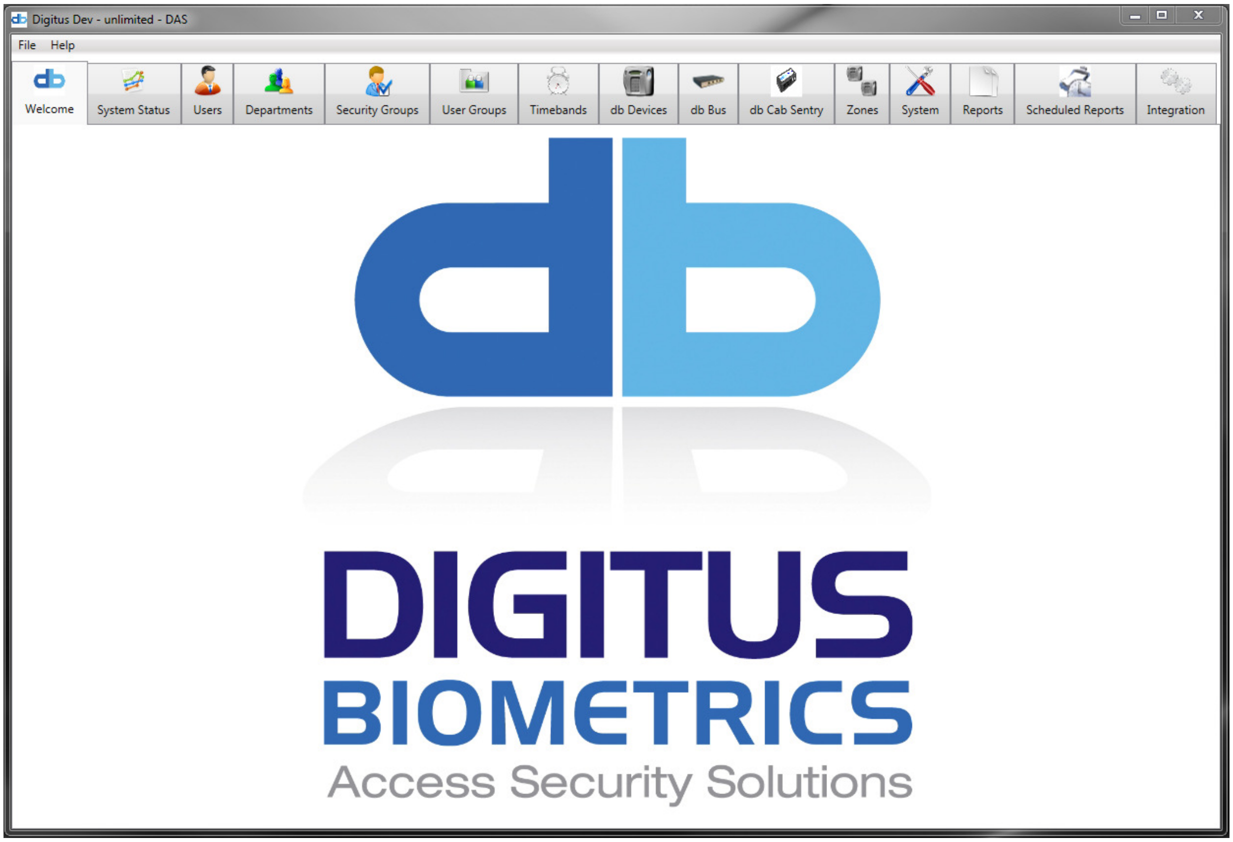
DAS-SQL Access Control System
Administration Manual



(Last updated: May 2015)

Table of Contents

Introduction - DAS-SQL Administration Manual

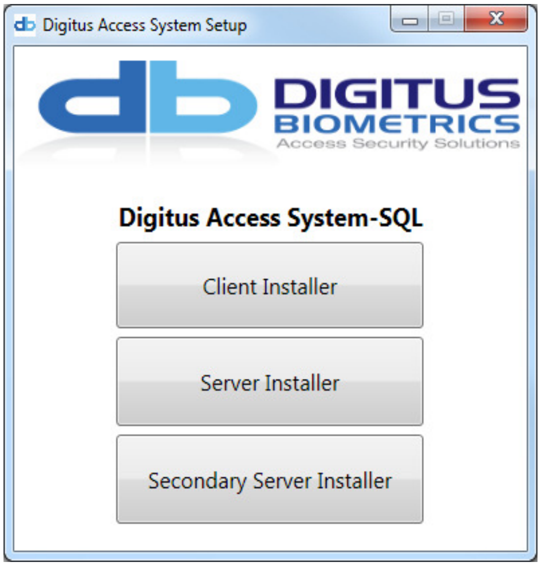
The DAS-SQL Access Control System is a full-featured access control system that uses PIN numbers, Fingerprint identification and RFID to control locking doors. The software is a client-server application in which one server can support multiple administrative clients. This manual is designed for system Users and Administrators.

Section 1 – Installing the DAS-SQL Server Software

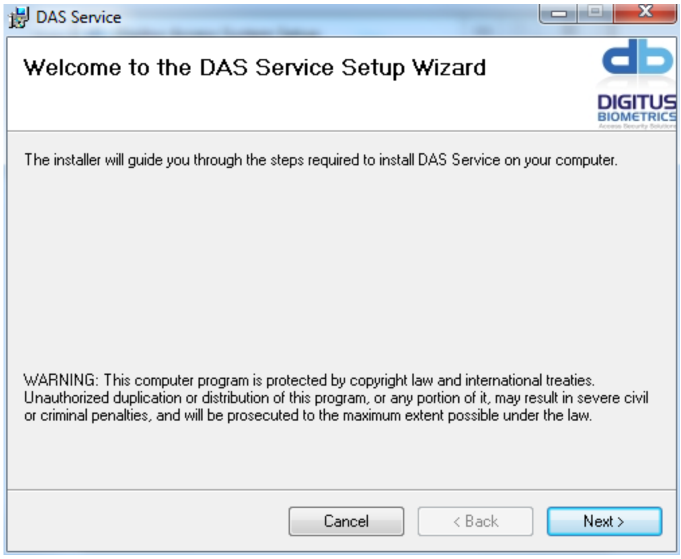
The DAS-SQL server runs as a Windows service called “BiometricAccessServer.” It starts automatically when the PC/Server starts up and requires no User interaction.

To install the DAS-SQL server software, insert the installation CD in the PC’s CD drive. **The installing User MUST be logged onto Windows as an Administrator or the installation will not complete properly.**

When the installer begins, chose “***Server Installer***” from the following screen:


Digitus Access System Setup
DIGITUS
BIOMETRICS
Access Security Solutions
Digitus Access System-SQL
Client Installer
Server Installer
Secondary Server Installer

You will then see a series of windows leading you through the installation process. The first one is:

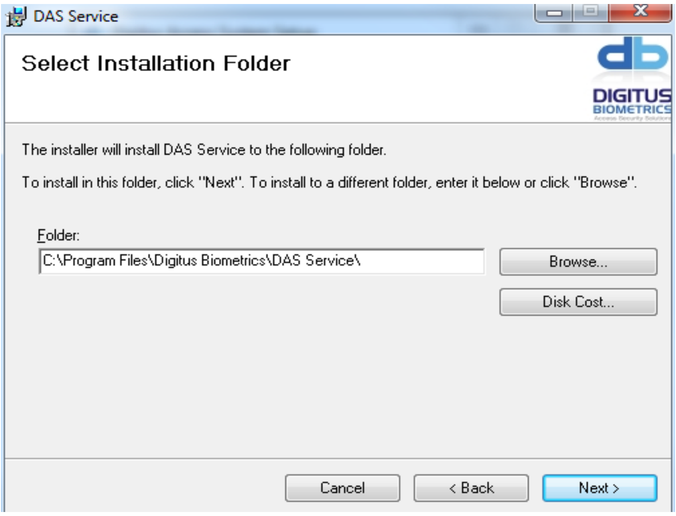


Welcome to the DAS Service Setup Wizard

The installer will guide you through the steps required to install DAS Service on your computer.

WARNING: This computer program is protected by copyright law and international treaties. Unauthorized duplication or distribution of this program, or any portion of it, may result in severe civil or criminal penalties, and will be prosecuted to the maximum extent possible under the law.

Click “***Next***” to allow the installer to select the installation directory.



DAS Service

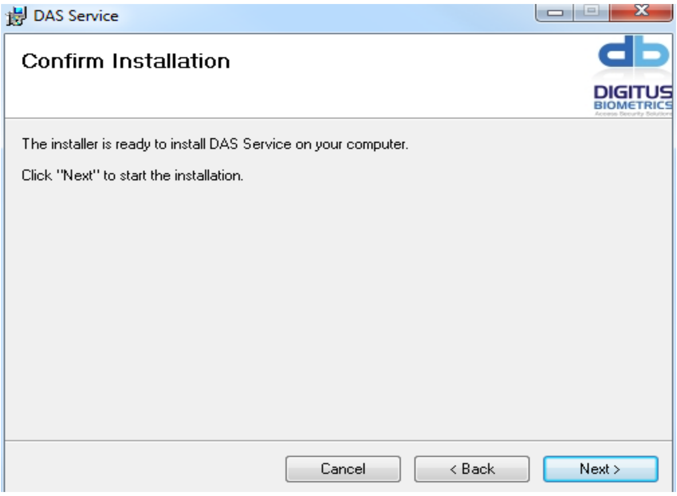
Select Installation Folder

The installer will install DAS Service to the following folder.

To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".

Folder: C:\Program Files\Digitus Biometrics\DAS Service\

When prompted to accept the terms of the software license, click the "***I Agree" button***". Click "***Next***" to confirm the installation.



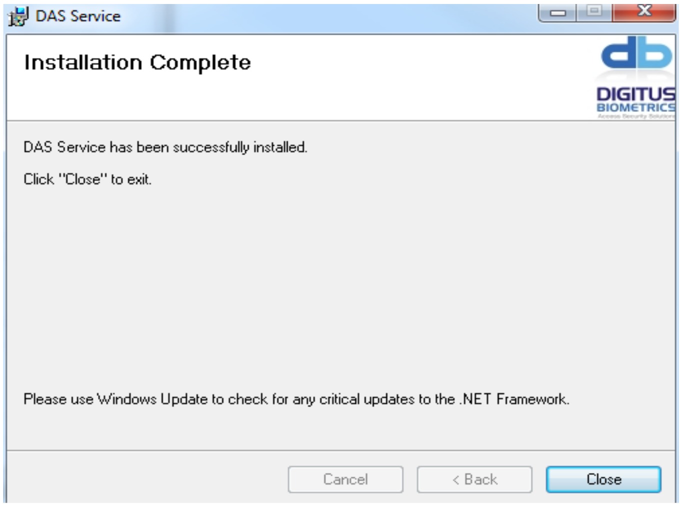
DAS Service

Confirm Installation

The installer is ready to install DAS Service on your computer.

Click "Next" to start the installation.

When the installation is complete, the following will be displayed.



DAS Service

Installation Complete

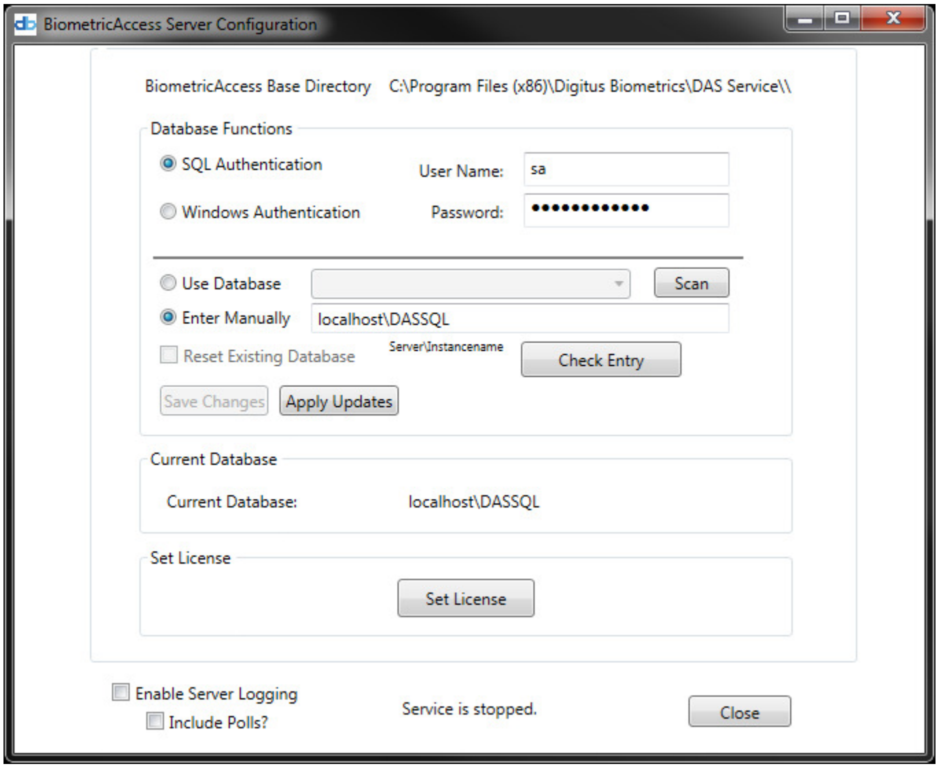
DAS Service has been successfully installed.

Click "Close" to exit.

Please use Windows Update to check for any critical updates to the .NET Framework.

The DAS-SQL server has now been installed.

After the server installation completes, the DAS-SQL server configuration utility will automatically start. This utility is used to set the database to be used by the server and to set the license file.



BiometricAccess Server Configuration

BiometricAccess Base Directory   C:\Program Files (x86)\Digitus Biometrics\DAS Service\\

Database Functions

● SQL Authentication   User Name: sa

○ Windows Authentication   Password: ••••••••••••

○ Use Database   Scan

● Enter Manually   localhost\DASSQL

□ Reset Existing Database   Server\Instancename   Check Entry

Save Changes   Apply Updates

Current Database

Current Database: localhost\DASSQL

Set License

Set License

□ Enable Server Logging

□ Include Polls?

Service is stopped.   Close

****SQL Authentication is strongly recommended for connectivity****

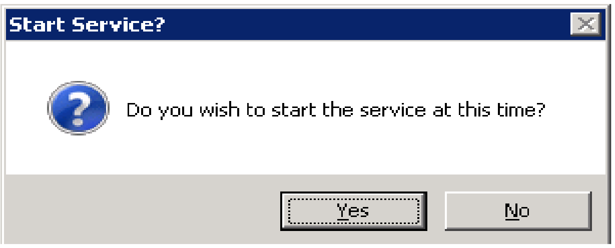
If an existing database has been installed on the server PC, it will be listed. If a different instance of a database is preferred, enter that manually. Click the "***Check Entry***" button to verify the database connection.

If an existing DAS-SQL database exists, it is possible to reset it to empty data. To do this, select the "Reset Existing Database" checkbox and click the "***Save Changes***" button. **NOTE: ALL DATA IN THE EXISTING DATABASE WILL BE DELETED AND THE SYSTEM WILL BE RESET TO A NEW SYSTEM STATE.** This means that all Users, door unit, Timebands, and all other data will be deleted. If an existing database is being deleted, make sure you have a record of all the door unit encryption keys as they cannot be reset once they are deleted.

Click the ***"Apply Updates"*** button to apply any changes in structure to the database itself. This can be done multiple times with no adverse effects to the database. This aligns the database with the DAS-SQL software and allows for more efficient and optimal access and display. It also ensures that the database tables are read correctly by DAS-SQL.

The DAS-SQL server must have a valid license to operate. To set the license file, click the "***Set License***" button. A file selection form will appear. Navigate to the license file and click the "Open" button. The license file will be copied to the correct location (the DAS-SQL server directory) and will be validated. If the validation fails, contact your dealer for help.

Click the "***Close***" button and the following prompt will be displayed:



Start Service?

Do you wish to start the service at this time?

Yes   No

Click "***Yes***" to start the "BiometricAccess" Service.

The "Enable Server Logging" check box enables the server to write a log file used for diagnostics. This is not a log file that can be used by the User; it is used only by technical support personnel to diagnose system issues.

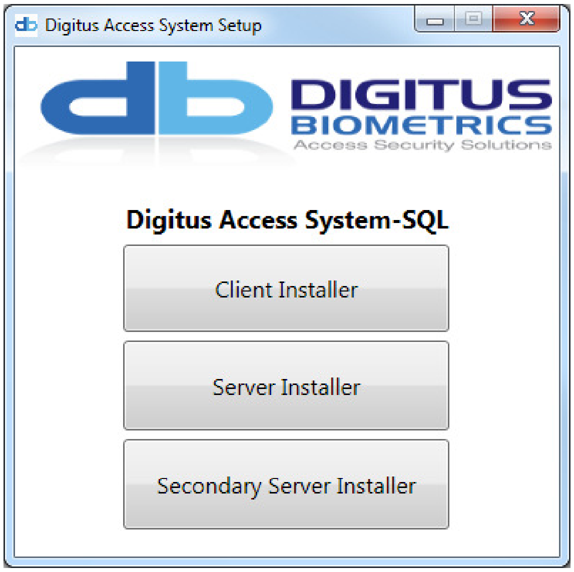
DO NOT ENABLE SERVER LOGGING UNLESS INSTRUCTED TO BY TECHNICAL SUPPORT PERSONNEL, AS THE LOG FILES WILL FILL THE SERVER HARD DRIVE VERY QUICKLY.

Section 2 – Installing the DAS-SQL Client

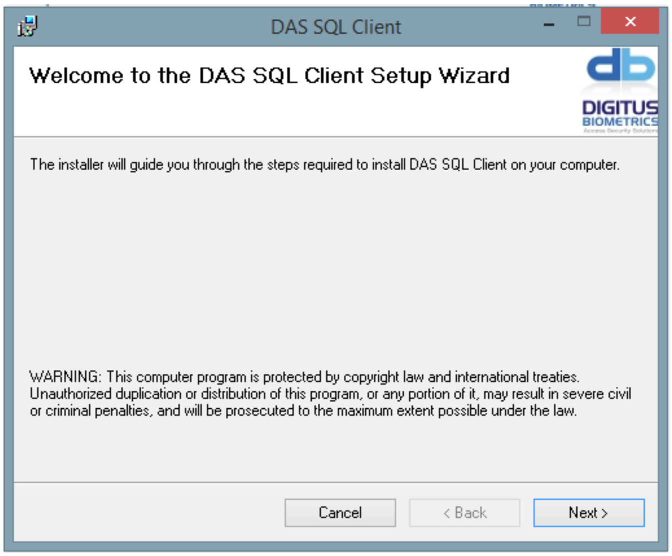
The DAS-SQL client is used to configure and monitor the access control system. It can be installed on the server PC or any other PC that can access the server via the network.

To install the DAS-SQL client software, insert the installation CD in the PC's CD drive. The installing User MUST be logged onto Windows as an Administrator or the installation will not complete properly.

When the installer begins, chose "***Client Installer***" from the following screen:


Digitus Access System Setup
DIGITUS BIOMETRICS
Access Security Solutions
Digitus Access System-SQL
Client Installer
Server Installer
Secondary Server Installer

You will then see a series of windows leading you through the installation process. The first one is:

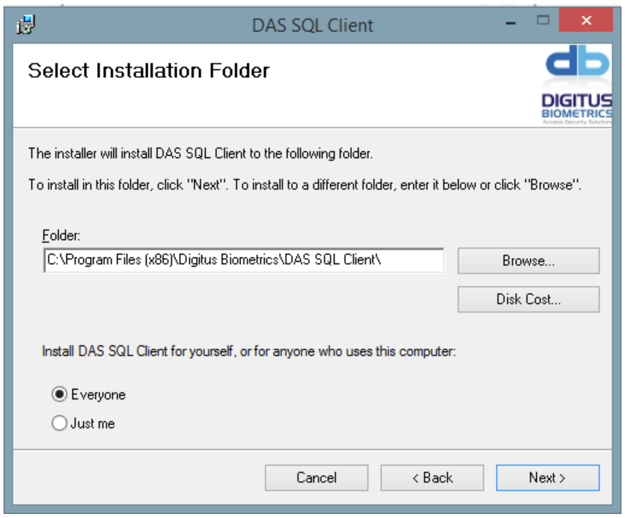


Welcome to the DAS SQL Client Setup Wizard

The installer will guide you through the steps required to install DAS SQL Client on your computer.

WARNING: This computer program is protected by copyright law and international treaties. Unauthorized duplication or distribution of this program, or any portion of it, may result in severe civil or criminal penalties, and will be prosecuted to the maximum extent possible under the law.

Click "***Next***" to allow the installer to select the installation directory.



Select Installation Folder

The installer will install DAS SQL Client to the following folder.

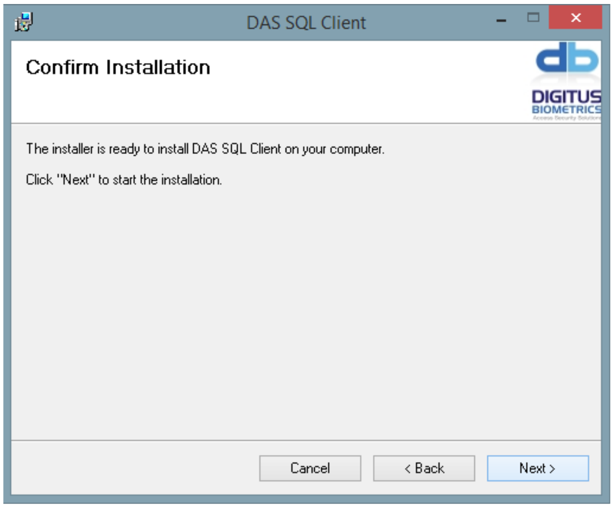
To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".

Folder:
C:\Program Files (x86)\Digitus Biometrics\DAS SQL Client\

Install DAS SQL Client for yourself, or for anyone who uses this computer:

● Everyone
○ Just me

Click "***Next***" to allow the installer to start installing the software.

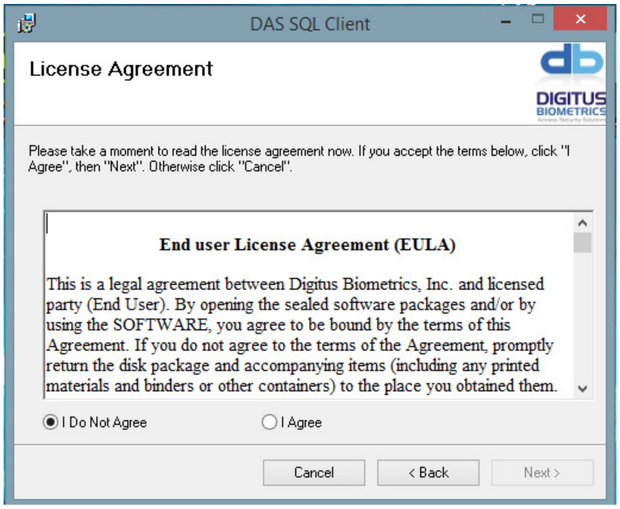


Confirm Installation

The installer is ready to install DAS SQL Client on your computer.

Click "Next" to start the installation.

When prompted to accept the terms of the software license, click the "***I Agree***" button and click "***Next***" to confirm the installation.



License Agreement

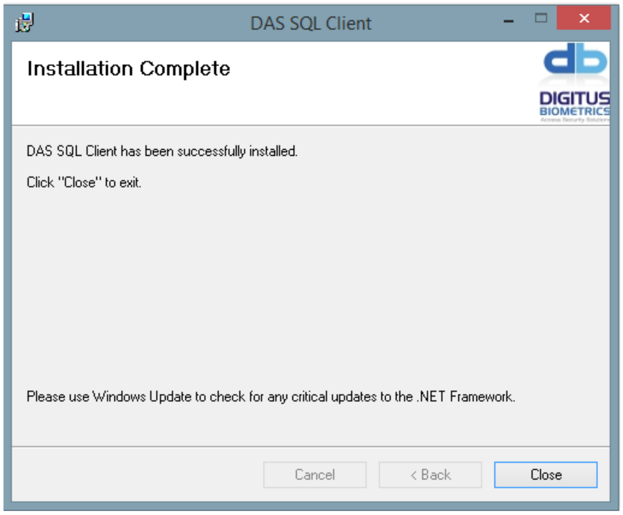
Please take a moment to read the license agreement now. If you accept the terms below, click "I Agree", then "Next". Otherwise click "Cancel".

End user License Agreement (EULA)

This is a legal agreement between Digitus Biometrics, Inc. and licensed party (End User). By opening the sealed software packages and/or by using the SOFTWARE, you agree to be bound by the terms of this Agreement. If you do not agree to the terms of the Agreement, promptly return the disk package and accompanying items (including any printed materials and binders or other containers) to the place you obtained them.

● I Do Not Agree ○ I Agree

When the installation is complete the following form will be displayed.



DAS SQL Client has been successfully installed.

Click "Close" to exit.

Please use Windows Update to check for any critical updates to the .NET Framework.

The DAS-SQL client has now been installed.

Section 3 – Understanding the DAS-SQL System

The **DAS-SQL system** consists of the Device units, Cabinet Units, a system server, and any number of client workstations. For information about the Device or Cabinet units, refer to the relevant hardware manuals.

The **DAS-SQL server** monitors the status of all db Devices, retrieving state and event logs (access attempts, alarms, and other events), and uploads Users and Timebands to the Devices. The server uses a database and allows connections from the clients. **DAS-SQL clients** are used to configure and monitor the system. See Sections 4 and 5 of this manual for detailed information about configuring and monitoring the system.

The various components of the configuration are the System Status, Users, Security Groups, User Groups, Timebands, db Devices, db Bus Devices, db Cab Sentry, System settings, Reports, and Scheduled Reports. Other components include Zones and Departments. Zones and Departments have no effect on who can access which Doors and when. They are merely administrative tools for easier management and reporting. In addition, the system can be configured to use Partitions.

Partitions are administrative objects that can be used to create “virtual systems” within the overall system. If an object (db Device, User, etc.) is placed into a Partition (or Partitions) it will be “visible” or accessible only to other objects in the same Partition(s). Thus, a large system can be configured to operate as a number of smaller, “virtual” systems which are “invisible” to each other. See the section on Partitions (4.12.7).

Selecting **Help** from any screen in the DAS-SQL Client will present three (3) options. The Installation Manual can be accessed by choosing **Contents**, the current licensing information can be viewed by choosing **License Information**, and the current Client and Service versions can be viewed by choosing **About**.

3.1 – Basic Process

The basic process for configuring a system is to set up the db Devices, db Bus Devices or db Cabinet Sentry devices. There are a number of device types: db Nexus II, db Nexus III, db Nexus II Duo, db Nexus III Duo, db Zero-U devices, db Bus Devices, and db Cabinet Sentry devices (see their individual hardware manuals for more information). All db Nexus and db Zero-U devices are configured using the “db Devices” tab on the client. db Bus Devices and db Cabinet Sentry devices have their own tabs.

3.2 – System Status (Section 4.2)

The System Status provides an overall status of the DAS-SQL system and all units and devices housed within the system. From this page, users can acknowledge alarms, check the status of doors and devices, unlock doors remotely, search users, lockdown and release the entire system as well as individual access points or zones, and view events in real time.

3.3 – Users (Section 4.3)

A User is a person who has some access to the system. Most Users are people who have access to particular Devices at particular times (TimeBands). Some Users may have access to configure the system – such as adding other Users, monitoring the system, or configuring the hardware (db Devices / db Bus Devices / Cabinet Sentry Devices). Each User can be assigned to one User Group. This User Group can be NONE (no access anywhere at any time), "<default> 24/7 All Doors", or a specific User Group. The User's access is determined by his or her assigned User Group.

When a single User is assigned a User Group, the data for that User is uploaded to each Device in the User Group. A good rule of thumb is that it takes approximately 10 seconds per User if two (2) fingerprint templates are used. Add another two (2) seconds for each additional fingerprint. Thus, if a User has 3 fingerprints assigned (two normal-fingers and one duress-finger); it will take approximately twelve seconds to upload that User's data to the Door unit.

If a Device unit is added to a User Group, all Users who use that User Group will be uploaded to the Device. If a User Group is assigned to 100 Users, it will take approximately 20 minutes to upload the Users to a Device. (Devices are updated concurrently, so data should be uploaded to all the Devices in the User Group in that 20 minute period.)

3.4 – Departments (Section 4.5)

Departments are administrative groups useful for management and logging. Departments are meant to act as a container for groups of users. Departments have no effect on access permissions, they are simply an administrative tool to make keeping track of Users easier.

3.5 – Security Groups (Section 4.6)

Similar to Departments, Security Groups are a collection of Users. Security groups offer another level of separation between users when used in conjunction with Dual Custody mode on specific Door unit types; db Nexus Duo II and III, all db Bus Devices, and Cabinet Sentry devices. This allows for another level of security on a Device, where you may require users to be from different security groups to successfully authenticate during dual-custody.

3.6 – User Groups (Section 4.7)

User Groups are permission sets that contain a number of Devices and an associated Timeband for each Device. For example, a User Group could be created called "Office Access," which contains two Devices ("Lobby" and "Hallway"). The "Lobby" Device could be assigned a Timeband allowing access from 8 AM to 5 PM, Monday through Friday. The "Hallway" Device could be assigned the same Timeband or one allowing access from 9 AM to 4 PM, Monday through Friday. This permission set (two Devices, each with an assigned Timeband) forms a "User Group."

3.7 – TimeBands (Section 4.8)

TimeBands are time periods during which access is allowed at a door. A Timeband is a 7-day set of time periods, and two time periods are allowed in each day. For example, it is possible to configure a Timeband for Mondays that allows access from 8 AM to 5 PM and again from 8 PM to midnight. The other days of the week would be left empty (no access during these periods). The system allows up to 99 Timebands to be configured in any order. The default Timeband allows for 24-hour, 7-day-per-week access.

3.8 – db Devices (Section 4.9)

Devices are a part of the secured site(s) hardware makeup. They consist of: db Nexus II, db Nexus II Duo, db Nexus III, db Nexus III Duo, and db Zero-U devices. Devices will be created and controlled via the db Device tab, and once confirmed are all monitored 24/7 from DAS-SQL and the System Status tab.

3.9 – db Bus Devices (Section 4.10)

Bus Devices differ from "db Devices" in their architecture. Multiple Devices are attached to a single Bus Controller via Remote Nodes. The db Bus Controller does not take in any direct user interaction. Instead, a bus has a series of Remote Nodes, which support a series of locks. The db Bus Controller also supports Enline units, used for end-of-row authentication. One db Bus Controller can support up to thirty two Remote Nodes, and each node currently supports connecting up to two locks (devices).

3.10 – db Cab Sentry (Section 4.11)

Cabinet Sentry units can be deployed in networked or standalone environments, and can be powered via power over Ethernet (PoE) or from an external power supply. A network-enabled db Cabinet Sentry system can take full advantage of DAS-SQL while a standalone configuration of db Cabinet Sentry is managed through a smartphone app built specifically for the db Cabinet Sentry access control system.

3.11 – Zones (Section 4.12)

Devices and db Bus Devices can be placed into Zones for easier management and reporting. Zones have no effect on User Groups (other than how the Devices are displayed in the User Group). They are simply a way to programmatically break up into sections the physical layout of devices and a tool to make system management and reporting easier.

3.12 – System (Section 4.13)

System refers to the DAS-SQL software system. This tab has the following sections:

- Client Settings – Configure the DAS-SQL server IP address and port number
- Email Server Settings – Configure the SMTP Email Server settings for email alerts and scheduled reports
- User-defined User Data Fields – Specify up to 12 user-defined data fields under each user account
- System Settings – Configure system-wide parameters, such as action and alarming notes and DAS-SQL Logon Methods
- SYSLOG setting – Allows you to specify a SYSLOG server for each Partition. All device events will automatically get forwarded to the specified SYSLOG server.
- Prox/Mifare Card Settings – Allows you to specify with RFID card types can be used with the system, and to configure certain card parameters
- iClass Card Configuration – Allows for configuration and programming of iClass cards
- Partitions – Define partitions to create "virtual systems" within the DAS-SQL system
- Servers – Add a number of secondary servers to "load-balance" over multiple server in larger systems
- Database Backup – Create backup copies of the SQL database
- System Self-Test – Runs a health test of the entire system.

3.13 – Reports (Section 4.14)

Reports provides detailed audit (log) reports and tremendous flexibility for defining report criteria. DAS-SQL can generate reports, allowing you to specify which users, which devices, and which event types to include. It's also possible to specify the required date ranges for the report. These reports can be customized and automated along with a list of standard reports. Reports can also be saved to run again at later dates or saved and used in conjunction with the scheduled reports feature.

3.14 – Scheduled Reports (Section 4.15)

Scheduled Reports provides a way for DAS-SQL to automatically generate and email reports at specified intervals. The reports are created and saved within the "Reports" tab and then schedules created on the "Scheduled Reports" tab.

3.15 - Integration (Section 4.16)

The "Integration Tab" allows for 3rd- party SNMP monitoring and AMAG Symmetry integration.

Section 4 – Configuring the DAS-SQL System

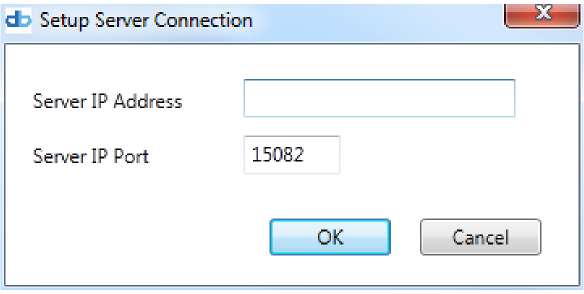
The DAS-SQL system is configured from the client. Start the client application and the welcome screen will be displayed (all other tabs will be disabled until a User is created and logs on). **Initial configuration MUST be done by a User logged onto Windows as an Administrator**. After initial configuration, any Windows user can use the client, but in order to change the client-specific settings (see System Settings features below), the Windows user must be an Administrator.

Note: If "User Account Control" is enabled in Windows, the DAS-SQL client application must be "Run as administrator" the first time it is run, because "Registry Keys" need to be written to the Windows Registry. To do this, browse to the folder where the DAS-SQL client software has been installed using Windows Explorer, the default location is "C:\Program Files (x86)\Digitus Biometrics\DAS SQL Client". Locate the file "BiometricAccessManagementClient.exe" and right-click on the file. Select "Run as administrator" and select to allow the program to run when prompted.

Note: this is only required the first time the DAS-SQL client is run, or whenever the server settings are being modified. If the client is not run this way, you'll receive an error stating that the windows couldn't save the Registry Keys.

4.1 – Initial Log on

To log on to the client, select the "File" menu item and select "Logon" from the displayed menu. If this is the first time this client has attempted to connect to the server, the User must enter the server's IP address and port number (default port: 15082) as shown below:

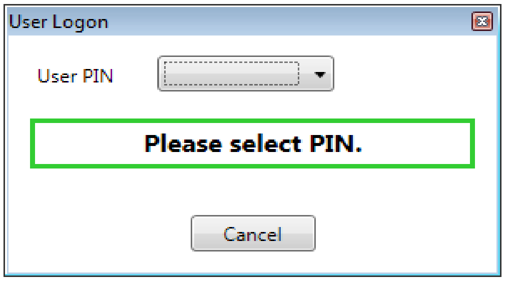


Setup Server Connection

Server IP Address

Server IP Port 15082

Enter the IP address (e.g. "192.168.1.100") of the PC/Server on which the DAS-SQL server is running. After this, click "***OK***" and the logon form will be displayed:



User Logon

User PIN

Please select PIN.

If the client successfully connects to the server, a list of all PINs for Users who have System Administration, Partition Administration, Monitor and Door Control, Personnel Setup, or System setup permissions will be displayed. Select your User PIN from the list. Depending on whether the system has been configured for fingerprint or password authentication, you will then either be prompted to place your finger on the USB scanner or to enter your password to log on.

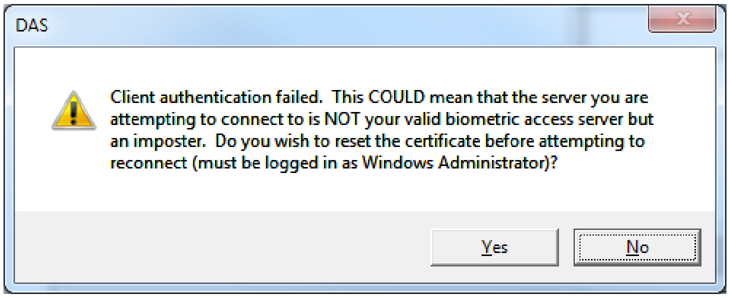
If no Users have been added to the system (i.e., this is the first logon to a new system), a System Administrator must be added before he or she can log on and configure the rest of the system. The system will display the User setup form (Section 4.4) with certain controls disabled so the User must be configured as a system setup User.

