# 4.19 Security

**RFP reference: 6.19 Security, Page 60**

In their proposals, Bidders should describe experiences defining and implementing multiple levels of security. Bidders should describe the security options including segregation of duty for the solution including:

- Role based and group based security;
- Levels of administration and the ability to delegate administration at a group level.
- Description to the depth of security levels available.
- Security reporting and audit trails for changes

**Deloitte has the experience, tools, and technology to provide DSCYF with a solution that is secure and abides by the IT information security policy, standards and guidelines outlined by the DSCYF. We understand that with the many distinct stakeholders that DSCYF requires, reliable security practices should represent the different viewpoints to sustain the confidentiality, integrity, and availability of the system. Deloitte provides a demonstrated security design that meets your role based access control, Security at group level, Security reporting and Audit trail requirements.**

Deloitte's proposed security solution provides **security controls** aimed at a **seamless** user experience, while **protecting the data** of the Delaware FACTS II. The proposed Delaware FACTS II is designed to improve the user experience, strengthen DSCYF's vision of Integrated Children Services model, replace current legacy systems and applications, and position DSCYF for future growth

section HIGHLIGHTS

- The Deloitte team leverages the leading practices and concepts for security from over seven statewide child services implementations.
- Flexible and configurable role based access control that meets your Child Welfare needs.
- We understand and have experience with Delaware technology standards and implement robust security provisions within them.

and expansion. Delaware FACTS II is aligned with your strategic goals as DSCYF implements effective practices and new business processes. Delaware FACTS II incorporates SACWIS specific security design patterns based on our experience in other states to accelerate your implementation of a standards compliant security architecture.

On closer look, benefits of our Security Framework, Role based Access, and Audit Trail, which we bring, includes:

| Delaware FACTS II Security Features | Delaware FACTS II Security Benefits |
|---|---|
| **Security Framework** | Provides Authentication mechanism, Secure Access control and a consolidated user activity monitoring and exception logging<br>Provides secure coding guidelines complimented with secure code review |
| **Role Based Access** | Configurable authorization console within the application for granular role based Security |
| **Audit Trail** | Customizable framework for logging audit trails and tracking<br>Tracks changes to key information<br>Tracks access of application at page, entity and user level |

**Table 4.19-1. Features and Benefits of Delaware FACTS II Security Framework.**

## Our Security Design Approach

Our proposed security design is derived from the best practices learned from our successful implementation in Washington DC, Alabama, Allegheny county Pennsylvania, West Virginia, Oklahoma and implementation of DCISII for the State of Delaware. We have in-depth knowledge of Delaware standards and technical infrastructure in combination with production proven solutions. Implementing a system that provides for diverse security policies starts with an in-depth analysis of security requirements. We take a holistic approach to security to not just provide the technical architecture and systems required for an efficient implementation but also work with our clients to address the procedural and governance aspects of security.

We understand that the nature of information that SACWIS data is highly sensitive such as restricted access to the biological identity of adopted child(ren), privacy protection for abused or neglected children, restricted access to case records pertaining to high profile individuals or incidents, restricted access to medical information of children. We recognize the need for mechanisms that cater to that sensitivity. This understanding has resulted in a focus on security throughout all the phases of the Software Development Life cycle (SDLC). We work collaboratively with DSCYF during the SDLC phase to define, derive, refine and implement detailed security rules and procedures to meet Delaware standards, policies, and procedures.

# Delaware FACTS II Security Design

Delaware FACTS II provides layers of security for a user to pass through before accessing data confirming authorized access to critical integrated children services program information. They are:

**Authentication.** Authentication is the process of verifying identify of an object or person. Often agencies share single active directory for all their users and an active directory entry does not authorize someone to access child welfare data. Keeping this in mind our solution has implemented two levels of authentication to verify the identity of users:

- **Active Directory Authentication.** Users of the agencies will have a unique identifier (USERID or Email address) that will be used to verify an active entry in the State of Delaware active directory using Lightweight Directory Access Protocol (LDAP) to sign in to our application. LDAP Authentication is illustrated in the below figure.

