EchoOneApp Security

Overview

EchoOneApp has an advanced, self-contained security system that allows a full range of permissions to be applied at both the user and group level. Access can be granted to data (items in the tree), screens, fields and combinations of each. The levels of access are defined as *Full Access, Edit Only, Read Only and Deny.*

Getting Started

Setting up the security in EchoOneApp is accomplished through these steps:

1. Creating the users and groups
2. Defining the security items
3. Setting access levels to the security items

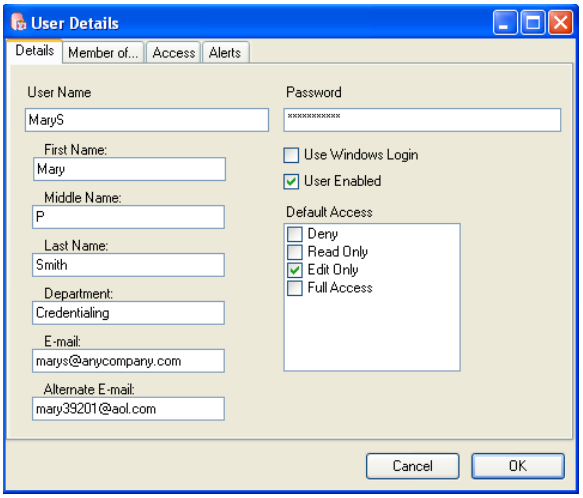
Users and Groups

Security settings can be applied at both the User and Group level. If there are several individuals using the software who will have the same security settings, it is easier to apply the settings to a group and make those users members of the group. If each user requires different security settings, the settings can be applied directly to each user. If a user is a member of a group and the user settings conflict with the settings of the group, the user settings will override those of the group.

Creating Users and Groups

Users:

To create a new user, click *Configure > Security*, or click the Security button in the toolbar. EchoOneApp includes three default users: Admin, Edit Only and Read Only. A new user must be created for each individual who uses EchoOneApp. Click the *Add* button to create a new user account.



User Name: MaryS

Password: ***********

First Name: Mary

Middle Name: P

Last Name: Smith

Department: Credentialing

E-mail: marys@anycompany.com

Alternate E-mail: mary39201@aol.com

□ Use Windows Login

☑ User Enabled

Default Access

□ Deny
□ Read Only
☑ Edit Only
□ Full Access

User Name: Enter the login name for the user. The User Name is not case sensitive. The user name must match the user’s Windows login name for the Windows Authentication feature to work correctly.

Password: Enter the password for the user. The password is case sensitive. This field can be left blank when using Windows Authentication.
First Name: Enter the user's first name.
Middle Name: Enter the user's middle name.
Last Name: Enter the user's last name.
Department: Enter the name of the department in which the user works.
E-mail: Enter the user's email address. This is used for the Email Alerts feature.
Alternate E-mail: Enter an alternate email address for the user if desired. This is used for the Email Alerts feature.
Use Windows Login: Check this box to use the Windows Authentication feature. When checked, this will check the login name of the user currently logged into Windows. If it matches a user name in EchoOneApp, it will bypass the EchoOneApp login screen. The EchoOneApp user name must match the Windows login name exactly. If *Use Windows Login* is not enabled, the user must type in a user name and password each time they log into EchoOneApp. When using Windows Authentication, the normal login screen can still be accessed by holding down the *Ctrl* key on the keyboard when launching the application.
User Enabled: Check this box to make the user active. If it is unchecked, the user account cannot be used to login to EchoOneApp. Based on your software license, active users are limited to a certain number. To check how many users are included in your software license, click *Help > About.*
Default Access: Select the default access for the user. Default access determines the overall access to EchoOneApp. If the user will have broad access to EchoOneApp, it is best to give them a high level of default access and limit access using specific security items. If a user is going to have very limited access to the program, it is best to give them a more restricted level of default access and enable access to specific security items.