After a User successfully logs onto the client, the tabs appropriate to that User's permissions will be enabled. These rights are explained under "User Details tab" (Section 4.4.1).

NOTE: DAS-SQL clients communicate with the server via secured sockets. These sockets use a certificate which is created by, and stored on, the server. The first time a client connects to the server a record is made on the client of the server's certificate identifier. If the client attempts to connect to another server, perhaps an application impersonating the DAS-SQL server, the client authentication will fail. Since the application's certificate will not match the server's certificate identifier stored on the client the connection will not be established.

4.1.1 – Server Certificate

If the server's certificate is changed, due to re-installing the server or other problems, the server's certificate will no longer match the certificate identifier stored on the client and the logon and connection will fail, displaying the following error message:



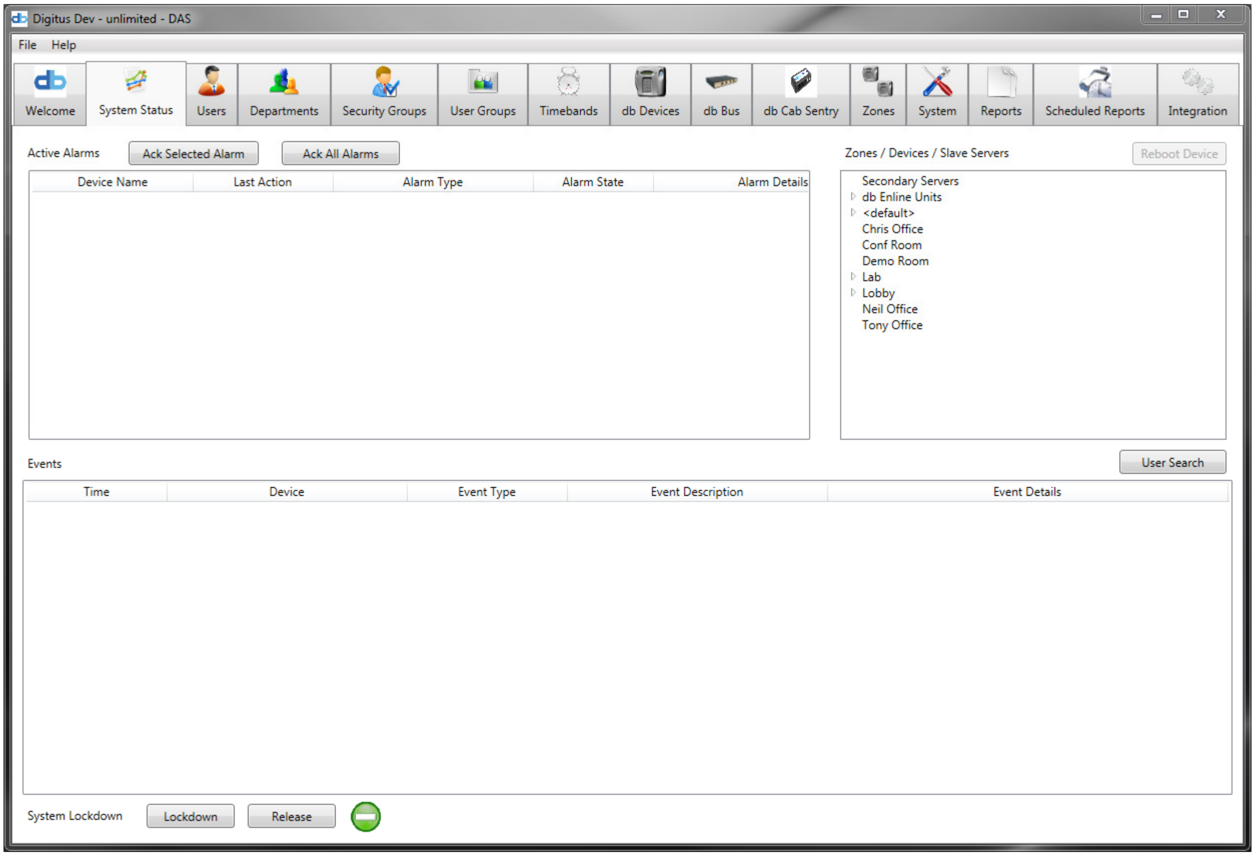
Client authentication failed. This COULD mean that the server you are attempting to connect to is NOT your valid biometric access server but an imposter. Do you wish to reset the certificate before attempting to reconnect (must be logged in as Windows Administrator)?

If the User knows the server's certificate has changed, and trusts the server, the server certificate identifier on the client can be reset to accept a new certificate from the server. To do this click the "***Yes***" button on the message box.

Note: for security reasons, the User MUST be logged into Windows as a Windows Administrator to reset the certificate.

4.2 – System Status Tab

The System Status tab is used to monitor and interact with system events, devices, alarms, and lockdowns. It's also a place where remote operation, such as door unlocks can be performed. See (Section 5) for further details involving the monitoring of the system.



4.2.1 – System Status Tab – Active Alarms List

The "Active Alarms" list shows any alarm that has been triggered within the system. The list provides users with the "Device Name", "Last Action" timestamp, "Alarm Type", "Alarm State", and "Alarm Details". Accompanying this are two different types of acknowledge buttons located above the list.

Device Name - States the unit on which the alarm was triggered.

Last Action - Shows the time the alarm occurred.

Alarm Type - States the event which caused the alarm to trigger.

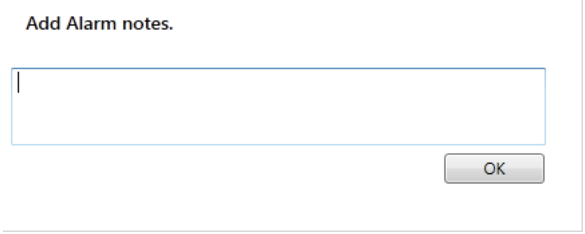
Alarm State - Shows the current status of that unit which may be "Active", "Acknowledged", or "Cleared".

Alarm Details - Shows more specific details of the alarm, the unit it occurred on, and the user who acknowledged the alarm if the alarm is still active and has been acknowledged.

Acknowledge Selected Alarm Button - This button requires that a specific row in the Alarms list be selected in order to acknowledge the alarm.

Acknowledge All Alarms Button - This button will acknowledge all current alarms in the alarm list.

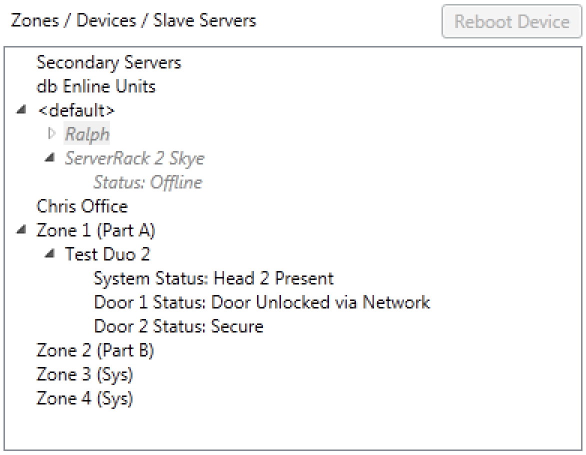
If the system is setup to require users to include a note about the alarm, then the user must supply a note about the alarm whenever an alarm is acknowledged. This feature is turned on or off via the “System tab” (Section 4.12.4).



Once the note has been entered and the “***OK***” button is clicked, the alarm will be removed from the list if the event which triggered the alarm has cleared. If the event is still in active then the Alarms list will show the alarm as being acknowledged, but it will not clear, until the condition that caused the alarm has gone away.

4.2.2 – System Status Tab – Zones/Devices/ Slave Servers List

This shows a list of all devices, grouped by zone. For each device, the current status of the device is shown.

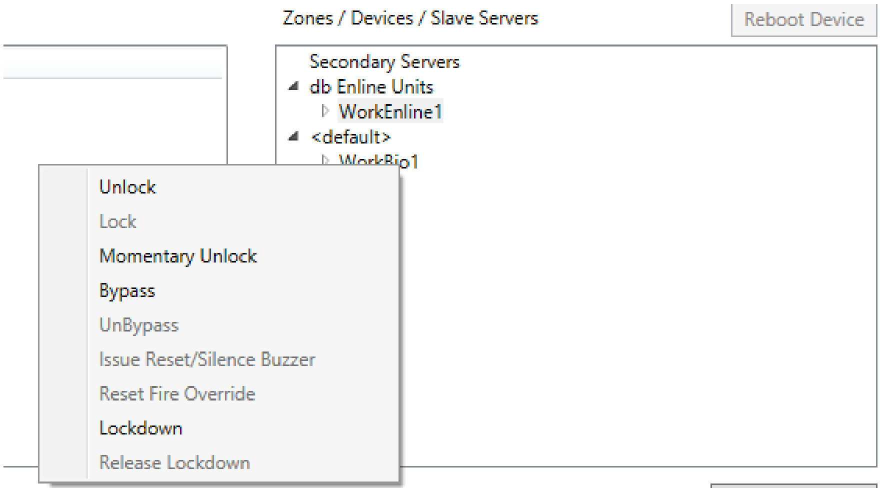


Secondary Servers
db Enline Units
◢ <default>
▷ *Ralph*
◢ *ServerRack 2 Skye*
Status: Offline
Chris Office
◢ Zone 1 (Part A)
◢ Test Duo 2
System Status: Head 2 Present
Door 1 Status: Door Unlocked via Network
Door 2 Status: Secure
Zone 2 (Part B)
Zone 3 (Sys)
Zone 4 (Sys)

Reboot Device - The reboot device button will perform a complete reboot of the selected unit.

In addition, certain remote operations can be performed on the device. This is done by right-clicking on the unit and selecting the desired action from the popup menu.

Status - Shows the current status of the unit.



Unlock and Lock - Unlock and lock commands can be issued to doors or cabinets through the network. This state will stay in place until another lock or unlock command is issued.

Momentary Unlock - Unlock command can be issued to doors or cabinets through the network. This state will only apply for the unit's entry delay (Sec 4.9.2).

Bypass and Un-Bypass - Alarms will not be triggered when a device is set to "bypass".

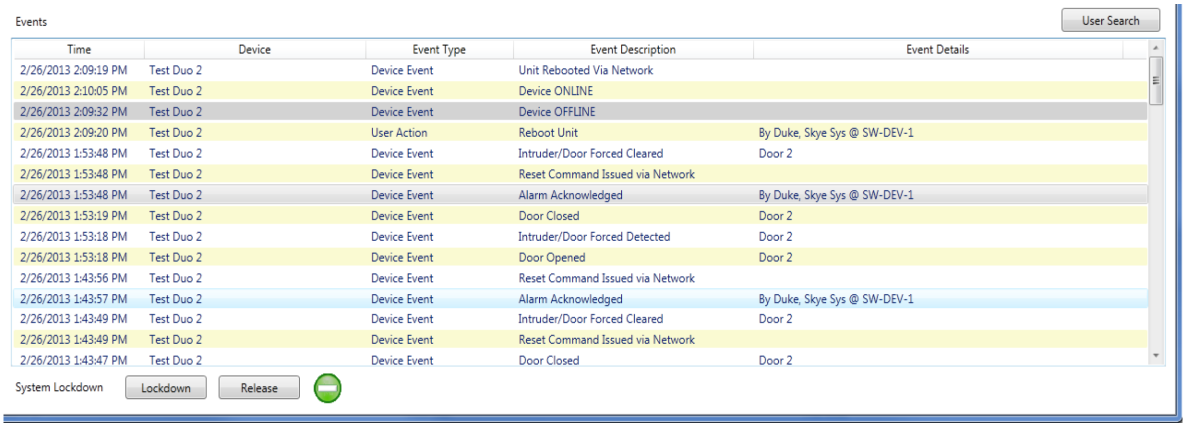
Reset/Silent Buzzer - This option give the user a way to forcefully stop a buzzer from sounding. This will only function if the event that triggered the alarm is no longer active.

Reset Fire Overrides - This option is to be used to reset the fire-override feature that triggered an unlocked event on a device.

Lockdown and Release - Lockdown puts the unit in lockdown mode locks the corresponding door or cabinet until the release command is issued.

4.2.3 – System Status Tab - Events List

The Events List displays real-time events as they occur on devices and/or within DAS-SQL.



Time	Device	Event Type	Event Description	Event Details
2/26/2013 2:09:19 PM	Test Duo 2	Device Event	Unit Rebooted Via Network	
2/26/2013 2:10:05 PM	Test Duo 2	Device Event	Device ONLINE	
2/26/2013 2:09:32 PM	Test Duo 2	Device Event	Device OFFLINE	
2/26/2013 2:09:20 PM	Test Duo 2	User Action	Reboot Unit	By Duke, Skye Sys @ SW-DEV-1
2/26/2013 1:53:48 PM	Test Duo 2	Device Event	Intruder/Door Forced Cleared	Door 2
2/26/2013 1:53:48 PM	Test Duo 2	Device Event	Reset Command Issued via Network	
2/26/2013 1:53:48 PM	Test Duo 2	Device Event	Alarm Acknowledged	By Duke, Skye Sys @ SW-DEV-1
2/26/2013 1:53:19 PM	Test Duo 2	Device Event	Door Closed	Door 2
2/26/2013 1:53:18 PM	Test Duo 2	Device Event	Intruder/Door Forced Detected	Door 2
2/26/2013 1:53:18 PM	Test Duo 2	Device Event	Door Opened	Door 2
2/26/2013 1:43:56 PM	Test Duo 2	Device Event	Reset Command Issued via Network	
2/26/2013 1:43:57 PM	Test Duo 2	Device Event	Alarm Acknowledged	By Duke, Skye Sys @ SW-DEV-1
2/26/2013 1:43:49 PM	Test Duo 2	Device Event	Intruder/Door Forced Cleared	Door 2
2/26/2013 1:43:49 PM	Test Duo 2	Device Event	Reset Command Issued via Network	
2/26/2013 1:43:47 PM	Test Duo 2	Device Event	Door Closed	Door 2

The list shows Time, Device, Event Type, Event Description, and Event Details.

Time - The timestamp when the event occurred.

Device - The Device name on which the event occurred.

Event Type - Shows whether it was an event that occurred on a device, within DAS-SQL or an action performed by a DAS-SQL user.

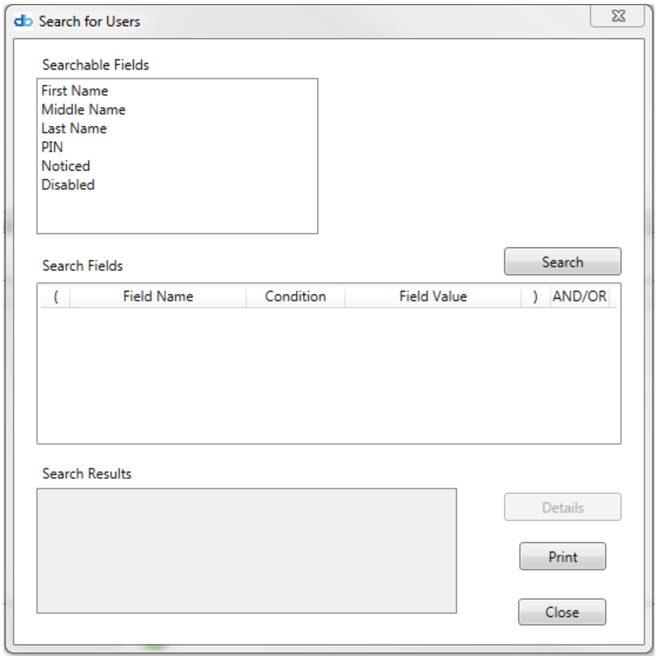
Event Description - A brief description of the actual event.

Event Details - Gives additional detail about the event. Double clicking on a detail with a User listed will bring up information on the User.

Lockdown - This button will force a total lockdown of all devices within the system. A popup confirmation is given before this action occurs. The icon to the right will turn red to indicate system is locked down

Release - This button will release all units from the lockdown state. The Icon to the right will turn green.

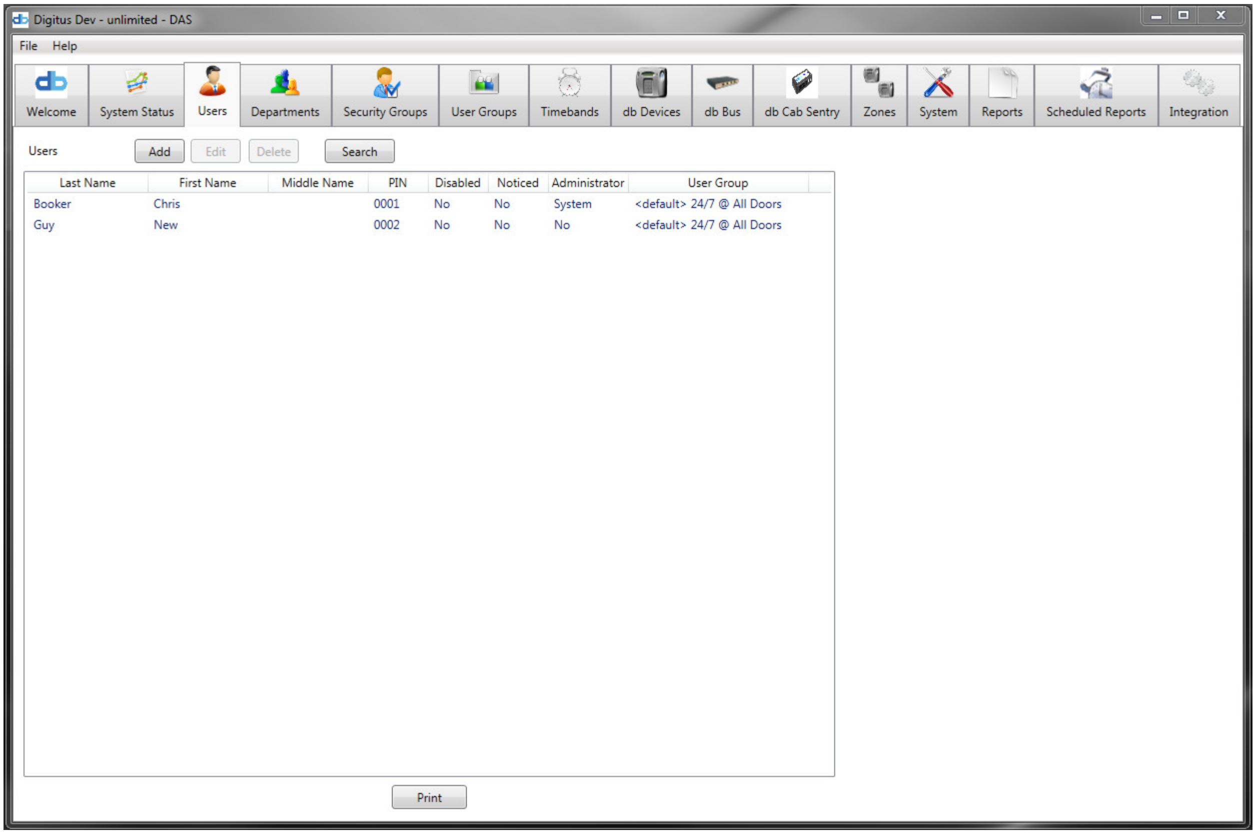
User Search - This button provides the window below and allows for quick searches of all the users within the system.



To use the searchable fields, left-click a desired field and drag and drop that field into the Search Fields box. Once done, add the desired value for the field and click search.

4.3 – Users Setup Tab

The Users Setup tab is used to configure system Users. By definition, a “User” is what card access systems typically call a “cardholder,” thus a “User” is someone who has permission to enter through certain doors at certain times. Each User can also have administrative permissions (what card access control systems typically call “users”) that allow that User to monitor system status and control devices, configure personnel, and configure the system hardware.



Last Name	First Name	Middle Name	PIN	Disabled	Noticed	Administrator	User Group
Booker	Chris		0001	No	No	System	<default> 24/7 @ All Doors
Guy	New		0002	No	No	No	<default> 24/7 @ All Doors

Currently configured Users are listed in the “Users” list. This list can be sorted by last name, first name, middle name, PIN, or User Group. “Left-click” the column header to sort by that column.

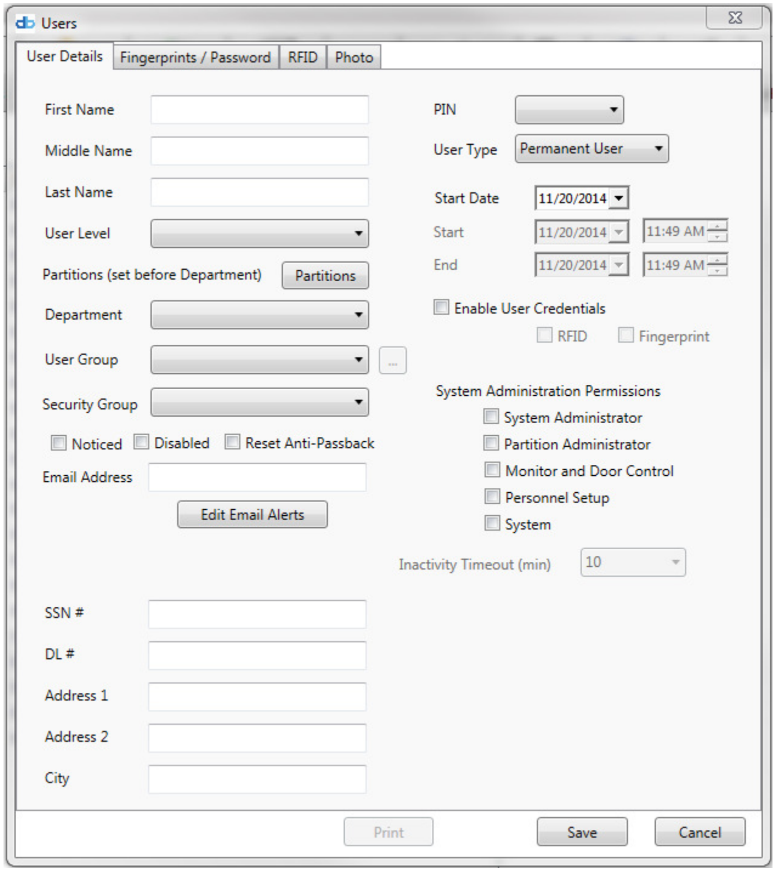
4.3.1 – Adding a New User

To add a new User, select the Users Setup tab click the “***Add”*** button or right-click on the Users list, which will produce a popup menu with the following options: Add, Edit, and Delete. If an existing User has been selected from the list, the “***Edit***” and “***Delete***” menu items will be enabled; if no User has been selected, only the “***Add***” menu item will be enabled. To edit an existing User, select the “***Edit*** “menu item and the User Setup form will be displayed. To delete a User, select “***Delete***” and the User will be deleted from the system.

NOTE: Deleting a User will remove him or her permanently from the system.

If a User is not to be removed permanently, it is recommended that the User be disabled, so the record remains but access is removed. The User can then be re-enabled at a later time if desired. Also note that only Users with “System Administrator” or “Partition Administrator” permission can edit or delete other Users with that permission, or assign that permission to Users.

4.4 – User Form



User Type: Permanent User

Start Date: 11/20/2014

Start: 11/20/2014 11:49 AM

End: 11/20/2014 11:49 AM

Inactivity Timeout (min): 10

The User Setup form has four tabs: User Details, Fingerprints/Password, RFID and Photo.

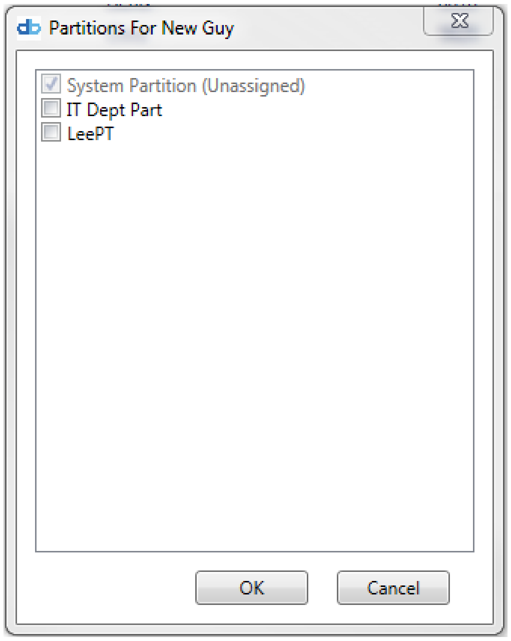
4.4.1 – User Form - User Details tab

The “User Details” tab contains the following fields:

“First Name,” “Middle Name,” and “Last Name.” Enter the User’s first, middle (optional) and last name.

The **User Level** control defines the User’s permission for the Devices he or she can access. There are two levels in this list: User and Manager. Users can only access certain Doors during their assigned schedules. In addition to accessing Devices, managers can also perform administrative tasks at the Devices (e.g., set the clock, configure network settings, and add or edit users locally).

The “***Partitions”*** button allows the User to be assigned to Partitions. Select the desired Partition(s) for this User from the selection form.



Partitions For New Guy

☑ System Partition (Unassigned)
□ IT Dept Part
□ LeePT

Departments are administrative groups useful for management and logging. You can select a Department for this User or use the <default> group. Departments have no effect on access permissions; they are simply an administrative tool to make keeping track of Users easier.

Note: Departments listed are filtered according to the Partition(s) to which the User is assigned. If a Department is assigned to the same Partition(s) it will be listed; if not, it will not be listed.

User Groups are used to grant the User specific permissions to access specific Devices at particular times (Timebands). User Groups **must be configured before they can be assigned to Users**, though the User can be assigned to the <default> 24/7 All Doors User Group, which will give full access (at all times) to all Devices.

Note: User Groups listed are filtered according to the Partition(s) to which the User is assigned. If a User Group is assigned to the same Partition(s) it will be listed; if not, it will not be listed.

Security Groups are used to assign a user into a specific security group, which is used in conjunction with dual-custody on specific Device types (db Nexus Duo II and III), all db Bus devices, and db Cabinet Sentry Devices.

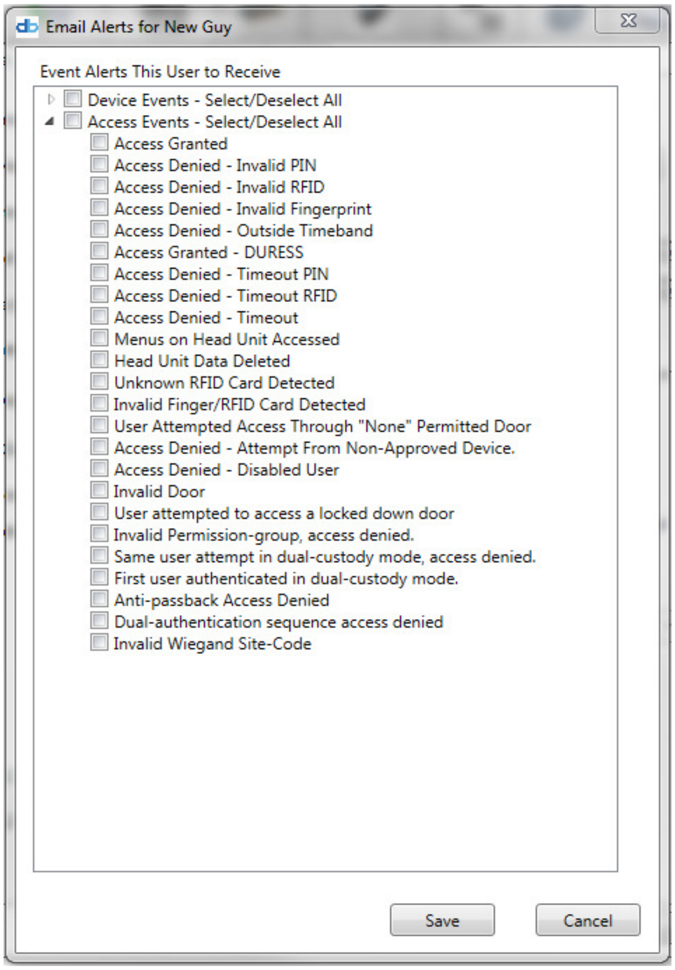
Note: Security Groups listed are filtered according to the Partition(s) to which the User is assigned. If a Security Group is assigned to the same Partition(s) it will be listed; if not, it will not be listed.

The **Noticed** checkbox allows a User to be flagged or noticed when he or she accesses a Door. When a "noticed" User access a Door, a message will be sent to all DAS-SQL clients, notifying them the User accessed a door. This is useful for tracking particular Users or in case the User must be contacted for some reason.

The **Disabled** check box allows the User to be disabled, that is, he or she will remain in the system, but his or her Door access permissions will be disabled or suspended.

The **Reset Anti-Passback** checkbox works with units that have anti-passback capability enabled. When checked and the user form is saved, the anti-passback state is reset for this user on all Devices. This is useful if a Device gets out of sync due to external factors (e.g. a user authenticates into a room but then does not authenticate when leaving, because they leave with someone else).

The **Email Address** field is used to enter an email address for this User. If an address is entered, and appropriate “Email Alerts” are enabled, this User will receive email alerts on system events. To configure which events the User will receive emails on, click the “***Edit Email Alerts***” button. The following form will be displayed.



Event Alerts This User to Receive

- ▷ ☐ Device Events - Select/Deselect All
- ◢ ☐ Access Events - Select/Deselect All
  - ☐ Access Granted
  - ☐ Access Denied - Invalid PIN
  - ☐ Access Denied - Invalid RFID
  - ☐ Access Denied - Invalid Fingerprint
  - ☐ Access Denied - Outside Timeband
  - ☐ Access Granted - DURESS
  - ☐ Access Denied - Timeout PIN
  - ☐ Access Denied - Timeout RFID
  - ☐ Access Denied - Timeout
  - ☐ Menus on Head Unit Accessed
  - ☐ Head Unit Data Deleted
  - ☐ Unknown RFID Card Detected
  - ☐ Invalid Finger/RFID Card Detected
  - ☐ User Attempted Access Through "None" Permitted Door
  - ☐ Access Denied - Attempt From Non-Approved Device.
  - ☐ Access Denied - Disabled User
  - ☐ Invalid Door
  - ☐ User attempted to access a locked down door
  - ☐ Invalid Permission-group, access denied.
  - ☐ Same user attempt in dual-custody mode, access denied.
  - ☐ First user authenticated in dual-custody mode.
  - ☐ Anti-passback Access Denied
  - ☐ Dual-authentication sequence access denied
  - ☐ Invalid Wiegand Site-Code

Select the desired events and click “Save.”

The **PIN** selection control chooses a PIN code for the User. Only unused (available) PIN numbers will be listed. If a number is not listed, it has already been assigned to another user. The PIN is used on certain Devices. The User enters the PIN at the Device, as one of the required credentials to identify him or herself.

The **User Type** control allows the User to be defined as “Permanent” or “Temporary”. Most Users will be permanent, but contractors or visitors might be assigned temporary permissions.

If a User is defined as Temporary, the Start and End date/time fields will be enabled. Select a start and end date and time for this User.

If a User is defined as Permanent, a delayed start date can be assigned so the User can be pre-enrolled before access is granted.

The **Enable User Credentials** control allows the credential settings specified on a Device (for certain types of unit) to be overwritten by the User-based credentials. For example, if a db Nexus Unit has RFID and Fingerprint enabled, and if User Credentials are enabled for a User with only RFID being specified, the User wouldn't be required to present a fingerprint to gain access.

System Administration Permissions are used to assign administrative permissions to Users. These permissions are “System Administrator” and “Partition Administrator”. These permissions are used to assign restricted User Groups to Users. If a User

Group is marked as “Requires Administrator Override to Assign,” that User Group can be assigned only to Users by a System or Partition Administrator. If a User without System or Partition Administrator permission needs to assign a restricted User Group to a User, a System or Partition Administrator must approve the assignment by scanning his or her fingerprint to validate approval.

System Administrators can configure settings in the “System Settings” tab, such as email configuration, create Partitions, and configure system default values. System Administrators can assign Partition Administrator permissions to other Users.

Partition Administrators can configure Devices, Users, Departments, Zones, and User Groups assigned to the same Partition(s) as the User with Partition Administrator permissions.

System and Partition Administrators have all other permissions by default.

Monitor and Door Control permission allows the User to access the Device Status tab on the DAS-SQL client. These Users can view the transaction list, acknowledge alarms, control doors (unlock/relock/momentary unlock, bypass/un-bypass alarms, lockdown/release lockdown) and Zones (lockdown/release lockdown). See the “System Status Tab” section below. This permission is useful for guards and other Users who do not need to configure personnel or the system hardware, but do need to monitor and control the doors and alarms.

Personnel Setup permission allows the User to configure User data – adding, editing, and deleting Users, as well as configuring Departments, Security Groups, User Groups, and TimeBands. This permission is useful for personnel managers or others who are responsible for enrolling or managing Users but do not need to monitor or control the Doors, and do not need to configure the system hardware.

System Setup permission allows the User to configure the system hardware (add, edit, and delete Devices). This permission should be given only to Users who understand how the system works, as reconfiguring the Devices can result in undesirable behavior.

Inactivity Timeout – Determines How long before a User is automatically logged off system.

Note: A User must have at least one of the “System Administration Permissions” to log on to the DAS-SQL client.

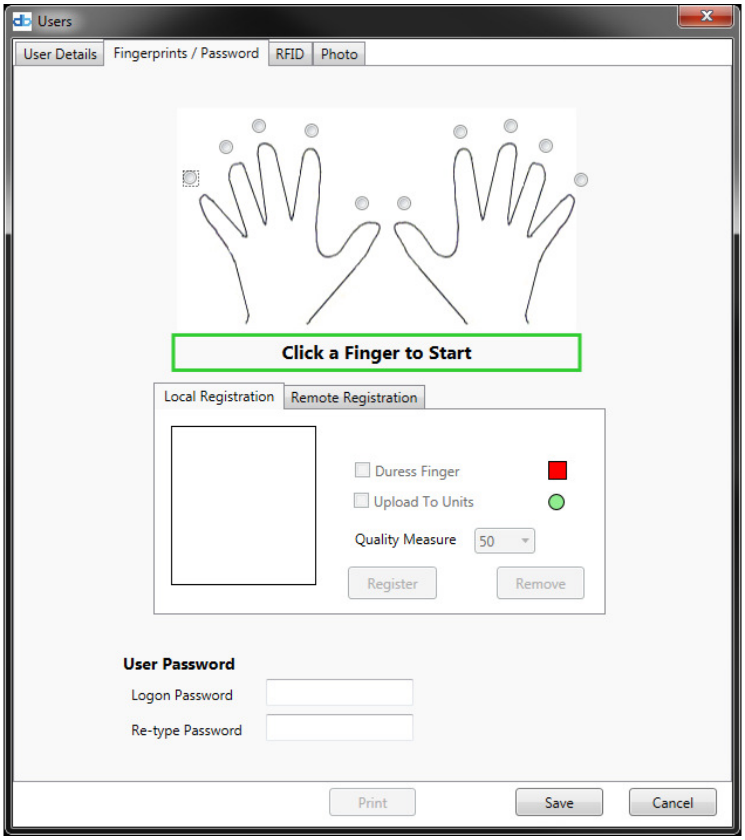
DAS-SQL allows the Administrator to define up to twelve **User-Defined Fields** using the “System Settings” tab (Section 4.12.3). User-defined fields are useful for entering such data as address, phone number, vehicle license plates, or other personnel data.

Note: For data integrity, all changes made on the Users Detail tab along with the modifying software administrator are logged and stored in the database and are retrievable via a report on the Reports Tab (Section 4.13). This report feature is listed on the Reports Tab under the Modification Details node in the Zone/Device Actions section.

4.4.2 – User Form – Fingerprints/Password tab

The “Fingerprints/Password” tab is used to register fingerprints that will be uploaded to the Devices to verify the User’s identity. The User Password, allows a System Administrator to assign a temporary password to a user. Passwords can be used instead of fingerprints to authenticate when logging into DAS-SQL. If the password is changed here, the next time a user logs into DAS-SQL, they will be prompted to change the password to one of their choice.

Local Registration



To register a fingerprint, select the finger by clicking on the round button above the desired finger. After a finger is selected, the display will change and say "Click Register." Click the "***Register***" button and place the User's finger on the scanner. It will be scanned and, if successful, will be scanned again for confirmation.

If the fingerprint quality is too low, an error message will be displayed and you will need to re-register the fingerprint. It is recommended that at least two fingers are registered for each User and that "pinky" fingers are not used.