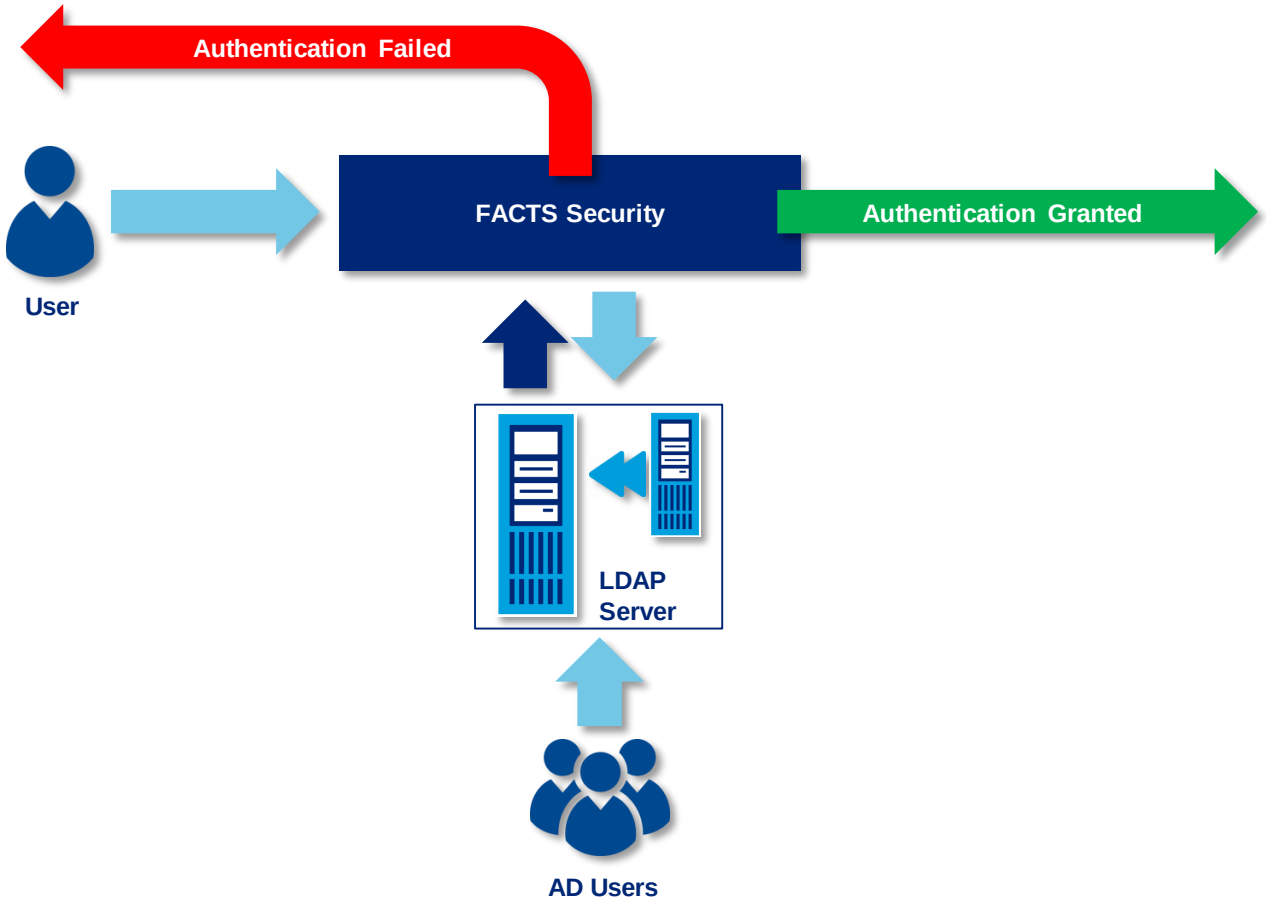



**Figure 4.19-1. Delaware FACTS II Authentication.**

DE_SACWIS-264

- **Delaware FACTS II Internal Authentication.** Proposed Delaware FACTS II internally maintains list of all authorized users and all users are validated against our internal staff directory. Upon successful authentication users are signed into Delaware FACTS II.

**Authorization.** Authorization enforces application and data security for users (or group of users) to access Delaware FACTS II information. It determines the user's access rights in the application. In other words, the authorization process determines which information or data a user can access. Authorization is illustrated in the below figure.