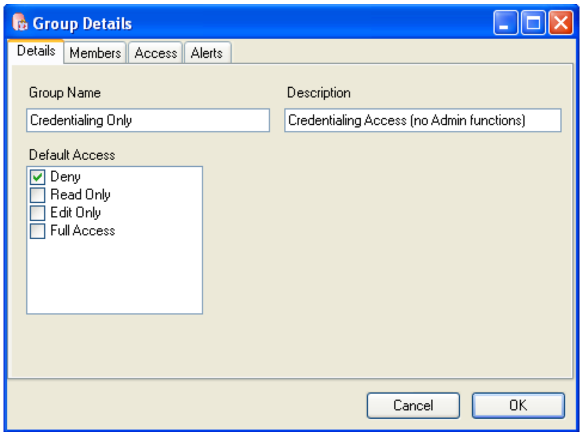
Default Access Levels

Deny: Blocked access. Completely blocks the user's access to the application.
Read Only: Read only access. Users can view data but cannot edit, delete, or add.
Edit Only: Read and Edit access. Users can add, read and edit but cannot delete.
Full Access: Full access to the application

Groups:

Security Groups are used to apply common access rights to several users. To add a group, click *Configure > Security*, and click the *Groups* button. The *Move Up* and *Move Down* buttons change the order of the security groups as it pertains to the security settings. A group that is higher up on the list will override any groups below it if they have conflicting security settings. Click *Add* to add a new security group.

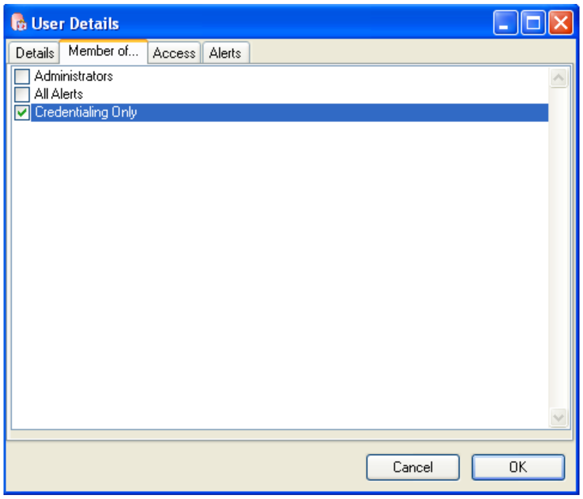
Give the group a name and a description. Choose a default access level.



Group Name: Credentialing Only
Description: Credentialing Access (no Admin functions)

Default Access
☑ Deny
☐ Read Only
☐ Edit Only
☐ Full Access

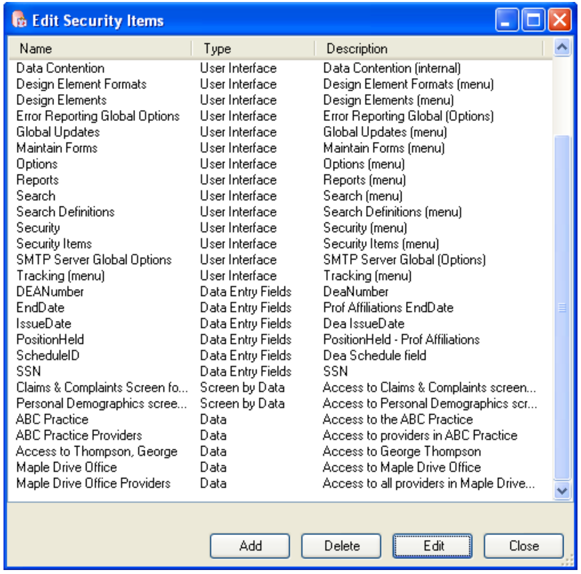
To assign users to a security group, go to the users list, select a user and click *Edit*. Click the *Member of…* tab and select the group(s) by clicking the checkbox next to each group.



□ Administrators
□ All Alerts
☑ Credentialing Only

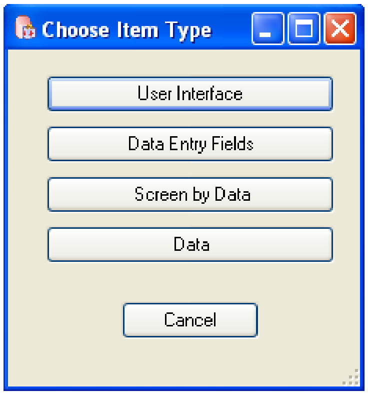
Security Items

Before setting the access levels to the users and groups, the individual security items must be defined. Click *Configure > Security Items* to access the security items screen. The list in the screenshot on the next page shows security items that are available to be applied to a user or group. Until the security item is added to this list, access to such items cannot be applied to users and groups.