The Quality Measure scale controls the quality of the fingerprint during enrollment and should only be changed from 50 in cases where a user's fingerprint is not accepted after repeated attempts have failed. When changed, it should be done incrementally.

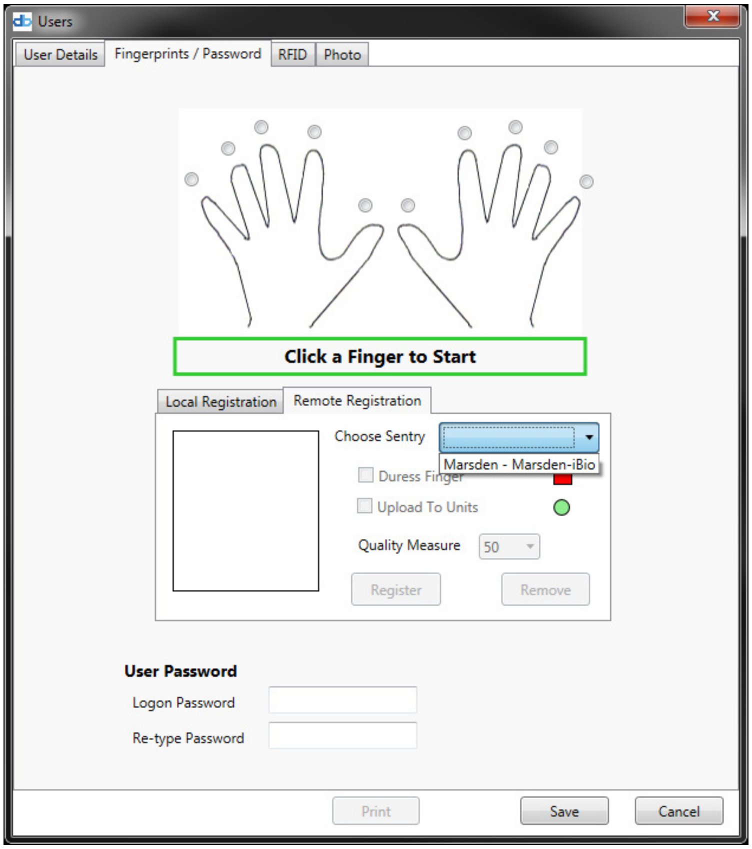
After the fingerprint is registered, the "Duress Finger" and "Upload To Units" checkboxes are enabled.

If this finger is to be used to activate a duress alarm, check the "Duress Finger" checkbox. Up to two fingers can be used as duress fingers.

Check the "Upload To Units" checkbox if this finger is to be uploaded to the Devices for access. Normally this will be selected. However, if a finger is to be used only for logging onto the DAS-SQL client, it will not be uploaded to the door units.

Up to ten (10) fingers can be registered for each User, but normally two is sufficient.

Remote Registration



Choose Sentry: Marsden - Marsden-iBio

□ Duress Finger 🟥

□ Upload To Units ●

Quality Measure: 50

Logon Password:

Re-type Password:

A db Sentry controller, with an attached BioLock, can now be used as a remote enrollment device. Click the drop-down box and select the Sentry that is convenient to the user that needs to be enrolled. The process will work the same as the USB enrollment once the Sentry has been chosen.

If the fingerprint quality is too low, an error message will be displayed and you will need to re-register the fingerprint. It is recommended that at least two fingers are registered for each User and that “pinky” fingers are not used.

The Quality Measure scale controls the quality of the fingerprint during enrollment and should only be changed from 50 in cases where a user’s fingerprint is not accepted after repeated attempts have failed. When changed, it should be done incrementally.

After the fingerprint is registered, the “Duress Finger” and “Upload To Units” checkboxes are enabled.

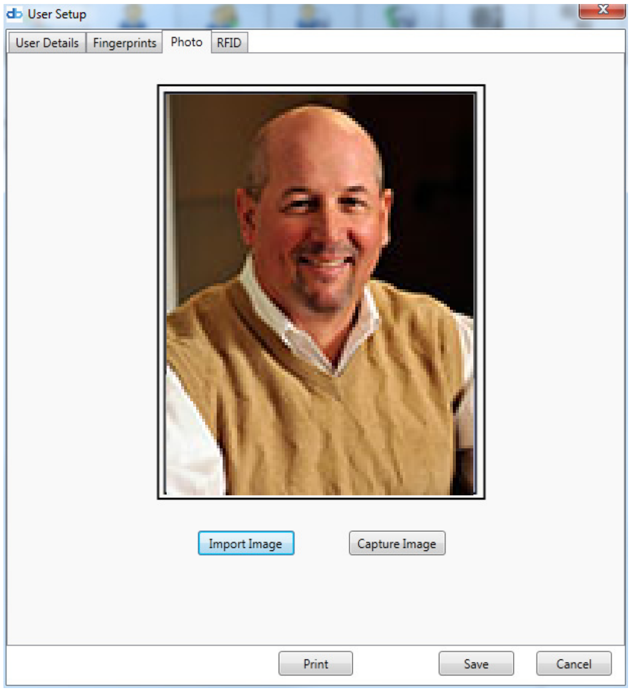
If this finger is to be used to activate a duress alarm, check the “Duress Finger” checkbox. Up to two fingers can be used as duress fingers.

Check the “Upload To Units” checkbox if this finger is to be uploaded to the Devices for access. Normally this will be selected. However, if a finger is to be used only for logging onto the DAS-SQL client, it will not be uploaded to the door units.

Up to ten (10) fingers can be registered for each User, but normally two is sufficient.

4.4.3 – User Form – Photo tab

The “Photos” tab allows a photo image file to be assigned to the User. This is useful for identifying a User or confirming an identity online.

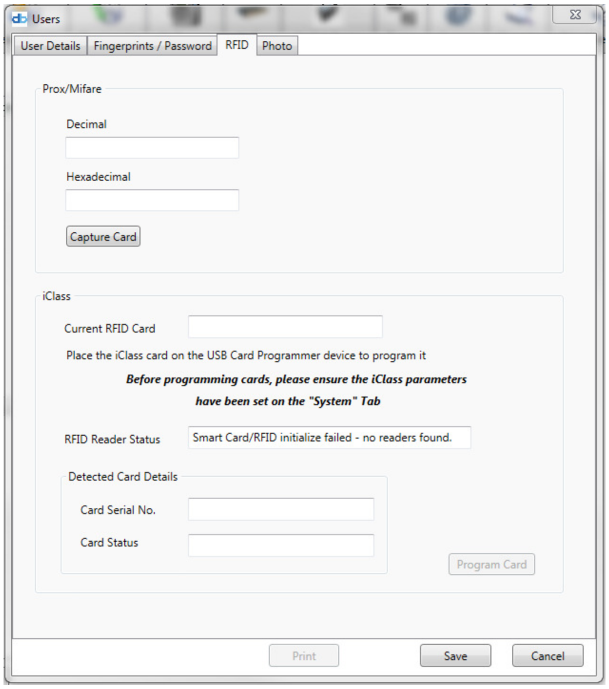


Click the "***Import Image***" button and navigate to the location of the image file to load. The image must be a JPEG (.jpg) image file.

Clicking "***Capture Image***" allows the Administrator to capture a User's image using a digital camera or webcam (selected on the "System Settings" tab).

4.4.4 – User Form – RFID tab

The "RFID" tab is used to enroll RFID Cards for Users to use as part of their authentication at the devices. 125KHz Proximity cards and Mifare cards, can either be entered manually in the text boxes, or be read via a USB card reader. To capture the card number via the USB reader, place the card on top of the reader and click the "***capture***" button. If keying in the card number manually, this can be entered in either decimal or hexadecimal format.



Decimal

Hexadecimal

Current RFID Card

Place the iClass card on the USB Card Programmer device to program it

Before programming cards, please ensure the iClass parameters have been set on the "System" Tab

RFID Reader Status: Smart Card/RFID initialize failed - no readers found.

Detected Card Details

Card Serial No.

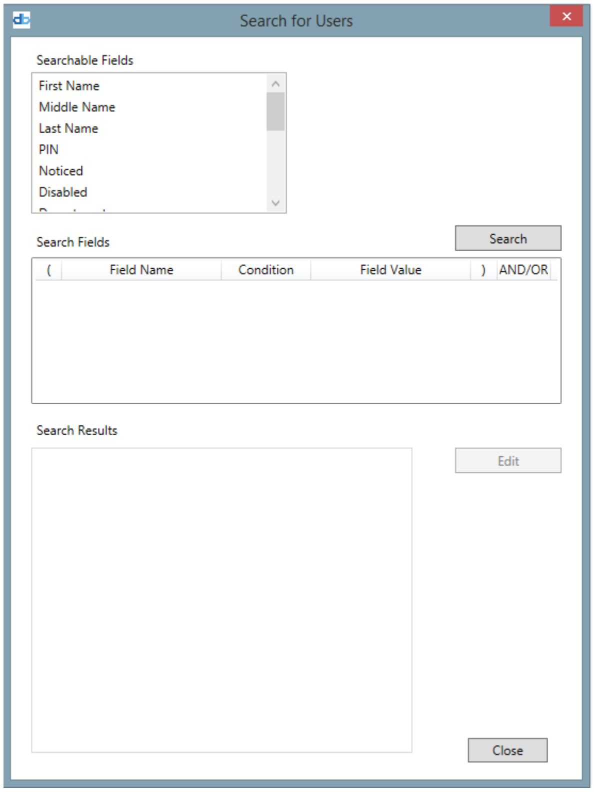
Card Status

To read or program a HID iClass card, place the card on the reader. The card will automatically be detected and its serial number displayed. The status of the card will also be displayed (if it has been programmed already, the User to which it is assigned will be shown).

To program the HID iClass card, LEAVE THE CARD ON THE READER WHEN THE "***SAVE"*** BUTTON IS PRESSED. The card will be programmed as the User data is saved. If the card is not left on the reader when the "***Save"*** button is clicked, the card will not be programmed.

When all User data has been entered, click the "***Save***" button to save the User data. If the User has been assigned to a User Group, the User's data will be uploaded to the Devices within that User Group. Uploading will normally begin within one minute and may take up to another minute before all data is uploaded to all the Devices within the User Group.

User Search - This button provides the window below and allows for quick searches of all the users within the system.

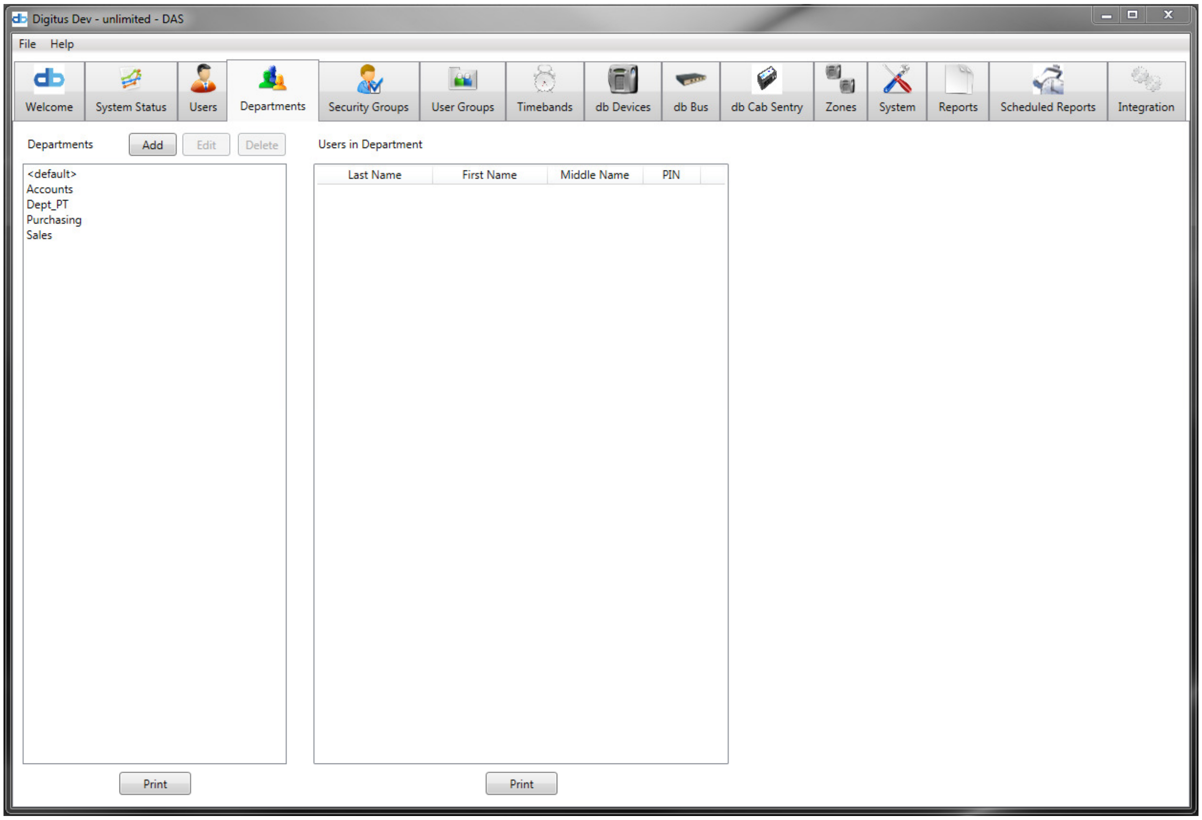


To use the searchable fields, left-click a desired field and drag and drop that field into the Search Fields box. Once done, add the desired value for the field and click "***Search"***.

4.5 – Departments Tab

Users can be assigned to Departments to make it easier to keep track of Users and to make reporting easier.

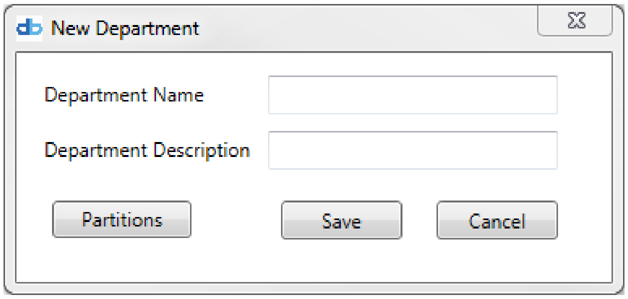
NOTE: Departments have no effect on Devices; they are merely administrative tools.



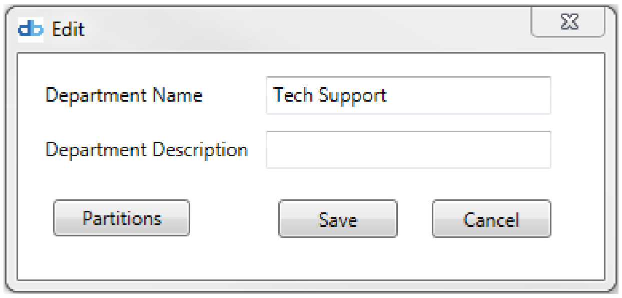
<default>
Accounts
Dept_PT
Purchasing
Sales

To view the Users in any given Department, left-click on the Department in the "Departments" list control. The Users in that Department will be displayed in the "Users in Department" list to the right. This list is sortable by last name, first name, middle name, or PIN. "Left-click" on the column header to sort.

To **add** a Department click on the "***Add***" Button, and input the name of the Department and a brief description.



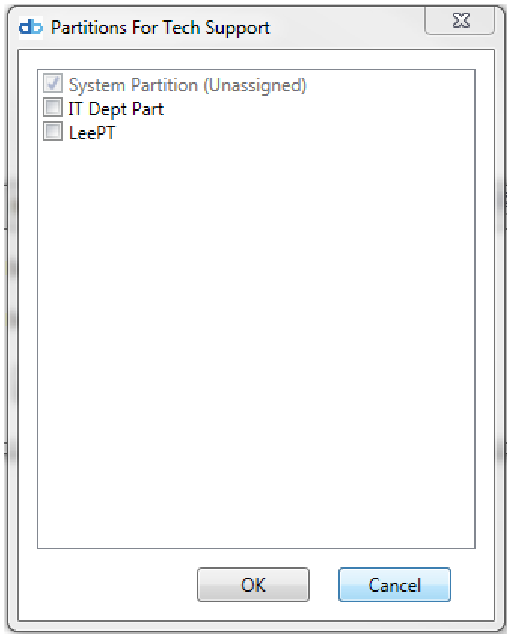
To **edit** a Department, select the Department and either right click on it and click edit or click on the "***Edit***" button.



Department Name: Tech Support
Department Description:

To **remove** a Department, , select the Department and either right click on it and click on delete or click on the "***Delete***" button. Users assigned to this Department will not be removed; their Department selection will be set to the <default> Department.

Departments can be assigned to Partitions to restrict visibility to Users in selected Partitions. To assign the Security Group to one or more Partitions, click the "Partitions" button.

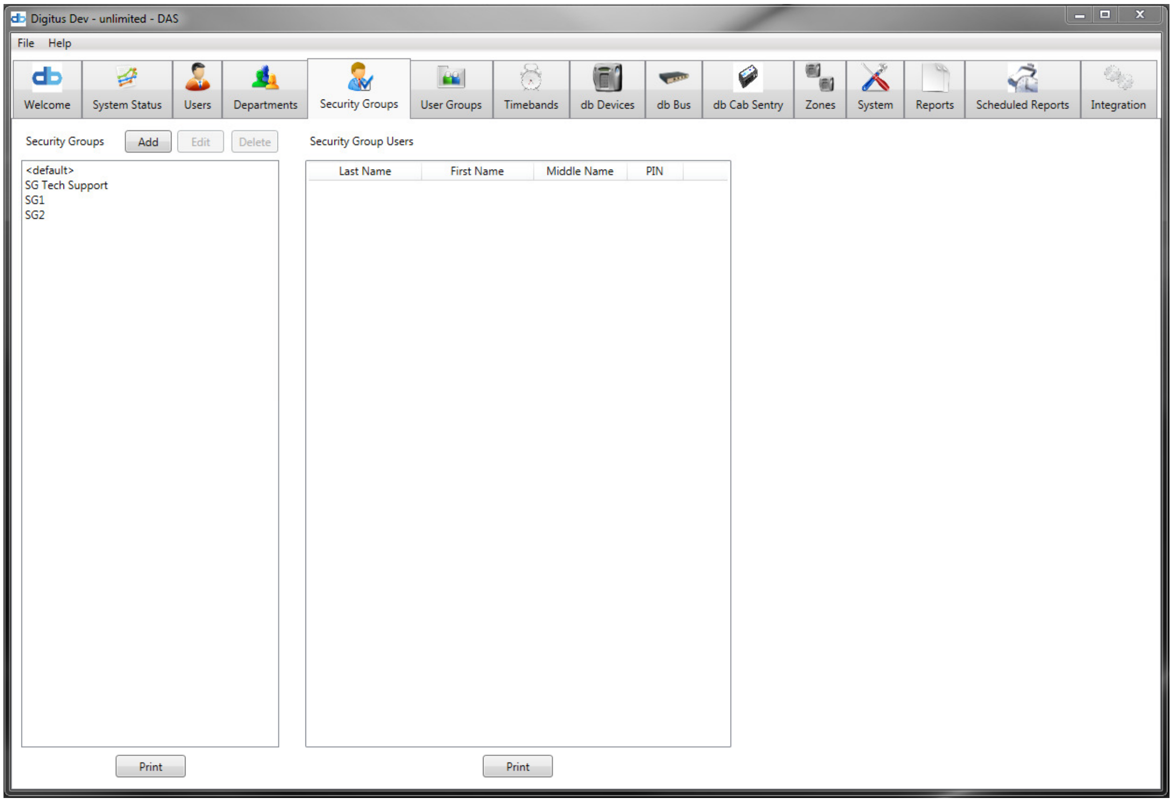


☑ System Partition (Unassigned)
□ IT Dept Part
□ LeePT

Select the desired Partition(s) and click "***OK***".

4.6 – Security Groups Tab

Similar to Departments, Security Groups (Section 4.6) are a collection of Users. Security Groups work in conjunction with the Dual-Custody feature, when "Use Security Groups" is enabled on specific Devices (db Nexus Duo II and III), all db Bus units, and db Cabinet Sentry. This allows for another level of security on a Device, where you require each user in dual-custody authentication to be from a different security group or each user to be from the same group.



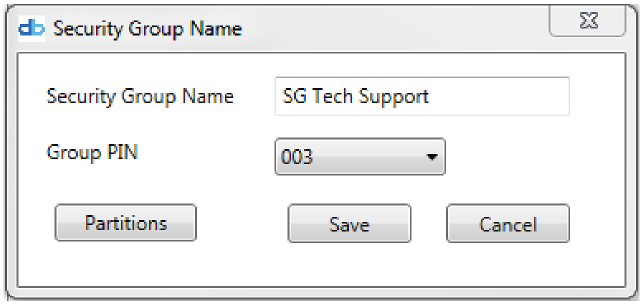
<default>
SG Tech Support
SG1
SG2

To **view** the Users in a specific Security Group, left-click on the group name in the "Security Groups" list control. The users in the Security Group will be displayed in the "Security Group Users" list control. Users are sortable by left-clicking the desired column header.

To **add, edit, or delete** a Security Group, select the Security Group, then select the appropriate button or right-click on the desired Security Group in the "Security Groups" list control. If right-clicking, a popup menu will be displayed with "Add," "Edit," and "Delete" menu items. If an existing Security Group has been selected, the "Edit" and "Delete" menu items will be enabled. If no Security Group has been selected, only the "Add" menu item will be enabled.

NOTE: Deleting a Security Group will remove all user connections to the group.

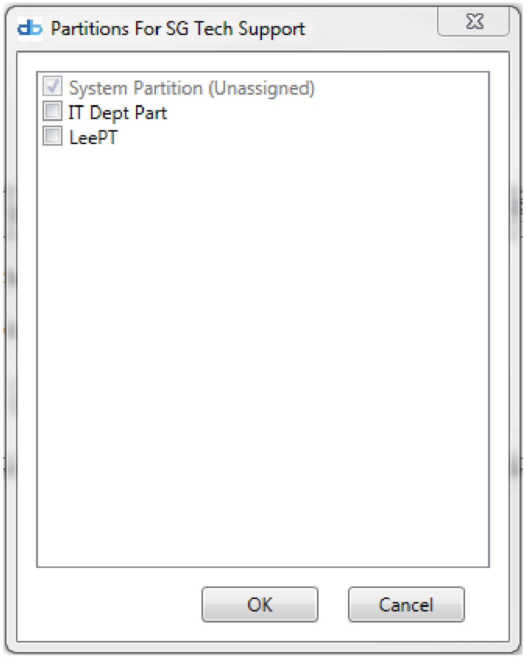
When adding or editing a Security Group, the following form is displayed:



Security Group Name: SG Tech Support
Group PIN: 003

Enter a name for the User Group to serve as reference. Assign a group PIN. Only non-used PINS will be shown.

Security Groups can be assigned to Partitions to restrict visibility to Users in selected Partitions. To assign the Security Group to one or more Partitions, click the “Partitions” button.



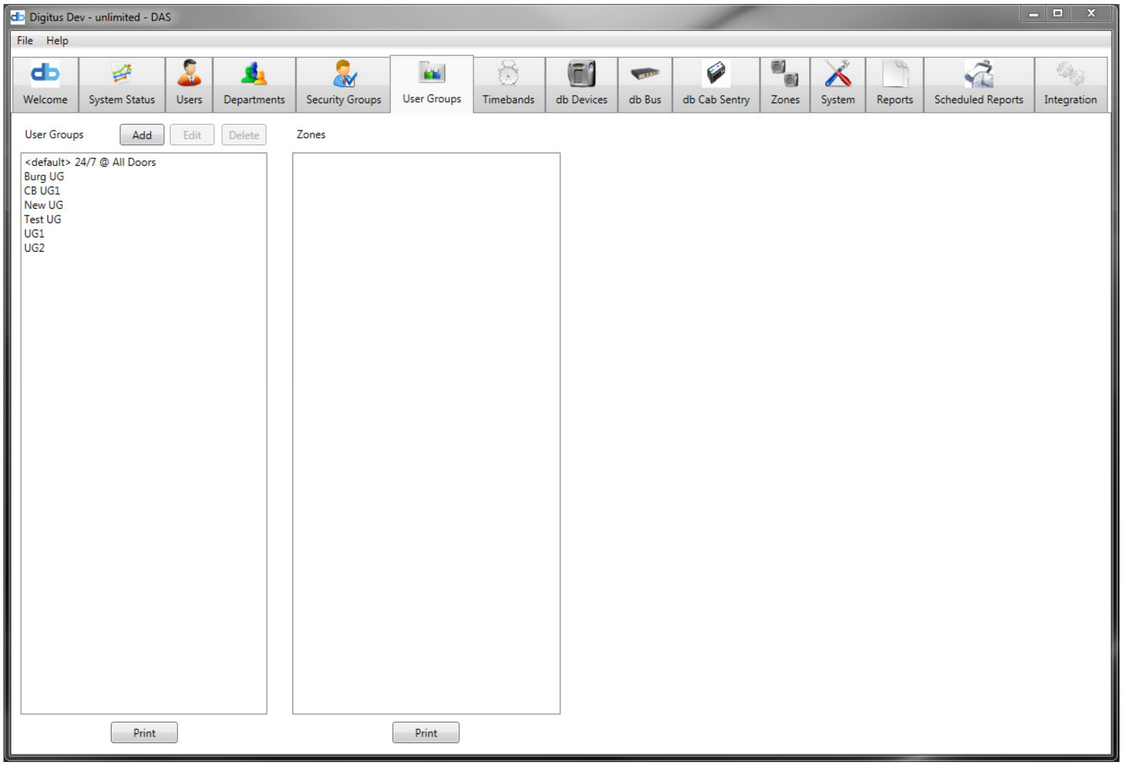
Partitions For SG Tech Support

☑ System Partition (Unassigned)
☐ IT Dept Part
☐ LeePT

Select the desired Partition(s) and click “***OK***”.

4.7 – User Groups Tab

User Groups are specific access permission sets that are assigned to Users. A User Group is a group of Devices with an assigned Timeband. When a User Group is assigned to a User, that User can access any Device in the User Group, during the time the Timeband assigned to that Door unit is valid.



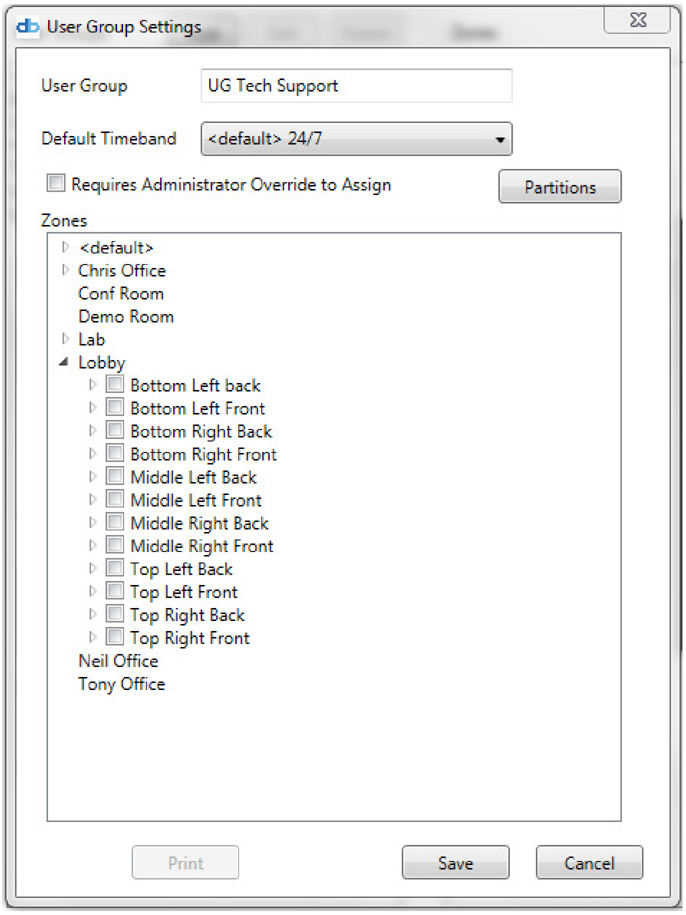
<default> 24/7 @ All Doors
Burg UG
CB UG1
New UG
Test UG
UG1
UG2

To **View** the Zones, Doors, and associated Timebands in any given User Group, left-click on the User Group in the "User Groups" list control. The Zones in that User Group will be displayed in the "Zones" list to the right. To view individual Doors and Timebands assigned to those Doors, expand the Zone(s) and Doors in that Zone.

To **Add, Edit, or Delete** a User Group, select the User Group, then select the appropriate button or right-click on the "User Groups" list control. A popup menu will be displayed with "Add," "Edit," and "Delete" menu items. If an existing User Group has been selected, the "Edit" and "Delete" menu items will be enabled. If no User Group has been selected, only the "Add" menu item will be enabled.

NOTE: Deleting a User Group will remove access permissions for all Users to which this User Group has been assigned. Before these Users can access any Doors a new User Group must be assigned to those Users.

When adding or editing a User Group, the following form is displayed:



User Group Settings

User Group: UG Tech Support

Default Timeband: <default> 24/7

□ Requires Administrator Override to Assign

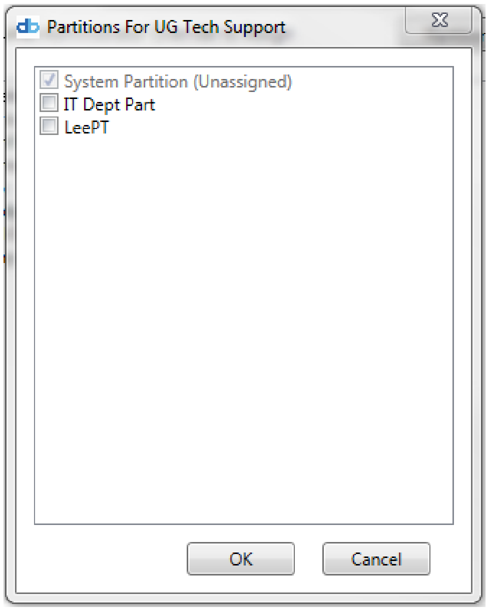
Zones

- <default>
- Chris Office
- Conf Room
- Demo Room
- Lab
- Lobby
  - □ Bottom Left back
  - □ Bottom Left Front
  - □ Bottom Right Back
  - □ Bottom Right Front
  - □ Middle Left Back
  - □ Middle Left Front
  - □ Middle Right Back
  - □ Middle Right Front
  - □ Top Left Back
  - □ Top Left Front
  - □ Top Right Back
  - □ Top Right Front
- Neil Office
- Tony Office

Enter a name for the User Group to serve as a reference. Select a Default Timeband from the list. This is the Timeband that will be assigned to any newly-selected Door Units by default.

If the “Requires Administrator Override to Assign” button is checked, only Administrators can assign this User Group to Users, or must scan their fingerprint to override the restriction.

User Groups can be assigned to Partitions to restrict visibility to Users in selected Partitions. To assign the User Group to one or more Partitions, click the “Partitions” button.



Partitions For UG Tech Support

- ☑ System Partition (Unassigned)
- □ IT Dept Part
- □ LeePT

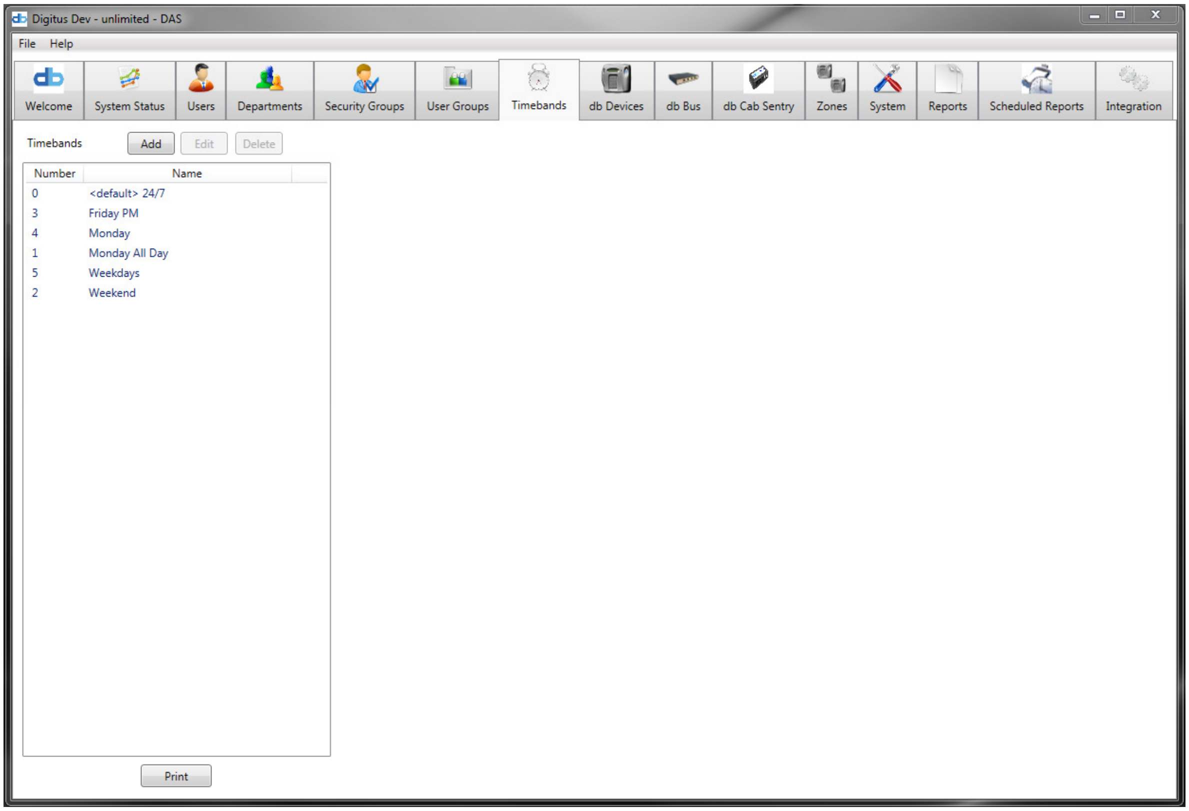
Select the desired Partition(s) and click "***OK***".

The "Zones" list displays all Zones configured on the system, filtered by their assigned Partitions. (If the User Group has been assigned to one or more Partitions, only Zones and Devices in those Partitions will be displayed.) Expand the Zone to view Devices assigned to that group. To add the Device to the User Group, check the box next to the Device name. Expand the Device node to view the assigned Timeband. Click on the Timeband to select a different Timeband from a drop-down list. Each Device in a User Group can have its own Timeband. If no Timeband is selected, the Device will not be included in the User Group.

When the User Group has been defined as required, click the "Save" button. If any current Users are affected by this User Group change, the data for those Users will begin uploading to the affected Devices within one (1) minute. Depending on how many Users this User Group is assigned, it may take some time (minutes to hours) before all Users are updated to all Devices. Normally it takes about 10 seconds per User to update a Device (though each Device's data is uploaded concurrently – uploading 100 Users usually takes about 1000 seconds, or about 16 minutes).

4.8 – TimeBands Setup Tab

Timebands are used to define when a User has access to a Device. The DAS-SQL system supports up to 99 Timebands, in addition to the <default> (24 hours per day, 7 days per week – full-time access) Timeband. A Timeband is a weekly, repeating set of time periods during which access is allowed. Up to two (2) time periods per day can be defined, in 15-minute segments.

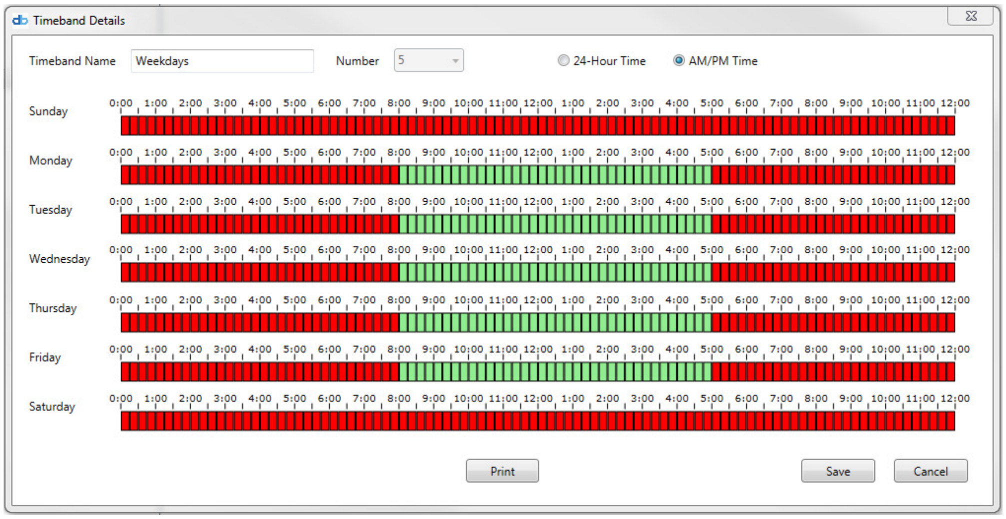


Number	Name
0	<default> 24/7
3	Friday PM
4	Monday
1	Monday All Day
5	Weekdays
2	Weekend

To **add, edit, or delete** a Timeband, select the Timeband, then select the appropriate button or right-click on the "Timebands" list control. A popup menu will be displayed with "Add," "Edit," and "Delete" menu items. If an existing Timeband has been selected, the "Edit" and "Delete" menu items will be enabled. If no Timeband has been selected, only the "Add" menu item will be enabled.