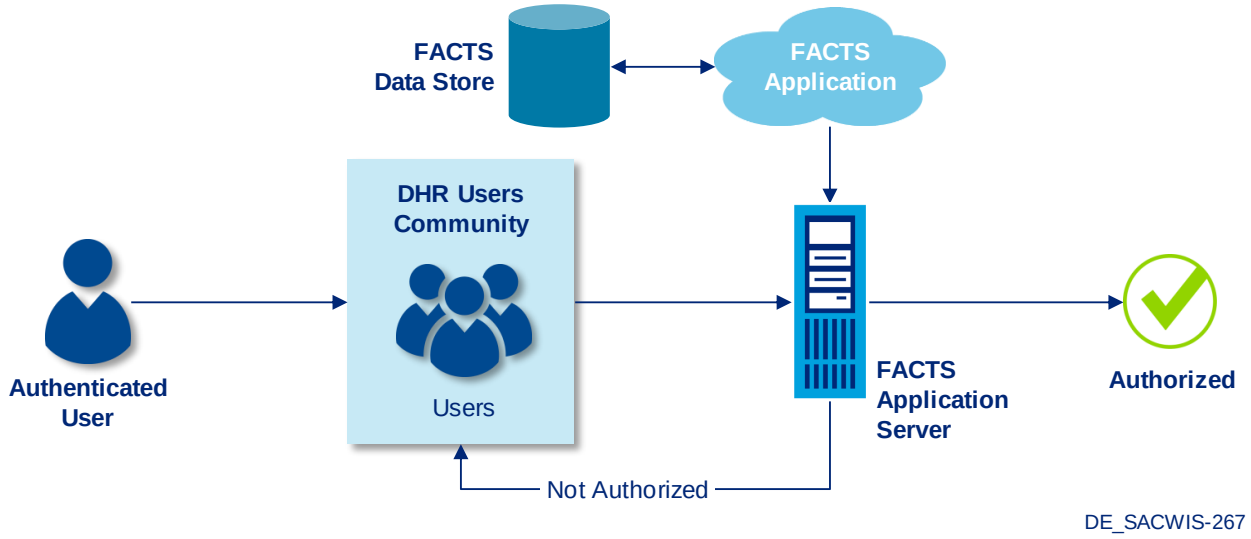



**Figure 4.19-2. Delaware FACTS II Authorization.**

The goals of our authorization service include:

- Providing users with access only to their job functions that they require to perform their jobs
- Categorizing types of users by role and restrict access based on those roles.
- Preventing users from accessing entities that they do not own or share
- Supporting entity data sharing by providing the ability to grant users with access to entity that they do not own

**Role Based Access Control (RBAC).** Role based access control is a form of application security focused at the user level that identifies a user based on the assigned role instead of the individual user identity. Detailed explanation of RBAC is provided in the next section.

**Data-Access Security.** While roles allow users to access various modules of application, data access is secured by assignment to a particular entity. Our security model supports primary, secondary and administrative assignments which are given to users based on their job function.

**Organization Hierarchy.** Organization hierarchy plays a key role in security to define entity access for supervisory job functions and restrict access to entities within a geographical area, typically a county in most cases. A worker gets access to an entity through assignments, however; users with supervisory job functions do not have assignments to entities but still may require access to perform supervisory tasks. Using the Organization hierarchy our solution allows supervisory functions to be performed on entities without a user having a physical assignment of such entities

**Application Security.** Our approach to application security is developed to assist DSCYF comply with the IT information security policy, standards and the related security guidelines prescribed by the standard. The following activities encompass application security:

- **Security Requirements and Secure Design.** Implementation of access control mechanisms based on identification of security requirements during the design phase
- **Secure Coding Guidelines and Secure Code Review.** Users input data is controlled through coding of validation techniques such as masked edit controls, strong password fields etc.
- **Directory Browsing.** Users are not allowed access to the directory structure on the application servers
- **Deployment Strategy.** An automated build and deployment process is used to deploy only the .NET code libraries and not the C# source code files on the application servers
- **Configuration File.** User access to configuration file that contains information such as server URLs, database location etc is disabled.
- **File Uploads.** The type of content that users can upload is restricted to basic file types such as PDF, Scanned Images, and Documents.

**Security Requirements and Secure Design.** During the design and construction phase, we identify security requirements for the Delaware FACTS II and analyze them to integrate into each security activity described within this section. During this phase, we work with the DSCYF's team to identify and analyze the applicable DSCFY's IT information security policy, standards and guidelines to incorporate into our approach to implement a secure Delaware FACTS II.

The proposed Delaware FACTS II solution's secure design incorporates coarse grained and fine grained access control mechanisms, application session management, user activity monitoring and logging. The access controls are designed along with the DSCYF based on the principle of least privilege, need-to-know and need-to-use basis. The secure design also incorporates the appropriate industry leading practices.

**Secure Coding Guidelines and Secure Code Review.** We establish secure coding principles to assist development of a secure Delaware FACTS II. The secure coding guidelines include at a minimum, the principles of strong input validation, default deny, principle of least privilege and access based on need-to-know/need-to-use.

We conduct a secure code review during the construction phase, focused to identify and mitigate insecure coding techniques and vulnerabilities that may lead to application security vulnerabilities. We perform review on the custom developed web application source code of the Delaware FACTS II.

**Directory Browsing.** The Internet Information Servers (IIS) that host the web application provides a feature called Directory Browsing. This feature lists the contents of a directory if no specific file name is given or if no index file is present. This feature is often used by malicious users to get sensitive information that is not intended for public viewing, such as work-in-progress pages, log files, backup files, etc. The Application Servers that hosts Delaware FACTS II will be configured to not allow any directory browsing.

**Deployment Strategy.** When a web application developed in ASP.Net is built it converts its entire source code into Dynamic Link Libraries (DLLs). In order to execute an ASP.Net application, it is sufficient to host only the DLLs and resource files (icons, images, etc.) on the application server. This confirms that in the event of a security breach no one is able to modify the application's behavior by rebuilding the source code. When Delaware FACTS II is finally hosted on the Production boxes, no source code is deployed as on the actual production environment. Only DLLs and resource files are hosted on the Internet Information Server.