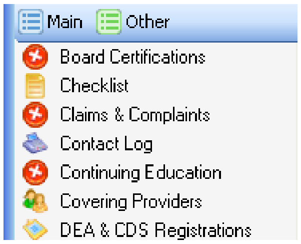
Name	Type	Description
Data Contention	User Interface	Data Contention (internal)
Design Element Formats	User Interface	Design Element Formats (menu)
Design Elements	User Interface	Design Elements (menu)
Error Reporting Global Options	User Interface	Error Reporting Global (Options)
Global Updates	User Interface	Global Updates (menu)
Maintain Forms	User Interface	Maintain Forms (menu)
Options	User Interface	Options (menu)
Reports	User Interface	Reports (menu)
Search	User Interface	Search (menu)
Search Definitions	User Interface	Search Definitions (menu)
Security	User Interface	Security (menu)
Security Items	User Interface	Security Items (menu)
SMTP Server Global Options	User Interface	SMTP Server Global (Options)
Tracking (menu)	User Interface	Tracking (menu)
DEANumber	Data Entry Fields	DeaNumber
EndDate	Data Entry Fields	Prof Affiliations EndDate
IssueDate	Data Entry Fields	Dea IssueDate
PositionHeld	Data Entry Fields	PositionHeld - Prof Affiliations
ScheduleID	Data Entry Fields	Dea Schedule field
SSN	Data Entry Fields	SSN
Claims & Complaints Screen fo...	Screen by Data	Access to Claims & Complaints screen...
Personal Demographics scree...	Screen by Data	Access to Personal Demographics scr...
ABC Practice	Data	Access to the ABC Practice
ABC Practice Providers	Data	Access to providers in ABC Practice
Access to Thompson, George	Data	Access to George Thompson
Maple Drive Office	Data	Access to Maple Drive Office
Maple Drive Office Providers	Data	Access to all providers in Maple Drive...

Click *Add* to add a new security item to the list of available items. See the descriptions of each security item below.



User Interface:

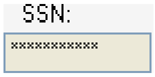
Access rights can be applied to any screen in the User Interface (UI). This includes data entry screens and the screens for the audit trail, reporting, forms, security, options, etc. The screenshot below shows Deny access to several data entry screens. Data entry screens that have blocked access are marked with a ✖ icon.



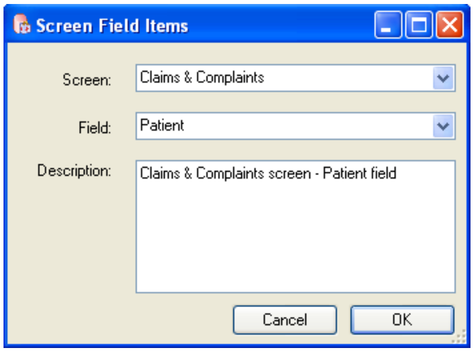
To add items to the list of available security items, select the item or items and click *OK.* Multiple items can be selected by holding down Shift or the Ctrl key. These items will now be shown in the list of available security items.

Data Entry Fields:

Field level security is a will limit or restrict access to a data entry field. The field level security is not specific to a single practice, office or provider record. If the field security is used, it will apply to the field across all records. The text or numbers in the field will be replaced with fixed number of asterisk (*) characters if Deny access is applied. In the case of a checkbox, the field will not be visible. The screenshot below shows blocked access to the Social Security Number field.


SSN: ************

Click the *Data Entry Fields* button to add a new Data Entry field security item.



Screen: Claims & Complaints

Field: Patient

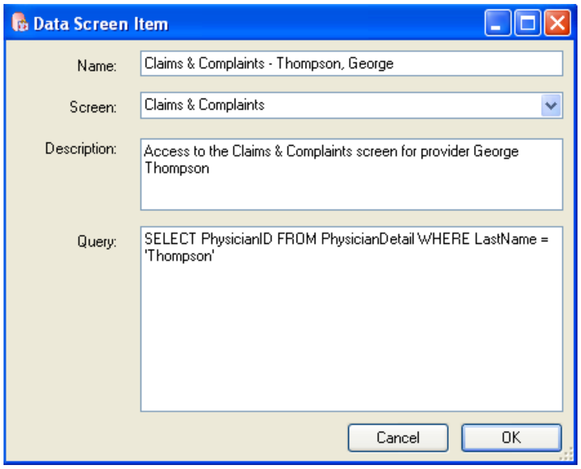
Description: Claims & Complaints screen - Patient field

Choose the screen/table that contains the field for which would like to restrict access. Once the screen has been selected, choose the specific field. Enter a detailed description and click OK. The field will then be added to the list of available security items.

