Figure 6 Group Welcome Message	7
Figure 7 Create User Window	10
Figure 8 Modify User	10
Figure 9 Authentication Providers Tab: Add New RADIUS Provider	12
Figure 10 Authentication Providers Tab: Add New LDAP Provider	13
Figure 11 Limit Configurators Logons.....	15

List of Tables

Table 1 Manual References	4
Table 2 Group Access Rights	8

1. INTRODUCTION

1.1 General

This document is valid as of Dragon PTN Release 4.3DR.

This document covers all the information about the login user management, security, access rights and roles in HiProvision and/or the Dragon PTN network. HiProvision User Management (=HiProvision UM) can be used after clicking the Users tile in the Dashboard.

You must be an Administrator to perform HiProvision UM. As a result, this document is only relevant for Administrators. Configurators and Monitors will not be able to perform HiProvision UM actions described further on. If you are not an Administrator, and you need access to HiProvision UM, ask your Administrator for an administrator user account.

In a nutshell, HiProvision User Management or HiProvision UM includes the following:

- ▶ Predefined users;
- ▶ Custom users;
- ▶ Organize users in three fixed groups:
 - ▶ Administrators;
 - ▶ Configurators;
 - ▶ Monitors;
- ▶ Language selection per user (license required);
- ▶ Each group has a fixed set of access rights;
- ▶ Access rights are factory set on the HiProvision dashboard tiles and cannot be changed.

A group defines what its users are allowed to do in the Dragon PTN network.

At the initial start of HiProvision, a user database must be created. This database will only be used for HiProvision UM and is completely separated from the network configuration database. Starting the HiProvision servers is not a prerequisite for performing HiProvision UM.

1.2 Manual References

Table 1 is an overview of the manuals referred to in this manual. ‘&’ refers to the language code, ‘*’ refers to the manual issue. All these manuals can be found in the HiProvision (=Dragon PTN Management System) Help function.

Table 1 Manual References

Ref.	Number	Title
[2Mgt]	DRA-DRM830-&-*	HiProvision Management Operation

2. USER DATABASE AT INITIAL STARTUP

When HiProvision is started for the very first time after installation, HiProvision automatically asks for a one-time creation of a user database.

The entire initial setup including the setup of the user database has been described in the chapter 'Steps for a basic setup' in the manual Ref.[2Mgt] in Table 1. After the installation and creation of the user database, go to chapter §3.

3. LOGON AND ENTER HIPROVISION UM

Prerequisites:

- ▶ The user database in §2 has been created or selected;
- ▶ HiProvision has started up and the dashboard is visible, see figure below.



Figure 1 Initial Dashboard View

1. Log in with an administrator account via the logon box, see figure below. If this is the first time logon (e.g after installation), use the predefined user **admin** with password **admin** to log in;
2. If the Users tile is still locked after logon, you don't have sufficient rights to perform HiProvision UM;
3. The logged on username is always visible in the Users tile, see figure below;
4. Log in/log off is always possible via the buttons  / ;
5. Click the unlocked Users tile to enter the HiProvision UM application;



Figure 2 HiProvision Logon Box

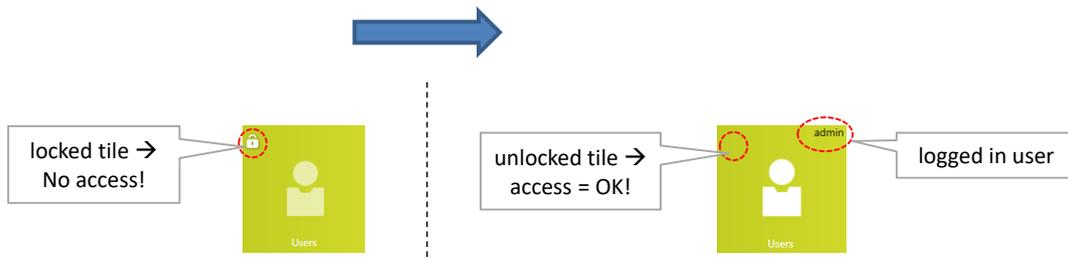


Figure 3 Users Tile: Locked/Unlocked

NOTE: HiProvision UM can be used without running the HiProvision servers behind the Servers tile.