NOTE: Deleting a Timeband will remove it from all User Groups that use this Timeband. Any Door units within those User Groups will be removed from the User Group, and any Users within the affected User Groups will no longer have access at the affected Doors.

When adding or editing a Timeband, the following form is displayed:



Timeband Name: Weekdays

Number: 5

○ 24-Hour Time ● AM/PM Time

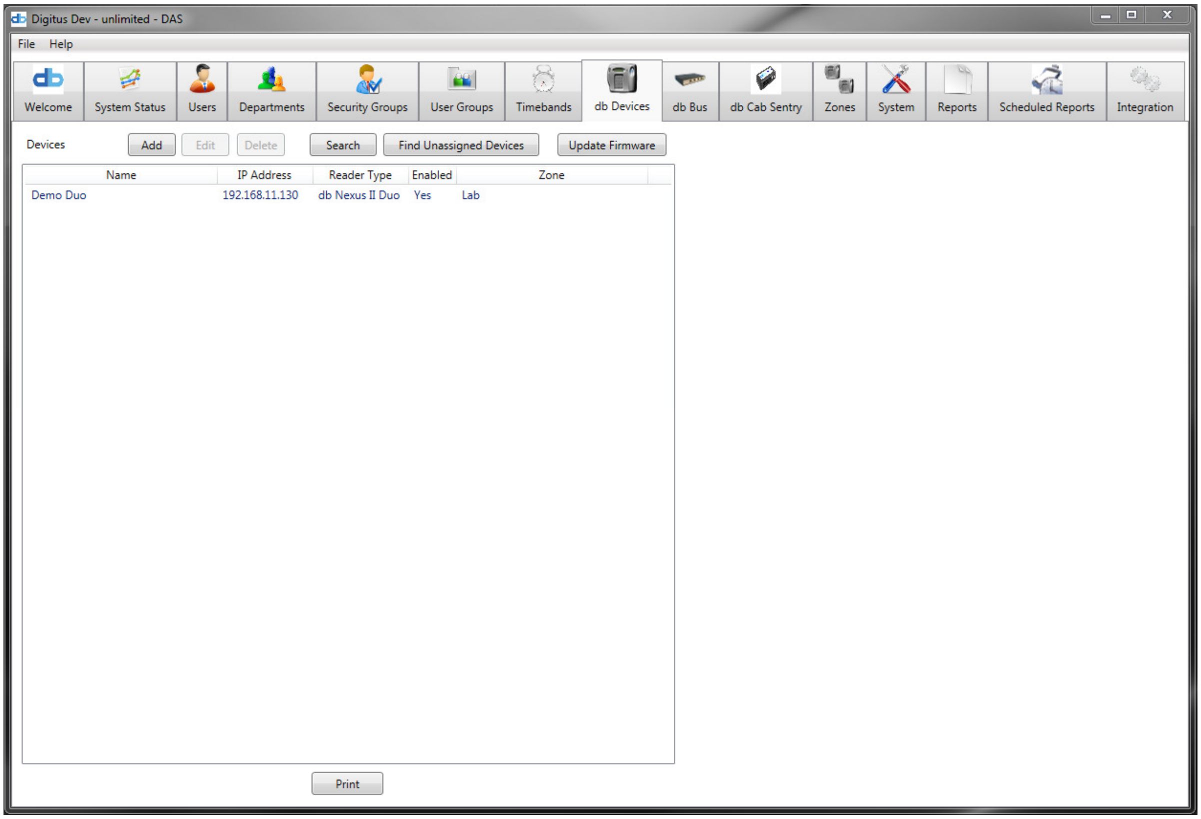
Enter the name of the Timeband (for reference) and select a schedule Number from the drop-down list. Only schedule numbers that have not been used will be listed. Select the "24-Hour Time" or "AM/PM Time" checkbox to display the times in the format desired.

Each Timeband can contain up to two (2) time period per day. To create a time period, click and hold the left-mouse button while placing it over the cell for the start time, drag to the desired end time, and release the mouse button. To remove or shorten the time period, click and hold the right mouse button over the cell desired, drag to the end of the time band, and release the mouse button. Time periods can be defined in 15-minute segments.

When the Timeband is defined as desired, click the "Save" button. Timebands normally will begin uploading to all units within one (1) minute and complete in a few seconds. Any affected User Groups will be updated at that time.

4.9 – db Devices Tab

The “db Devices” tab contains all configured Devices (excluding db Bus Devices) and allows them to be edited, as well as new Devices added.



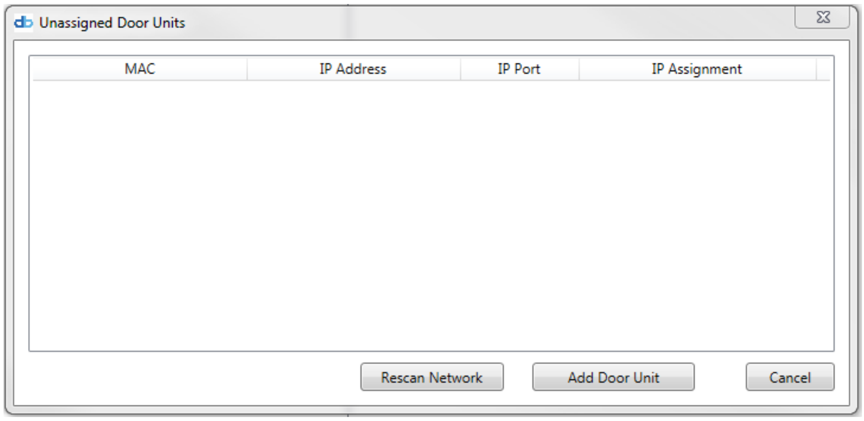
Name	IP Address	Reader Type	Enabled	Zone
Demo Duo	192.168.11.130	db Nexus II Duo	Yes	Lab

Currently configured Devices are shown in the “Devices” list. This list can be sorted by Name, IP Address, or Zone. To sort the Devices, left-click on the column header.

To **add, edit, or delete** a Device, select the Device, then select the appropriate button or right-click on the “Device” list control. A popup menu will be displayed with “Add,” “Edit,” and “Delete” menu items. If an existing Device has been selected, the “Edit” and “Delete” menu items will be enabled. If no Device has been selected, only the “Add” menu item will be enabled.

4.9.1 – db Devices Tab – Finding unassigned doors

It is possible to manually add a Device. However, it is easier to let the server scan the network and report any Devices it finds that have not yet been configured. To do this, click the “Find Unassigned Devices” button. The following form will be displayed:



Unassigned Door Units

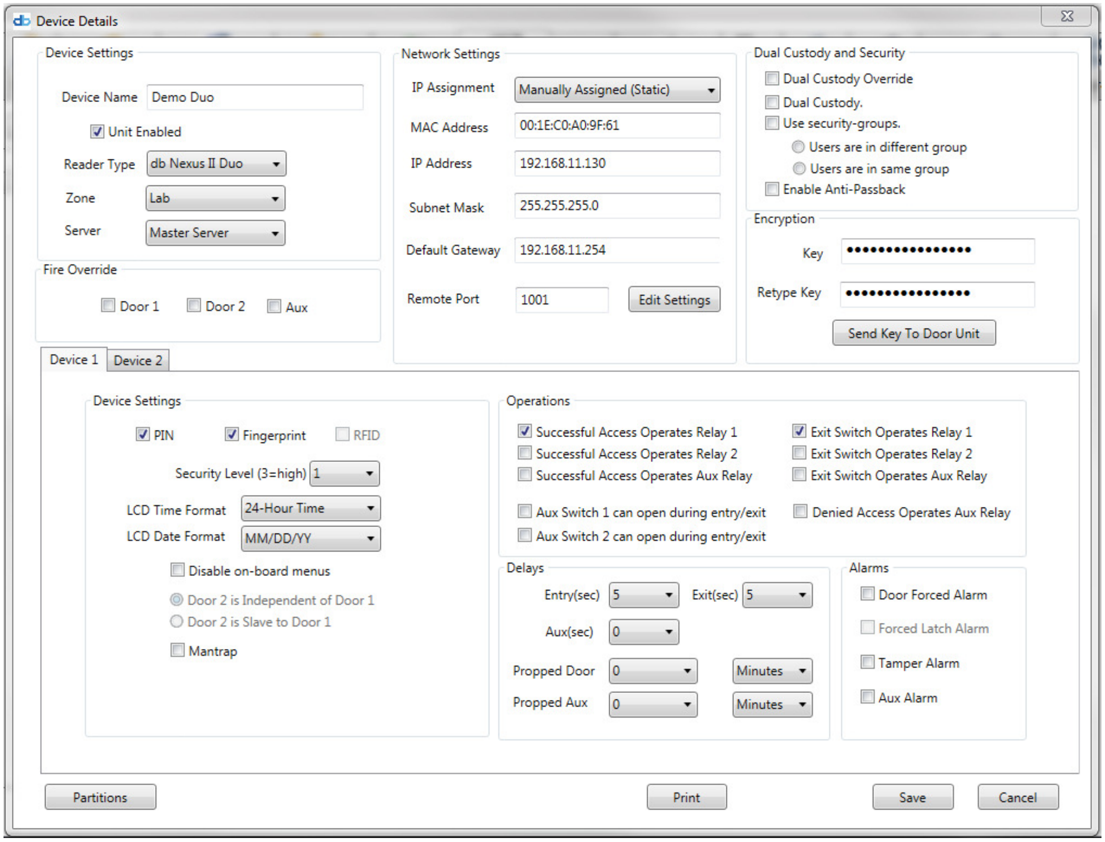
MAC	IP Address	IP Port	IP Assignment

NOTE: It will take approximately ten (10) seconds for the server to scan the network for new Devices.

To add a Device, select it from the list of newly-found units by double-clicking on the entry or selecting it and clicking the "Add Device" button.

The "Details" form will be displayed to complete the new Device setup.

4.9.2 – db Devices Tab – Setting up Device Operations



Device Details

Device Settings
Device Name: Demo Duo
☑ Unit Enabled
Reader Type: db Nexus II Duo
Zone: Lab
Server: Master Server

Fire Override
□ Door 1 □ Door 2 □ Aux

Network Settings
IP Assignment: Manually Assigned (Static)
MAC Address: 00:1E:C0:A0:9F:61
IP Address: 192.168.11.130
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.11.254
Remote Port: 1001

Dual Custody and Security
□ Dual Custody Override
□ Dual Custody.
□ Use security-groups.
○ Users are in different group
○ Users are in same group
□ Enable Anti-Passback

Encryption
Key: ••••••••••••••••
Retype Key: ••••••••••••••••

Device 1 | Device 2

Device Settings
☑ PIN ☑ Fingerprint □ RFID
Security Level (3=high): 1
LCD Time Format: 24-Hour Time
LCD Date Format: MM/DD/YY
□ Disable on-board menus
○ Door 2 is Independent of Door 1
○ Door 2 is Slave to Door 1
□ Mantrap

Operations
☑ Successful Access Operates Relay 1
□ Successful Access Operates Relay 2
□ Successful Access Operates Aux Relay
☑ Exit Switch Operates Relay 1
□ Exit Switch Operates Relay 2
□ Exit Switch Operates Aux Relay
□ Aux Switch 1 can open during entry/exit
□ Aux Switch 2 can open during entry/exit
□ Denied Access Operates Aux Relay

Delays
Entry(sec): 5 Exit(sec): 5
Aux(sec): 0
Propped Door: 0 Minutes
Propped Aux: 0 Minutes

Alarms
□ Door Forced Alarm
□ Forced Latch Alarm
□ Tamper Alarm
□ Aux Alarm

4.9.2.1 The Device Settings Section

Device Name - Name for the new Device unit.
Unit Enabled determines whether the Device Unit will be online or offline. If "Unit Enabled" is not checked, no events will be received from the Device and no Users will be uploaded to the Device Unit.

Unit Enabled – Must be checked for DAS-SQL to communicate with the unit.

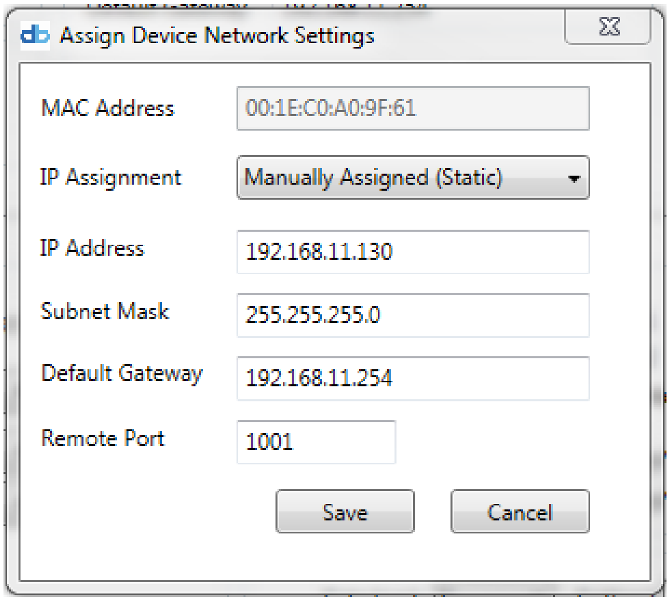
Reader Type for this Device unit refers to the specific unit's type.
If the Device Unit is a db Zero-U or db Nexus Duo II or III, then the "Send Key to Unit" button will be enabled. This is used to program the encryption key for the unit. This can be done only once (without a special utility to reset the unit).

Zone is to which this Device is to be assigned. (If no Zones have been configured, this Device can be assigned to the "<default>" Zone.) If the Device has been assigned to a Partition, only Zones in that Partition will be listed.

Server selection is used when multiple, dedicated servers are being used to handle your access units. This control allows the user to determine to which server the unit will be dedicated.

4.9.2.2 The Network Settings Section

This section displays the current network settings for the Device unit hardware. To change these settings, click the "***Edit Settings***" button. The following form will be displayed:



Assign Device Network Settings

MAC Address: 00:1E:C0:A0:9F:61

IP Assignment: Manually Assigned (Static)

IP Address: 192.168.11.130

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.11.254

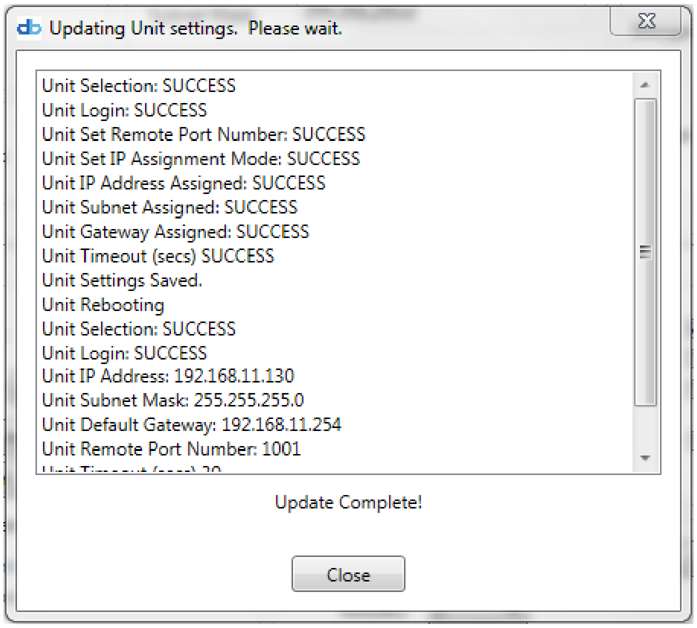
Remote Port: 1001

This form allows the Device unit's network settings to be reconfigured. The network adapter in the Device can use a fixed (static) IP address or an automatically assigned address (DHCP). Note that if "Automatic (DHCP)" is selected, the unit will receive an address assigned by the network DHCP server, but the IP address (the ' . . .' address) must be used (not a "computer name").

To change the IP settings (IP Address, Subnet Mask, Default Gateway, and Remote [IP] Port), enter that data in the appropriate fields. Consult your network administrator for information about what these are and how they should be set. Once the settings have been entered, click the "***Save***" button.

The purpose of these settings is to change the data in the Device's setup data, as well as to reprogram the Device unit's network adapter.

NOTE: If these changes require updating the Device unit's network adapter, select "Yes" when asked if you wish to "Send Settings to Unit?" If no, the data will be entered into the database but not sent to the Device unit. If yes, the data will be sent to the Device unit. As it is being sent, the following status window will appear:



Updating Unit settings. Please wait.

```
Unit Selection: SUCCESS
Unit Login: SUCCESS
Unit Set Remote Port Number: SUCCESS
Unit Set IP Assignment Mode: SUCCESS
Unit IP Address Assigned: SUCCESS
Unit Subnet Assigned: SUCCESS
Unit Gateway Assigned: SUCCESS
Unit Timeout (secs) SUCCESS
Unit Settings Saved.
Unit Rebooting
Unit Selection: SUCCESS
Unit Login: SUCCESS
Unit IP Address: 192.168.11.130
Unit Subnet Mask: 255.255.255.0
Unit Default Gateway: 192.168.11.254
Unit Remote Port Number: 1001
Unit Timeout (secs) 30
```

Update Complete!

When the Device unit upload is complete, a confirmation message appears. The status window can be closed and Device unit data entry continued.

The DAS-SQL server communicates with the Devices via encrypted communication (see Encryption below). When a db Nexus II or III Device is installed, the installer or manager enters an encryption key on the head unit. This encryption key must be entered in the "Door Details" form for the server to communicate with the Door unit.

4.9.2.3 The Dual-Custody and Security Section

Dual-Custody Override - This option works in tandem with Dual-Custody. It requires the first two users who enter a room to enter together, but allows each subsequent user to enter individually. This option also requires that every, following, separate user, which have entered the room, exit before the first two users can leave.

Dual-Custody - Requires two users to authenticate on a Device before access is granted.

Use Security Groups - Works in conjunction with the Security Groups Tab. When used, a selection must be made as to whether each person must be from the same Security Group or from different Security Groups.

Enable Anti-Passback- Selecting this option prevents a user from entering a previously exited room in which they did not authenticate to leave. (e.g. If a person authenticates when entering a room, but then leaves without authenticating, that person cannot re-enter the room.)

Enter the key in the "Key" field and in the "Retype Key" field. This is a user selected key that needs to only be entered once.

NOTE: This key MUST be exactly 16 digits long.

4.9.2.4 Device 1 and Device 2 Settings and Operations Section

The following applies to both Device 1 and 2. These are tabbed within the page and device 2 is only available when using a Duo type unit. Otherwise, only device 1 is available for editing.

Device Settings Section

PIN - Number entered into keypad. Selection requires users to enter a pin.

Fingerprint- requires users to supply a fingerprint.

RFID – selection requires a RFID card to be read.

Security Level - selects the threshold for the fingerprint reader. For maximum security, select 3.

LCD Time Format and LCD Date Format - determine the units display format of time and date.

Disable on-board Menu - Disables the on-board menus on db Nexus and db Nexus Duo Devices.

If the Device Unit supports two doors, select whether door 2 is independent of door 1 or acts as a slave of door 1 (both doors unlock together on a valid access).

Mantrap – Determines if the Device uses the Mantrap feature.

Operations Section

This section allows the operator to determine certain courses of actions to take when certain events arise on the door unit.

Successful Access Operates Relay 1 - successful access will trigger Relay 1

Successful Access Operates Relay 2 - successful access will trigger Relay 2

Successful Access Operates Aux Relay - successful access will trigger the Aux Relay

Aux Switch 1 can open during entry/exit - Aux switch 1 will open during unit entry or exit

Aux Switch 2 can open during entry/exit - Aux switch 2 will open during unit entry or exit

Exit Switch Operates Relay 1 - A pressed exit switch triggers relay 1

Exit Switch Operates Relay 2 - A pressed exit switch triggers relay 2

Exit Switch Operates Aux Relay - A pressed exit switch triggers the aux relay

Denied access Operates Aux Relay - Denied entry triggers the aux relay

Delays Section

This section is for setting the units delays once an event is activated.

Entry Delay determines how long the User has to open the door after User access has been granted access.

Exit Delay determines how long the door will remain unlocked when the User presses the egress or exit button.

Aux Delay determines how long the auxiliary relay is fired for.

Propped Door determines how many minutes (or seconds for some Reader types) a door can remain open before a "Propped/Held Door" alarm is triggered.

Propped Aux determines how many minutes (or seconds for some Reader types) an aux switch can remain open before a "Propped Aux" alarm is triggered.

Alarms Section

This section allows various alarm type to be enabled/disabled on a device.

Door forced (intruder) alarms on this Door, select the "Door Forced Alarms" checkbox.

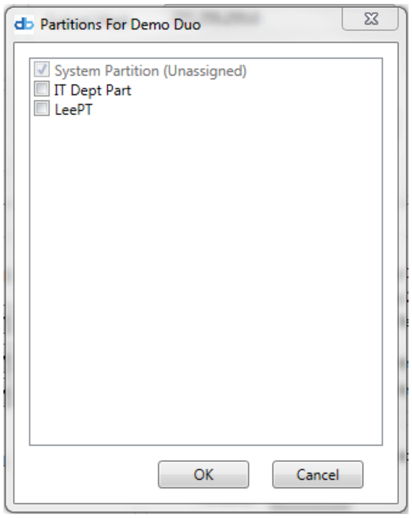
Forced Latch Alarm (intruder) alarms for illegal operations on a door latch.

Tamper Alarm (unit tampering) alarms created when a unit is tampered.

Aux Alarm (Aux triggers) Alarms created when the aux is triggered.

4.9.2.5 Partitions Button

Devices can be assigned to Partitions to restrict visibility and access to selected Partitions. To select the Partitions to which this Device is assigned, click the "***Partitions***" button.



Partitions For Demo Duo

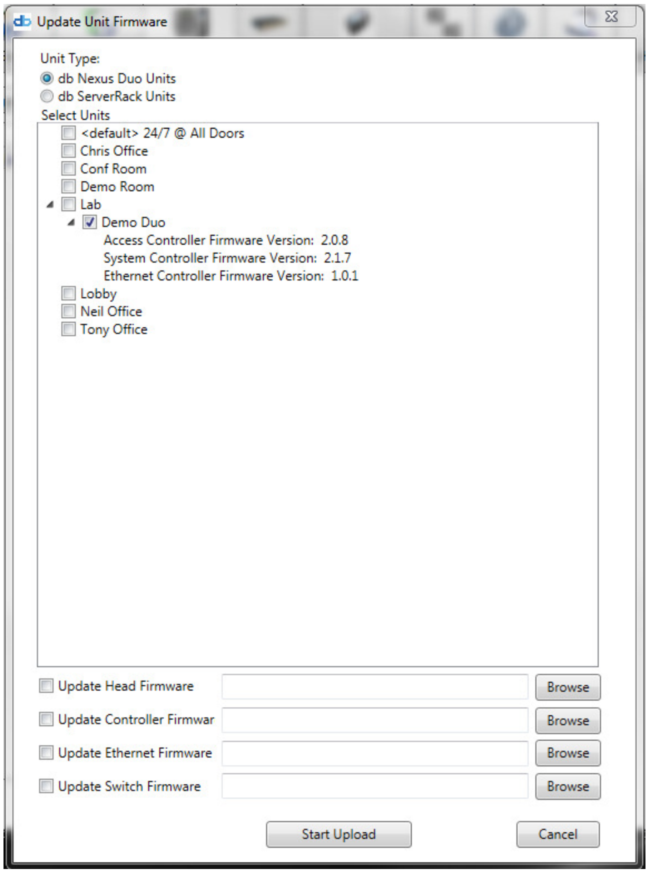
☑ System Partition (Unassigned)
□ IT Dept Part
□ LeePT

Select the desired Partition(s) and click "***OK***".

NOTE: When a new Device unit is added, all Timebands will be uploaded to the Device. Any Users who have been assigned to the <default> (24/7, all doors) User Group will be uploaded to the new Device as soon as possible. User uploading will normally begin within one (1) minute and may take several minutes depending on how many Users are assigned to the <default> Group (see User and User Group settings above for details).

4.9.3 – db Devices Tab – Updating Unit Firmware

Periodically, new firmware updates are released that need to be uploaded to the Digitus devices. To do this, use the "***Update Firmware***" button on the device tab. The window below shows a list of devices grouped by zones, allowing you to select which devices are to be updated.



Update Unit Firmware

Unit Type:
● db Nexus Duo Units
○ db ServerRack Units

Select Units
- □ <default> 24/7 @ All Doors
- □ Chris Office
- □ Conf Room
- □ Demo Room
- □ Lab
  - ☑ Demo Duo
    - Access Controller Firmware Version: 2.0.8
    - System Controller Firmware Version: 2.1.7
    - Ethernet Controller Firmware Version: 1.0.1
- □ Lobby
- □ Neil Office
- □ Tony Office

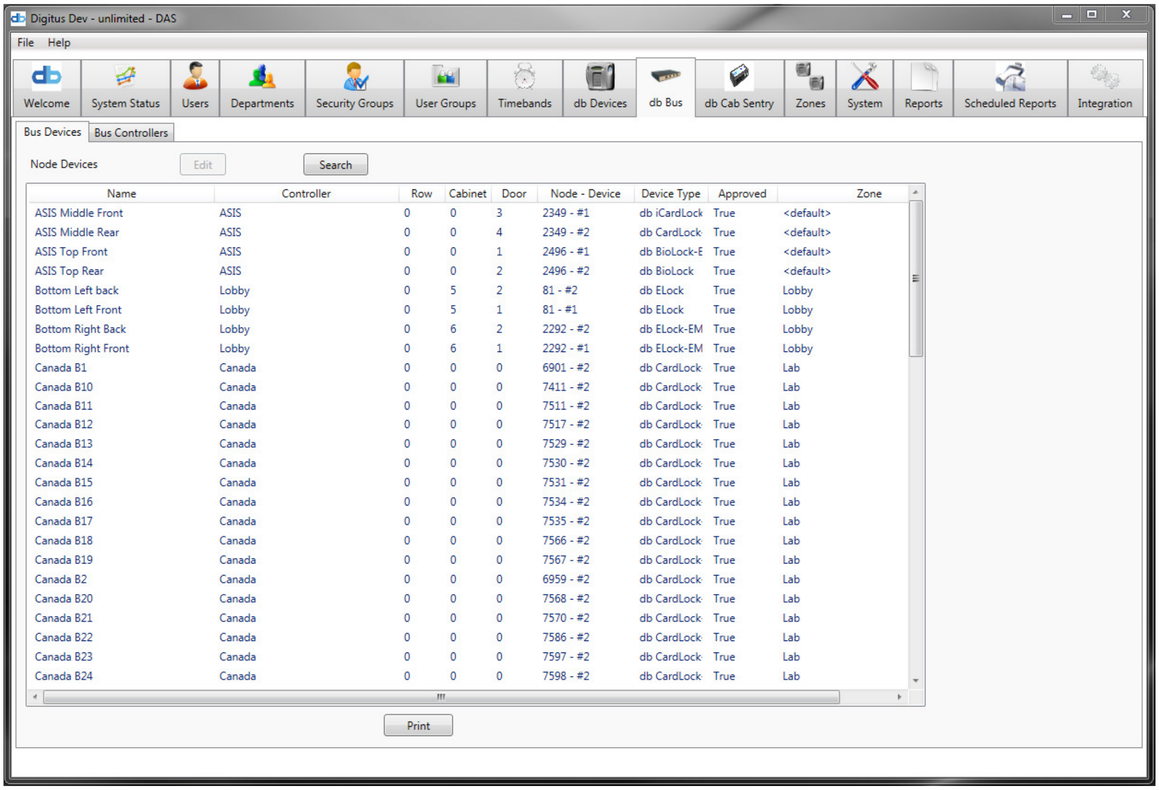
□ Update Head Firmware
□ Update Controller Firmwar
□ Update Ethernet Firmware
□ Update Switch Firmware

To Update - Select the Unit type for updating, then select which devices are to be updated from the list. Once the device selection has been made, select which firmware files are to update by checking one or more checkboxes next to the hardware names. Select each file, using the "***Browse***" button. Once all files have been selected, click the "***Start Upload***" button to begin the firmware update. Depending on what files are being updated, this process can take three to fifteen minutes. A progress bar shows the update's progress. Once done, DAS-SQL provides a confirmation that the hardware was correctly updated. Confirming this acknowledgement returns you to the db Devices tab.

4.10 – db Bus Devices Tab

Bus Devices are used with up to 32 cabinets/64 cabinet door locks. They employ a system that uses a Bus Controller, which is wired through a group of 32 Nodes with each node supporting up to 2 Devices. The db Bus Device tab contains two tabs: the db Devices tab and db Bus Controllers tab. The db Devices tab (Section 4.10.1) is a list of all the Devices currently known to the system, while the db Bus Controller tab (Section 4.10.4) is a list of each Bus Controller known to the DAS-SQL System.

4.10.1 – Bus Devices Sub-tab

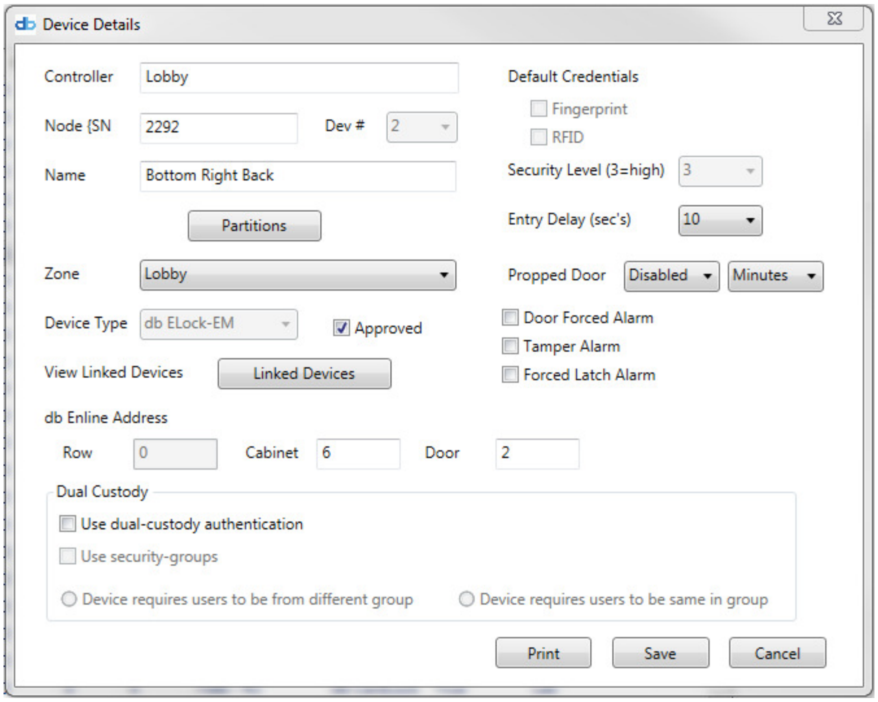


Name	Controller	Row	Cabinet	Door	Node - Device	Device Type	Approved	Zone
ASIS Middle Front	ASIS	0	0	3	2349 - #1	db iCardLock	True	<default>
ASIS Middle Rear	ASIS	0	0	4	2349 - #2	db CardLock	True	<default>
ASIS Top Front	ASIS	0	0	1	2496 - #1	db BioLock-E	True	<default>
ASIS Top Rear	ASIS	0	0	2	2496 - #2	db BioLock	True	<default>
Bottom Left back	Lobby	0	5	2	81 - #2	db ELock	True	Lobby
Bottom Left Front	Lobby	0	5	1	81 - #1	db ELock	True	Lobby
Bottom Right Back	Lobby	0	6	2	2292 - #2	db ELock-EM	True	Lobby
Bottom Right Front	Lobby	0	6	1	2292 - #1	db ELock-EM	True	Lobby
Canada B1	Canada	0	0	0	6901 - #2	db CardLock	True	Lab
Canada B10	Canada	0	0	0	7411 - #2	db CardLock	True	Lab
Canada B11	Canada	0	0	0	7511 - #2	db CardLock	True	Lab
Canada B12	Canada	0	0	0	7517 - #2	db CardLock	True	Lab
Canada B13	Canada	0	0	0	7529 - #2	db CardLock	True	Lab
Canada B14	Canada	0	0	0	7530 - #2	db CardLock	True	Lab
Canada B15	Canada	0	0	0	7531 - #2	db CardLock	True	Lab
Canada B16	Canada	0	0	0	7534 - #2	db CardLock	True	Lab
Canada B17	Canada	0	0	0	7535 - #2	db CardLock	True	Lab
Canada B18	Canada	0	0	0	7566 - #2	db CardLock	True	Lab
Canada B19	Canada	0	0	0	7567 - #2	db CardLock	True	Lab
Canada B2	Canada	0	0	0	6959 - #2	db CardLock	True	Lab
Canada B20	Canada	0	0	0	7568 - #2	db CardLock	True	Lab
Canada B21	Canada	0	0	0	7570 - #2	db CardLock	True	Lab
Canada B22	Canada	0	0	0	7586 - #2	db CardLock	True	Lab
Canada B23	Canada	0	0	0	7597 - #2	db CardLock	True	Lab
Canada B24	Canada	0	0	0	7598 - #2	db CardLock	True	Lab

The **db Devices** sub-tab shows the Devices that are attached to a db Bus in the System. Devices can be edited from here, but new devices cannot be added or existing devices deleted from here. Adding and deleting of db Bus devices is done via the db Bus Controllers sub-tab.

4.10.2 – Editing Bus Devices

To **edit** a device, select the device to be edited in the list and click the "***edit"*** button at the top of the list. Alternatively right-clicking directly on a device and selecting edit from the pop-up menu or double-clicking the device, will also load the device's properties screen.



Device Details

Controller: Lobby

Node {SN: 2292

Dev #: 2

Name: Bottom Right Back

Zone: Lobby

Device Type: db ELock-EM

☑ Approved

db Enline Address

Row: 0

Cabinet: 6

Door: 2

Dual Custody

□ Use dual-custody authentication

□ Use security-groups

○ Device requires users to be from different group

○ Device requires users to be same in group

Default Credentials

□ Fingerprint

□ RFID

Security Level (3=high): 3

Entry Delay (sec's): 10

Propped Door: Disabled, Minutes

□ Door Forced Alarm

□ Tamper Alarm

□ Forced Latch Alarm

Controller – Name of db Bus Controller that the device is connected to. This field is read-only and cannot be edited.

Node SN – The serial number of the node that the device is physically attached to. This field is read-only and cannot be edited.

DEV# - Identifies Which Node port is being used. This field is read-only and cannot be edited.

Name – A name should be assigned to the device, making it easily identifiable within the system

Partitions – Devices on the bus controller can be added to Partitions via the "***Partition"*** button. Click "***OK"*** once the desired partition(s) is selected.

Zone - Device can be assigned to a zone, allowing for easier management and reporting of the devices.

Device Type – The actual type of device, e.g. db BioLock or db ELock. *This field is read-only and cannot be edited.*

Approved – This enables/disables the device within the system.

Linked Devices – This button allows the user to view the devices this device is linked with. Editing or linked devices, you must be done via the db Bus Controllers sub-tab.

db Enline Address- The db Enline units, provide a method to authenticate at the end of a row of cabinets in a data center. When a user is attempting to gain access to a cabinet, they must first identify which cabinet (and even which door on that cabinet) they are attempting to access, by using a combination of row, cabinet and door number. The numbering configuration is defined via the db Bus Controllers tab, and the configuration selected will determine which fields are enabled or disabled of this screen. For example, if the configuration required just a cabinet number and door number be entered, these fields will be enabled, but row number will be disabled. For each enabled field, a value must be entered that corresponds to the numbering configuration. The numbering configuration allows you to select the number of digits for each value, for example it could be configured to require a 3-digit cabinet number, followed by a 1-digit door number. If values less than the number of digits required are entered, leading zeros will be required when entering the number at the db Enline unit. For example, the configuration requests a 3-digit cabinet number, but "23" is entered in the "cabinet" field, the user would need to key "023".