Screen by Data:

This is a combination of User Interface and Data security. Users can have restricted access to specific data entry screen for specific practices, offices and providers. To add a Screen by Data security item, click the *Screen by Data* button.

Type a Name for the security item and select the screen. Enter a detailed description. The Query box should contain a SQL query that returns the ID(s) for a company, department, or employee. See the **Sample SQL Queries** section for more information about creating SQL queries for data security. In the example below, the *Claims & Complaints* specifically for the provider *George Thompson* is defined.



Name: Claims & Complaints - Thompson, George

Screen: Claims & Complaints

Description: Access to the Claims & Complaints screen for provider George Thompson

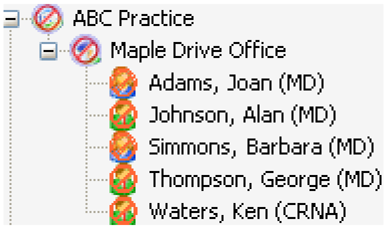
Query:

```
SELECT PhysicianID FROM PhysicianDetail WHERE LastName =
'Thompson'
```

Data:

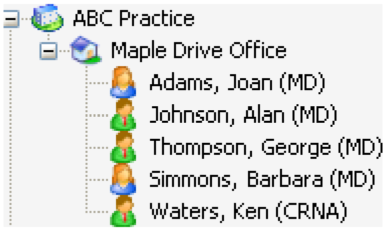
Data Security can be applied to restrict or grant a user or group's access to items in the information tree (combination of practices, offices and providers). The screenshot below shows blocked access to a practice, office and all the providers within the office. When a user attempts to click on a blocked item, they get a message that informs them that they do not have access to that information.

Blocked:



ABC Practice
Maple Drive Office
Adams, Joan (MD)
Johnson, Alan (MD)
Simmons, Barbara (MD)
Thompson, George (MD)
Waters, Ken (CRNA)

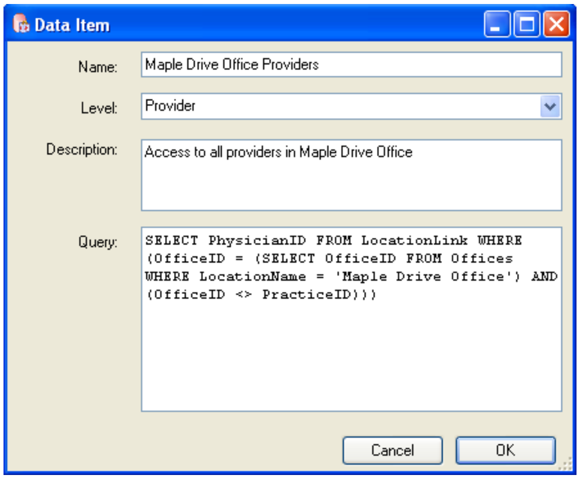
Full Access:



ABC Practice
Maple Drive Office
Adams, Joan (MD)
Johnson, Alan (MD)
Thompson, George (MD)
Simmons, Barbara (MD)
Waters, Ken (CRNA)

To add a Data security item, click the *Data* button.

Type a Name for the security item and choose the level of the data to restrict (practice, office, provider). Type a detailed description of the data item in the Description box. The Query box should contain a SQL query that returns the ID number(s) for a practice, office or provider. See the **Sample SQL Queries** section for more information about creating SQL queries for data security.



Data Item

Name: Maple Drive Office Providers

Level: Provider

Description: Access to all providers in Maple Drive Office

Query:

```
SELECT PhysicianID FROM LocationLink WHERE
(OfficeID = (SELECT OfficeID FROM Offices
WHERE LocationName = 'Maple Drive Office') AND
(OfficeID <> PracticeID)))
```

Sample SQL Queries for Data Security

In order to define an EchoOneApp Data security item, a SQL query must be created that will return the ID number for the specific practice, office or provider. These ID numbers correspond to the data in the tree. Below are common sample queries.

NOTE: Substitute italicized fields between the single quotes with name specific name of practice, office or provider. The data can be identified by any field, not just the name. The queries below use the practice name, office name, and provider's last name to identify the record(s). The *xPractice*, *xOffice* and *xLastName* variables are placeholders for the actual Practice names, Office names, and Provider last names, respectively.