**Configuration File.** A typical web application stores all its configurable information in "web.config" files. These files contain information such as database connection strings and location of State Management Server. By default, Internet Information Server does not allow "web.config" files to be viewed through HTTP requests, so this information cannot be accessed. Delaware FACTS II also uses a "web.config" file to store configuration information such as, the database connection string, location of State Management Server. This confirms disabling of access through HTTP requests.

**File Uploads.** Several web applications provide features to upload files directly to the application. A malicious user may take advantage of this functionality and upload an executable file or script which can be executed at a later stage. The application must not allow any unauthorized files to be uploaded since, the same files can provide a malicious user with the ability to read web configuration settings, delete/move existing files etc. Delaware FACTS II provides a File Cabinet functionality which allows users to upload files onto the server. However, the type of file a user can upload is restricted. For example, File Cabinet only allows users to upload files of type ".doc", ".pdf" and ".tif".

## Role Based and Group Based Security

Delaware FACTS II combines role based security, data access security and organization hierarchy to provide access to users to perform their job functions or tasks.

**Role-Based Security Control (RBAC).** Role based access control is a form of application security focused at the user level that identifies a user based on the assigned role instead of the individual user identity. Delaware FACTS II uses role-based security to provide user authorization and user access to the application resources. Roles are represented as "Position Titles" in Delaware FACTS II and are defined by standard job functions within the organizational structure. Each position title is given a set of security codes that grant specific permissions to the position title to ensure appropriate access is given to the user. A set of users can be assigned to the same position title where the set of users share the same security privileges or restrictions as depicted in the image below.