4. HIPROVISION UM APPLICATION

4.1 General

After entering the Users Tile, the default view below is shown. It has two main sections:

- ▶ Groups and Users: by default, only the groups are visible;
- ▶ Users Log: this is a logging history of all the HiProvision UM actions that are performed.

Groups and Users	First Name	Last Name	Authentication Provider	Blocked	Failed Login Attempts	Logged In	Login Message	Language
Administrators							<input type="checkbox"/>	
Configurators							<input type="checkbox"/>	
Monitors							<input type="checkbox"/>	

Timestamp	User	Message
29/01/2018 07:35:12	admin	User admin logged in
29/01/2018 07:37:10	admin	User admin logged off
06/02/2018 05:39:46	admin	User admin logged in
06/02/2018 07:38:47	admin	User admin logged off
17/02/2018 09:22:10	admin	User admin logged in
17/02/2018 09:23:33	admin	User admin logged off
12/03/2018 19:22:41	admin	User admin logged in
12/03/2018 19:23:13	admin	User admin logged off
12/03/2018 19:23:20	admin	User admin logged in
12/03/2018 19:23:23	admin	User admin logged off

Figure 4 HiProvision UM Default View, Groups

After expanding the Groups and Users section, the available users per group appear. At first time use, these are the predefined users with the following userid/password:

- ▶ admin/admin
- ▶ scripting/scripting;
- ▶ config/config;
- ▶ monitor/monitor.

The screenshot shows the 'USERS' section of the HiProvision dashboard. A table lists users grouped into Administrators, Configurators, and Monitors. Callouts highlight the 'Authentication' column (Local), the 'Currently logged in' checkbox, and the 'users (=username)' column. Below the table is a 'USERS LOG' section showing recent events.

Groups and Users	First Name	Last Name	Authentication Provider	Locked	Failed Login Atte...	Logged In	Login Message	Language
Administrators								
admin	admin	admin	Local	<input type="checkbox"/>	0	<input checked="" type="checkbox"/>		English (United Kingdom)
JeffT	Jeff	Thomas	Radius1	<input type="checkbox"/>	0	<input type="checkbox"/>		English (United Kingdom)
Johnw	John	Williams	Local	<input type="checkbox"/>	0	<input type="checkbox"/>	<input checked="" type="checkbox"/>	English (United Kingdom)
reportengine	reportengine	reportengine	Local	<input type="checkbox"/>	0	<input type="checkbox"/>		English (United Kingdom)
scripting	scripting	scripting	Local	<input type="checkbox"/>	0	<input type="checkbox"/>		English (United Kingdom)
Configurators								
config	config	config	Local	<input type="checkbox"/>	0	<input type="checkbox"/>		English (United Kingdom)
Monitors								
monitor	monitor	monitor	Local	<input type="checkbox"/>	0	<input type="checkbox"/>		English (United Kingdom)

Timestamp	User	Message
07/11/2018 16:58:14	admin	User JeffT added by admin
07/11/2018 16:56:31	admin	User Johnw added by admin
07/11/2018 16:52:24	admin	User admin logged in
07/11/2018 16:52:19	system	Login failed for unknown user a

Figure 5 (Predefined) Users in Groups

4.2 Group Access Rights

Users are organized in three fixed groups with each group a fixed set of access rights. Access rights per group are factory set on the HiProvision dashboard tiles and cannot be changed. An overview of the groups and their rights can be found in the table below.

4.3 Group Actions

It is possible to assign a Group login welcome message. Just select the group by clicking its row in the table and click  to modify the group. The window below pops up. You can fill out a login message. If you enable it, this message will pop up for a user that logs on from that group, on the condition that the user itself has not a personal login message on user level, see further. If the user has a personal login message, it overrules the group login message and only the personal login message will be shown.

The dialog box has a title bar and contains the following elements:

- Login Message Enabled:** A checkbox that is checked.
- Login Message:** A text input field containing the text "Hello Administrator, welcome!".
- Buttons:** "OK" and "Cancel" buttons at the bottom.

