



## Password-Reset Practices

*Jenny Rains*

*Research Analyst, HDI*

When a group of IT service or technical support professionals gather, one can almost always expect to hear murmuring about password resets as you walk through the room. On average, about three out of every ten tickets received by support centers are related to password resets. These findings help explain why password-reset practices remain a topic of interest for the IT service and technical support community.

This HDI Research Corner survey collected responses from 339 respondents from April 20 to May 16, 2011. The results revealed that even though 20 percent of support centers report that less than 10 percent of their tickets are about password resets, over 30 percent of tickets are password-reset related in more than one-third of support centers. This month's report reveals some of the current practices surrounding password resets and the ticket volume associated with these types of calls.

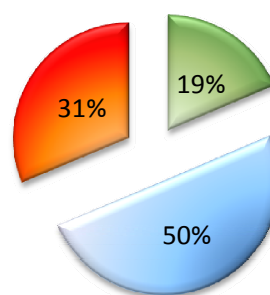
## Survey Results

### *Self-reset*

Most organizations (69%) allow their customers to reset at least some of their passwords without contacting the support center. Surprisingly, those organizations that do not allow customers to reset any passwords have a lower password-reset ticket volume than those who do. In support centers that allow their customers to reset all passwords themselves, about 34 percent of their tickets are related to password resets; in support centers that prohibit customers from resetting their passwords, the password-reset ticket average is 26 percent.

### Can customers reset passwords without contacting the support center?

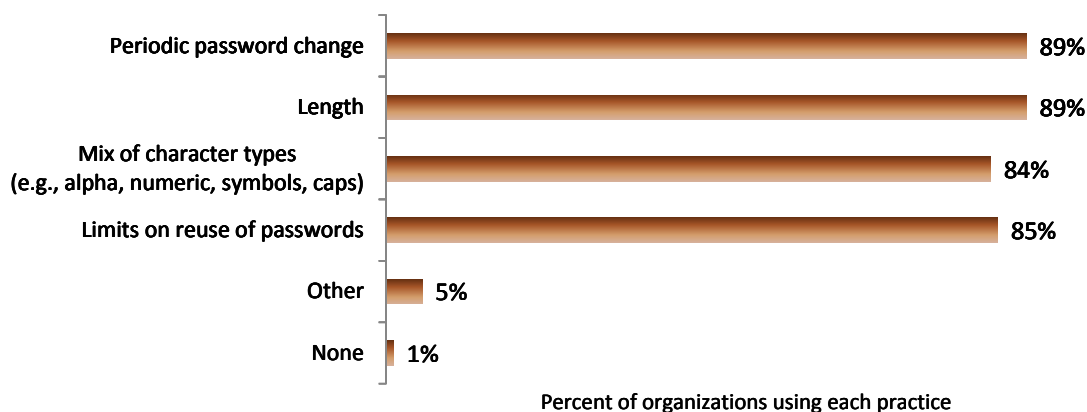
■ All passwords ■ Some passwords ■ No



### *Password Strength*

Without some level of security, passwords are just letters and numbers. Many organizations have requirements that ensure the security of their customers' passwords. One of the most common methods is the periodic password change. This has become a standard practice in the industry, with 89 percent of organizations requiring periodic password resets. Most organizations (52%) require customers to change their passwords every ninety days. Twenty-eight percent of organizations require more frequent resets (e.g., thirty days, forty-five days, sixty days, etc.), and 18 percent require less frequent changes (e.g., every four months, six months, annually, etc.). For some organizations, the reset schedule is application specific. And to further secure their customers' passwords, most organizations (85%) set limits on the reuse of passwords when they are reset or changed.

## Password strength requirements

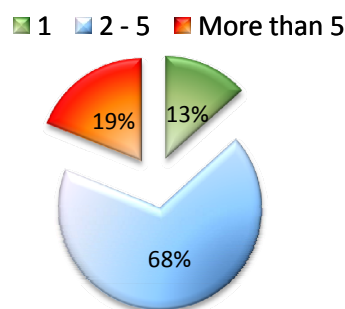


Setting requirements for the content of passwords, such as length (89%) and mix of character types (84%), such as alpha, numeric, symbols, and caps, is another common practice. Additional content restrictions were reported in the “other” category. For instance, some organizations prohibit words that can be found in the dictionary, while others ban proper names or company names. Only one percent of organizations has no requirements at all.

### Password Volume

Most organizations require customers to remember multiple passwords; only 13 percent report requiring customers to remember just one password. This group also has the lowest password-reset ticket volume (25%). Meanwhile, in 68 percent of organizations, customers are responsible for keeping track of two to five passwords. Nineteen percent of organizations require customers to remember more than five passwords, and in these organizations, the password-reset ticket average is 32 percent.

### Number of passwords customers are responsible for remembering



### Conclusion

Many organizations have implemented self-help features that enable customers to reset their own passwords. One of the major driving factors of this initiative is freeing up support center staff to address more critical tickets. However, while the survey results do not imply a direct relationship between empowered customers and a decrease in password-reset ticket volume, they do seem to support the use of a single sign-on system. After all, fewer passwords result in fewer calls about resetting them.

*For further discussion about password-reset practices, visit [www.HDIConnect.com](http://www.HDIConnect.com) to share your observations and reactions with your peers. Tell us what's working, or not working, in your organization.*

For all available HDI Research Corner reports, visit [www.ThinkHDI.com/BePartOfTheCorner](http://www.ThinkHDI.com/BePartOfTheCorner).

Copyright © 2011 United Business Media LLC. All rights reserved.

