What are Deskpro security best practices?

Ben Henley - 2018-04-17 - Comentarios (0) - Using Deskpro

Here are the steps you should consider to increase the security of your helpdesk.

Limit admin privileges

Any account with admin privileges can edit all other accounts on the helpdesk. Ensure that admin access is available only to the staff who need it. To check this, go to **Admin > Agents** and which agent accounts which are marked with a wrench icon. Admin accounts should consider using strong passwords and enabling IP whitelisting.

Stronger password policy

Set a custom agent password policy in **Agents > Settings** in the admin interface.

By default, agent accounts only need a 5 character password, but to improve security you should specify a longer password and require a mixture of lower-case and upper-case characters, numbers and symbols.

You can also specify a **Maximum password age** in days, after which the agent will have to change their password, and opt to forbid password reuse.

You should ensure that login rate-limiting is enabled for both agents and users, in **Admin > Setup > Rate Limiting**.

Have agents monitor logins or login attempts

Consider enabling agent notifications for logins and failed login (under **Other Notifications > Account**), and training agents to alert you if they see a login attempt they don't recognise.

Install the Resolve User Hostnames app

Install this app from **Admin > Apps** to have the helpdesk display which hostname users and agents on a ticket connect from. The hostnames are available through the Reports system, so you can create a custom report to look for suspicious activity. For example, if your agents only reply to tickets from inside your network, you could create a report to look for agent messages with an external hostname.

IP Whitelisting

Enable IP whitelisting in **Admin > Agents > Settings**. This means that agents can only log in from IP addresses that are trusted; when an agent logs in from an untrusted IP address, they are sent a link to verify the IP address by email. This security measure means that it is difficult for an attacker to log in to your helpdesk even if they know an agent account password.

You should train your agents to check that the IP address is actually correct before clicking the link, in case an attacker tries to log in at the same time they do.

You can choose how long an IP address is trusted before it needs to be verified again, and you can opt to apply IP whitelisting to admin accounts only.

Restrict session length

By default, agents will be logged out automatically after an hour of inactivity.

You can reduce this time in **Agents > Settings > Session Settings** if you want to limit the chance for somebody to use an agent's account when they leave their computer unattended. If this is an issue, you should also disable the option for agents to use **Remember me** to store their login details as a cookie.

You can also select **Require Activity** to automatically log out inactive agents.

Review logs regularly

Under **Agents > Audit Log**, you can see a log of all actions taken by admin accounts.

In Deskpro Download, you should also monitor the logs under **Server > Error Logs**.

Deskpro On-Premise security

You should follow the standard security precautions for any web application when installing and maintaining Deskpro on your own servers.

1. Change ownership of the installed files to the webserver or to a dedicated user other than root.

2. Make Deskpro application files non-writeable by the webserver. You can go a step further and make them non-writeable by any account; if you do this, you will need to install updates manually. The data/ directory must always be writeable by the cron/Scheduled Task user and the webserver.

3. Move the data/ directory outside of the web root directory. Specify the new path in config.php using the **$DP_CONFIG['dir_data']** variable.

4. Configure the web server not to execute or serve files in the data/ directory. This ensures that even if a malicious PHP file is written to data/, it cannot execute.

5. Use a non-root MySQL user and edit config.php with the new account details.

6. Check that the data/ directory is not served to the web. The installer checks this, but double-check that going to /data/ on your installation returns a 403 error.

7. If /admin/ and /agent/ do not need to be accessed from outside your organization, you could configure your webserver so that they are only accessible through your intranet/VPN.