Figure 6 Group Welcome Message

Table 2 Group Access Rights

Tile Group	Dashboard Tile	Logged Off	Logged On					
			Servers Stopped			Servers Started		
			Administrators	Configurators	Monitors	Administrators	Configurators	Monitors
✓ = Access allowed (=unlocked tile): clicking the tile opens the application behind it; --- = Access denied (=locked tile): clicking the tile does nothing, no application will be opened;								
Administration	Database	---	✓	✓	---	✓	✓	---
	Servers (+Redundancy)	---	✓	✓	✓	✓	✓	✓
	Users (=HiProvision UM)	---	✓	---	---	✓	---	---
	Licenses	---	✓	✓	✓	✓	✓	✓
Configuration	Discovery	---	---	---	---	✓	✓	---
	Network Hardware	---	---	---	---	✓	✓	---
	Connections	---	---	---	---	✓	✓	---
	Layouts	---	---	---	---	✓	✓	---
	Protocols	---	---	---	---	✓	✓	---
Monitoring	Network	---	---	---	---	✓	✓	✓
	Large Network	---	---	---	---	✓	✓	✓
	Events	---	---	---	---	✓	✓	✓
	Performance	---	---	---	---	✓	✓	✓
	Alarms	---	---	---	---	✓	✓	✓
	Assurance	---	---	---	---	✓	✓	✓
	Protocols	---	---	---	---	✓	✓	✓
Tools	Software	---	---	---	---	✓	---	---
	External Devices	---	✓	✓	---	✓	✓	---
	Inventory (used in HiProvision Add-on: Generic Reporting Engine)	---	---	---	---	✓		
	Add-ons	---	✓	✓	---	✓	✓	---
	Advanced	---	✓	✓	---	✓	✓	---
	Help	✓	✓	✓	✓	✓	✓	✓
Note: In case of HiProvision Redundancy and the Redundancy is up and running, the access rights on the Standby Server are the same as indicated above with 'Servers Stopped'.								

4.4 User Actions

The GROUPS and USERS menu bar has the buttons below. Find more information further on.

- ▶ : refreshes all the data in the window;
- ▶ : create a new user, add it to a group (see §4.4.1);
- ▶ : modifies the selected user (see §4.4.2);
- ▶ : deletes the selected user from a group (see §4.4.3);
- ▶ : blocks a user from HiProvision (=deny access) (see §4.4.4);
- ▶ : unblocks a user from HiProvision (=grant access) (see §4.4.5);
- ▶ : resets or clears user specific saved HiProvision settings (see §4.4.6);
- ▶ : options (see §4.4.7):
 - ▶ User Authentication via authentication providers (Local, RADIUS, LDAP);
 - ▶ Configure the maximum amount of logged on Configurators.

4.4.1 Create User

1. In the Groups and Users section, click the  button. The window below pops up;
2. Select a User Group to which the new user must be assigned;
NOTE: The amount of users with configuration permission, allowed to login at the same time in in the Dragon PTN network, can be configured as well via the options button, see §4.4.6.
3. Select an Authentication Provider. If you don't have external user authentication (e.g. RADIUS), just select 'Local'.
4. Fill out all the other fields. All fields are required except for the Login Message fields.
5. Password fields (only If 'Local' was selected as Authentication Provider): fill out the password which is case sensitive.
6. Select the preferred language for this user:
 - ▶ English (=default): no voucher or license required;
 - ▶ Chinese, Polish, German, Spanish: voucher or license required, see 'SERIAL KEY / VOUCHERS / LICENSE PACK ' in Ref. [2Mgt] in Table 1.
7. When this user logs on later on in HiProvision, HiProvision will be displayed in this selected language;
8. If the Login Message Enabled is checked, a pop-up box with the Login Message will appear at Logon for that specific user;
9. Click the OK button to create the user in the selected User Group.