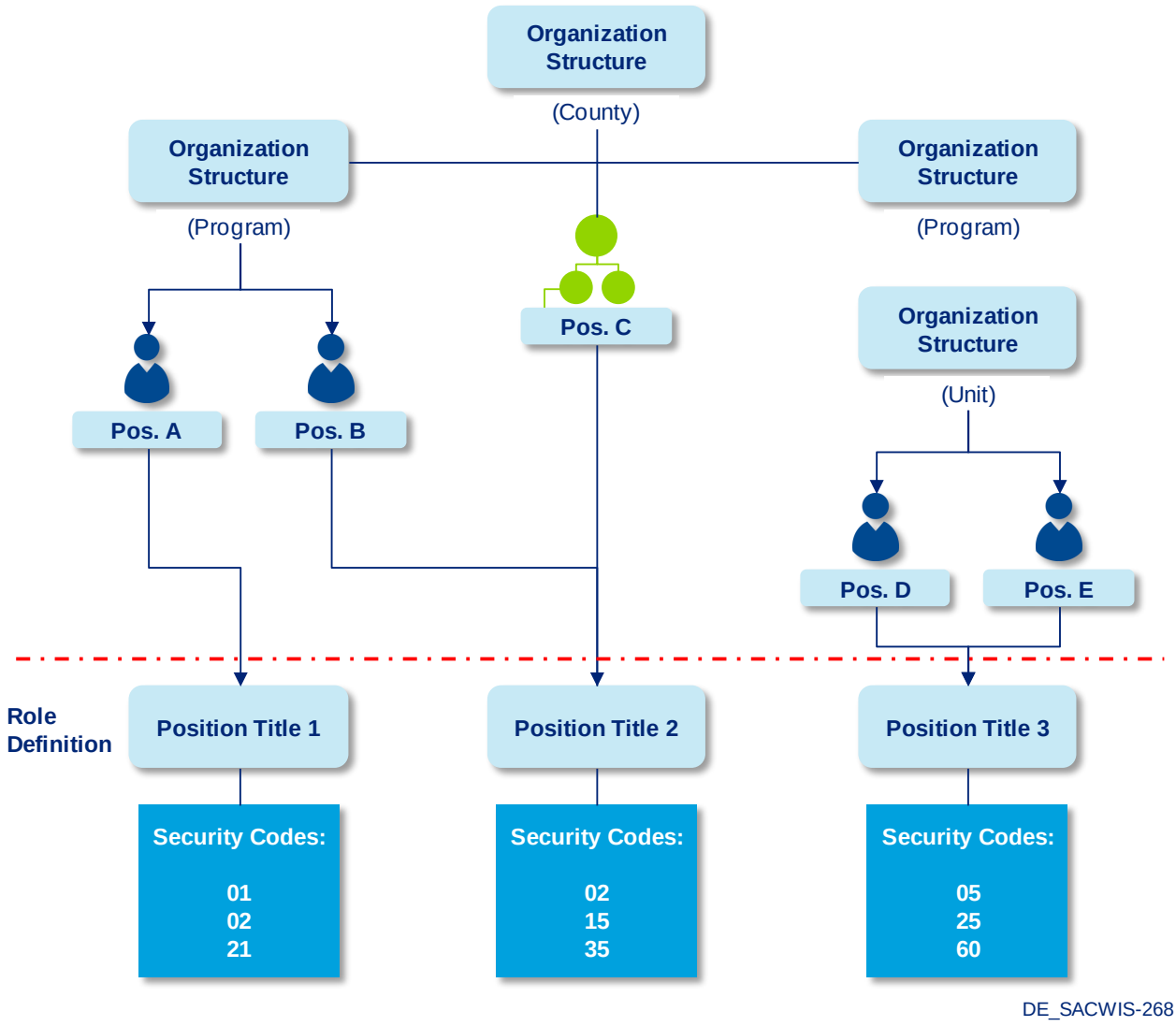



**Figure 4.19-3. Delaware FACTS II Role-Based Security.**

**Role-Based Security Offers Flexibility and is Easier to Manage.** By managing security access through position titles, a change in job responsibility does not pose a daunting task to the system administrator. For example, if a new feature is added to the application, access to the new feature in the application can easily be given by adding a security code that grants access to the new feature to the respective position title. After a successful log in and authorization occurs, the user is granted permission to access the new feature.

In unique situations special Security codes are defined to allow users to perform actions within an entity depending on nature and criticality of the job function. These situations are:

- **Supervisory Functions.** Supervisory functions requires additional security for restricting certain features of application to specific users
- **Sensitive Data.** Delaware FACTS II supports added level of security required for accessing sensitive data in situations such as restricted entities, adoptive parents' data providing additional security restricting access to specific users. Delaware FACTS II allows high profile cases to be restricted and all restricted cases can be accessed only by staff with special security role.

**Data-Access Security.** While roles allow users to access various modules of application, data access is secured by assignment to a particular entity. Our security model supports primary, secondary and administrative assignments that are given to users based on their job function.

**Organization Hierarchy.** Organization hierarchy plays a key role in security to define entity access for supervisory job functions and restrict access to entities within a geographical area typically a county in most cases. A worker gets access to an entity through assignments, however; users with supervisory job functions will not have assignments to entities but still may require access to perform supervisory tasks. Using the Organization hierarchy Delaware FACTS II allows supervisory functions to be performed on entities without having a physical assignment to entities

## Levels of Administration and the Ability to Delegate Administration at a Group

In Delaware FACTS II, every user has a security position and each position has default security assigned. On creation of a new user, default security is assigned depending upon the position of the user. Administrator can assign additional security on top of the default assigned security levels and for the position, default security can be modified. In Delaware FACTS II each Security level maps to a job-function a worker performs in day-today life. For example, security level 18 is given to staff persons who have authority to approve other's work. Whoever has a supervisory role within DSCYF is given security level 18 to approve work within Delaware FACTS II like Case planning, Placement etc. By assigning different security levels to DSCYF staff Delaware FACTS II segregates duties or job-functions a staff can perform within Delaware FACTS II.

The table that follows lists sample security levels we created for Alabama FACTS which is a transfer of DC FACES.NET application. Just as we customized the security levels from DC FACES.NET to meet security requirements specific to the State of Alabama, we can customize them to meet the job functions of DSCYF.

| Security Code | Security Level Description |
|---|---|
| 1 | Read (view) only capability for an individual case record |
| 2 | a) Read (view) only capability for open and closed cases (except adoption, post adoption and restricted) b) Read (view) only capability for all providers, except Contracts, Adoptive and FC Homes information |
| 3 | Read (view) only capability for all providers |
| 4 | a) Read access to all training screens (e.g., individual training record) b) Ability to record and update training enrollment data |
| 5 | Read (view) only capability for open and closed APS/CPS cases, except restricted cases |
| 6 | a) Ability to enter Intakes (I&R, Prevention) b) Ability to associate (or link) an Intake to another Intake or Intake to a case. This action can only be completed with Supervisor approval. c) Ability to delete ticklers that are marked as user deletable |
| 7 | Ability to enter Intakes and Investigations (AANE, CAN, Preventions) |
| 8 | a) General update capability for open cases statewide (except adoption, post-adoption and restricted), except Administrative Review, Placement Status, ILP, and selected Abscondance information b) Ability to delete ticklers that are marked as user deletable c) Ability to enter/update requests for demand payments d) Ability to create Purchase Orders and Disbursements |
| 9 | a) Ability to update Placement Status information |
| 10 | Ability to update TPR information |
| 11 | Ability to update Contact, Collateral, Visitation Log, Travel Plan, Court Complaint, Court Hearing, Court Motion, Court Parental Rights, Court Status, Court # and Court Order information as required by external users |
| 12 | a) Ability to update Invoice information as required by external providers b) Ability to notify caseworkers that a child has been placed with a provider |
| 13 | a) Ability to enter client account deposits b) Ability to enter client account interest |
| 14 | Ability to assign from any Program Area, Unit, or worker to any other Program Area, Unit, or worker |
| 15 | Ability to update ICPC information |
| 16 | Ability to enter/update open adoption cases |
| 17 | Ability to enter/update non-contracted providers, except Contracts information. |