Default Credentials

Fingerprint – Device requires a fingerprint to authenticate.

RFID – Device requires a RFID card to authenticate.

Security Level - Selects the quality threshold for the fingerprint reader.

Entry Delay - The amount of time the door will unlock for, allowing a user to open the cabinet. If the cabinet hasn't been opened within this time period, it will re-lock again.

Propped Delay - The amount of time the door or latch can be left open before creating an alarm. This can be set in minutes or seconds.

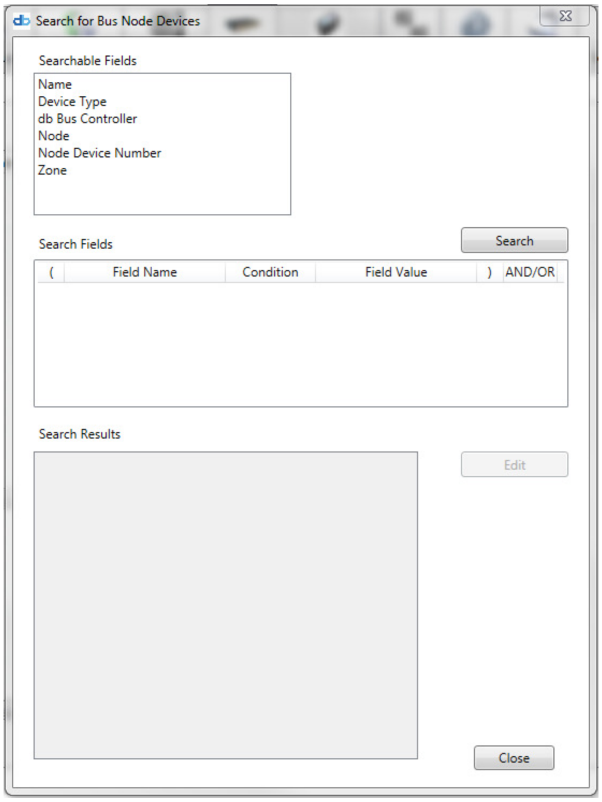
Door Forced Alarm- Activates when the cabinet door is opened, but it's not preceded by a user authentication.

Tamper Alarm – Each device port as a tamper port. This can be used to monitor a side or roof panel of a cabinet. If the panel is opened, an immediate tamper alarm will be generated.

Forced Latch Alarm – Activates when the door latch is opened, but it's not preceded by a user authentication

Dual Custody
Use Dual-Custody Authentication – Requires two users to authenticate before access is granted.
Use Security Groups - Works in conjunction with the Security Groups Tab. When used, a selection must be made as to whether each person must be from the same Security Group or from different Security Groups.

4.10.3 – Searching db Devices

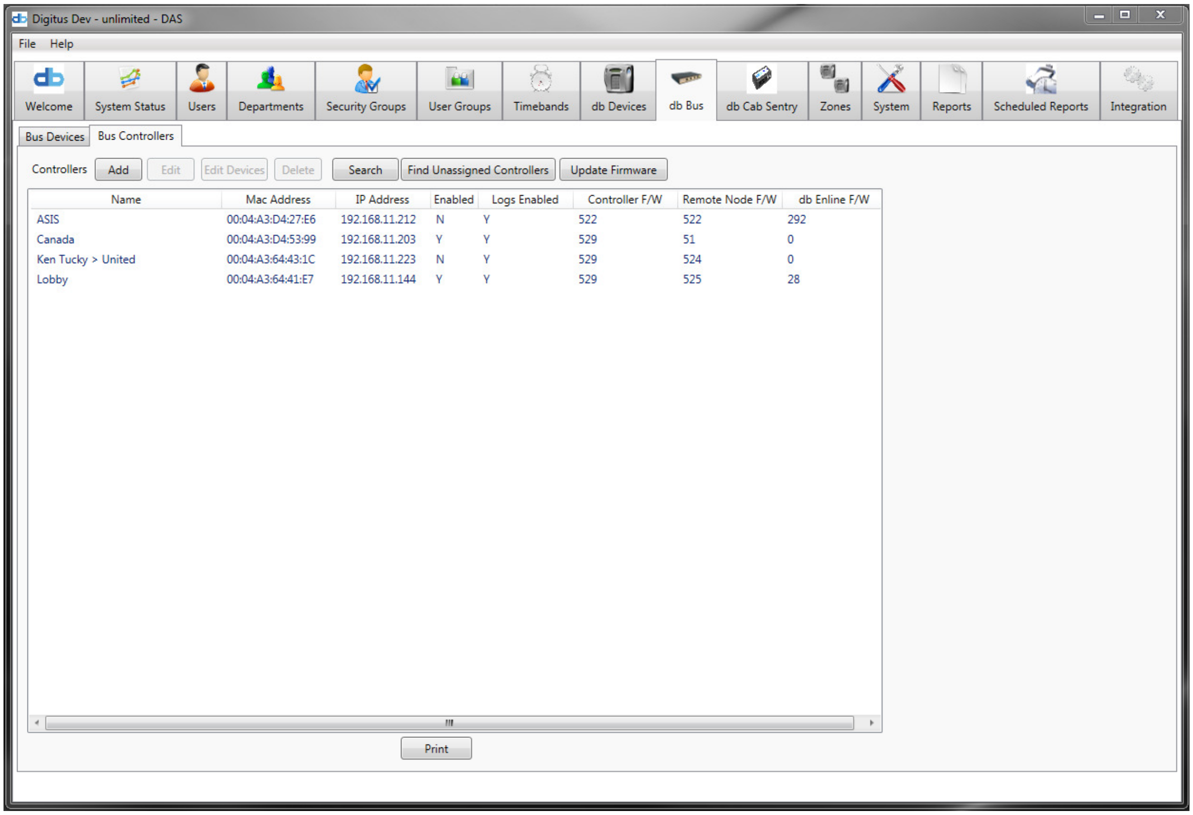


To **search** for a Device, select the "***Search***" button above the device list.

To create a search, Click and Drag one or more Searchable Fields at the top into the Search Fields box. The condition can be set by left-clicking the current value and selecting another from the drop down control. Enter a value for the "Field Value" column. If you wish to add another Searchable field, then you'll need to add an "AND" or an "OR" to your search fields. (eg: Name Like My AND Bus Controller = B). To **delete** a Search Field, right-click the row and select delete from the pop-up box.

If the search produces any results, then these will be displayed in the Search Results list control. You can edit a result by double clicking the row or single click selecting the row and then clicking the edit button.

4.10.4 – db Bus Controllers Sub-tab

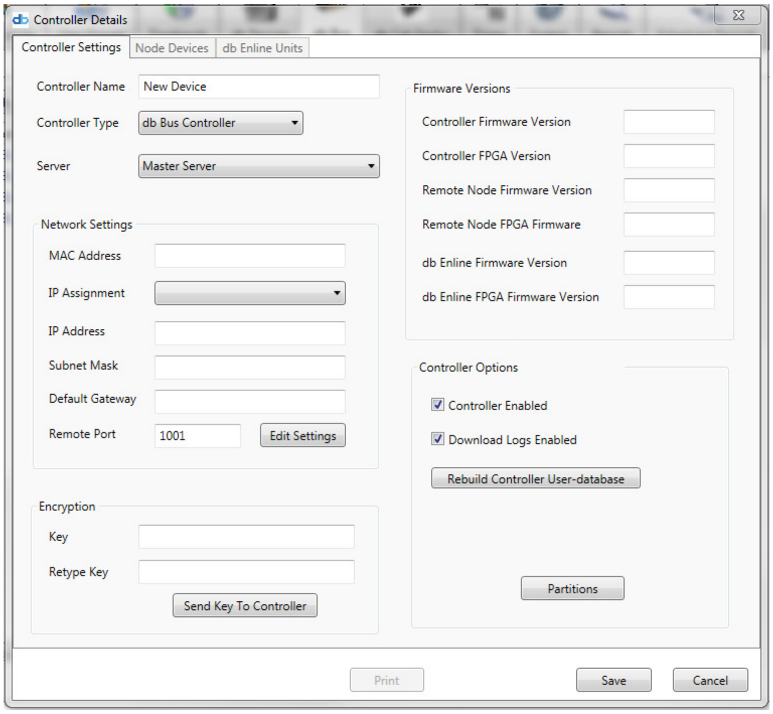


Name	Mac Address	IP Address	Enabled	Logs Enabled	Controller F/W	Remote Node F/W	db Enline F/W
ASIS	00:04:A3:D4:27:E6	192.168.11.212	N	Y	522	522	292
Canada	00:04:A3:D4:53:99	192.168.11.203	Y	Y	529	51	0
Ken Tucky > United	00:04:A3:64:43:1C	192.168.11.223	N	Y	529	524	0
Lobby	00:04:A3:64:41:E7	192.168.11.144	Y	Y	529	525	28

The **db Bus Controllers** sub-tab shows all Bus Controllers that exist in the DAS-SQL system. To **add** a controller manually, select the "***Add***" button or right-click an empty slot in the Controller list and select the Add from the pop-up menu. To **Edit** or **delete** a controller, select the controller then select the appropriate button or select the controller and then right-click and select the desired option from the pop-up box. To **edit** multiple devices attached to a controller, select the controller and click on the Edit Devices button. To **search** through a list of already established controllers, select the "***Search***" button. To **find** controllers on your network, use the "***Find Unassigned Controllers***" button. To **update firmware** on the Unit select "***Update Firmware***".

Adding/Editing a Controller

Select the "***Add***" or "***Edit***" button or right-click the controller in the list and select Add or Edit from the pop-up box.



Controller Name: New Device

Controller Type: db Bus Controller

Server: Master Server

Remote Port: 1001

☑ Controller Enabled

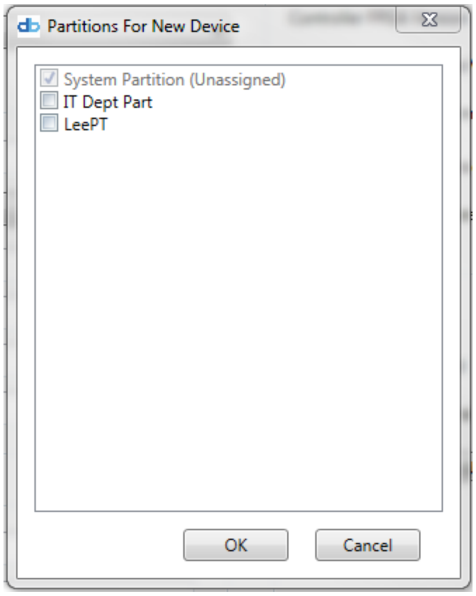
☑ Download Logs Enabled

Controller Name – Desired name for the Controller.

Controller Type – Defaults to db Bus Controller.

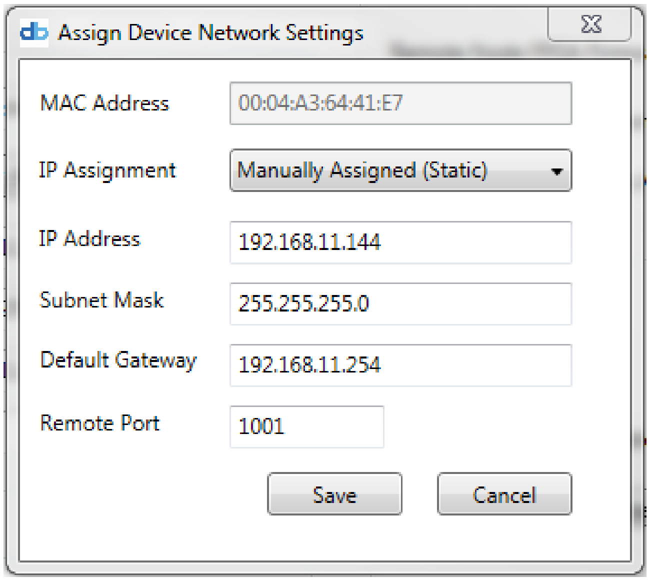
Controller Enabled – Sets the controller to on with the DAS-SQL system.
Server – Leave this as "Master Server".

Partitions – Places a controller into a Partition(s).



☑ System Partition (Unassigned)
☐ IT Dept Part
☐ LeePT

Network Settings – Allows user to change the network configurations. Click the "***Edit"*** button to edit the network options.



Assign Device Network Settings

MAC Address 00:04:A3:64:41:E7

IP Assignment Manually Assigned (Static)

IP Address 192.168.11.144

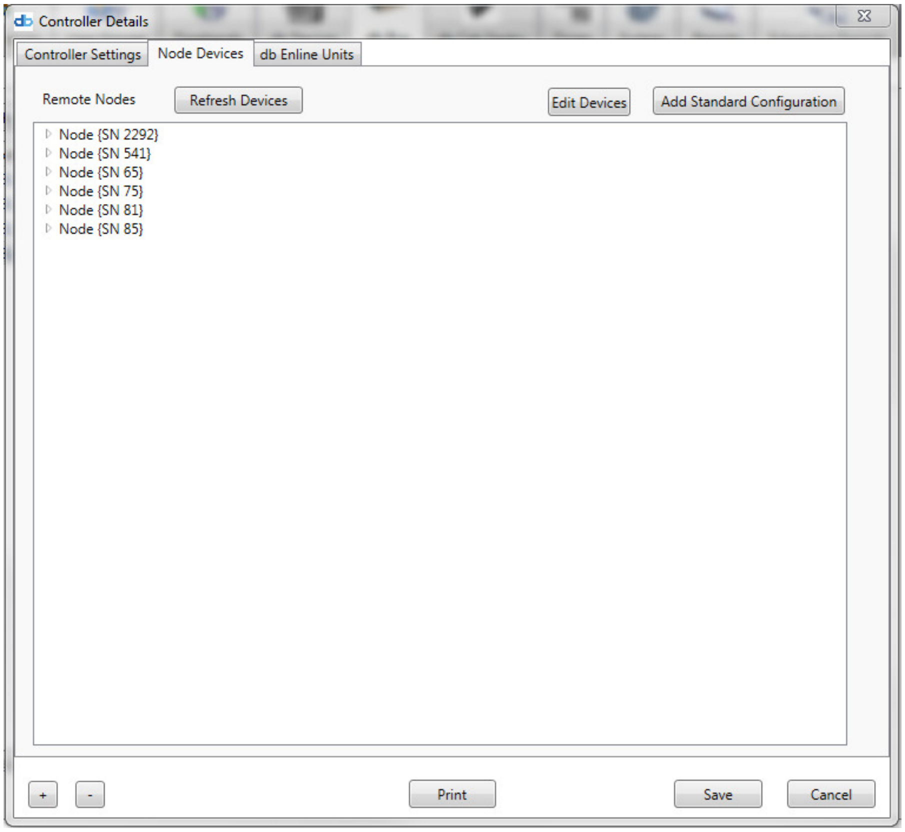
Subnet Mask 255.255.255.0

Default Gateway 192.168.11.254

Remote Port 1001

Encryption Key - This key is chosen by the user and must be 16 characters long. This key will be sent to the controller only once at initialization. Click the "***Send Key to Controller***" button.

Node Devices Tab
This tab shows all Nodes and devices connected to the selected Controller. Select the "Node Devices" tab in the Controller Details window. A Controller can support 32 nodes and each node can currently hold 2 devices (ELock, BioLock, etc…).



Controller Details

- Node {SN 2292}
- Node {SN 541}
- Node {SN 65}
- Node {SN 75}
- Node {SN 81}
- Node {SN 85}

Once the hardware setup is complete, you can retrieve all nodes connected a controller by clicking “***Refresh Devices***”. After clicking the button, wait approximately 30 seconds for the list to refresh. db BioLocks are automatically detected by the Bus Controller. All other device need to be added manually.

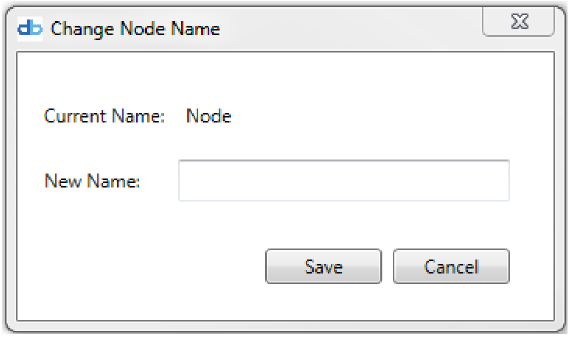
Plus **Button -** Expands all nodes on the page

Minus **Button –** Collapses all nodes on the page.

Adding a Device to a Node – Right-Click the desired node and select “Add Device from the pop-up menu. Select the correct device number, which is determine by which ports the device is connected to – only unused numbers will be available. Provide a name for the device, select the device type, and approve the device.

NOTE: The device will be ignored by DAS-SQL and the db Bus Controller until it has been approved.

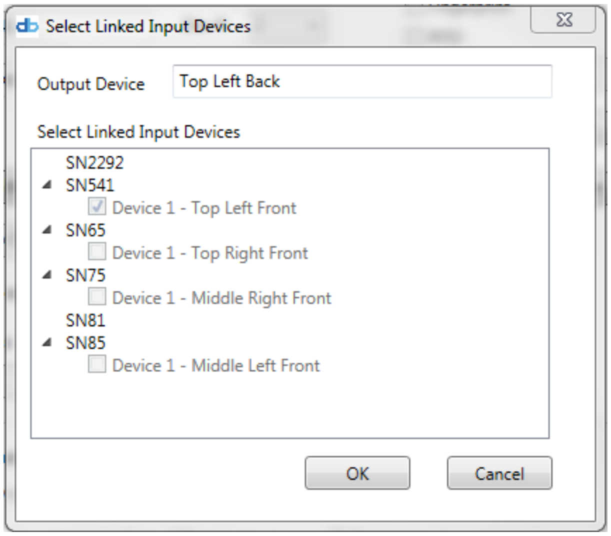
Changing the Node Name - To change the name of the Node, right-Click the Node in the “Remote Nodes” List and select “Change Node Name” from the pop-up menu. The screen below will be displayed. Enter a Node name and click Save.



Current Name: Node

New Name:

Linking Devices – This provides a feature where multiple doors can be opened simultaneously, from a single user authentication. Typically this feature is used where a db BioLock or db CardLock is installed and the front door of a cabinet and you want both the front and back doors to unlock at the same time. Click the “***Linked Devices***” button next to the Device. Select which additional devices you want to unlock, following authentication on this device.

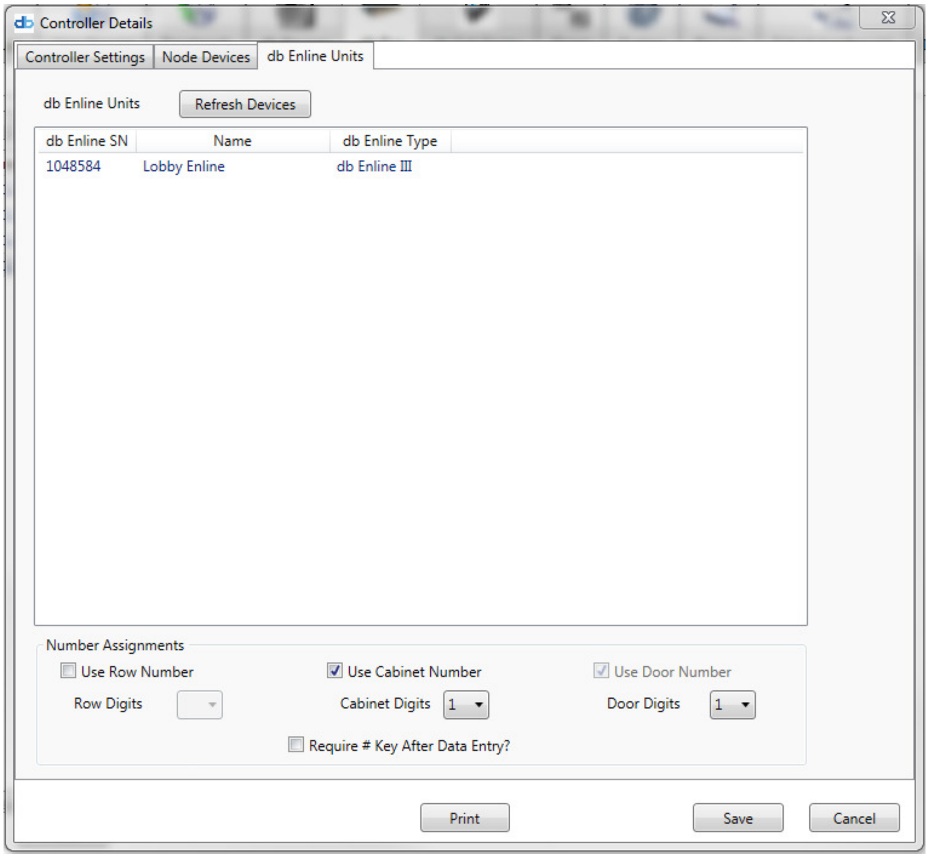


Output Device: Top Left Back

Select Linked Input Devices

- SN2292
- SN541
  - ☑ Device 1 - Top Left Front
- SN65
  - □ Device 1 - Top Right Front
- SN75
  - □ Device 1 - Middle Right Front
- SN81
- SN85
  - □ Device 1 - Middle Left Front

db Enline Units Tab - The db Enline units provide a method to authenticate at the end of a row of cabinets in a data center. When a user is attempting to gain access to a cabinet, they must first identify which cabinet door they are attempting to access, by using a combination of row, cabinet and door number.



Controller Details

Controller Settings | Node Devices | db Enline Units

db Enline Units Refresh Devices

db Enline SN	Name	db Enline Type
1048584	Lobby Enline	db Enline III

Number Assignments

☐ Use Row Number Row Digits

☑ Use Cabinet Number Cabinet Digits: 1

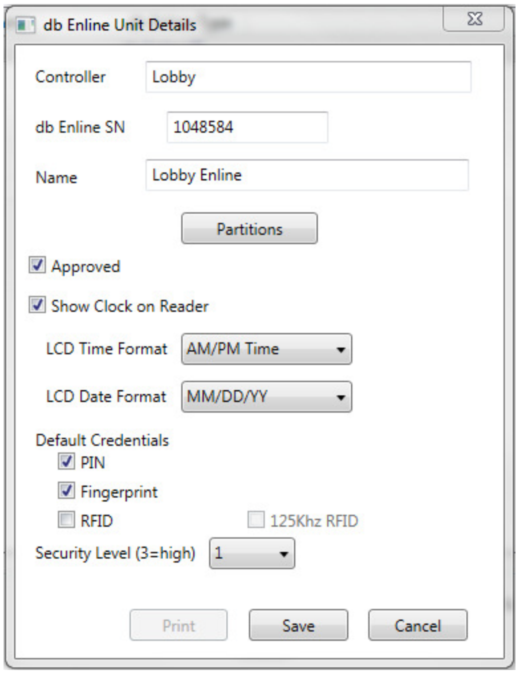
☑ Use Door Number Door Digits: 1

☐ Require # Key After Data Entry?

This sub-tab shows all db Enline units that are connected to the db Bus Controller. To **refresh** the list, click the "***Refresh Devices***" button.

Editing Enline Details

To edit a specific db Enline, double click on the Enline's row in the db Enline Units list.



db Enline Unit Details

Controller: Lobby

db Enline SN: 1048584

Name: Lobby Enline

☑ Approved

☑ Show Clock on Reader

LCD Time Format: AM/PM Time

LCD Date Format: MM/DD/YY

Default Credentials

☑ PIN

☑ Fingerprint

☐ RFID ☐ 125Khz RFID

Security Level (3=high): 1

Controller - Name of db Bus Controller that the device is connected to. This field is read-only and cannot be edited.

db Enline SN- The factory assigned serial number of the db Enline unit. This field is read-only and cannot be edited.

Partitions – Provides the partition screen, allowing the device to be assigned to specific partitions.

Approved – This device, like all others, must be approved for DAS-SQL and the db Bus Controller to recognize it as a working device.

Show Clock on Reader – The date and time will be displayed on the LCB of the db Enline unit.

LCD Time Format – Selects the format of the time on the LCD; AM/PM (1:00PM) or 24-hour (13:00).

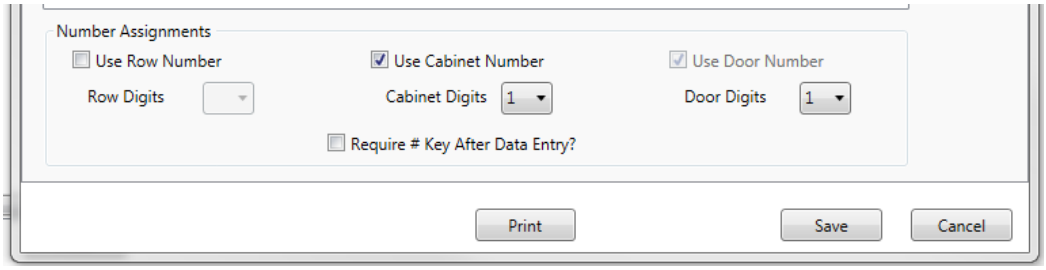
LCD Date Format- Selects the format of the date on the LCD; mm/dd/yyyy or a dd/mm/yyyy format.

Default Credentials

PIN - Requires the user to enter a PIN when accessing a cabinet via the db Enline unit.
Fingerprint - Requires the user to provide a fingerprint when accessing a cabinet via the db Enline unit.
RFID - Requires the user to present a RFID card when accessing a cabinet via the db Enline unit.

Security Level - Selects the quality threshold for the fingerprint reader.

Number Assignments - Defines the criteria for identifying how cabinets are identified at a db Enline unit. It's possible to have up to three identification parameters, Row, Cabinet and Door. Each parameter is enabled by checking the respective checkbox and selecting the number of digits from the dropdown combo. If "Require # Key After Data Entry", is checked, the user must press the "#" key after each step. This allows them to review what they've key in, before proceeding to the next item.



Number Assignments

☐ Use Row Number
Row Digits

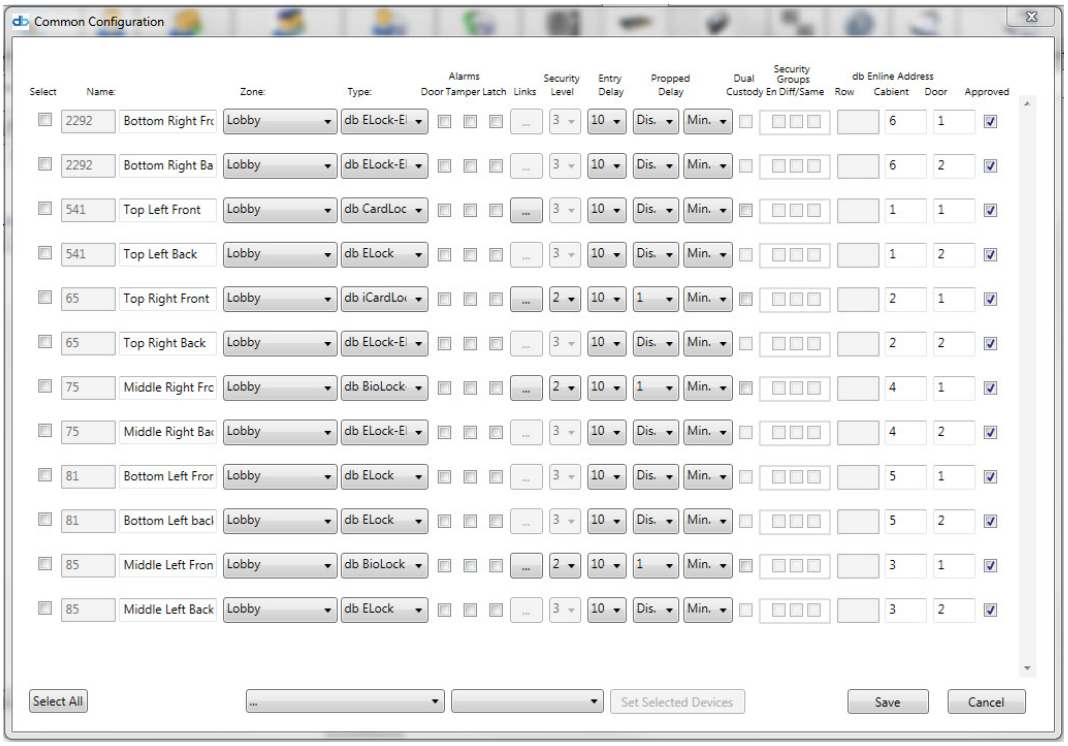
☑ Use Cabinet Number
Cabinet Digits 1

☑ Use Door Number
Door Digits 1

☐ Require # Key After Data Entry?

4.10.4.1 - EDIT DEVICES

The **Edit Devices** Button allows for the editing of multiple Devices from one screen.



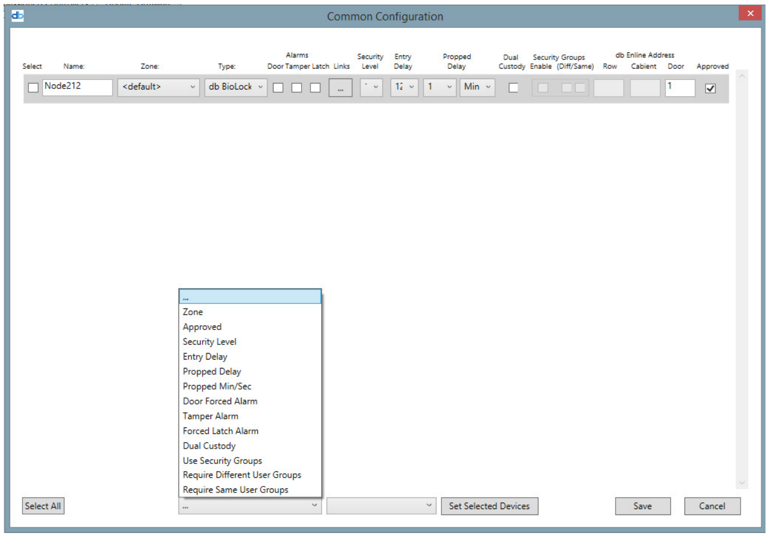
Common Configuration

Select	Name:		Zone:	Type:	Alarms Door	 Tamper	 Latch	Links	Security Level	Entry Delay	Propped Delay		Dual Custody	Security Groups En Diff/Same	db Enline Address Row	 Cabient	 Door	Approved
□	2292	Bottom Right Frc	Lobby	db ELock-El	□	□	□	...	3	10	Dis.	Min.	□	□□□		6	1	☑
□	2292	Bottom Right Ba	Lobby	db ELock-El	□	□	□	...	3	10	Dis.	Min.	□	□□□		6	2	☑
□	541	Top Left Front	Lobby	db CardLoc	□	□	□	...	3	10	Dis.	Min.	□	□□□		1	1	☑
□	541	Top Left Back	Lobby	db ELock	□	□	□	...	3	10	Dis.	Min.	□	□□□		1	2	☑
□	65	Top Right Front	Lobby	db iCardLoc	□	□	□	...	2	10	1	Min.	□	□□□		2	1	☑
□	65	Top Right Back	Lobby	db ELock-El	□	□	□	...	3	10	Dis.	Min.	□	□□□		2	2	☑
□	75	Middle Right Frc	Lobby	db BioLock	□	□	□	...	2	10	1	Min.	□	□□□		4	1	☑
□	75	Middle Right Ba	Lobby	db ELock-El	□	□	□	...	3	10	Dis.	Min.	□	□□□		4	2	☑
□	81	Bottom Left Fror	Lobby	db ELock	□	□	□	...	3	10	Dis.	Min.	□	□□□		5	1	☑
□	81	Bottom Left bacl	Lobby	db ELock	□	□	□	...	3	10	Dis.	Min.	□	□□□		5	2	☑
□	85	Middle Left Fron	Lobby	db BioLock	□	□	□	...	2	10	1	Min.	□	□□□		3	1	☑
□	85	Middle Left Back	Lobby	db ELock	□	□	□	...	3	10	Dis.	Min.	□	□□□		3	2	☑

The **Common Configuration** screen shows all of the connected Devices. Depending on the number of devices that need to be changed you can use the "***Select all Button***" to select all the Devices and then deselect the devices you don't want to change or you can select the Devices you want to change by clicking on the Select box next to each Device.

Once the Device is selected, current settings can be changed by selecting values from a drop down menu or checking a box. To apply the changes click on the "***Save***" button.

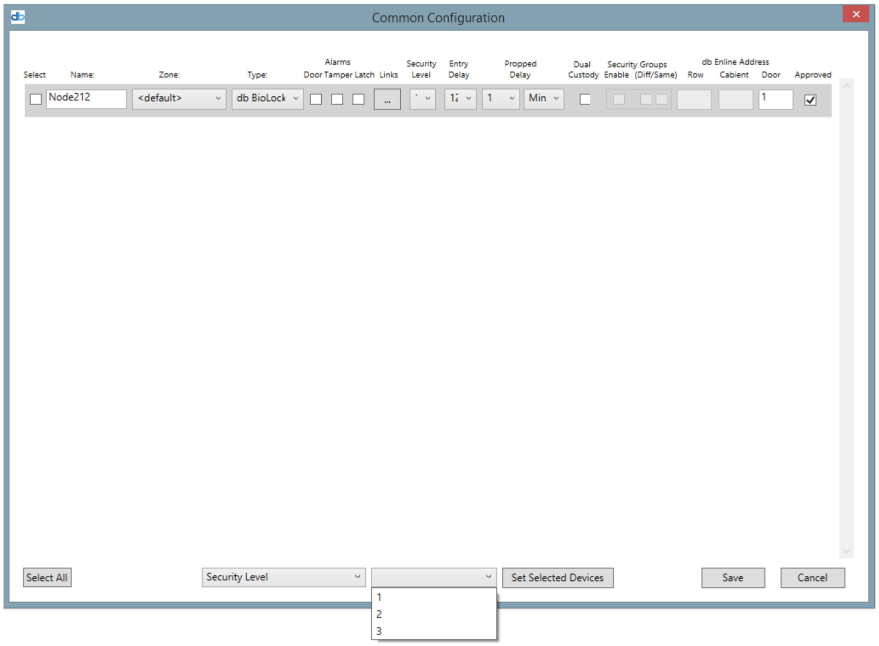
If multiple Devices require the same changes (all Devices need to be changed to security level 2), select the Devices that need to be changed. Click on the Left Combo box at the bottom of the page and select the setting that is to be changed.



Common Configuration

Select	Name:	Zone:	Type:	Alarms Door	 Tamper	 Latch	Links	Security Level	Entry Delay	Propped Delay		Dual Custody	Security Groups Enable	 (Diff/Same)	db Enline Address Row	 Cabient	 Door	Approved
□	Node212	<default>	db BioLock	□	□	□	...	[illegible]	12	1	Min	□	□	□□			1	☑

Click on the Right Combo Box button and select the new value. Click on the "***Set Selected Device***" button then click "***Save*** ".

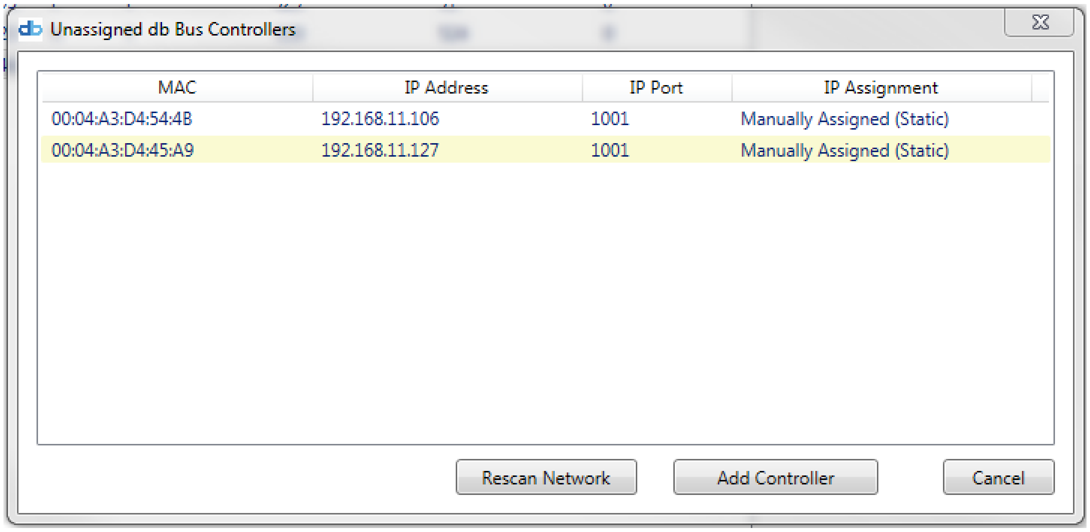


Select	Name:	Zone:	Type:	Alarms			Links	Security Level	Entry Delay	Propped Delay		Dual Custody	Security Groups		db Enline Address			Approved
				Door	Tamper	Latch							Enable	(Diff/Same)	Row	Cabient	Door	
□	Node212	<default>	db BioLock	□	□	□	...	˙	12	1	Min	□	□	□ □			1	☑

Multiple settings can be changed for selected Device(s). Click the Left Combo Box, select setting to change, Click the Right Combo Box to select the new value setting. Click the "***Set Selected Device"*** button. Now click the Left Combo Box again and select a different setting to change, set the value, click "***Set Selected Devices***" button. After all the settings that need to be changed are entered Click on the "***Save***" button and the new changes will be transferred to the Devices.