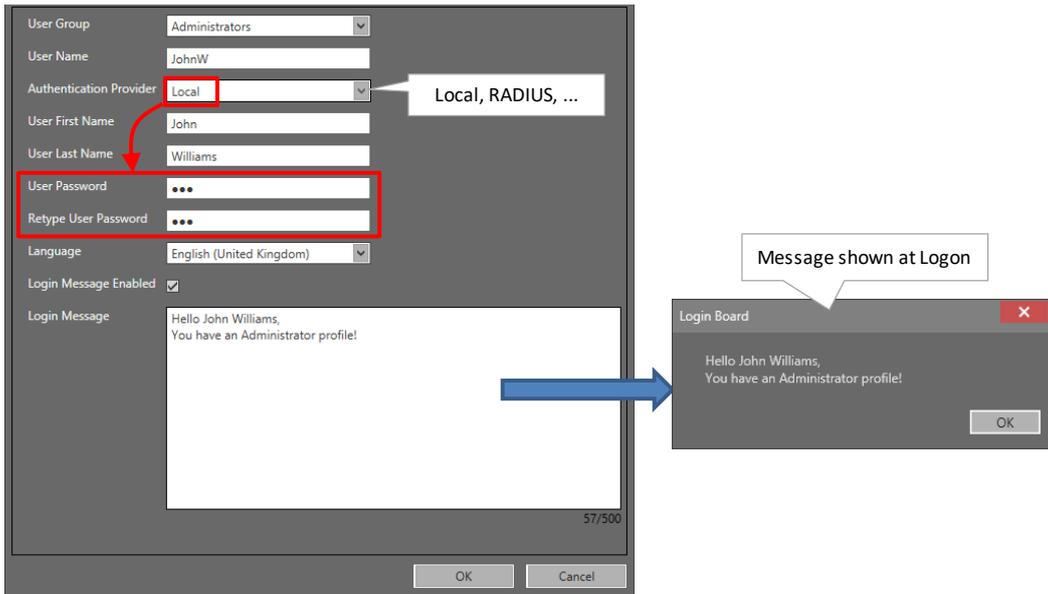


Figure 7 Create User Window

4.4.2 Modify User

1. In the Groups and Users section, click the  button. The window below pops up;
2. All the fields, except the User Group and User Name, can be modified. If you change the Language and you want HiProvision to run immediately in the new selected language for this user, HiProvision must be restarted first.
3. Make your modifications and click the OK button.

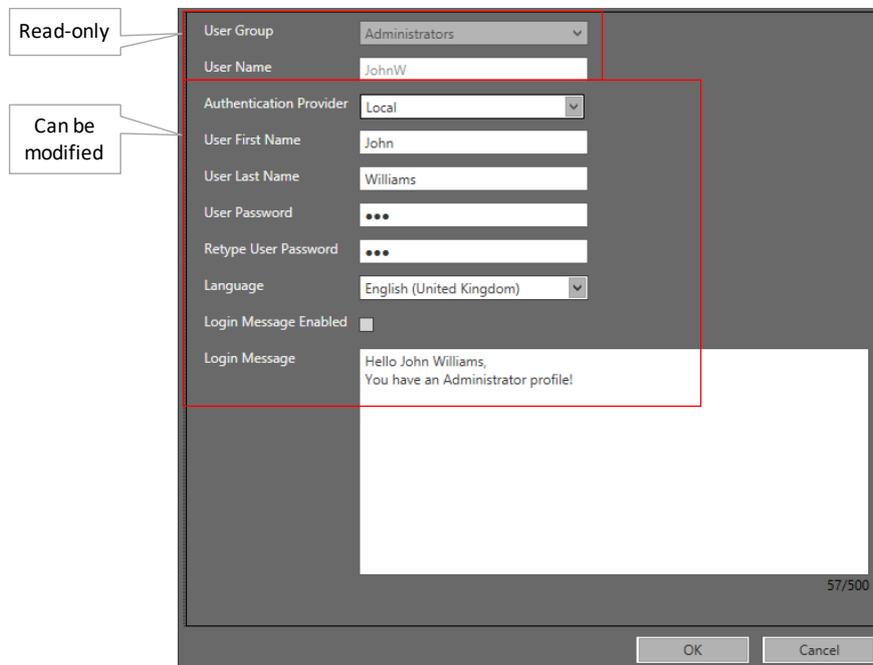


Figure 8 Modify User

CAUTION: Lost passwords cannot be recovered. A new password can be assigned instead via modifying the user and changing the password.

4.4.3 Delete User

1. In the Groups and Users section, expand the groups (= clicking ► in front of the groups) and select the user that must be deleted;
2. Click the  button to delete the user.