Search by Name

Return a specific practice by name

SELECT OfficeID FROM dbo.Offices WHERE (OfficeID = PracticeID) AND (LocationName = 'xPractice')

Return a specific office by name

SELECT OfficeID FROM dbo.Offices WHERE (OfficeID <> PracticeID) AND (LocationName = 'xOffice')

Return all offices within a specific practice, which is identified by name

SELECT OfficeID FROM dbo.Offices WHERE (PracticeID = (SELECT DISTINCT PracticeID FROM dbo.Offices AS Offices_1 WHERE (LocationName = 'xPractice'))) AND (OfficeID <> PracticeID)

Return all providers within a specific practice, which is identified by name
SELECT DISTINCT PhysicianID FROM dbo.FullLink WHERE (OfficeID IN (SELECT OfficeID FROM dbo.Offices WHERE (LocationName = 'xPractice') AND (OfficeID = PracticeID)))

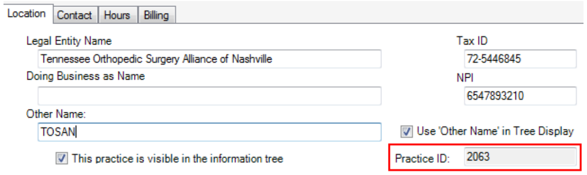
Return all providers within a specific office, which is identified by name
SELECT DISTINCT PhysicianID FROM dbo.FullLink WHERE (OfficeID IN (SELECT OfficeID FROM dbo.Offices WHERE (LocationName = 'xOffice') AND (OfficeID <> PracticeID)))

Return all providers with a specific last name
SELECT PhysicianID FROM dbo.PhysicianDetail WHERE LastName = 'xLastName'

Search by ID

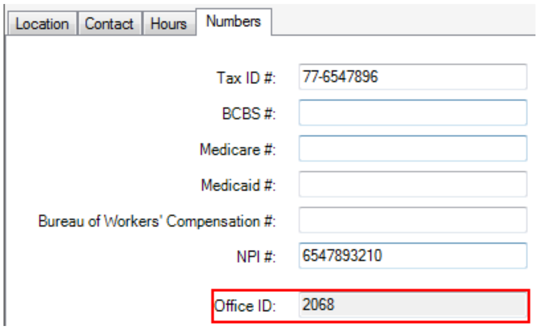
Practices and offices should be referenced by their ID numbers whenever possible. If multiple entities share the same name, e.g., multiple offices have the same legal entity name, then this may be mandatory to obtain expected results.

Practice ID numbers are located on the Location tab of the Demographics screen.



Legal Entity Name: Tennessee Orthopedic Surgery Alliance of Nashville
Doing Business as Name:
Other Name: TOSAN
☑ This practice is visible in the information tree
Tax ID: 72-5446845
NPI: 6547893210
☑ Use 'Other Name' in Tree Display
Practice ID: 2063

Office ID numbers are located on the Numbers tab of the Demographics screen.



Tax ID #: 77-6547896
BCBS #:
Medicare #:
Medicaid #:
Bureau of Workers' Compensation #:
NPI #: 6547893210
Office ID: 2068

Whenever possible, use the queries below for identifying entities in preference to those above using names. Using ID numbers will speed processing by your database server, thus causing less impact on performance.

NOTE: Substitute italicized fields between the single quotes with name specific name of practice, office or provider. The data can be identified by any field, not just the name. The queries below use the practice's ID and/or office's ID to identify the record(s). The *xPracticeID* and *xOfficeID* variables are placeholders for the actual Practice ID and Office ID, respectively. The *xID* variable (and its numbered variants) can be replaced with either practice or office IDs without alteration.

Return a single practice, which is identified by its ID
SELECT xPracticeID

Return all offices within a single practice, which is identified by Office ID
SELECT DISTINCT OfficeID FROM dbo.Offices WHERE (PracticeID = xPracticeID) AND (PracticeID <> OfficeID)