4.10.5 – db Bus Devices – Finding Unassigned db Bus Controllers

Clicking the "Find Unassigned Controllers" button on the "db Bus Controller" sub-tab will display the window below.

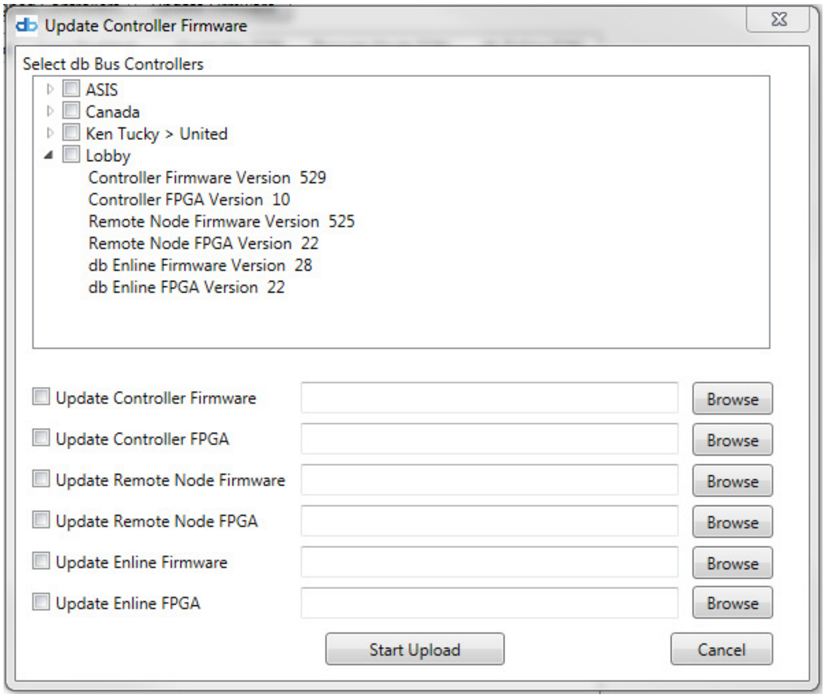


MAC	IP Address	IP Port	IP Assignment
00:04:A3:D4:54:4B	192.168.11.106	1001	Manually Assigned (Static)
00:04:A3:D4:45:A9	192.168.11.127	1001	Manually Assigned (Static)

This window shows all db Bus Controllers that are responding to a UDP broadcast DAS-SQL's call on the network. **Please note this feature will only discover db Bus Controllers that are on the same network-segment as the DAS-SQL Service.** To rescan the network, select the "Rescan Network" button. Once db Bus Controllers have been discovered, to add a controller, select the controller from within the list and click the "Add Controller" button, or double-click the controller in the list. The process for adding the db Bus Controller to DAS-SQL is then the same as adding a controller manually, shown in Section 4.10.4.

4.10.6 – db Bus Devices Tab – Updating Unit Firmware

The "***Update Firmware***" button on the "db Bus Controller" sub-tab provides the window below.



Update Controller Firmware

Select db Bus Controllers

- □ ASIS
- □ Canada
- □ Ken Tucky > United
- □ Lobby
  - Controller Firmware Version 529
  - Controller FPGA Version 10
  - Remote Node Firmware Version 525
  - Remote Node FPGA Version 22
  - db Enline Firmware Version 28
  - db Enline FPGA Version 22

□ Update Controller Firmware

□ Update Controller FPGA

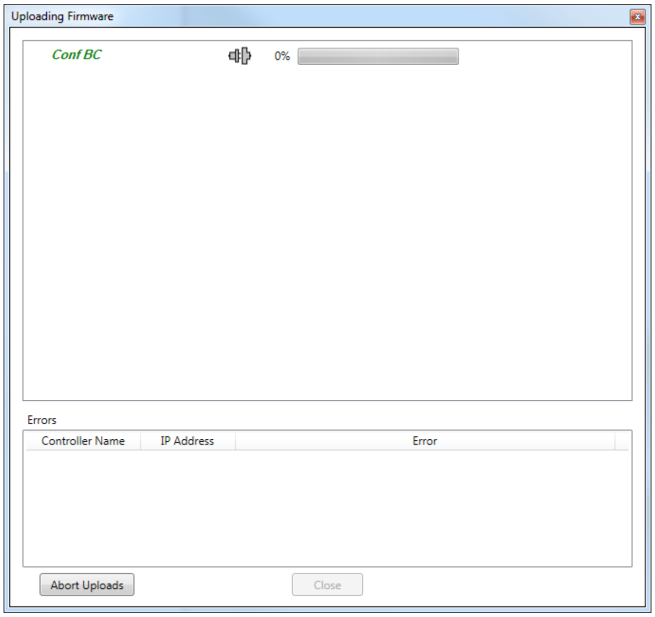
□ Update Remote Node Firmware

□ Update Remote Node FPGA

□ Update Enline Firmware

□ Update Enline FPGA

This window shows the current firmware version of the db Bus Controllers in the system. To update the controller's firmware, select the controller to be updated, select the relevant components by checking the checkboxes next to each item, and then browse to the relevant file. Once everything has been selected, click the "***Start Upload***" button. A progress and percentage image will show the update's progress.



Uploading Firmware

Conf BC 0%

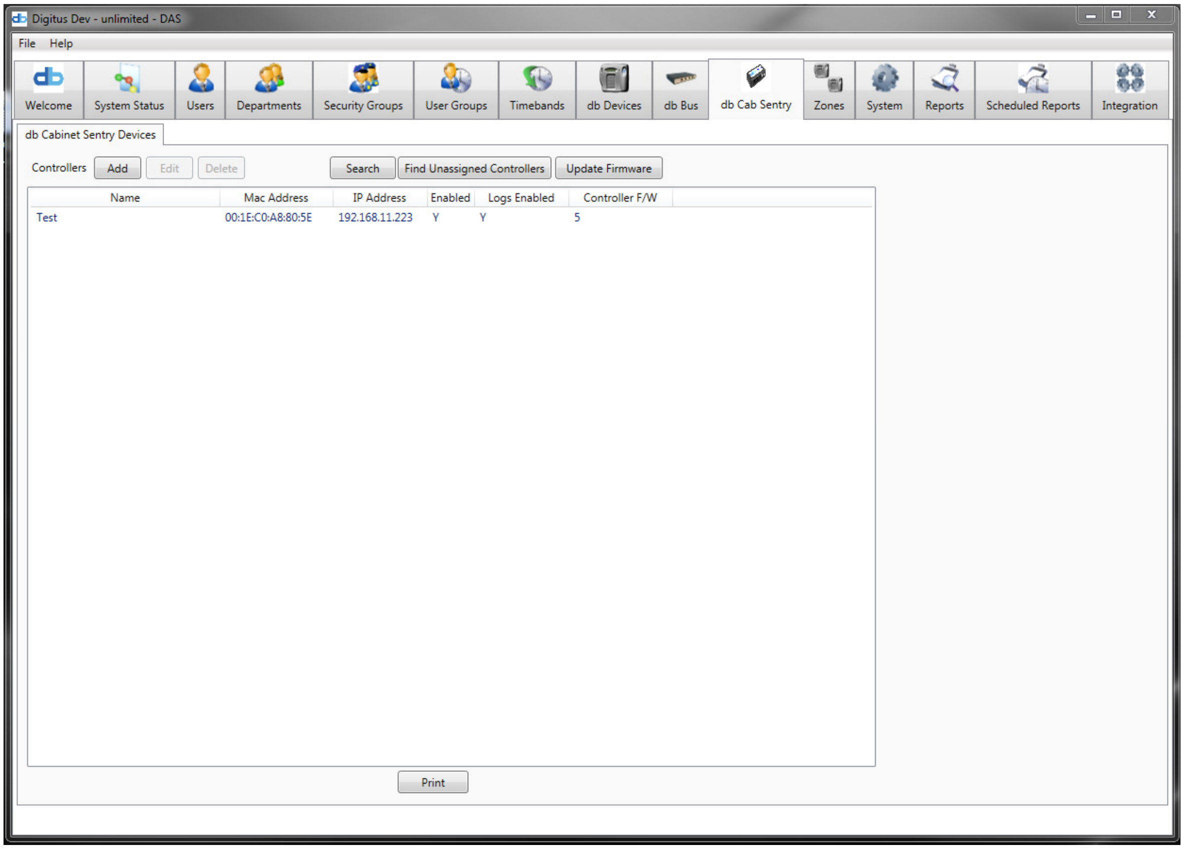
Errors

Controller Name	IP Address	Error

<span style="color:red">**NOTE:** This information must be entered correctly for DAS-SQL to properly update the hardware.</span>

4.11 – db Cab Sentry Tab

The "db Cab Sentry" tab contains all configured Cabinet Sentry Devices and allows them to be edited, as well as new Devices added.



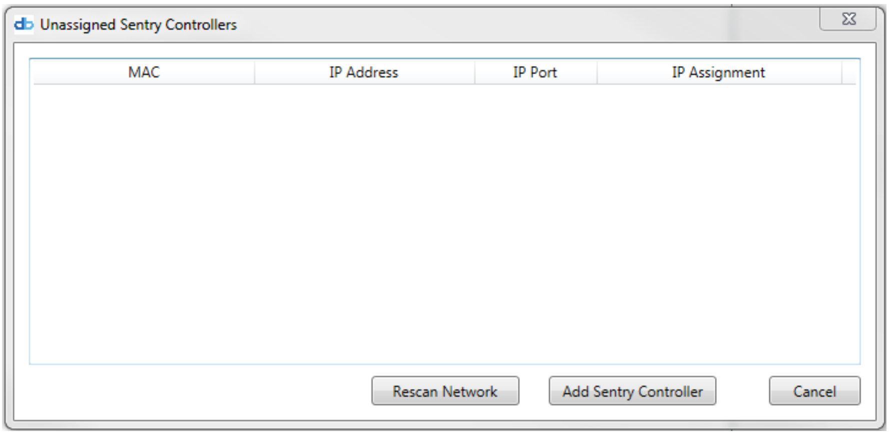
Name	Mac Address	IP Address	Enabled	Logs Enabled	Controller F/W
Test	00:1E:C0:A8:80:5E	192.168.11.223	Y	Y	5

Currently configured Devices are shown in the "Devices" list. This list can be sorted by Name, IP Address, or Zone. To sort the Devices, left-click on the column header.

To **add, edit, or delete** a Device, select the Device, then select the appropriate button or right-click on the "Device" list control. A popup menu will be displayed with "Add," "Edit," and "Delete" menu items. If an existing Device has been selected, the "Edit" and "Delete" menu items will be enabled. If no Device has been selected, only the "Add" menu item will be enabled.

4.11.1 – db Cab Sentry Tab – Finding unassigned controllers

It is possible to manually add a Controller. However, it is easier to let the server scan the network and report any Controllers it finds that have not yet been configured. To do this, click the "Find Unassigned Controllers" button. The following form will be displayed:



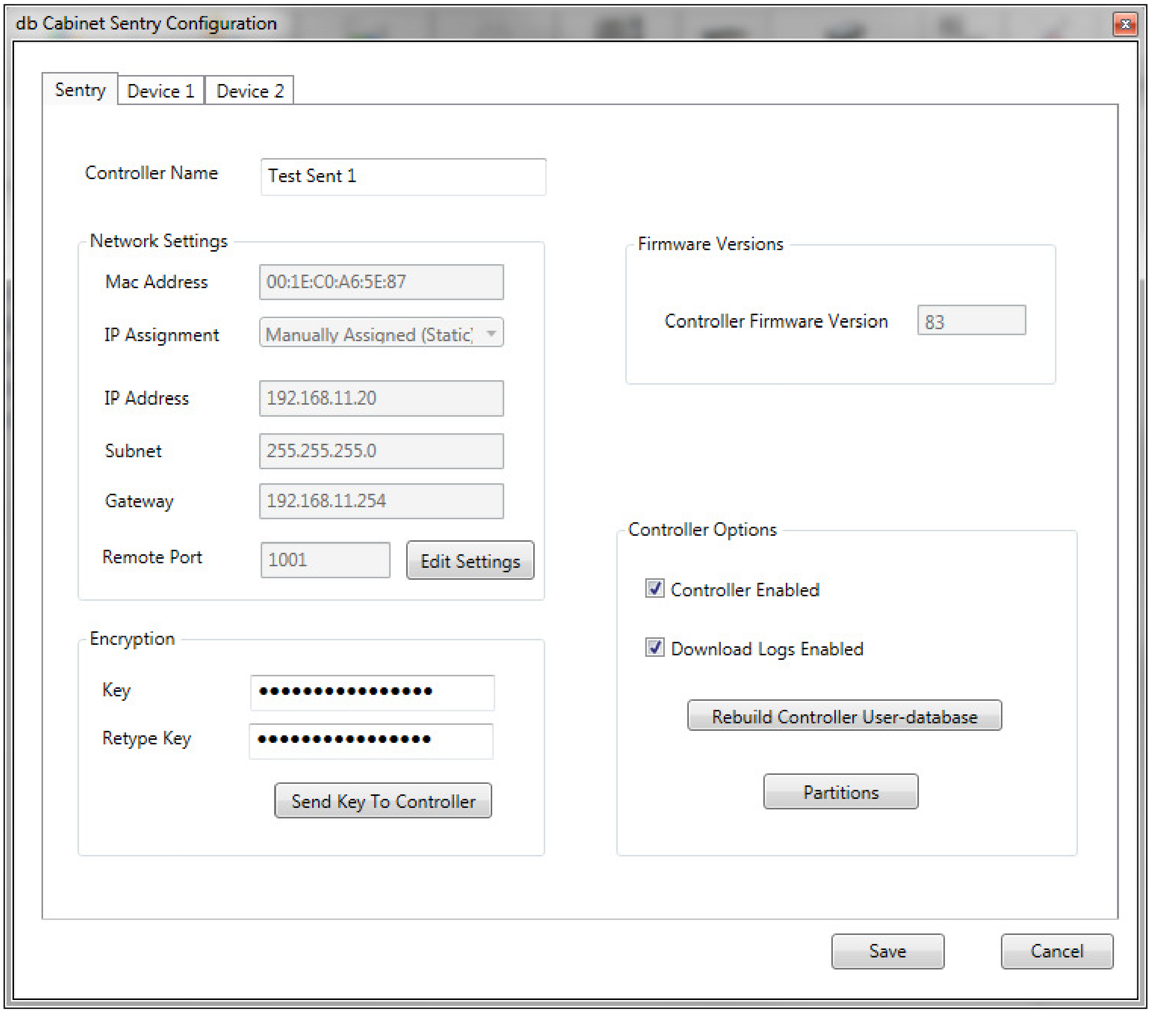
MAC	IP Address	IP Port	IP Assignment

NOTE: It will take approximately ten (10) seconds for the server to scan the network for new Controllers.

To add a Controller, select it from the list of newly-found units by double-clicking on the entry or selecting it and clicking the “Add Sentry Controller” button.

The “db Cabinet Sentry Configuration” form will be displayed to complete the new Controller setup.

4.11.2 – db Cab Sentry Tab – Setting up Controller



db Cabinet Sentry Configuration

Controller Name: Test Sent 1

Network Settings

Mac Address: 00:1E:C0:A6:5E:87

IP Assignment: Manually Assigned (Static

IP Address: 192.168.11.20

Subnet: 255.255.255.0

Gateway: 192.168.11.254

Remote Port: 1001

Encryption

Key: ●●●●●●●●●●●●●●●●

Retype Key: ●●●●●●●●●●●●●●●●

Firmware Versions

Controller Firmware Version: 83

Controller Options

☑ Controller Enabled

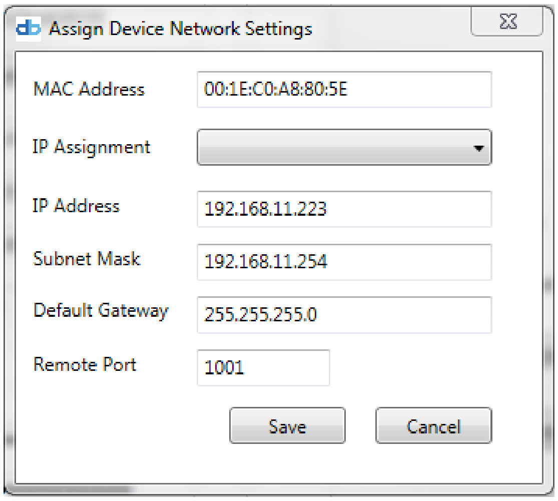
☑ Download Logs Enabled

4.11.2.1 - The Sentry Tab

Controller Name – Name for the new Sentry Controller

4.11.2.2 - The Network Settings Section

This section displays the current network settings for the Controller unit hardware. To change these settings, click the “***Edit Settings***” button. The following form will be displayed:



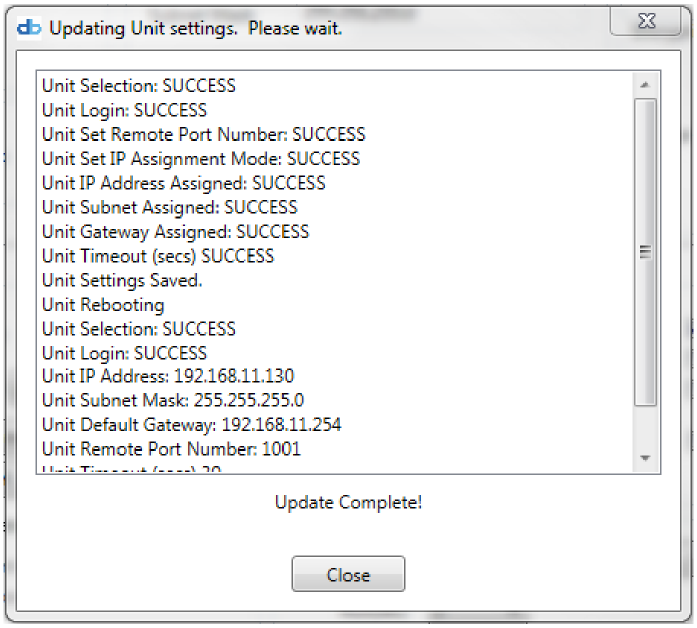
MAC Address	00:1E:C0:A8:80:5E
IP Assignment	
IP Address	192.168.11.223
Subnet Mask	192.168.11.254
Default Gateway	255.255.255.0
Remote Port	1001

This form allows the Device unit's network settings to be reconfigured. The network adapter in the Device can use a fixed (static) IP address or an automatically assigned address (DHCP). Note that if "Automatic (DHCP)" is selected, the unit will receive an address assigned by the network DHCP server, but the IP address (the ' . . .' address) must be used (not a "computer name").

To change the IP settings (IP Address, Subnet Mask, Default Gateway, and Remote [IP] Port), enter that data in the appropriate fields. Consult your network administrator for information about what these are and how they should be set. Once the settings have been entered, click the "***Save***" button.

The purpose of these settings is to change the data in the Device's setup data, as well as to reprogram the Device unit's network adapter.

NOTE: If these changes require updating the Device unit's network adapter, select "Yes" when asked if you wish to "Send Settings to Unit?" If no, the data will be entered into the database but not sent to the Device unit. If yes, the data will be sent to the Device unit. As it is being sent, the following status window will appear:



```
Unit Selection: SUCCESS
Unit Login: SUCCESS
Unit Set Remote Port Number: SUCCESS
Unit Set IP Assignment Mode: SUCCESS
Unit IP Address Assigned: SUCCESS
Unit Subnet Assigned: SUCCESS
Unit Gateway Assigned: SUCCESS
Unit Timeout (secs) SUCCESS
Unit Settings Saved.
Unit Rebooting
Unit Selection: SUCCESS
Unit Login: SUCCESS
Unit IP Address: 192.168.11.130
Unit Subnet Mask: 255.255.255.0
Unit Default Gateway: 192.168.11.254
Unit Remote Port Number: 1001
```

Update Complete!

When the Device unit upload is complete, a confirmation message appears. The status window can be closed and Device unit data entry continued.

The DAS-SQL server communicates with the Controller via encrypted communication (see Encryption below). When a db Cabinet Sentry is installed, the installer or manager enters an encryption key on the head unit. This encryption key must be entered in the "Door Details" form for the server to communicate with the Door unit.

4.11.2.3 - The Encryption Section

Enter the key in the "Key" field and in the "Retype Key" field. This is a user selected key that needs to only be entered once.

This key MUST be exactly 16 digits long.

4.11.2.4 - The Firmware Versions Section

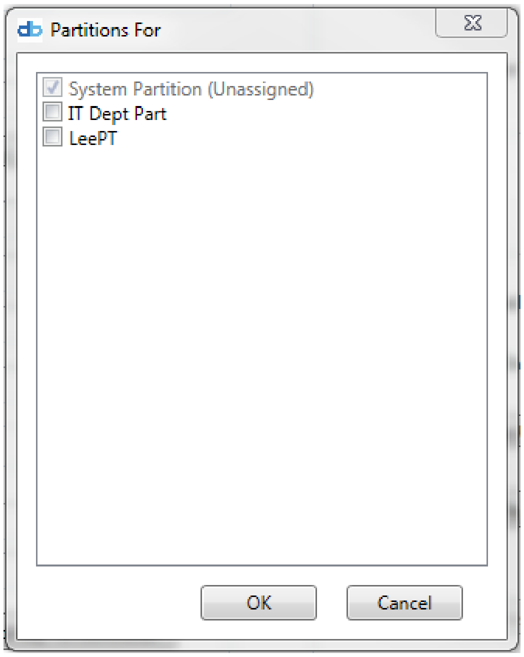
Shows the current firmware version on the Controller

4.11.2.5 - The Controller Options

Enable or disable the Controller

4.11.2.6 - Partitions Button

Devices can be assigned to Partitions to restrict visibility and access to selected Partitions. To select the Partitions to which this Device is assigned, click the "***Partitions***" button.



Partitions For

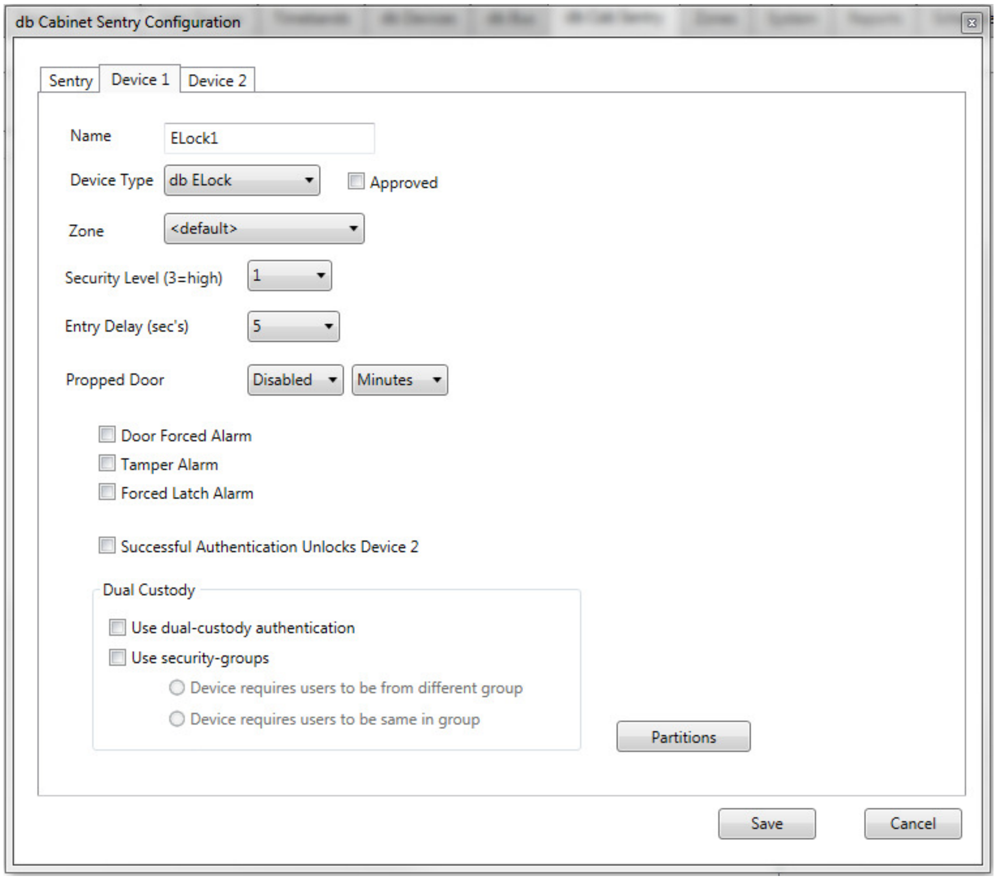
☑ System Partition (Unassigned)
☐ IT Dept Part
☐ LeePT

Select the desired Partition(s) and click "***OK***".

NOTE: When a new Device unit is added, all Timebands will be uploaded to the Device. Any Users who have been assigned to the <default> (24/7, all doors) User Group will be uploaded to the new Device as soon as possible. User uploading will normally begin within one (1) minute and may take several minutes depending on how many Users are assigned to the <default> Group (see User and User Group settings above for details).

4.11.2.7 - Device 1 and Device 2 Tabs

The following applies to both Device 1 and 2.



Name ELock1

Device Type db ELock ☐ Approved

Zone <default>

Security Level (3=high) 1

Entry Delay (sec's) 5

Propped Door Disabled Minutes

☐ Door Forced Alarm
☐ Tamper Alarm
☐ Forced Latch Alarm

☐ Successful Authentication Unlocks Device 2

Dual Custody
☐ Use dual-custody authentication
☐ Use security-groups
○ Device requires users to be from different group
○ Device requires users to be same in group

Device Name - Name for the new Device unit.
Unit Approved determines whether the Device Unit will be online or offline. If "Unit Approved" is not checked, no events will be received from the Device and no Users will be uploaded to the Device Unit.

Reader Type for this Device unit refers to the specific unit's type.
If the Device Unit is a db Zero-U or db Nexus Duo II or III, then the "Send Key to Unit" button will be enabled. This is used to program the encryption key for the unit. This can be done only once (without a special utility to reset the unit).

Unit Approved – Must be checked for DAS-SQL to communicate with the unit.

Zone is to which this Device is to be assigned. (If no Zones have been configured, this Device can be assigned to the "<default>" Zone.) If the Device has been assigned to a Partition, only Zones in that Partition will be listed.

Security Level selects the threshold for the fingerprint reader. For maximum security, select 3.

Entry Delay determines how long the User has to open the door after User access has been granted access.

Propped Door determines how many minutes (or seconds for some Reader types) a door can remain open before a "Propped/Held Door" alarm is triggered.

Door forced (intruder) alarms on this Door, select the "Door Forced Alarms" checkbox.

Tamper Alarm (unit tampering) alarms created when a unit is tampered.

Forced Latch Alarm (intruder) alarms for illegal operations on a door latch.

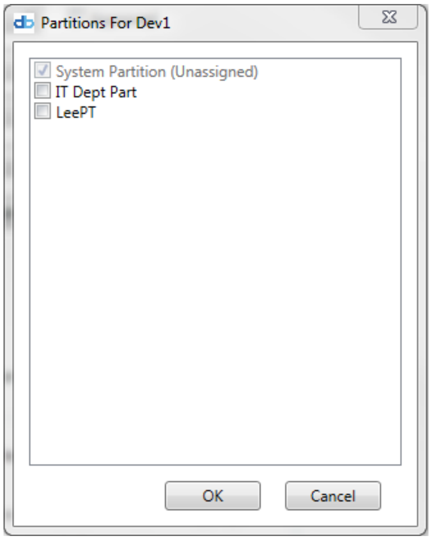
Successful Authentication Unlocks Device 1 or 2 enables one point of authentication to unlock both locks.

Dual-Custody - Requires two users to authenticate on a Device before access is granted.

Use Security Groups - Works in conjunction with the Security Groups Tab. When used, a selection must be made as to whether each person must be from the same Security Group or from different Security Groups.

Partitions

Devices can be assigned to Partitions to restrict visibility and access to selected Partitions. To select the Partitions to which this Device is assigned, click the “***Partitions***” button.



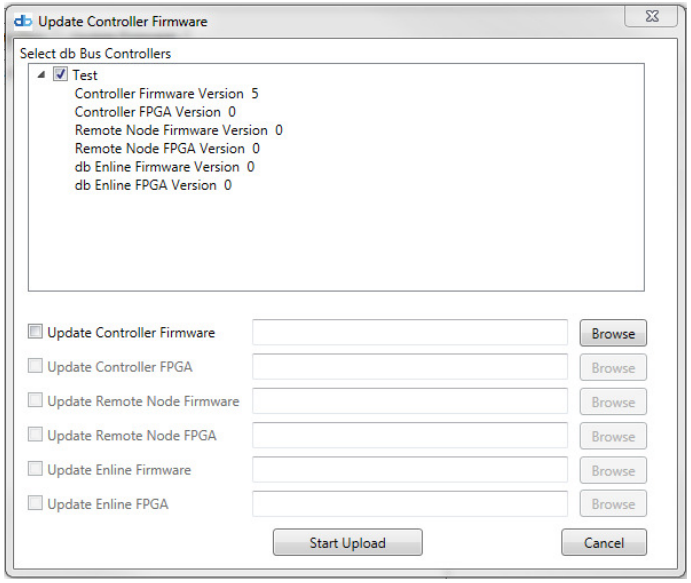
☑ System Partition (Unassigned)
□ IT Dept Part
□ LeePT

Select the desired Partition(s) and click “***OK***”.

NOTE: When a new Device unit is added, all Timebands will be uploaded to the Device. Any Users who have been assigned to the <default> (24/7, all doors) User Group will be uploaded to the new Device as soon as possible. User uploading will normally begin within one (1) minute and may take several minutes depending on how many Users are assigned to the <default> Group (see User and User Group settings above for details).

4.11.2.8 – db Cab Sentry Tab – Updating Unit Firmware

Periodically, new firmware updates are released that need to be uploaded to the Digitus devices. To do this, use the “***Update Firmware***” button on the device tab. The window below shows a list of devices grouped by zones, allowing you to select which devices are to be updated.



Update Controller Firmware

Select db Bus Controllers

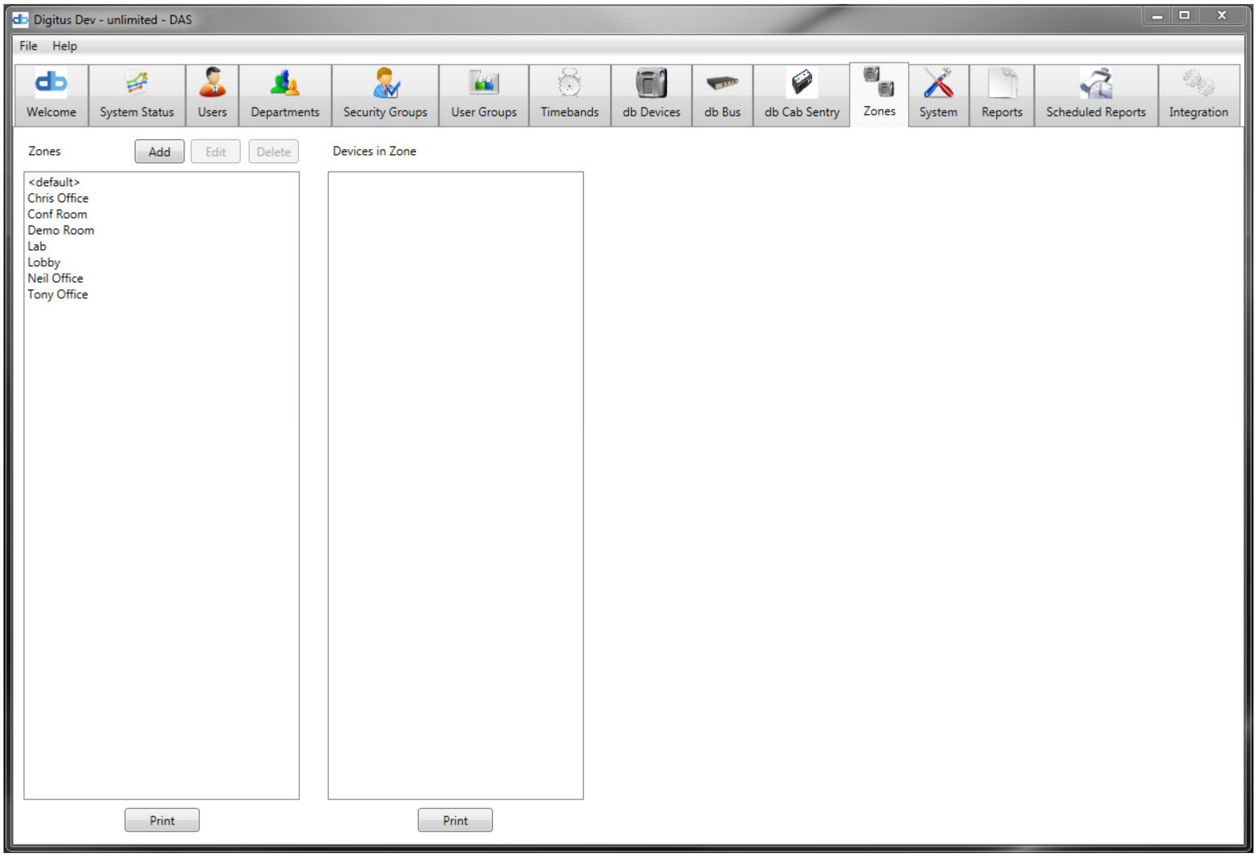
☑ Test
Controller Firmware Version 5
Controller FPGA Version 0
Remote Node Firmware Version 0
Remote Node FPGA Version 0
db Enline Firmware Version 0
db Enline FPGA Version 0

□ Update Controller Firmware
□ Update Controller FPGA
□ Update Remote Node Firmware
□ Update Remote Node FPGA
□ Update Enline Firmware
□ Update Enline FPGA

To Update - Select the Unit type for updating, then select which devices are to be updated from the list. Once the device selection has been made, select which firmware files are to update by checking one or more checkboxes next to the hardware names. Select each file, using the “***Browse***” button. Once all files have been selected, click the “***Start Upload***” button to begin the firmware update. Depending on what files are being updated, this process can take three to fifteen minutes. A progress bar shows the update’s progress. Once done, DAS-SQL provides a confirmation that the hardware was correctly updated. Confirming this acknowledgement returns you to the db Devices tab.

4.12 – Zones Setup Tab

All Devices units can be placed into Zones for easier management and reporting. Zones have no effect on User Groups (other than how the Devices are displayed in the User Group). They are simply a tool to make system management and reporting easier.



Zones

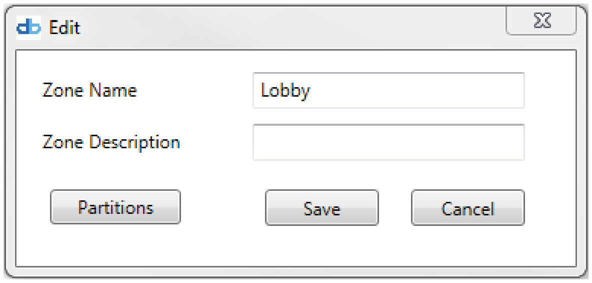
<default>
Chris Office
Conf Room
Demo Room
Lab
Lobby
Neil Office
Tony Office

To **view** the Devices in any given Zone, left-click on the Zone in the "Zones" list control.

To **add, edit, or delete** a Zone, Select a Zone, select a button or right-click on the "Zone" list control. A popup menu will be displayed with Add, Edit, and Delete menu items. If an existing Zone has been selected, the Edit and Delete menu items will be enabled. If no Zone has been selected, only the Add menu item will be enabled.

NOTE: If an existing Zone is deleted, any Devices assigned to that Zone will be re-assigned to the <default> Zone.

