

SMARTDEFLECT - USER GUIDE

Securing servers from potential cyber attacks requires a proactive solution. That's why BCDVideo developed the SMARTdeflect app. Within the app, system administrators will enjoy several crucial features to remotely safeguard against any threat.



- Windows Server compatibility
- Optional administrator specified PINs for users
- Optional email notifications for user login, failed login, or login attempt over an administrator specified number
- Remotely disable the server
- Optional mandatory restart for user login beyond set number of failed login attempts
- User interface for administrators to adjust basic settings
- Self-generating PINs
- Two-factor authentication

INSTALLATION INSTRUCTIONS

- Download the SMARTdeflect.Setup.exe file. Double click the file.
- Click "Run".
- Click "Yes".
- Choose where you would like to install the program. (Default: C: Program Files SMARTdeflect)
- Click "Next".
- Choose where and what you would like the Start Menu folder to be called. Or check the lower checkbox if you don't want a start menu item.
- Click "Next".
- Check the checkbox if you would like a desktop shortcut.
- Click "Next".
- Verify all the information is correct and click "Install".
- Leave the checkbox checked if you would like to launch SMARTdeflect and click "Finish".

GENERAL TAB

The General Tab is split into two main sections: the security settings and the multi factor authentication setup table. The security settings allow the administrator to increase the security that is implemented in the login process. The multi factor authentication setup is for the administrator to assign specific users their PINs, 2FA codes, or smart card + PIN combination.

SECURITY SETTINGS

The first item on this tab allow the administrators to specify how many failed login attempts a user can have before they get kicked out of the system. It defaults to 5, but it can be customized to the administrators choosing. If a user exceeds this amount they will receive a notice when they try to login that they need an administrator's assistance to proceed. This value can be reset in two ways: an administrator can open the SMARTdeflect application and reset the user's count manually, or everyone's count is reset when the server reboots.

WARNING: Setting additional smart card security on domain account (accounts that are not specific to the current machine) can cause all login attempts to fail.

The Security Settings section also has two checkboxes in order to require a PIN/Two Factor Authentication Code or a smart card (or both if both checkboxes are checked).

WARNING: If one of these check boxes is checked, no users without that authentication form set in the Multi Factor Authentication table will NOT be able to login.

MULTI FACTOR AUTHENTICATION

The table that take up the lower portion of the General tab has a row for every user that exists on the system. Here each user can be assigned a static PIN, up to 32 characters, or a two factor authentication code that can be paired up with a secondary device, such as a mobile phone or a laptop. This setting is changed with the drop down box in the "Security Type" column, and the code can be reset with the button to the right of it. This drop down box will also prompt a warning if the administrator wants to lower the security of one of the users to encourage users to use a high level of account security.

Each user can also be assigned a smart card with a corresponding PIN. Just click on the "Add Smart Card" button with the corresponding smart card inserted. Then type in the same numeric PIN into the PIN field and confirmation field and click "Ok".

If a user already has a smart card setup for them, this information can be edited with the same button, but the text will be changed to "Edit Smart Card". Then the smart card can be changed with the entry of a new smart card, the pin can be changed, or the smart card can be deleted from the users account.

Note: Users that are not local administrators will be logged out when they remove their SmartCard.

E-MAIL TAB

SMTP SETTINGS

On the right hand side of this tab there is space to set up SMTP server settings so that emails can be sent from the server to the administrators. This would require a network connection, but not necessarily a public one. There is a button under these settings that can be used to try to send a test email to the administrator address(es) in the top left corner and any error or output will be printed in the window.

EMAIL NOTIFICATIONS

There is a field for Admin Email Addresses in the top left corner of this tab. This can fit any number of email addresses separated by semi-colons. The administrator can then choose whether they want to get notifications when users have successful or unsuccessful log n attempts by using the check boxes near the bottom. The machine name will also be included in this email to help distinguish between different servers.

REMOTE RESTRICTIONS

The emails about successful log ins attempts will also include a link pointing back to the IP address or host name specified in the text box on the page. This link can be used to remotely boot users off the server in the case of a compromised account. The link is live for 10 minutes after the email is sent to prevent accidents from happening. If a user gets booted off the server, they will have the same restrictions as someone who had too many failed log in attempts. They will need a reboot or an administrator before they can log in again.

REMOTE DESKTOP

This software does not enable Remote Desktop by default, but it does write to a few settings that allow for all three fields to be visible from a remote connection. It must allow for computers that are NOT running Network Level Authentication in as well as some other registry settings. If these are changed, remote desktop may become more difficult for users that are using the PINs or two factor authentication.

FOR ADDITIONAL HELP

For additional assistance with set-up and troubleshooting, please contact BCDVideo's Technical Support by calling (844) 462-2384 or submit a support ticket at: <https://www.bcdvideo.com/support-ticket/>