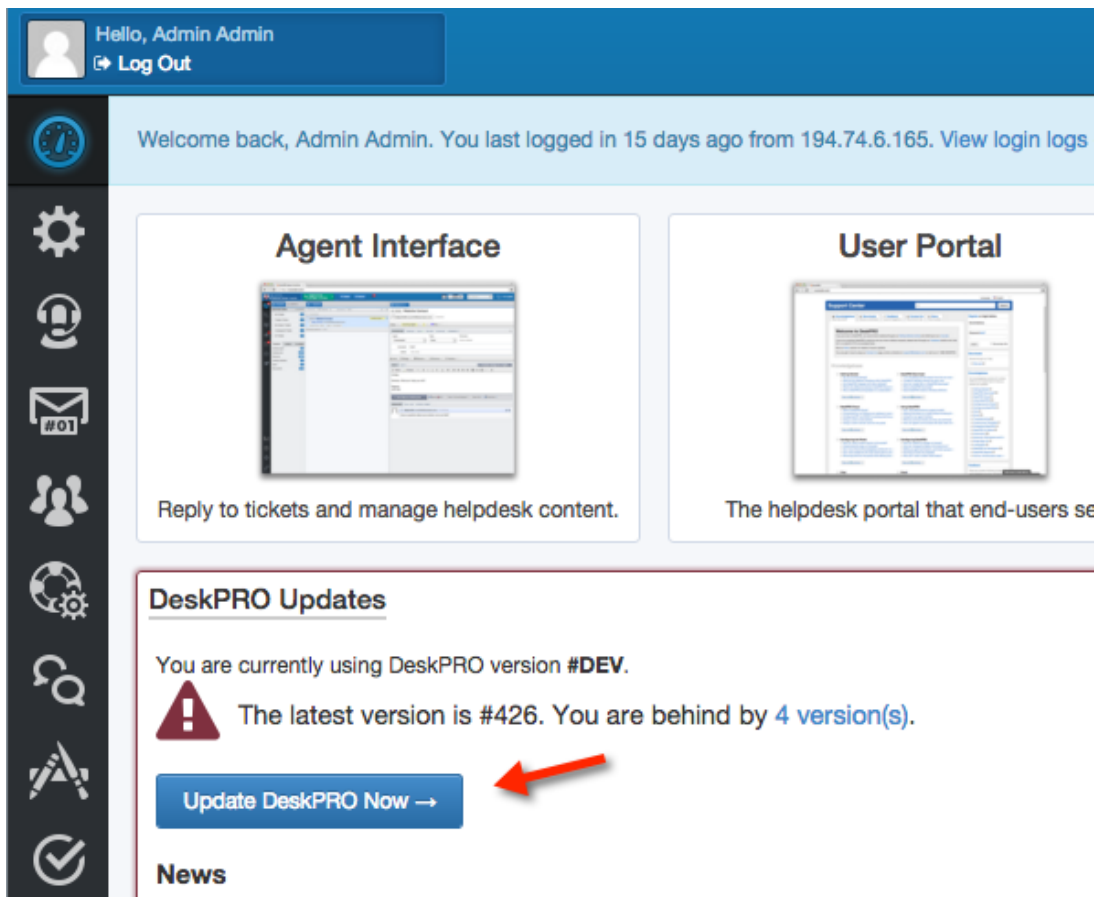


## DeskPRO Build #426 Released

2015-10-29 - Chris Padfield - Comments (2) - Deskpro Releases

This release fixes a critical security issue that affects earlier DeskPRO On-Premise versions. It is important that you update your DeskPRO installation **immediately**.

In most cases, you can update from the admin interface home page using the automatic updater:



The screenshot shows the DeskPRO Admin Interface. At the top, a blue header bar displays "Hello, Admin Admin" and a "Log Out" button. Below this, a light blue banner reads "Welcome back, Admin Admin. You last logged in 15 days ago from 194.74.6.165. View login logs". The main content area is divided into two columns: "Agent Interface" (with a screenshot of the agent interface and the text "Reply to tickets and manage helpdesk content.") and "User Portal" (with a screenshot of the user portal and the text "The helpdesk portal that end-users see"). Below these is a "DeskPRO Updates" section. It states "You are currently using DeskPRO version #DEV." and "The latest version is #426. You are behind by 4 version(s)." A red warning triangle icon is next to this text. A blue button labeled "Update DeskPRO Now →" is positioned below the text, with a red arrow pointing to it. At the bottom left, a "News" section is partially visible.

If that does not work, please either:

a) Use the [command-line updater](#).

b) [Manually update your helpdesk.](#)

If you have any problems updating, please immediately contact DeskPRO Support at [support@deskpro.com](mailto:support@deskpro.com).

The DeskPRO team apologies for the inconvenience caused by this urgent security release but stresses the urgency of upgrading your DeskPRO installation immediately.

Note: The Cloud platform is NOT affected.

---

### Comments (2)

Comments (2)

**SP Stephen Pienaar**

9 years ago

I would be helpful to know which versions of Deskpro are affected. We upgrade Deskpro fairly frequently (monthly) but not necessarily every single new version released. If we knew if our installed version was vulnerable, it would help us prioritise the upgrade.

**Ben Henley**

8 years ago

You should assume that any version before 426 is vulnerable.