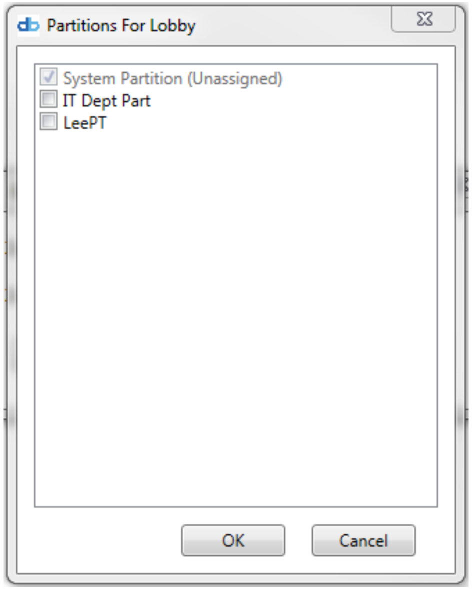
To edit a Zone, select the appropriate menu item in the "Zones" list, and the following form will appear:



Zone Name: Lobby

Zone Description:

Zones can be assigned to Partitions to restrict visibility access to Users in selected Partitions. To assign the Zone to one or more Partitions, click the "***Partitions***" button.



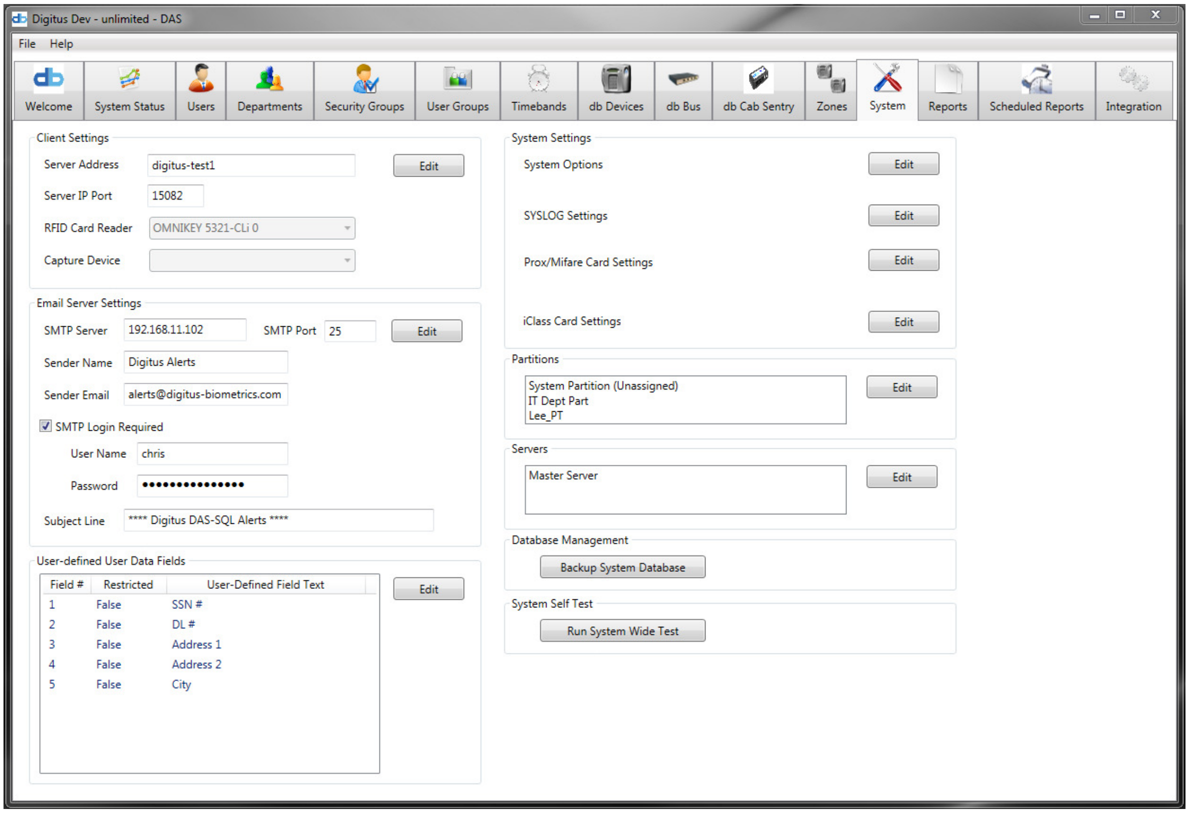
☑ System Partition (Unassigned)
□ IT Dept Part
□ LeePT

Select the desired Partition(s) and click "***OK***."

Enter a name and (optionally) a description for the Zone. Click "Save" when done.

4.13 – System Setup Tab

The "System Setup" tab is used to define global or system-wide settings. Some of these are necessary for system operation (such as the Server Address and Server IP Port), and the remainder are optional (i.e., "User-defined User Data Fields").



Client Settings

Server Address	digitus-test1
Server IP Port	15082
RFID Card Reader	OMNIKEY 5321-CLi 0
Capture Device	

Email Server Settings

SMTP Server	192.168.11.102
SMTP Port	25
Sender Name	Digitus Alerts
Sender Email	alerts@digitus-biometrics.com
☑ SMTP Login Required	
User Name	chris
Password	•••••••••••••••
Subject Line	**** Digitus DAS-SQL Alerts ****

User-defined User Data Fields

Field #	Restricted	User-Defined Field Text
1	False	SSN #
2	False	DL #
3	False	Address 1
4	False	Address 2
5	False	City

System Settings

System Options

SYSLOG Settings

Prox/Mifare Card Settings

iClass Card Settings

Partitions

System Partition (Unassigned)
IT Dept Part
Lee_PT

Servers

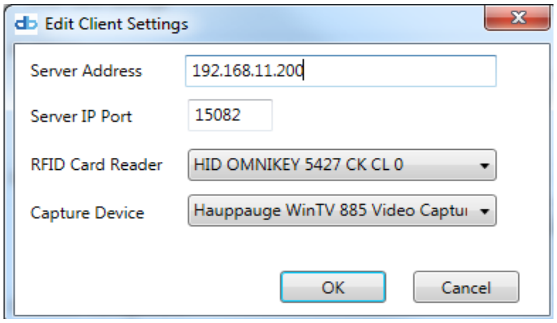
Master Server

Database Management

System Self Test

4.13.1 – System Setup Tab – Client Settings

To change the Server Address, IP port, RFID card reader, or video capture device, click the "***Edit***" button in the "Client Settings" section. The following form is displayed:



Server Address	192.168.11.200
Server IP Port	15082
RFID Card Reader	HID OMNIKEY 5427 CK CL 0
Capture Device	Hauppauge WinTV 885 Video Captu

Enter the new DAS-SQL server address and IP port number. These settings will take affect only after the User logs off the client and attempts to log on again.

Select a connected RFID card reader to program RFID cards (if applicable).

Select a connected video capture device for User photos (if applicable).

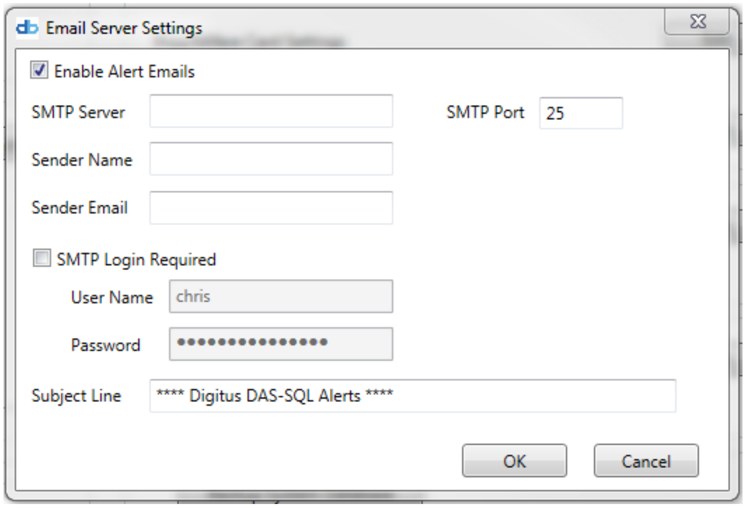
Note: To change the client-specific settings, the User must be logged onto Windows as an Administrator.

Note: If “User Account Control” is enabled in Windows, the DAS-SQL client application must be “Run as administrator” as change the Client Settings, because “Registry Keys” need to be written to the Windows Registry. To do this, browse to the folder where the DAS-SQL client software has been installed using Windows Explorer, the default location is “C:\Program Files (x86)\Digitus Biometrics\DAS SQL Client”. Locate the file “BiometricAccessManagementClient.exe” and right-click on the file. Select “Run as administrator” and select to allow the program to run when prompted.

Click “***OK***” when done and the data will be saved.

4.13.2 – System Setup Tab – Email Server Settings

“Email Server Settings” defines the email server and Sender information to send email alert messages to Users. To edit these settings, click the “***Edit***” button.



Email Server Settings

☑ Enable Alert Emails

SMTP Server

SMTP Port 25

Sender Name

Sender Email

□ SMTP Login Required

User Name chris

Password ●●●●●●●●●●●●●●●

Subject Line **** Digitus DAS-SQL Alerts ****

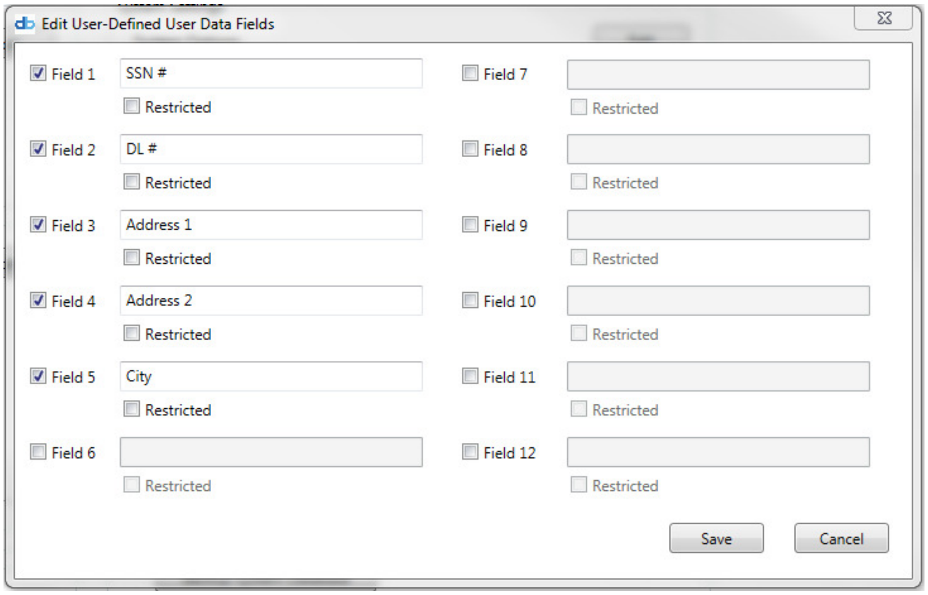
On the “Email Server Settings” form, enter the email server address (SMTP Server), SMPT port, sender name, and sender email. If the SMTP server requires a login, check that box and enter the User name and password. A subject line for the email message can be entered.

Click “***OK***” to save the email server data.

4.13.3 – System Setup Tab – User Defined Data Fields

“User-defined User Data Fields” are fields that can be assigned to User configuration to allow saving information such as address, phone number, license plate number, etc. To edit these fields, click the “Edit” button in the “User-defined User Data Fields” section. The following form will appear:

To enable a field, select its checkbox and enter a caption. This caption will be displayed in the User setup form. These field captions can be up to twenty-five (25) characters long.

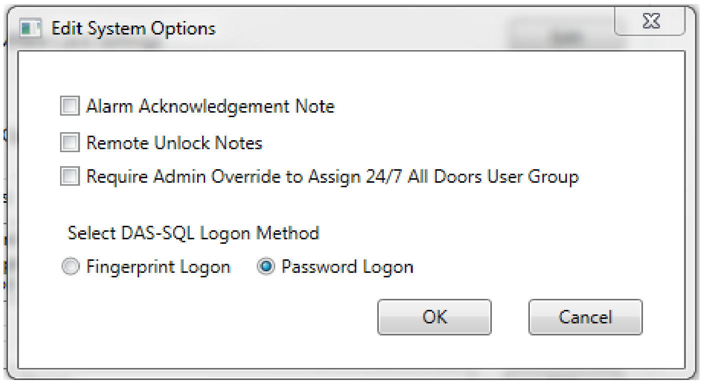


Edit User-Defined User Data Fields

☑ Field 1	SSN # □ Restricted	□ Field 7	 □ Restricted
☑ Field 2	DL # □ Restricted	□ Field 8	 □ Restricted
☑ Field 3	Address 1 □ Restricted	□ Field 9	 □ Restricted
☑ Field 4	Address 2 □ Restricted	□ Field 10	 □ Restricted
☑ Field 5	City □ Restricted	□ Field 11	 □ Restricted
□ Field 6	 □ Restricted	□ Field 12	 □ Restricted

4.13.4 – System Setup Tab – System Options

To change the "System Settings," click the "***Edit***" button for that section.



Edit System Options

□ Alarm Acknowledgement Note
□ Remote Unlock Notes
□ Require Admin Override to Assign 24/7 All Doors User Group

Select DAS-SQL Logon Method

○ Fingerprint Logon ● Password Logon

Alarm Acknowledgement Note - Works with the System Status tab and Alarm events. If selected, the operator will be required to enter a note when acknowledging alarms that have occurred in the system. These notes are stored in the database and can be reviewed via a report run from the reports tab.

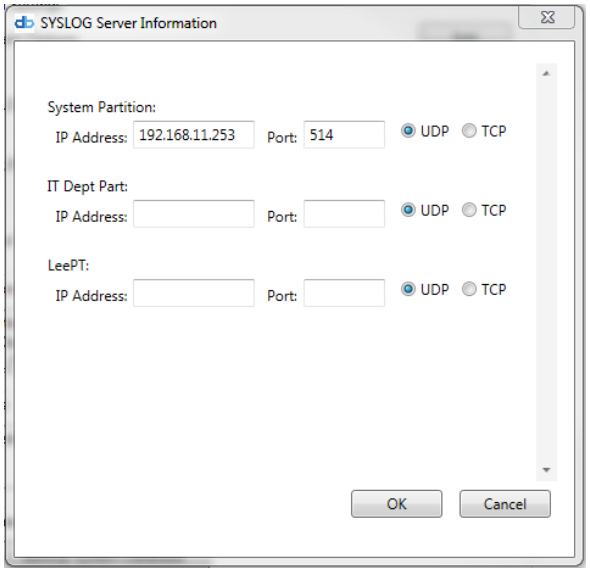
Remote Unlock Note - Similar to the Alarm Acknowledgement, this option requires the operator to provide a reason for a network unlock of a door. Again, this information is stored in the database and can be viewed via a report from the reports tab.

Require Admin Override to Assign 24/7 All Door User Group – If checked, a system administrator can only assign a user to the <Default 27/7 All Doors> User Group

DAS-SQL can use either **Fingerprint** authentication or **Password** authentication for logging into the DAS-SQL Client. This applies to all DAS-SQL software administrators.

4.13.5 – System Setup Tab – SYSLOG Settings

DAS-SQL is able to automatically push out all events via SYSLOG. You can enter a different SYSLOG server for each Partition defined in DAS-SQL.



System Partition:

IP Address: 192.168.11.253 Port: 514 ● UDP ○ TCP

IT Dept Part:

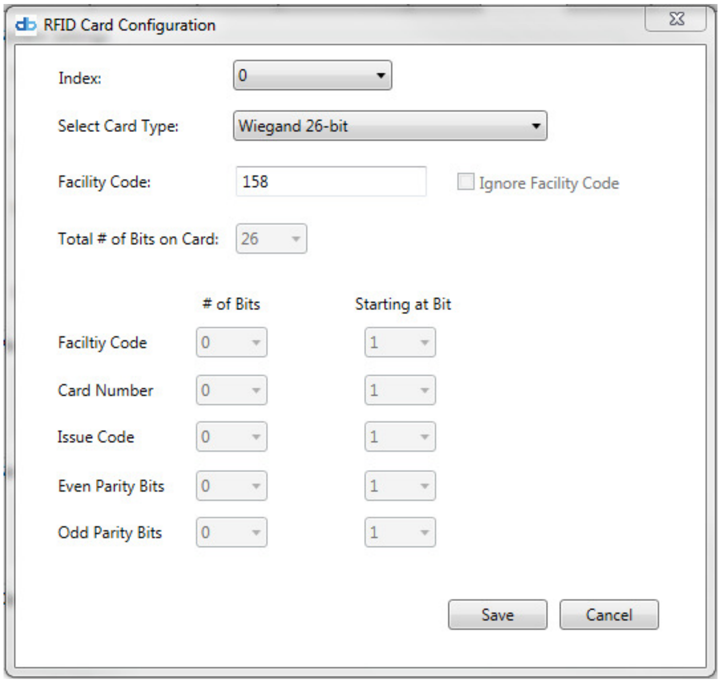
IP Address: Port: ● UDP ○ TCP

LeePT:

IP Address: Port: ● UDP ○ TCP

4.13.6 – System Setup Tab – Prox/Mifare Card Settings

Up to 8 different card types can be used simultaneously within the system. Using the screen below, select the next available Index number and configure the card type and facility code settings.



Index: 0

Select Card Type: Wiegand 26-bit

Facility Code: 158 ☐ Ignore Facility Code

Total # of Bits on Card: 26

	# of Bits	Starting at Bit
Faciltiy Code	0	1
Card Number	0	1
Issue Code	0	1
Even Parity Bits	0	1
Odd Parity Bits	0	1

4.13.6 – System Setup Tab – iClass Card Settings

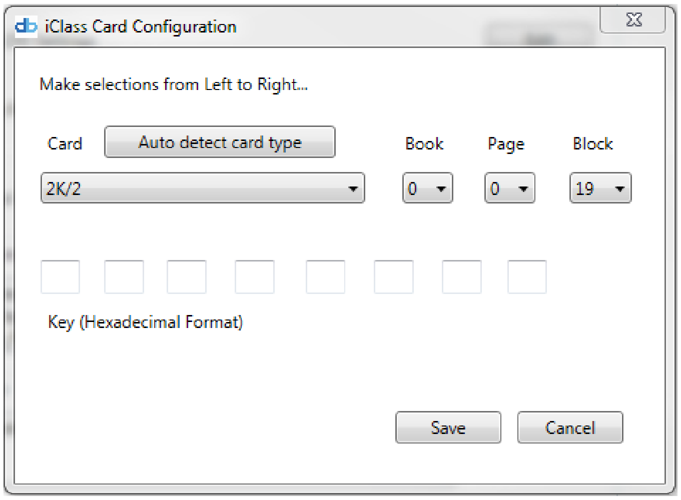
Using the screen below iClass Cards can be configured.

The card type can be automatically detected by placing a card on the Omnikey reader and clicking *"**Auto detect card type**"* button. Alternatively and card type card can be manually selected.

Once the correct card has been selected, chose the Book, Page and Block locations that Digitus will use to store its data on the iClass Card. If the cards are being used with another 3rd-party system, you should specify a different location than is being used by the 3rd-party system.

Enter an 8-byte Encryption Key (in hexadecimal format).

Note: this key should only be changed one-time and should be set prior to programming any iClass cards.


iClass Card Configuration

Make selections from Left to Right...

Card: 2K/2

Book: 0

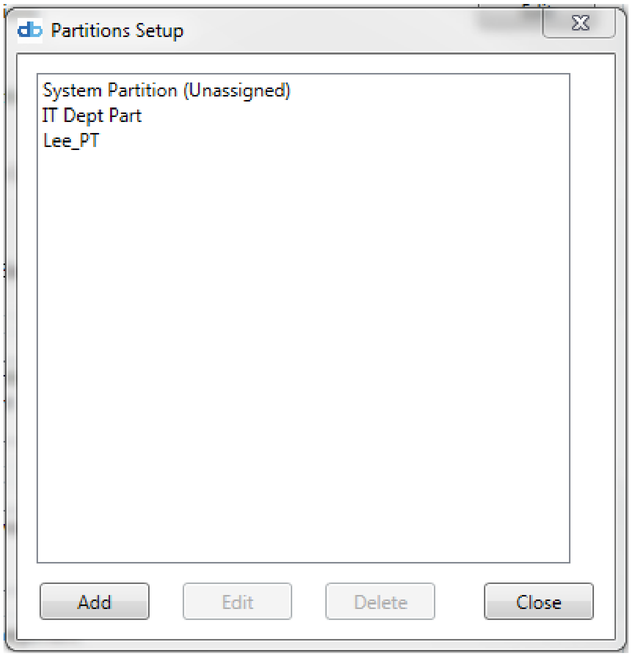
Page: 0

Block: 19

Key (Hexadecimal Format)

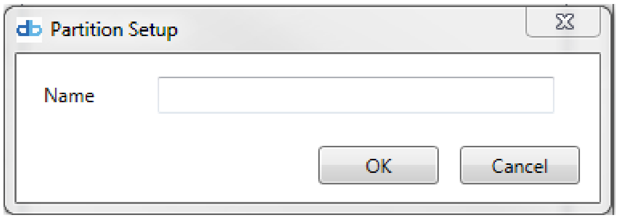
4.13.7 – System Setup Tab – Partitions

The Partitions section lists currently configured Partitions. To edit or add Partitions, click the respective buttons.


Partitions Setup

System Partition (Unassigned)
IT Dept Part
Lee_PT

To **add** a new Partition, click the "***Add***" button. To **edit** an existing Partition, select that Partition from the list and click the "***Edit***" button. To **delete** a Partition, select that Partition and click the "***Delete***" button. When editing or adding a Partition, the following form is displayed.



NOTE: "System Partition (Unassigned)" cannot be edited or deleted.

Explanation of Partitions:

Partitions are used to create "virtual systems" within a larger system. By default (if no partitions are configured) every object is accessible or "visible" to every other object. For example, any User who has Personnel setup permission can see all User records and assign permissions to those Users (except that only Administrators can assign permissions to other Administrators). Likewise, Users can see, and be assigned permissions for, all Devices, Zones, User Groups, and Departments.

It is sometimes desirable to "segment" or partition the system into sections that are visible only to Users within those sections. For example, a system might be used to control access in a number of buildings, and the Users restricted to access or control within those buildings. By creating a Partition, a User with "Monitor" permission can see only Doors within that Partition. Thus a User can control and monitor certain Doors in a system and not even know other doors exist.

Likewise, a User with "Personnel" setup permission might be restricted to assigning access to certain Doors and certain Users and not even know other Doors or Users exist.

By default, objects (Users, Devices, Departments, etc.) that are not specifically assigned to a Partition are in the "System Partition (Unassigned)". That means they are visible to all Users and have access (or can be assigned access) to all devices. Once an object has been assigned to at least one Partition, it is no longer visible to Users or has access to devices in other Partitions.

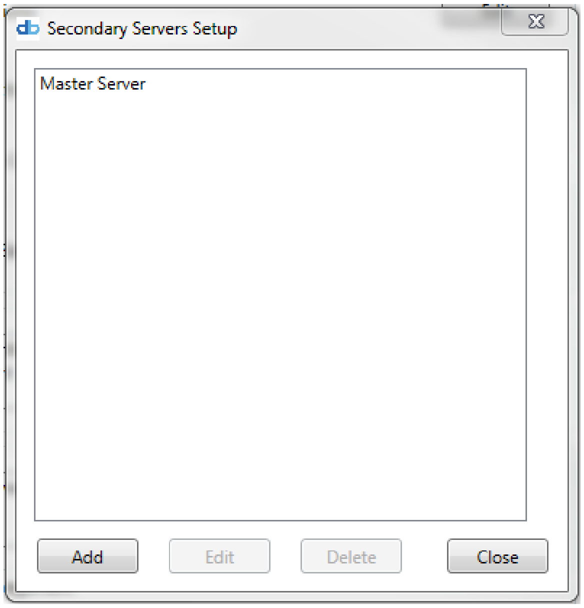
Only Users with "System Administrator" permissions can create, edit, or delete Partitions. System Administrators can view all objects (Users, Devices, Departments, etc.) regardless of their assigned Partitions.

"Partition Administrators" have Monitor, Personnel, and System configuration permission to any objects in Partitions to which they are assigned. A System Administrator must assign Partitions to a Partition Administrator. Partition Administrators can assign Partitions to objects in their Partitions, but objects in other Partitions will not be visible or accessible to Partition Administrators.

In practical terms, this means that any User assigned to one or more Partitions can be assigned access only to Devices, Zones, or User Groups in those Partitions. Users who are monitoring the system will see only Devices, and receive events and alarms for Devices, in the Partitions to which they are assigned. Users with setup permissions will see only Users, Devices, Departments, Zones, and User Groups in the Partitions to which they are assigned. Thus, objects in Partitions to which a User is not assigned will be invisible to that User.

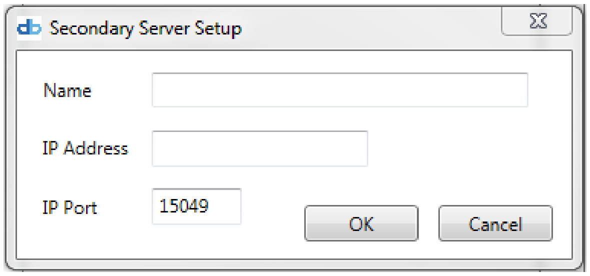
4.13.8 – System Setup Tab – Servers

To **add, edit,** or **delete** a server, click the "***Edit***" button in the Server section of the System Tab screen. A default "Master Server" should be the only server if there are no plans to have additional servers running on the network.



Master Server

To **add** a new server, click the "***Add***" button.



IP Port 15049

Within the Add window, create a Name and add the IP address and Port that DAS-SQL will use to communicate with new server.

To **delete** a server, select the server and click the "***Delete***" Button

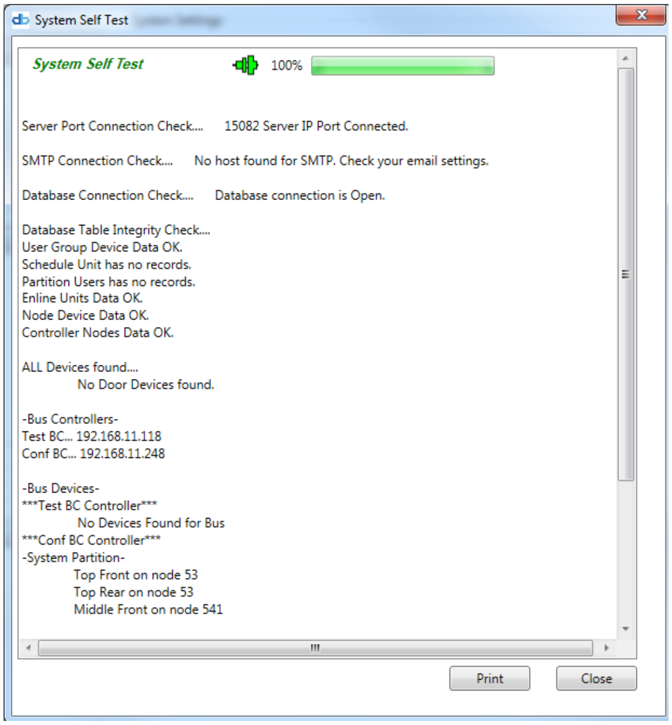
Note: Only servers other than the "Master Server" can be edited or deleted.

4.13.9 – System Setup Tab – Database Management

The "***Backup System Database***" button will create a full copy of the current Databases and store it in a backup folder on the SQL Server.

4.13.10 – System Setup Tab – System Wide Test

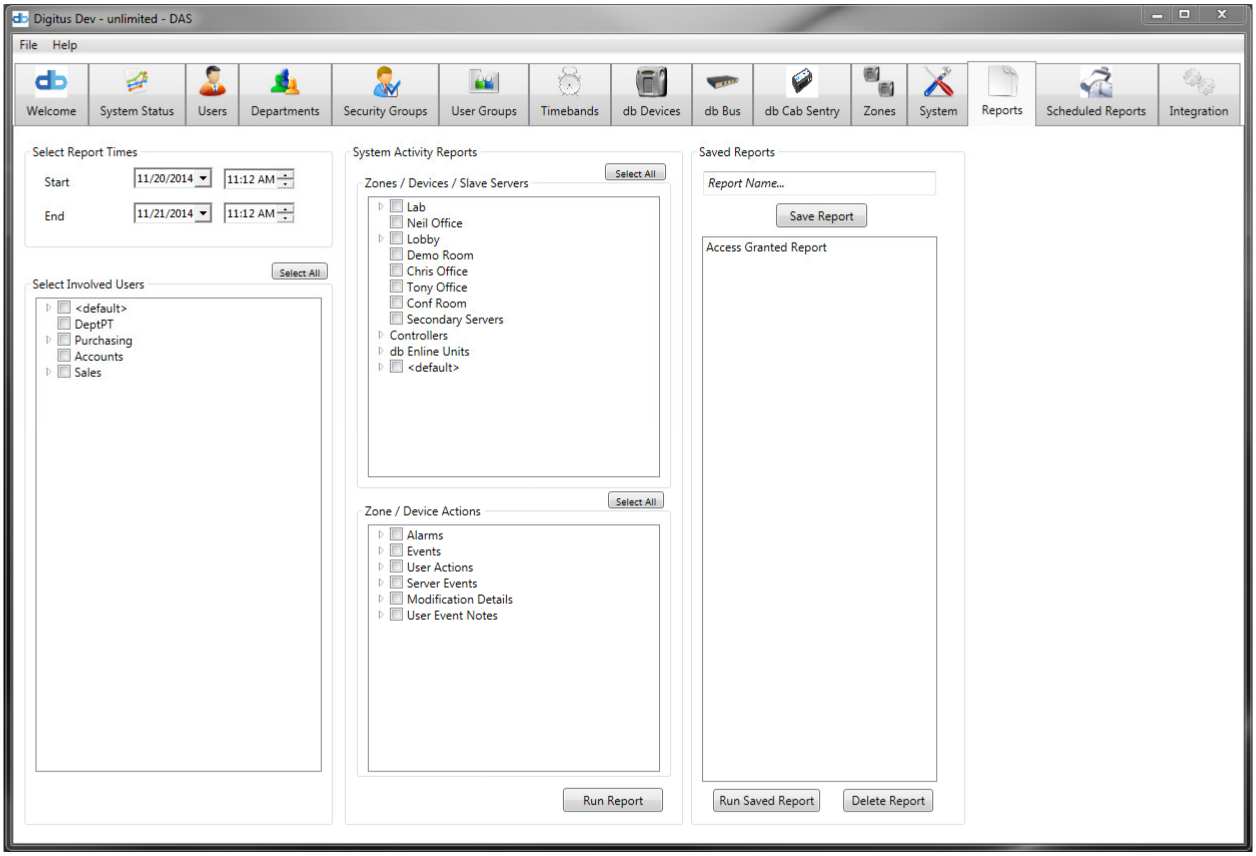
The "***Run System Wide Test***" button runs a health check of the entire system. It checks things like the server connection, the SMTP connection, a database connection check, and various data integrity checks and also checks the status of all devices in the system.



```
Server Port Connection Check....     15082 Server IP Port Connected.

SMTP Connection Check....     No host found for SMTP. Check your email settings.

Database Connection Check....     Database connection is Open.

Database Table Integrity Check....
User Group Device Data OK.
Schedule Unit has no records.
Partition Users has no records.
Enline Units Data OK.
Node Device Data OK.
Controller Nodes Data OK.

ALL Devices found....
            No Door Devices found.

-Bus Controllers-
Test BC... 192.168.11.118
Conf BC... 192.168.11.248

-Bus Devices-
***Test BC Controller***
            No Devices Found for Bus
***Conf BC Controller***
-System Partition-
           Top Front on node 53
           Top Rear on node 53
           Middle Front on node 541
```

4.14 –Reports Tab

The “Report Tab” allows users to run various reports against operation events, alarms, user actions, user modifications, server events, user notes of events and other data captured by the DAS-SQL system. See (Section 6) for further details on Reports and Printing.



Start 11/20/2014 11:12 AM

End 11/21/2014 11:12 AM

Reports selection is broken down into four sections.

Report times - Allows you to search for events and/or alarms within a specific time period.

Involved Users - Allows you to determine which users in the system the report should contain. Users are grouped by department.

Note: Users in red are deleted users.

Zones/ Devices/ Slave Servers – Allows you to select which Devices, db Enline Units and secondary servers to contain in the report. Devices are grouped by zone.

Zone/ Device Actions - Allow you to select which event types and/or alarms to contain in the report.

NOTE: Any combination of alarm event report can be run simultaneously with the exception of “Modification Details” and “User Event Notes”. These two items cannot be run with any other criteria, and will de-select all other selected items, if checked.

Saved Reports – Reports can be saved to run again at a later date. To save a report, first select the desired criteria and provide a “Report Name” in the text field, then click the “Save Report” button. The saved report will immediately show up in the saved report list view.

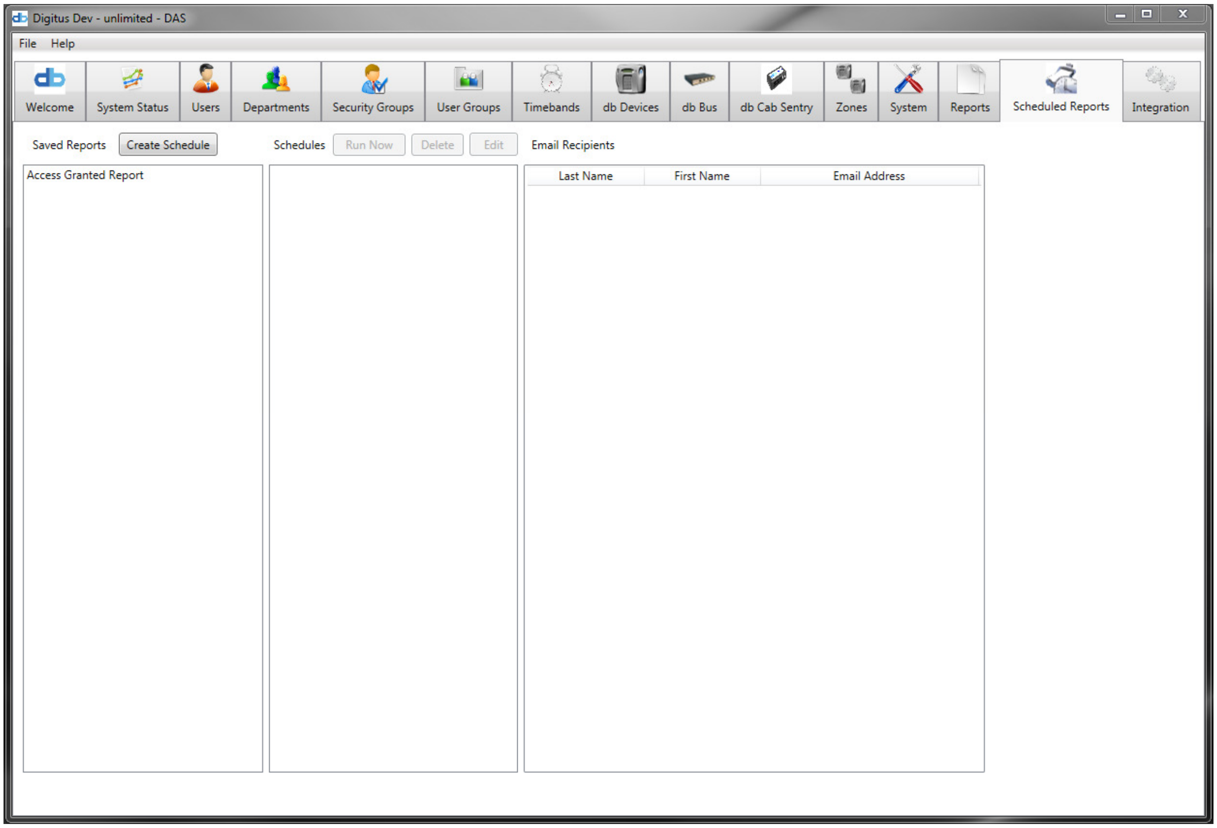
To “Run” a saved report, select the desired report name and the desired timeframe from “Report Times” and clicking the “Run Saved Report” button.

To delete a saved report, select the report in the list and click the “Delete Report” button. Before the delete occurs, you are prompted to confirm the delete action.

NOTE: Saved reports work in conjunction with Scheduled Reports. A saved report must be present before a schedule can be created.