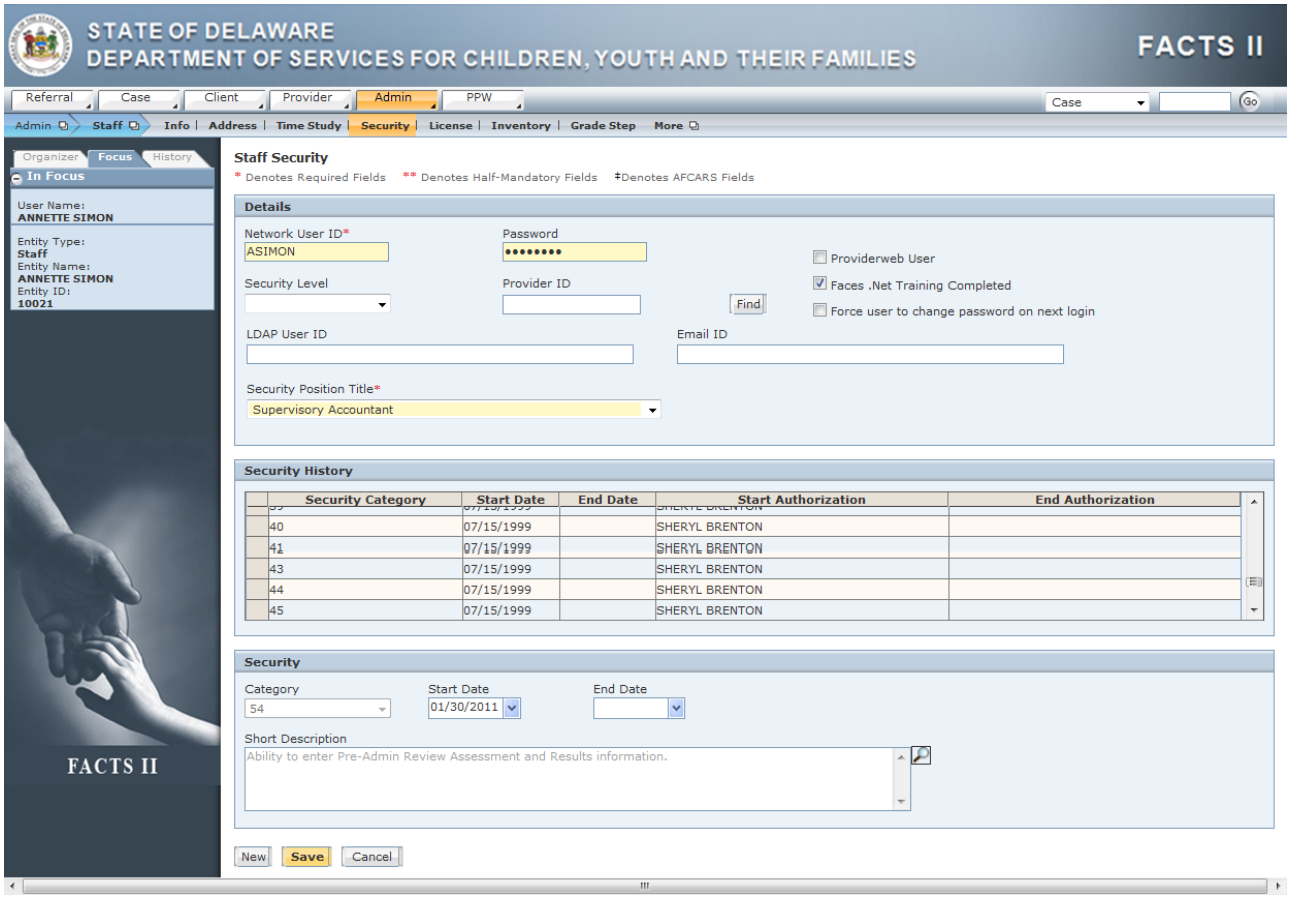
| Security Code | Security Level Description |
|---|---|
| 18 | a) Ability to record general approvals b) Ability to assign from the Unit Inbox to any jurisdiction Inbox (primary assignments) or to a specific worker within the user's units (applies to both primary and secondary assignments). Any of these assignments can be made from the Workload screen, the Unit Inbox screen or the Assign screen within an open case. c) Ability to designate a case or referral as restricted and assign the restricted case/referral as specified in 18b (above). Restrictions will not apply to "other" assigned work (e.g. home studies, foster home, and adoptive records). d) Ability to close a case e) Ability to delete all ticklers (even those not marked as user deletable) f) Ability to read/update on-call information |
| 19 | Ability to approve demand payments |
| 20 | Ability to delete data from the system |
| 21 | Read only capability for personnel screens (e.g., individual staff information) |
| 22 | Ability to read (view) restricted and closed cases if not the case owner or supervisor |
| 23 | Ability to enter/update staff information and assign staff persons to units |
| 24 | a) Ability to make assignments from the Jurisdiction Inbox (to another Jurisdiction Inbox, a Unit/Group Inbox associated with the user's jurisdiction, or a worker within the jurisdiction) including restricted cases, adoption, etc. (To review a restricted case, it must be assigned to a supervisor or a worker) b) Ability to view all workloads |
| 25 | Ability to enter/update staff information and organizational structure (assign program areas to servers, units to program areas) |
| 26 | a) Ability to view open and closed and update Post-adoption cases b) Ability to search on adoptive name |
| 27 | Ability to view/update sealed link information |
| 28 | Ability to enter adoption subsidy information |
| 29 | Ability to enter/update contracted providers, except Contracts information |
| 30 | Ability to enter/update contracted providers |
| 31 | Ability to update QA/CA information on QA Summary screen |
| 32 | Ability to update Administrative Review information, including File Cabinet functionality |
| 33 | Ability to enter/update IV-E eligibility and other eligibility determination information |
| 34 | a) Ability to enter training/licensure hours for those attending training b) Ability to record/maintain training data (e.g. courses, trainers) |
| 35 | Ability to update Independent Living Program (ILP) information |
| 36 | Ability to restore archived cases |
| 37 | a) Ability to hold payments b) Ability to enter client withdrawals c) Ability to enter accounts receivable |
| 38 | Ability to assign all security categories, except financial security categories |
| 39 | Ability to update/maintain the system picklist values and other system administrative tables |
| 40 | Ability to assign all security categories, including financial security categories |
| 41 | Obsolete Security Code |