4.4.4 Block User / Deny Access

When a user must be completely denied access to HiProvision and Dragon PTN, there are two options:

- ▶ Delete the user: this is more a permanent solution, see §4.4.3;
- ▶ Block the user: this is more a temporary solution. The user remains in the list but has no access rights at all. Later on, the user can be easily unblocked again if desired.

A user has access when its Blocked checkbox is unchecked. This user can be denied access as follows:

1. In the Groups and Users section, expand the groups (= clicking ► in front of the groups) and select the (unblocked) user whom must be blocked;
2. Click the  button to block the selected user;
3. The Blocked checkbox for this user will be checked. As a result, the user will have no access the next time the user logs in in HiProvision.

NOTE: It is possible that a Configurator is not able to log in although he has access. This could be because of a limitation on the Configurators logons, see §4.4.7.

4.4.5 Unblock User / Grant Access

A user has no access when its Blocked checkbox is checked. This user can be granted access again as follows:

1. In the Groups and Users section, expand the groups (= clicking ► in front of the groups) and select the user whom must be unblocked;
2. Click the  button to unblock the selected user;
3. The Blocked checkbox for this user will be unchecked. As a result, the user will have access again the next time the user logs in in HiProvision;

4.4.6 Reset / Clear Saved HiProvision Settings

a. Which HiProvision Settings?

See 'Save User HiProvision Settings' in Ref. [2Mgt] in Table 1.

b. Reset / Clear

It is possible that a user has saved its HiProvision settings as described in the paragraph above.

To reset or clear these saved settings (if any) e.g. to start HiProvision again with a default setup:

1. Click the user row to select the user;
2. Click the  button to clear/reset its saved settings;
3. If the user logs on again in HiProvision, he will have a default HiProvision setup.

4.4.7 Options

Click the  button to configure following options:

a. Authentication Providers Tab - General

An authentication provider is an instance or mechanism via which HiProvision users can authenticate to log on into HiProvision.

b. Authentication Providers Tab - Local

The 'Local' provider is by default available. When a user uses this authentication, a userid and password must be configured into HiProvision itself (see §4.4.1).

c. Authentication Providers Tab - RADIUS

RADIUS (=Remote Authentication Dial In User Service) is a client/server protocol to authenticate users to an external user network service.

HiProvision can act as a RADIUS client that authenticates HiProvision/Dragon PTN users to such a network service via the RADIUS protocol. To configure this, a new RADIUS Authentication Provider must be created via clicking the Add button. Select the RADIUS Type, fill out a provider Name and click the OK button.

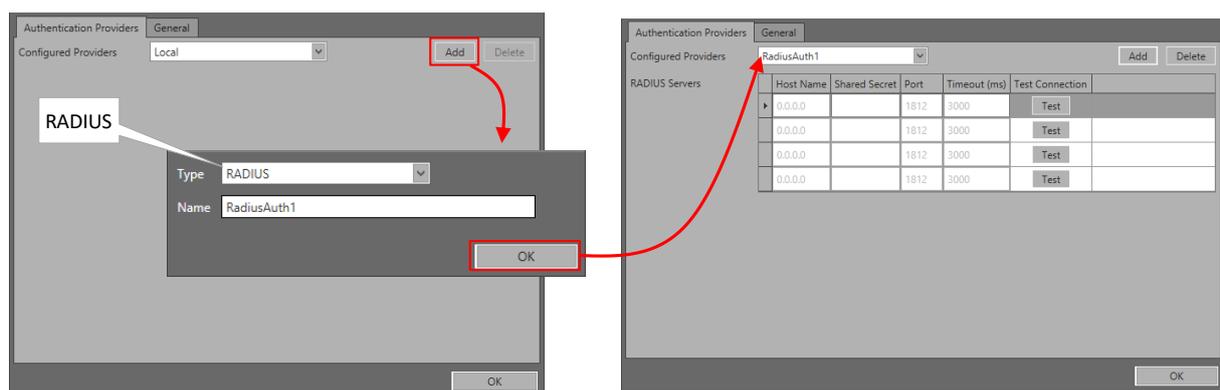


Figure 9 Authentication Providers Tab: Add New RADIUS Provider

From now on, the new provider can be selected from the Configured Providers drop-down list to configure it further. Each RADIUS provider includes 4 RADIUS servers that can be configured for authentication. When authenticating a user against this provider, the first server will be used. When that server does not respond within the specified 'Timeout' (in ms), the second server is used, etc.

