Check In Verify Configuration

Operation

Working in conjunction with Image Recall at a Security checkpoint, Facial Recognition, or other Location requirements, Check-In Verify requires a cardholder to present credentials at a specific reader before granted access to any other reader in the system. Systems may assign more than one reader as a Check-In Verify site. Once verified, the credentials are active according to the Access Level assigned. Verified Access can be revoked at a predetermined time, or immediately when using a Check-Out Reader.

Configuration

To enable Check-In, Verify:

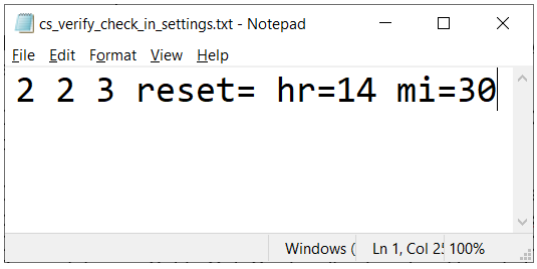
1. Upgrade the software to 5.0.33/6.0.33 or higher.

2. Flash all DSX controllers to V3214 or higher.

3. In DataBase, select the Location Tab and edit each Location that is to use this new feature. On the Y/N Tab select "Enable Antipassback" and select "Forgive AntiPassback Each Day" if you want everyone's status to be revoked each day at a predetermined time. **If not, you must have a Check-Out Reader.**

4. In DataBase select Hardware and then Devices. Edit the Devices that are to be Check-In Readers, on the Options 2 Tab select Zone 1 AntiPassback Type to be "IN". If there are Check-Out Readers, they must have their Zone 1 Antipassback Type set to "Out". If the IN reader will be used repeatedly in the same day without an OUT reader set the Antipassback Zone 1 Type to be Entry Soft.

5. If Comm Server is set to run as a service, stop the DSXCOMM service. Also close the program and navigate to the WinDSX folder where the software is loaded. In the C:\WinDSX\RunData\ folder edit the cs_verify_check_in_settings.txt file. Use the example to edit your file to meet your needs. Enter the Location number to implement the feature followed by device numbers of any device/reader in the location that should be excluded followed by the hour and minute that location should be reset. Resetting causes all card holders in that location to Check-In again. Make the modifications listed above in this file and Re-start the DSXCOMM service or program. Data is space delimited in the file. _ is a space in this example. Loc#_ExcludedDevices_Reset= hr=## mi=## This sample indicates Location 2 has check in verify enabled, devices 2 and 3 are excluded and card holders are reset at 2:30pm every day.



6. Set CS.exe (comm server) to run as a Service on the Comm Server PC if it is not already and start the Service. Use instructions found on the system flash drive, utilities folder.

7. Restart the DSX program. In Workstation force a full download to all locations.

8. If anyone is going to use "Remote Desktop" to make database changes, you will need to setup a Client PC for them to remote into.

9. Test – Card reads will receive an "Denied Check-In Verify Failed" until they are IN Zone 1 (used at the Check-In Reader).

10. Card Holders can be set to Override Check-In Verify on the Card Data Entry Screen by selecting "Override AntiPassback".

11. Card Holder can be set to "Out" or "Not Checked IN" with a Zone 1 OUT Reader or manually in Workstation/Location Operations/Antipassback Forgive. Enter the Card number and click OK to Check that Person Out. Enter 0 to Set Everyone Out. Be careful, once Set to Out, Cards will not work until read at a Check-In Reader.

12. Be careful when forcing full downloads from Workstation as this will set all Card Holders to a Neutral Status. Full downloads should be held off until after hours.

13. If Card Holders have more than one credential each credential must be used at a Check-In Reader before it will be Granted Access anywhere else.

14. Check-In Verify operates within a Location. If multiple Locations are involved, each one will require a Check-In Verify Reader to implement the feature in that Location.