| Security Code | Security Level Description |
|---|---|
| 42 | Ability to enter rates for providers |
| 43 | Ability to view/enter funding source information |
| 44 | Ability to update Central Files Unit information |
| 45 | Ability to access cases District-wide |
| 46 | Ability to enter/update Community providers, except Contracts information |
| 47 | a) Ability to approve automatic payments b) Ability to back out payments c) Ability to approve withdrawals from client accounts d) Ability to enter/change payment plans e) Ability to update funding source f) Ability to create purchase orders and disbursements |
| 48 | Ability to enter Absondance information |
| 49 | Ability to enter Diligent Search information |
| 50 | Ability to access specified Management Reports |
| 51 | Ability to enter Child Fatality Reviews |
| 52 | Ability to access screens for Closed Cases |
| 53 | Ability to approve the 2nd tier Guardianship requests. |
| 54 | Ability to enter Pre-Admin Review Assessment and Results information. |
| 55 | Ability to read Client Search Results, Client Info, Payment History and Parental Rights Screens. |
| 56 | Ability to do Client Search for CPR (Child Protection Register) |
| 57 | Ability to Update old Court Orders |
| 58 | Ability to change Home Removal Date and Home Return Date. |
| 59 | Ability to Request ICPC - 2nd Level |
| 60 | Second Level Approval for Program Managers for two level supervisory approval requests that are not position based |
| 61 | Unapprove capability for the opening up investigations. |
| 62 | Ability to enter OCP service by OCP staff. |
| 63 | Read (view) only capability on the FTM Screens |
| 64 | Ability to Update on the FTM Screens |
| 65 | Ability to add Placement Unit Entry Dates on Placement Entry Screens |
| 66 | Ability to Add Emergency Placements |
| 67 | Provider Update for ProviderWeb Application |
| 68 | Provider View for ProviderWeb Application |
| 69 | Agency Update for ProviderWeb Application |
| 70 | Agency View for ProviderWeb Application |
| 71 | Ability to do Update on the MPD Investigation Details/MPD Contacts Screens |
| 72 | Read Only (View) Access on Intake/Investigation Screens |
| 73 | Ability to update the Facility tab on the contracts screen. |

| Security Code | Security Level Description |
|---|---|
| 74 | Help Desk Update for Client Merge and Client Unmerge |
| 75 | Ability to Update the Medicaid Prior Authorization Screen |
| 76 | Read (view) only capability for open and closed adoption cases |

**Table 4.19-2. Security Levels.**

The security roles described above are easy to configure through the use of online screens. The figure below depicts the process of assigning security to a user. Only authorized staff persons such as administrators have access to this screen which enables them to add, update or remove security levels to staff within DSCYF.