- Host Name (default 0.0.0.0): Fill out the IP address of the RADIUS server;

- ▶ Shared Secret (default = empty): the RADIUS client (=HiProvision) authenticates to the RADIUS server using the filled out Shared Secret;
- ▶ Port (default = 1812): Port number used for RADIUS authentication;
- ▶ Timeout (ms) (default = 3000 ms): Amount of time that HiProvision (=RADIUS Client) waits for a response from the RADIUS server. When no response has been received, the next server in the list will be used etc...
- ▶ Test Button: Click this button to test the connection between the RADIUS client (=HiProvision) and the RADIUS Server.

d. Authentication Providers Tab - LDAP

Prerequisite: HiProvision acts as an LDAP client and supports the settings below. As a result, the connected LDAP server must be configured accordingly:

- ▶ AuthType: Basic;
- ▶ ProtocolVersion: 3;
- ▶ (LDAP-S) Only over TLS v1.2.

LDAP (=Lightweight Directory Access Protocol) is a client/server protocol to authenticate users to an external directory services platform. A directory service manages users, passwords, computer accounts etc... in a network. Some examples of directory services:

- ▶ AD (=Active Directory);
- ▶ OpenLDAP;
- ▶

HiProvision can act as an LDAP client that authenticates HiProvision/Dragon PTN users to such a directory service via the LDAP protocol. To configure this, a new LDAP Authentication Provider must be created via clicking the Add button. Select the LDAP Type, fill out a provider Name and click the OK button.

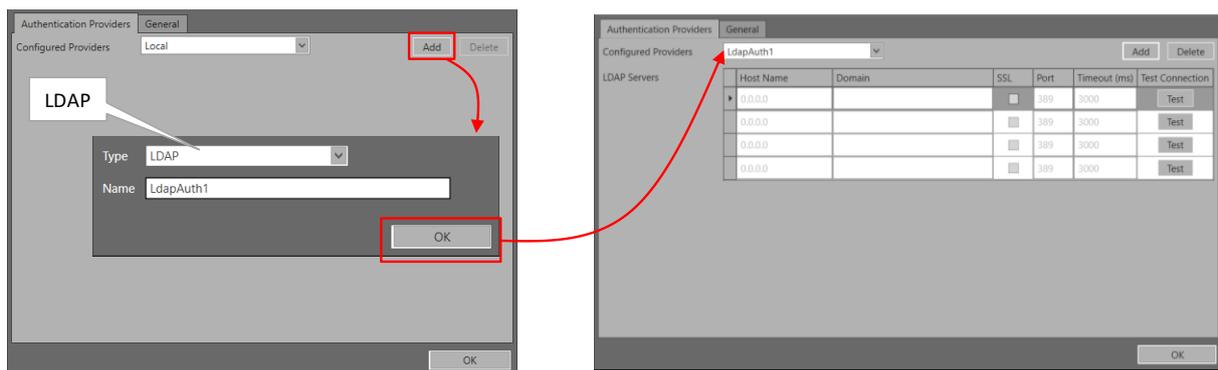


Figure 10 Authentication Providers Tab: Add New LDAP Provider

From now on, the new provider can be selected from the Configured Providers drop-down list to configure it further. Each LDAP provider includes 4 LDAP servers that can be configured for authentication. When authenticating a user against this provider, the first server will be used. When that server does not respond within the specified 'Timeout' (in ms), the second server is used, etc.

- ▶ Host Name (default 0.0.0.0): Fill out the IP address of the LDAP server;
- ▶ Domain: Each LDAP server has its own LDAP domain to which users belong. Fill out the domain for this LDAP server. As a result, e.g. UserX can be authenticated as UserX instead of UserX@domain. UserX should be the 'cn' of the configured user. The user that is authenticated is constructed using for example: 'cn=UserX, ou=Users, dc=belden, dc=com'. If no domain is provided in the configuration the user is authenticated using 'UserX' (the provided username is used without additional formatting). Note: cn=common name, dc = domain component, ou = Organizational unit;
- ▶ SSL (default = unchecked):
 - ▶ Unchecked: the connection data between LDAP client is and server is not encrypted and unsecure;
 - ▶ Checked: the connection data between LDAP client is and server is encrypted and secure;
- ▶ Port (default = 389): Port number used for LDAP authentication;
- ▶ Timeout (ms) (default = 3000 ms): Amount of time that HiProvision (=LDAP Client) waits for a response from the LDAP server. When no response has been received, the next server in the list will be used etc...
- ▶ Test Button: Click this button to test the connection between the LDAP client (=HiProvision) and the LDAP Server.

e. General Tab (Logged on Configurators)

All Administrators and Monitors can always log in simultaneously onto the Dragon PTN network. The options below can limit the Configurators group log in.