4.15 – Scheduled Reports Tab

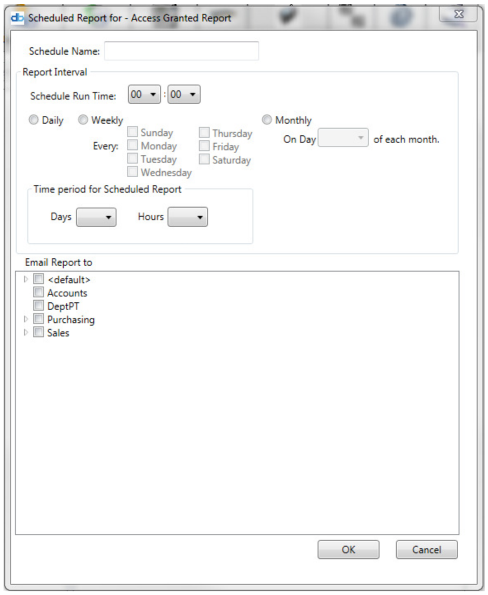
Scheduled Reports are saved reports that are automatically generated by the system and emailed to a number of recipients at specified time intervals.



Access Granted Report

Located on the Scheduled Reports tab are three list views that supply the user with a list of saved reports, a list of schedules for each saved report, and the recipients for each schedule.

To create a schedule, left-click a saved report from the "Saved Reports" list and click the "Create Schedule" button, or right-click saved report and select "Create Schedule" from the pop-up menu, the screen below will be displayed.


Scheduled Report for - Access Granted Report
Report Interval
Time period for Scheduled Report
Email Report to
OK
Cancel

Schedule Name:

Schedule Run Time: 00 : 00

○ Daily ○ Weekly ○ Monthly

Every: □ Sunday □ Monday □ Tuesday □ Wednesday □ Thursday □ Friday □ Saturday

On Day of each month.

Days Hours

□ <default>
□ Accounts
□ DeptPT
□ Purchasing
□ Sales

Select Name – User defined name for the schedule.

Report Interval box

Schedule Run Time – This is the time the report will run and be sent out to all recipients.

Select **Daily, Weekly,** or **Monthly** to determine the frequency of the scheduled report. If Weekly is selected, choose which day(s) of the week the report is to be run. If Monthly is selected, choose which day of the month the report is to be run.

Time Period for Scheduled Report - This is the amount of historic data that will be contained in the scheduled report. E.g. If a report is selected to run daily at 00 00, with "Days" set to 1, then the report would run each day at midnight and include the past 24 hours of data.

Email Report to – Determines which users will receive the scheduled report via email.

Click "OK' to save the schedule.

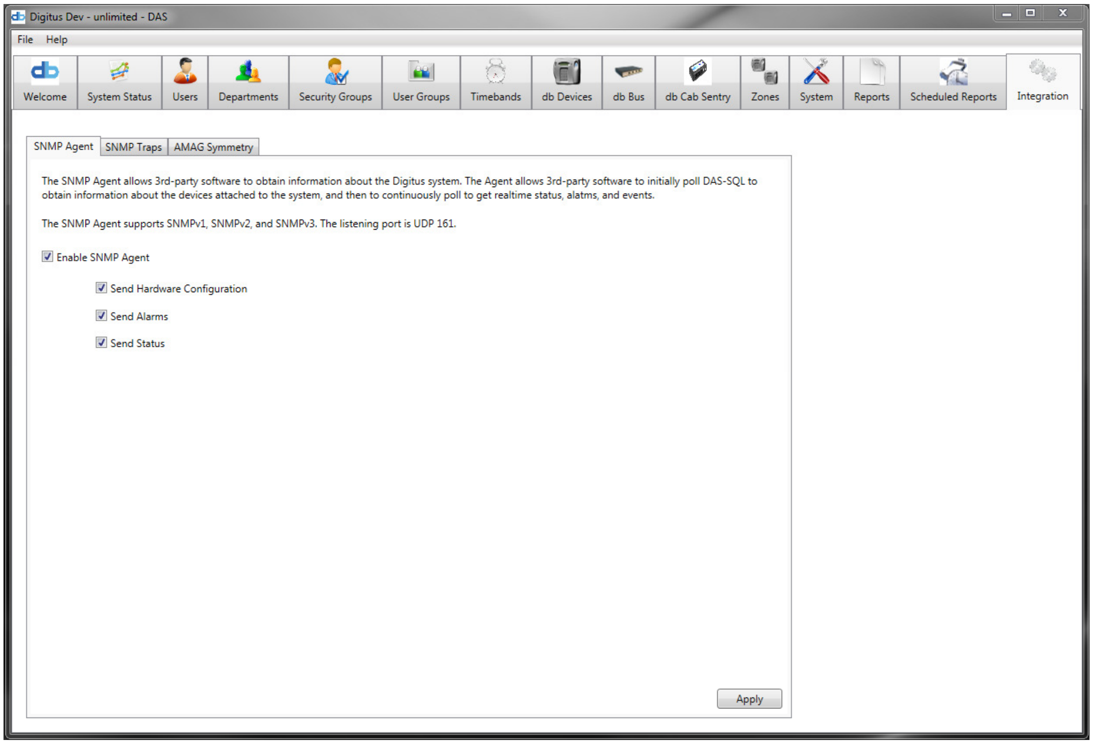
To **edit** or **delete** a scheduled report, select the report from the "Saved Reports" list, and then select the scheduled report that is to be edited or deleted. Once selected, the edit and delete buttons, which are at the top of the scheduled list, will become active and available to the user.

4.16 – Integration Tab

The “Integration Tab” allows users to enable SNMP agents and traps for communication with 3rd-party applications for monitoring as well as AMAG Symmetry integration.

4.16.1 – SNMP Agent Tab

Enable SNMP Agent and select what is available for 3rd-party monitoring.



The SNMP Agent allows 3rd-party software to obtain information about the Digitus system. The Agent allows 3rd-party software to initially poll DAS-SQL to obtain information about the devices attached to the system, and then to continuously poll to get realtime status, alatms, and events.

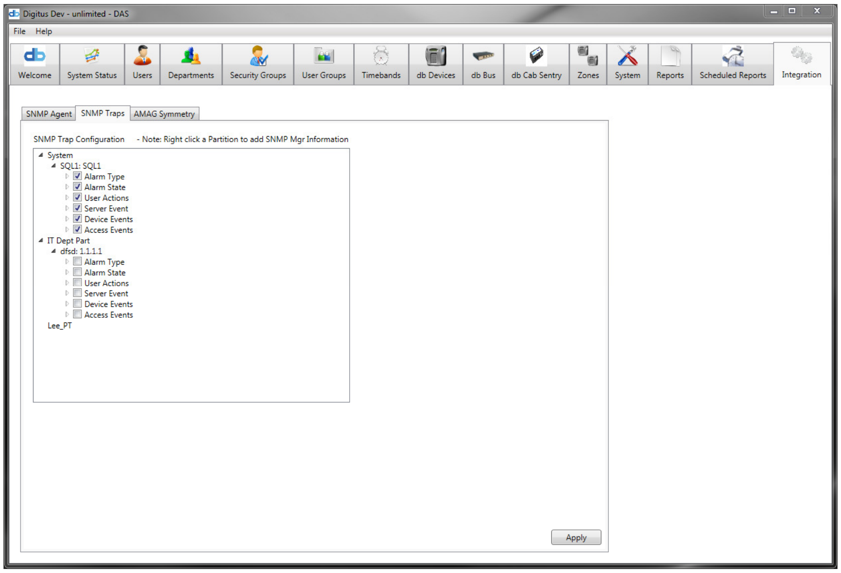
The SNMP Agent supports SNMPv1, SNMPv2, and SNMPv3. The listening port is UDP 161.

☑ Enable SNMP Agent

- ☑ Send Hardware Configuration
- ☑ Send Alarms
- ☑ Send Status

4.16.2 – SNMP Traps Tab

Enable and configure SNMP traps by Partition.



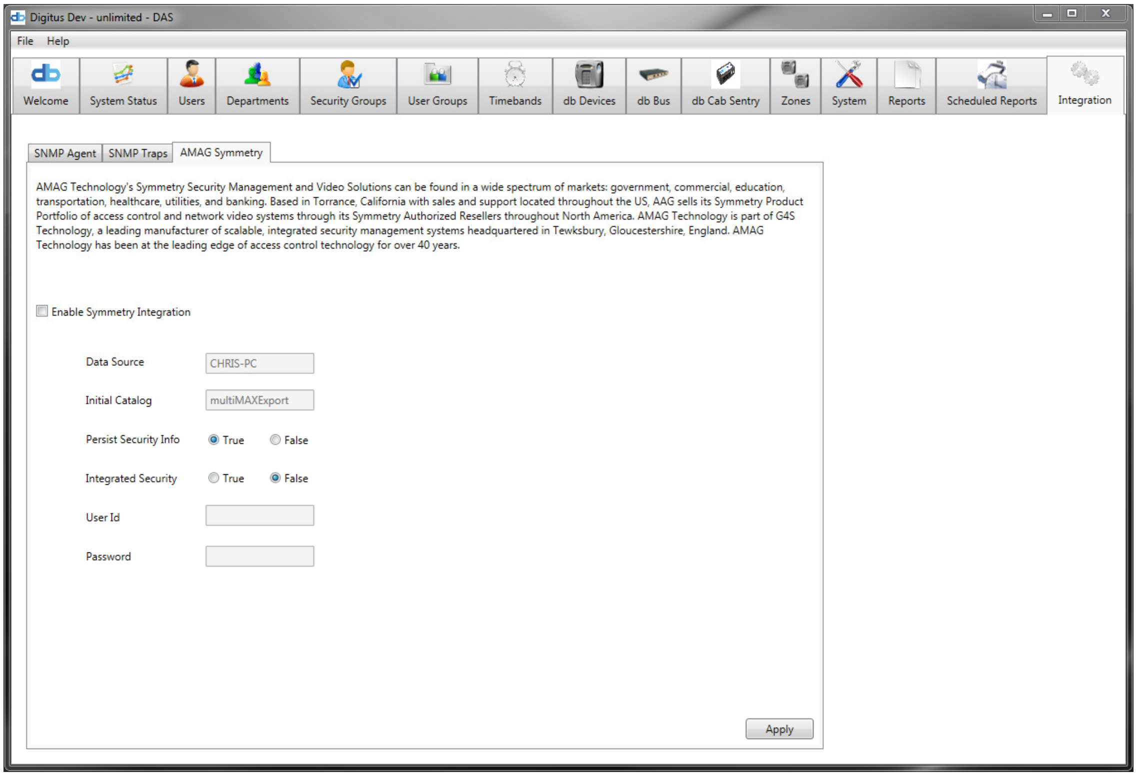
SNMP Trap Configuration - Note: Right click a Partition to add SNMP Mgr Information

- System
  - SQL1: SQL1
    - ☑ Alarm Type
    - ☑ Alarm State
    - ☑ User Actions
    - ☑ Server Event
    - ☑ Device Events
    - ☑ Access Events
- IT Dept Part
  - dfsd: 1.1.1.1
    - □ Alarm Type
    - □ Alarm State
    - □ User Actions
    - □ Server Event
    - □ Device Events
    - □ Access Events
- Lee_PT

NOTE: Right click on a Partition to add SNMP Manager Information.

4.16.3 – AMAG Symmetry Tab

Enables Symmetry Integration



AMAG Technology's Symmetry Security Management and Video Solutions can be found in a wide spectrum of markets: government, commercial, education, transportation, healthcare, utilities, and banking. Based in Torrance, California with sales and support located throughout the US, AAG sells its Symmetry Product Portfolio of access control and network video systems through its Symmetry Authorized Resellers throughout North America. AMAG Technology is part of G4S Technology, a leading manufacturer of scalable, integrated security management systems headquartered in Tewksbury, Gloucestershire, England. AMAG Technology has been at the leading edge of access control technology for over 40 years.

☐ Enable Symmetry Integration

Data Source: CHRIS-PC

Initial Catalog: multiMAXExport

Persist Security Info: ● True ○ False

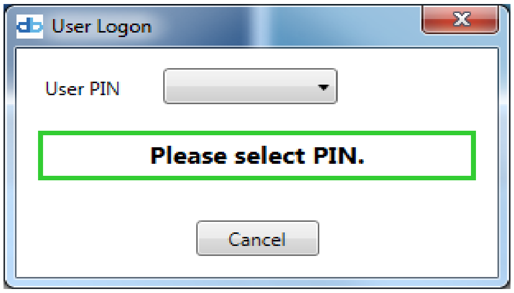
Integrated Security: ○ True ● False

User Id:

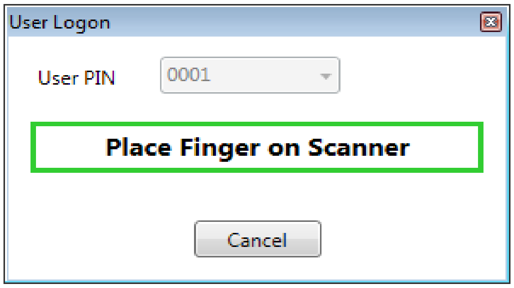
Password:

Section 5 – Monitoring and Controlling the DAS-SQL System

The status of the DAS-SQL system can be monitored from the DAS-SQL client. Logging onto the client is as described in Section 3. Simply start the client, select the “File” menu, and select the “Logon” menu item from the File menu. When the Logon form is displayed, select the appropriate User PIN and place your finger on the scanner or enter your password as indicated.



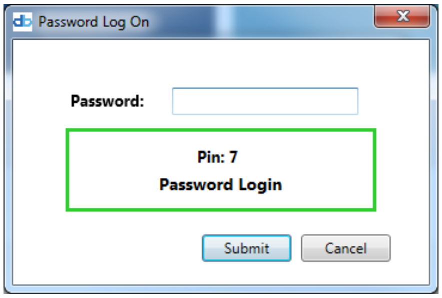
Please select PIN.



User PIN: 0001

Place Finger on Scanner

Or



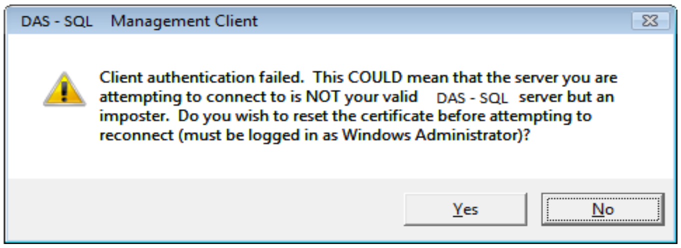
Pin: 7
Password Login

If the logon succeeds, and the User has Monitor permissions, the System Status tab will be enabled.

The System Status tab has several controls to display various types of events and states.

Note: DAS-SQL clients communicate with the server via secured sockets. These sockets use a certificate which is created by, and stored on, the server. The first time a client connects to the server a record is made on the client of the server’s certificate identifier. If the client attempts to connect to another server, perhaps an application impersonating the DAS-SQL server, the client authentication will fail, as the application’s certificate will not match the server’s certificate identifier stored on the client.

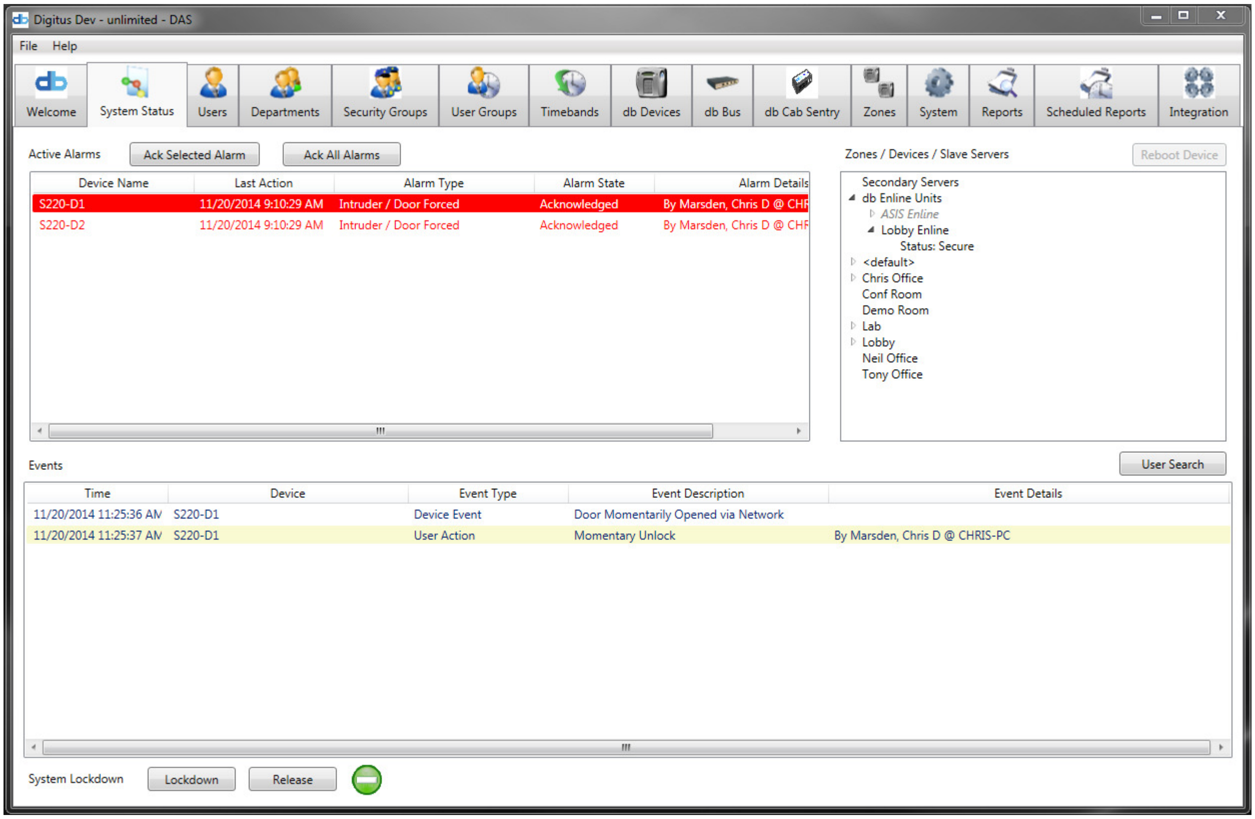
If the server’s certificate is changed, due to re-installing the server or other problems, the server’s certificate will no longer match the certificate identifier stored on the client, and the logon and connection will fail. An error message (below) will be displayed.



Client authentication failed. This COULD mean that the server you are attempting to connect to is NOT your valid DAS - SQL server but an imposter. Do you wish to reset the certificate before attempting to reconnect (must be logged in as Windows Administrator)?

If the User knows the server’s certificate has changed, and trusts the server, the server certificate identifier on the client can be reset to accept a new certificate from the server. To do this, click the “Yes” button on the message box.

Note: for security reasons, the User MUST be logged into Windows as a Windows Administrator to reset the certificate.



Device Name	Last Action	Alarm Type	Alarm State	Alarm Details
S220-D1	11/20/2014 9:10:29 AM	Intruder / Door Forced	Acknowledged	By Marsden, Chris D @ CHF
S220-D2	11/20/2014 9:10:29 AM	Intruder / Door Forced	Acknowledged	By Marsden, Chris D @ CHF

Secondary Servers
db Enline Units
ASIS Enline
Lobby Enline
Status: Secure
<default>
Chris Office
Conf Room
Demo Room
Lab
Lobby
Neil Office
Tony Office

Time	Device	Event Type	Event Description	Event Details
11/20/2014 11:25:36 AM	S220-D1	Device Event	Door Momentarily Opened via Network	
11/20/2014 11:25:37 AM	S220-D1	User Action	Momentary Unlock	By Marsden, Chris D @ CHRIS-PC

Active Alarms List

The upper left section of the screen above is the Active Alarms control. This control displays any active Door alarms. Possible alarm types are as follows:

Door Forced – This alarm is generated when a Door is forced open while locked. The Door must be configured to process door forced alarms (“Enable Door Forced Alarms” must be checked). The door forced alarm has three (3) states: Active, Cleared, and Acknowledged. The Active state means the alarm has been received but no User interaction (acknowledgement) has taken place, and the door has not been shut. The Cleared state means the door has been closed (the point has reset). The Acknowledge state means that a User has acknowledged the alarm from a DAS-SQL client. When the alarm has been both cleared and acknowledged (in either order) the alarm will be removed from the Active Alarms list and the door buzzer will quit sounding.

Door Held – This alarm is generated when a Door is held open beyond its assigned “Propped Door” time. The door held/propped alarm has three (3) states: Active, Cleared, and Acknowledged. The Active state means the alarm has been received but no User interaction (acknowledgement) has taken place, and the door has not been shut. The Cleared state means the door has been shut (the point has reset). The Acknowledge state means that a User has acknowledged the alarm from a DAS-SQL client. When the alarm has been both cleared and acknowledged (in either order) the alarm will be removed from the Active Alarms list and the door buzzer will quit sounding.

Duress Alarm – This alarm is generated when a User biometrically authenticates at a Device with a finger defined as a “duress finger.” The duress alarm has two (2) states: Active and Acknowledged. The Active state means the alarm has been received but no User interaction (acknowledgement) has taken place. The Acknowledge state means that a User has acknowledged the alarm from a DAS-SQL client. When the alarm has been acknowledged the alarm will be removed from the Active Alarms list. Duress alarms should be considered highest priority alarms.

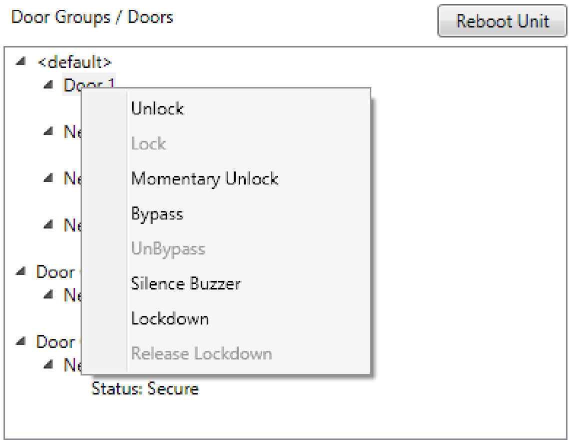
Tamper Alarm – This alarm is generated when the Device tamper switch is activated. The tamper alarm has three (3) states: Active, Cleared, and Acknowledged. The Active state means the alarm has been received but no User interaction (acknowledgement) has taken place, and the tamper switch has not reset. The Cleared state means the tamper switch has been reset. The Acknowledge state means that a User has acknowledged the alarm from a DAS-SQL client. When the alarm has been both cleared and acknowledged (in either order) the alarm will be removed from the Active Alarms list and the door buzzer will quit sounding.

Zones / Device List

At the upper right of the screen is the Zones / Device control. This control provides access to status and control features of each Device on the system. The Devices are organized under their assigned Zone. To view the Devices in a zone, expand the Zone. To see the status of an individual Device, expand that Device node.

Device Control

To control a Device, right-click the Device and a popup menu will list the permitted commands.



Status: Secure

To send a command to the Device, select the command from the menu. It normally will take less than two (2) seconds for a command to execute and the new status will be displayed for the affected Device. An “Action Request By User” transaction will appear in the “Events” list, followed by the appropriate “Unit Event” when (and if) the requested action occurs.

The supported Door commands are:

Unlock/Relock – These commands will unlock or re-lock a Door for an indefinite amount of time. Manually unlocking a Door will override any door forced or door held alarm while the Door is unlocked. A Door can be unlocked or relocked by any User having Monitor permissions.

Momentary Unlock – This causes the Door release relay to activate for the time period defined for normal access events (the “Entry Delay” value defined for the Device). The Door will relock automatically when the Entry Delay time is reached.

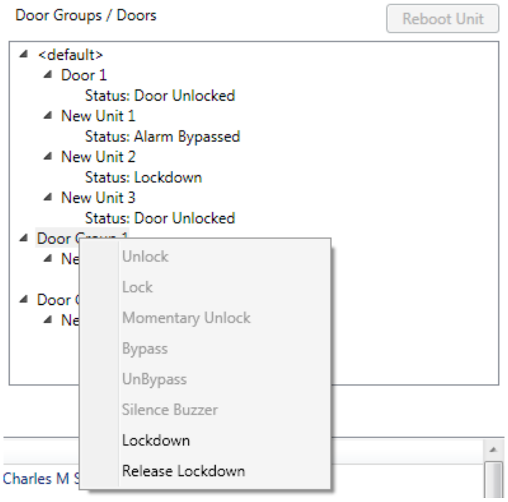
Bypass/Unbypass – These commands cause the DAS-SQL server to ignore any door forced, door held, or tamper alarms while the Door alarms are bypassed. Duress alarms will still be processed. The Device buzzer WILL STILL SOUND if a door forced or door held alarm occurs, but the alarm will not be annunciated at the DAS-SQL client.

Silence Buzzer – This command will send a “Silence Buzzer” command to the Device. It will be effective only if 1) the buzzer is sounding and 2) the alarm triggering point (door switch, tamper switch) has been reset to normal state. A “Silence Buzzer” command is useful if the alarm event processing becomes “out of order” and the buzzer does not quit sounding after the alarm point resets and the alarm is acknowledged (i.e., it is a manual “silence” command to override normal alarm processing).

Lockdown/Release Lockdown – These commands force the Device into (or release from) the lockdown state. In the lockdown state, the Device will not allow any Users access to the controlled area. Releasing the lockdown will allow the Door to function normally.

Zone Control

To control a Zone, select the Zone node and right-click. A popup menu will list the permitted commands.



To send a command to the Zone, select the command from the menu. It normally will take less than two (2) seconds for a command to execute and the new status will be displayed for the affected Device(s). An "Action Request By User" transaction will appear in the "Events" list for each Device, followed by the appropriate "Unit Event" when (and if) the requested action occurs.

The supported Zone commands are:

Lockdown/Release Lockdown – These commands force all Devices in the Zone into (or release from) the lockdown state. In the lockdown state, the affected Devices will not allow any Users access to the controlled area. Releasing the lockdown will allow the affected Devices to function normally. It is possible to lockdown or release from lockdown any individual Device in the Zone independently, regardless of the lockdown state of the Zone.

Reboot Unit Command

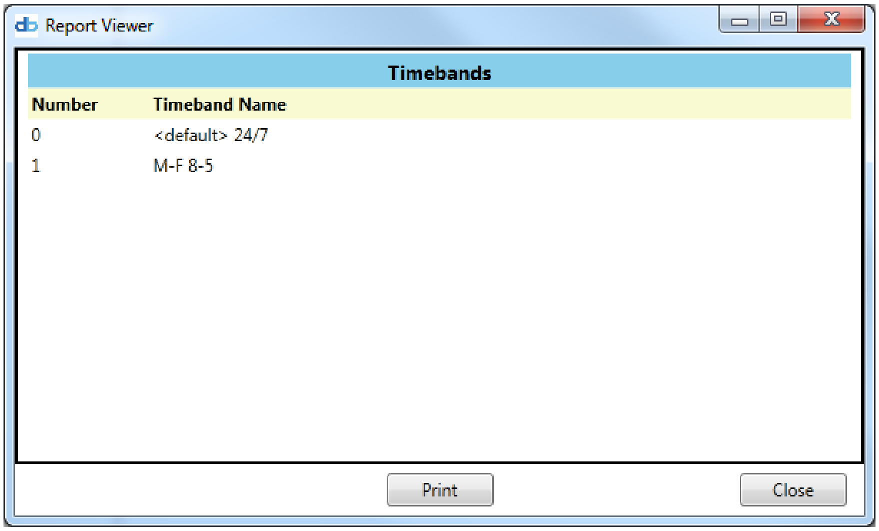
It may become necessary at times to force a Device to perform a "soft reboot" to restore it to normal operation. This is very rare, and if the Device stops functioning properly, it is normally either a configuration error, a hardware problem (requiring repair), or a network communication issue. However, it is sometimes helpful (at least as a first step in diagnosing a problem) to reboot the Device from the DAS-SQL client. To reboot a Device, select the Device from the Zones / Devices list and click the "Reboot Unit" button.

Normally the Device (if reboot is successful) will go offline and come back online within a few seconds.

If the problem is not corrected after rebooting the Device, the next step is usually to power cycle the unit ("hard reboot"), and then begin more intensive troubleshooting procedures.

Section 6 – System Reports

System reports are available in a variety of places. Normally there is a "Print" button on each tab to print out the list of items in that tab. The list is displayed in a formatted form, as in the example Timebands report below.

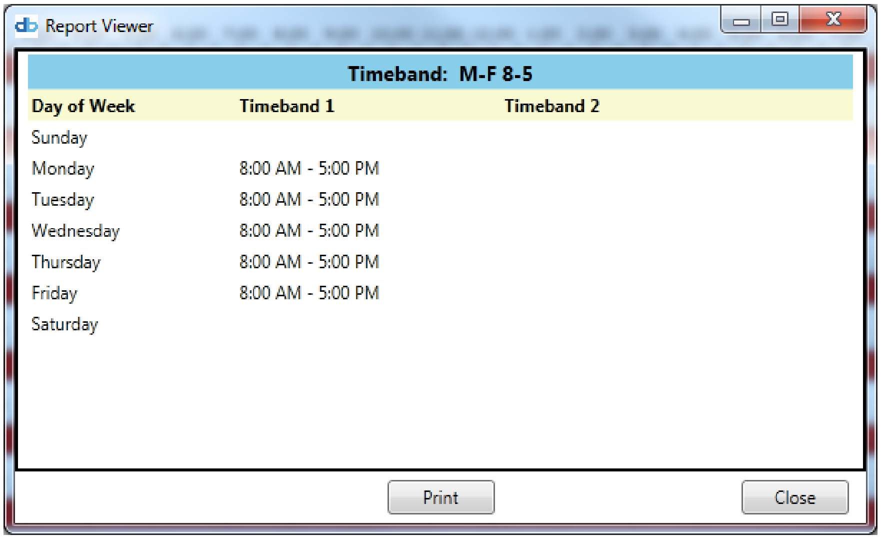


Timebands

Number	Timeband Name
0	<default> 24/7
1	M-F 8-5

To **print** the report to a printer, click the "Print" button on the Report Viewer form.

To **print** a report for an individual item, such as the "M-F 8-5" Timeband listed above, open the setup form for that Timeband and click the "Print" button on the form. Here is a report on that Timeband:

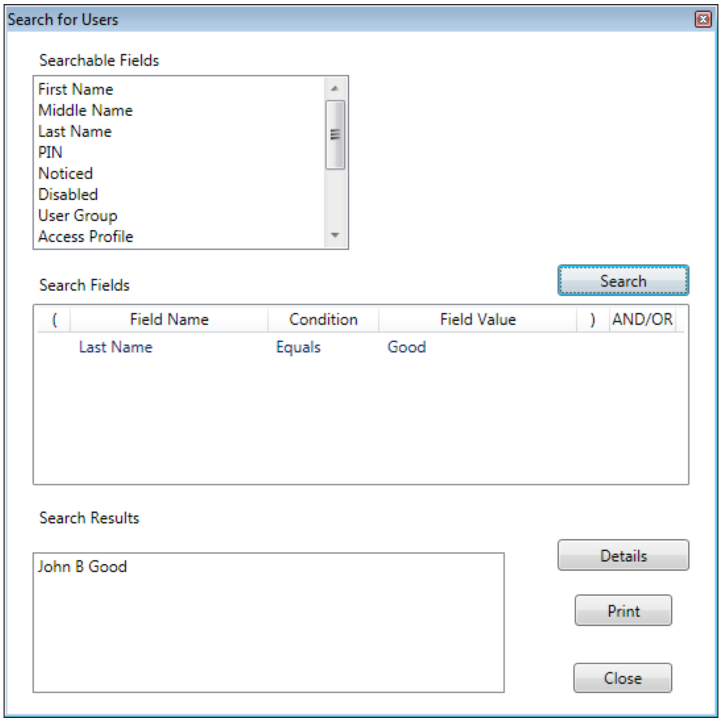


Timeband: M-F 8-5

Day of Week	Timeband 1	Timeband 2
Sunday		
Monday	8:00 AM - 5:00 PM	
Tuesday	8:00 AM - 5:00 PM	
Wednesday	8:00 AM - 5:00 PM	
Thursday	8:00 AM - 5:00 PM	
Friday	8:00 AM - 5:00 PM	
Saturday		

Most configuration tabs and forms have "***Print***" buttons on them to create a System Report.

The System Status tab also allows searching for Users by data fields. Click the "***User Search***" button and the search form appears.



Search for Users

Searchable Fields

First Name
Middle Name
Last Name
PIN
Noticed
Disabled
User Group
Access Profile

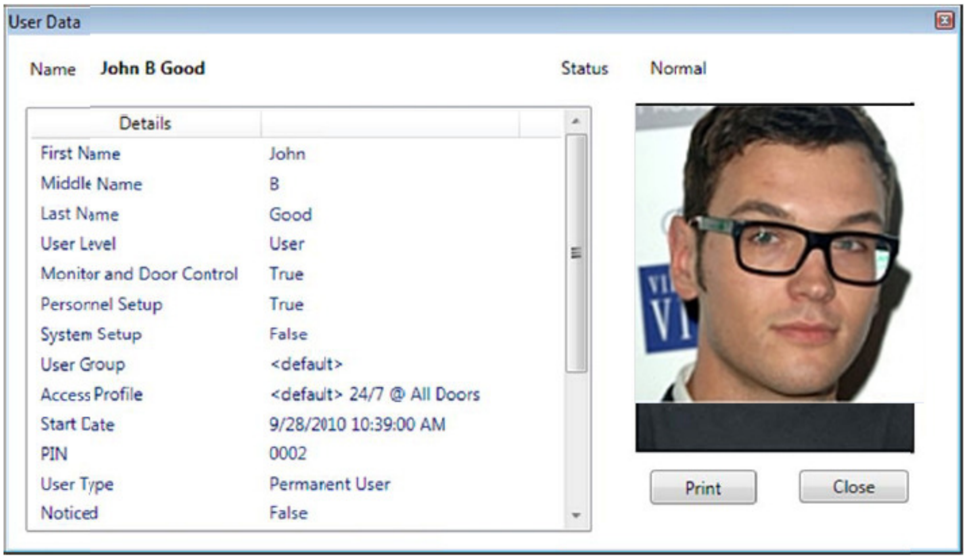
Search Fields

(	Field Name	Condition	Field Value	)	AND/OR
	Last Name	Equals	Good		

Search Results

John B Good

To perform a search, drag the search field item from the “Searchable Fields” control into the “Search Fields” control. Select the “Field Value” and enter the data (in this case the last name). Nested (“ ((...) AND (...)) “) search parameters can be defined for complex searches. When all the search parameters are selected, click the “***Search***” button. The list of matching Users will appear in the “Search Results” control. Select the desired User and click “Details” (or double-click the User) to display the following form:



User Data

Name **John B Good** Status Normal

Details	
First Name	John
Middle Name	B
Last Name	Good
User Level	User
Monitor and Door Control	True
Personnel Setup	True
System Setup	False
User Group	<default>
Access Profile	<default> 24/7 @ All Doors
Start Date	9/28/2010 10:39:00 AM
PIN	0002
User Type	Permanent User
Noticed	False

This data can be printed by clicking the “Print” button.

Appendix A – Maintenance Issues

Replacing a Device Unit

A Device contains all Timebands defined on the system and all Users who have access to that Device (determined by the User Group). When a new Device unit is installed to replace an existing one, the Timeband and User information must be uploaded to that Device.

After the Device has been replaced, it must be configured in the DAS-SQL client. Once the new Device is configured, all Timebands will be uploaded to it automatically (though this might take several minutes, depending on how many Timebands are configured).

To upload the Users assigned to that Device (by the User Groups), it is necessary to remove the Device from any User Group to which it has been assigned, and re-add the Device to the User Group. This should be done in two steps: Remove the Device, click "Save", re-edit the User Group, and re-add the Device to the User Groups. This will cause the Users assigned to the User Groups to be uploaded to the new Device. This might take up to an hour, depending on the size of the system. A good rule of thumb is that it takes approximately 10 seconds per User if two (2) fingerprint templates are used. Add another two (2) seconds for each additional fingerprint. Thus, if a User has three fingerprints assigned (two normal and one for duress), it will take approximately 12 seconds to upload that User's data to the Device. If a User Group is assigned to 100 Users, it will take approximately 20 minutes to upload the Users to a Device.

DIGITUS
BIOMETRICS
Access Security Solutions

Digitus Biometrics, Inc.
2 East Bryan Street, Ste 502
Savannah, GA 31401 USA

Phone: 912-231-8175
Fax: 912.629.9478
www.digitus-biometrics.com
support@digitus-biometrics.com

Specifications subject to change without notice.