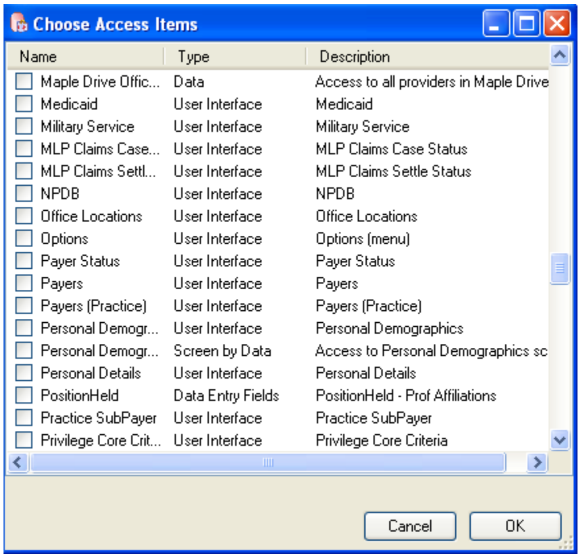
Return all providers within a single office or practice, which is identified by its ID
SELECT DISTINCT PhysicianID FROM dbo.FullLink WHERE (OfficeID = xID)

Return all providers within multiple offices or practices, which are identified by their IDs
SELECT DISTINCT PhysicianID FROM dbo.FullLink WHERE OfficeID IN (xID1, xID2, xID3, xID4)

Access to Security Items

The final step in setting up security is to set the access level to each of the security items for each group and user. To grant or restrict access to specific security items for a User, click *Configure > Security*. Select the User, click *Edit*, and click the *Access* tab. For Groups, click *Configure > Security*. Click the Groups button. Select the Group, click *Edit*, and click the *Access* tab.

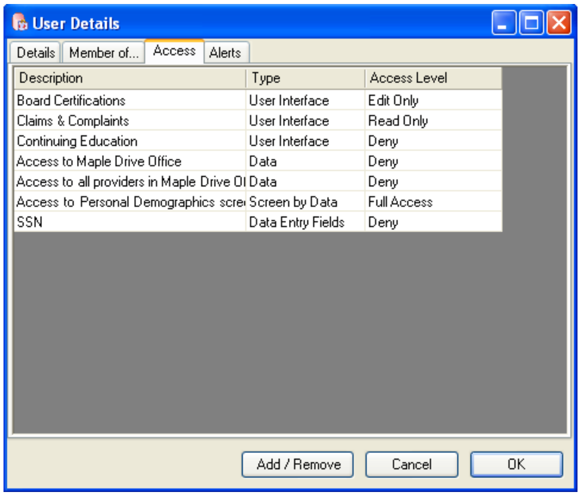
Click the *Add/Remove* button to open the list of available security items.



Name	Type	Description
☐ Maple Drive Offic...	Data	Access to all providers in Maple Drive
☐ Medicaid	User Interface	Medicaid
☐ Military Service	User Interface	Military Service
☐ MLP Claims Case...	User Interface	MLP Claims Case Status
☐ MLP Claims Settl...	User Interface	MLP Claims Settle Status
☐ NPDB	User Interface	NPDB
☐ Office Locations	User Interface	Office Locations
☐ Options	User Interface	Options (menu)
☐ Payer Status	User Interface	Payer Status
☐ Payers	User Interface	Payers
☐ Payers (Practice)	User Interface	Payers (Practice)
☐ Personal Demogr...	User Interface	Personal Demographics
☐ Personal Demogr...	Screen by Data	Access to Personal Demographics sc
☐ Personal Details	User Interface	Personal Details
☐ PositionHeld	Data Entry Fields	PositionHeld - Prof Affiliations
☐ Practice SubPayer	User Interface	Practice SubPayer
☐ Privilege Core Crit...	User Interface	Privilege Core Criteria

Click the check box next to each item to apply them to the user or group. Once security items have been selected, click *OK*. Select the Access Level for each item by clicking the drop down box in the *Access Level* column.

Deny: Blocked access. Completely blocks the user's access to the security item.
Read Only: Read only access. Users can view data but cannot edit, delete, or add.
Edit Only: Read and Edit access. Users can add, read and edit but cannot delete.
Full Access: Full access to the security item.



Description	Type	Access Level
Board Certifications	User Interface	Edit Only
Claims & Complaints	User Interface	Read Only
Continuing Education	User Interface	Deny
Access to Maple Drive Office	Data	Deny
Access to all providers in Maple Drive Of	Data	Deny
Access to Personal Demographics scre	Screen by Data	Full Access
SSN	Data Entry Fields	Deny

Click *OK* to save the changes. If the changes apply to a user that is currently logged in, EchoOneApp must be closed and re-opened for the changes to take effect.