- ▶ Limit Logged on Configurators:
 - ▶ Unchecked: the number of simultaneous Configurator logons onto the Dragon PTN network is unlimited;
 - ▶ Checked (=default): the number of simultaneous Configurator logons onto the Dragon PTN network is limited up to the value filled out in the field 'Maximum logged on configurators';
- ▶ Maximum Logged on Configurators (default=5, range [1..10]): If previous checkbox has been checked, configure the maximum allowed number of simultaneous Configurators logons onto the Dragon PTN network.

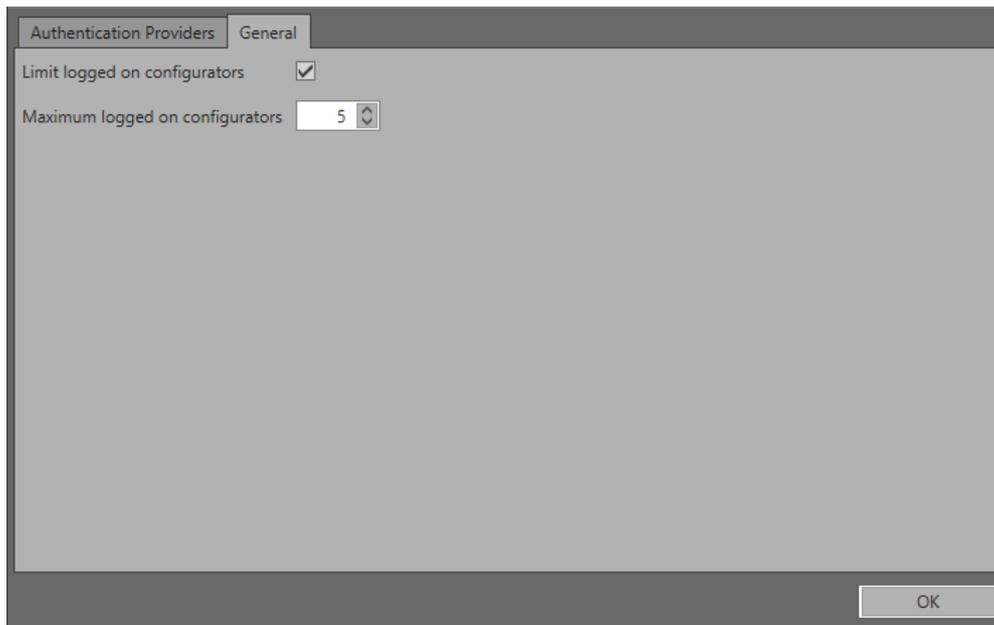


Figure 11 Limit Configurators Logons

4.5 Users Log

This section shows all the HiProvision UM events that were performed by which user. The last event appears by default on top of the list.

It is also possible to write or log these HiProvision UM events in a log file. This log file can be found in `<HiProvision install path>\Logging\System Logging\LogEvents\userevents.log`. Following button in the toolbar can be used for this file logging:

- ▶  (normal, disabled): the file logging of HiProvision UM events is disabled. Nothing will be written into the log file. Clicking this button enables the HiProvision UM file logging and turns the button into an enabled state;
- ▶  (highlighted, enabled): the file logging of HiProvision UM events is enabled. Clicking this button disables the HiProvision UM file logging and turns the button into a disabled state.

5. ABBREVIATIONS

AD	Active Directory
CN	Common Name
DC	Domain Component
LDAP	Lightweight Directory Access Protocol
OU	Organizational Unit
PTN	Packet Transport Network
RADIUS	Remote Authentication Dial In User Service
UM	User Management