DE_SACWIS-519

**Figure 4.19-4. Security Assignment.**

## Security Reporting and Audit Trails for Changes

Our team implements a number of safeguards to protect against unauthorized data access, accidental destruction, and other hazards. We work closely with State security staff to support monitoring and respond to any unauthorized data access. The Audit Trail functionality not only captures user activity but also enables analysis and reporting of such activities through online screens and reports.

**Delaware FACTS II Audit Trail.** Delaware FACTS II offers several distinct audit trail approaches that, when taken together, allow the system administrators to monitor the user activity across the application. These security control measures are implemented at database level and web application level. The application provides read only access to critical data items like timestamps and other audit trail related information so as to prevent the users from making changes to these data items.

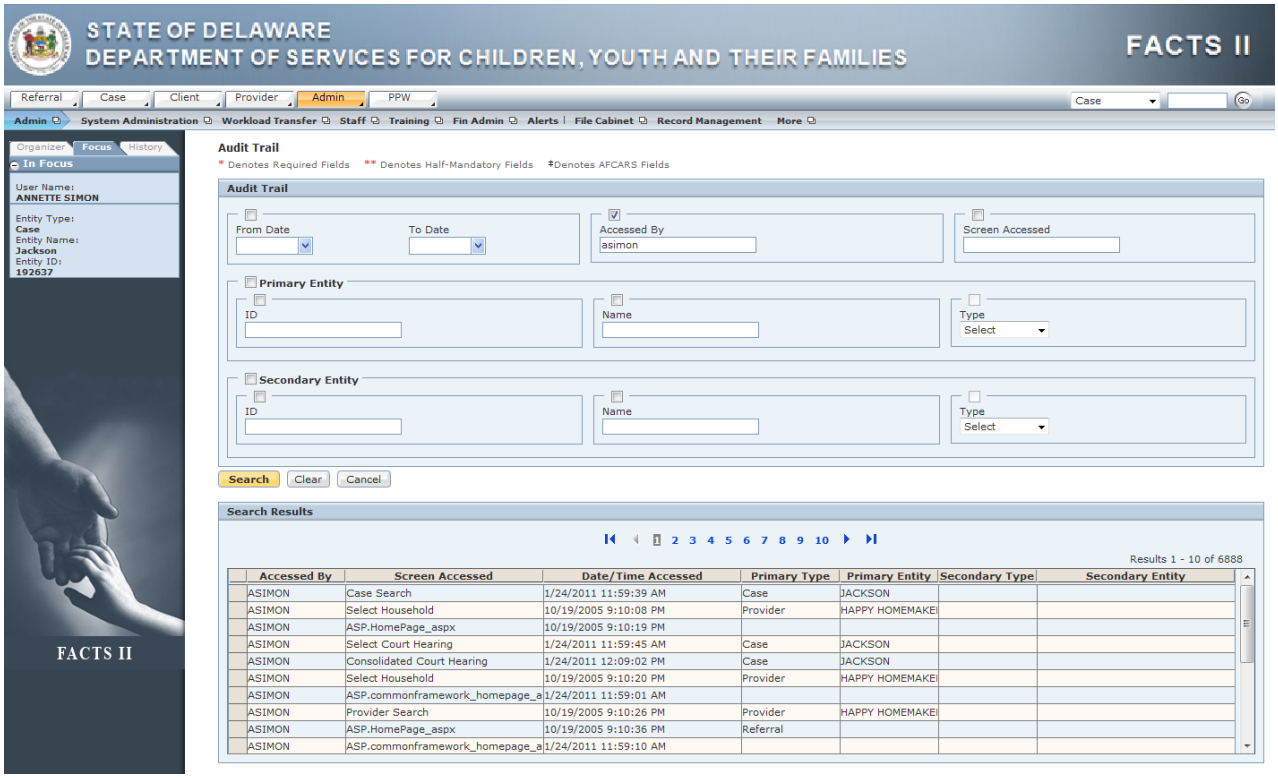
**Monitoring User's Database Operations.** At database level, Delaware FACTS II database includes audit trail information which includes date and time and the user ID of the person who originated the database transaction. Data Access Layer within our application internally captures the necessary information and stores the following into the database:

- The last user (Application User ID) who updated the database record
- The timestamp at which the data was updated by the user

**Monitoring User's Web Application Activity.** At the application level, Delaware FACTS II captures detailed audit information that records every user activity while he/she navigates across the application screens. Not only does the application keep track of screens accessed by the user but, it also keeps track of entities whose data the user accessed while navigating the application screens. Delaware FACTS II captures the following pieces of information:

- User who accessed the screen
- Screens and data accessed by a user
- Time and date of access
- Entities in focus (referrals, case, providers, clients, staff members, etc.)
- IDs of entities in focus

The figure that follows depicts the audit trail information that can be accessed by the system administrators. It enables administrators to search and sort audit trail based on a variety of conditions as shown in the figure itself.




DE_SACWIS-265

**Figure 4.19-5. Audit Trail Screen.**